Microsoft

Microsoft Dijital Savunma Raporu 2022

Tehdit ortamını aydınlatmak ve dijital savunmayı güçlendirmek.

İçindekiler

Bu rapordaki veri, içgörü ve olaylar, aksi belirtilmedikçe Temmuz 2021 ile Haziran 2022 (2022 Microsoft mali yılı) arası döneme aittir.

Bu raporu görüntüleme ve bu raporda gezinme konusunda en iyi deneyimi elde etmek için Adobe web sitesinden ücretsiz olarak indirebileceğiniz Adobe Reader'ı kullanmanızı öneririz.

Tom Burt'ün Rapor Tanıtımı

Müşteri Güvenliği ve Güveni'nden Sorumlu Kurumsal Başkan Yardımcısı

"Dünya çapındaki ürün ve hizmet ekosistemimizden gelen, analizini yaptığımız trilyonlarca sinyal, dünya genelindeki dijital tehditlerin şiddetini, kapsamını ve ölçeğini ortaya koymaktadır"

Mevcut ortamımıza ilişkin son durum...

Tehdit ortamının kapsamı ve ölçeği

Parola saldırılarının hacmi, yalnızca bir yılda %74 artışla saniyede tahminen 921 saldırıya yükseldi.

Siber suçları ortadan kaldırma

Bugüne kadar Microsoft, siber suçlular tarafından kullanılan 10.000'den fazla etki alanı ve ulus devlet aktörleri tarafından kullanılan 600 etki alanını ortadan kaldırdı.

Güvenlik açıklarını ele alma

Fidye yazılımı olay müdahale etkileşimlerimizin %93'ünde, ayrıcalık erişimi ve yanal hareket üzerindeki kontrollerin yetersiz olduğu sonucuna ulaşıldı.

23 Şubat 2022 tarihinde siber güvenlik dünyası yeni bir çağa, hibrit savaş çağına adım attı. O gün, füzeler fırlatılmadan ve tanklar sınırların ötesine geçmeden saatler önce, Rus aktörler Ukrayna hükümetinin teknolojisine ve finans sektörü hedeflerine karşı büyük ve yıkıcı bir siber saldırı başlattı. Üçüncüsü yayımlanan Microsoft Dijital Savunma Raporu (MDDR) yıllık baskısında Ulus Devlet Tehditleri bölümü altında bu saldırılar ve bunlardan alınacak dersler hakkında daha fazla bilgi edinebilirsiniz. Bulutun, siber saldırılara karşı en iyi fiziksel ve mantıksal güvenliği sağlaması ve Ukrayna'da değeri kanıtlanmış tehdit istihbaratı ve uç nokta korumasında ilerlemelere olanak tanıması, alınan bu derslerde içindeki en önemli husustur.

Her ne kadar siber güvenlik alanında yıl içinde kaydedilen gelişmeleri konu edinen bir çalışmanın bu noktadan başlaması gerekiyor olsa da, bu yılki raporda çok daha fazlası derinlemesine ele alınmaktadır. Raporun ilk bölümünde siber suçluların faaliyetlerine, ikinci bölümde ise ulus devlet tehditlerine odaklanıyoruz. Her iki grup da saldırılarının karmaşıklığını büyük ölçüde artırdı, böylece eylemlerinin etkisinin önemli ölçüde artmasını sağladı. Rusya manşetlere konu olurken, İranlı aktörler, iktidarın el değiştirmesinin ardından İsrail'i hedef alan yıkıcı saldırılar ve ABD'deki kritik altyapıyı hedef alan fidye yazılımlarının yanı sıra korsanlık ve sızdırma operasyonları başlatarak saldırılarını artırdı. Çin de Güneydoğu Asya'da ve dünyanın güneyindeki başka bölgelerde ABD nüfuzuna karşı koymak, kritik veri ve bilgileri çalmak amacıyla casusluk çabalarını artırdı.

Üçüncü bölümde ele alındığı üzere, yabancı aktörler de dünyanın dört bir yanında yer alan bölgelerde propaganda yoluyla etkileme operasyonlarını gerçekleştirebilmek için son derece etkili teknikler kullanıyor. Örneğin Rusya, Ukrayna'yı işgalinin haklılığı konusunda kendi vatandaşını ve diğer birçok ülke vatandaşını ikna etmek için çok fazla ter dökerken, bir yandan da Batı'da COVID aşılarının itibarını sarsan propagandalar yaptı ve aynı anda kendi ülkesindeki etkinliği de artırmaya çalıştı. Buna ek olarak aktörler, dördüncü bölümde ele alınan ağlara ve kritik altyapıya giriş noktaları olarak Nesnelerin İnterneti (IoT) cihazlarını veya Operasyonel Teknoloji (OT) kontrol cihazlarını giderek daha fazla hedeflemektedir. Rapor'un son bölümünde, siber dayanıklılık alanında bu yıl kaydedilen gelişmeleri incelerken, geçen yıl içinde Microsoft'a ve müşterilerimize yönelik saldırılara karşı yaptığımız savunmadan elde ettiğimiz içgörüleri ve aldığımız dersleri sunuyoruz.

Her bölümde, Microsoft'un benzersiz bakış açısı temel alınarak öğrenilen önemli dersler ve içgörüler sunulmaktadır. Dünya çapındaki ürün ve hizmet ekosistemimizden gelen, analizini yaptığımız trilyonlarca sinyal, dünya genelindeki dijital tehditlerin şiddetini, kapsamını ve ölçeğini ortaya koymaktadır. Microsoft, müşterilerimizi ve dijital ekosistemi bu tehditlere karşı savunmak için gerekli adımları atmaktadır; müşterilerimize yönelik milyarlarca kimlik avı girişimini, kimlik hırsızlığını ve diğer tehditleri belirleyen ve engelleyen teknolojimiz hakkında bilgi edinebilirsiniz.

Tom Burt'ün Rapor Tanıtımı

Devamı

Ayrıca, siber suçlular ve ulus devlet aktörleri tarafından kullanılan altyapıyı ele geçirmek ve bunları kapatmak ve bir ulus devlet aktörü tarafından tehdit edildiğinde veya saldırıya uğradığında müşterileri bilgilendirmek için yasal ve teknik araçlar da kullanıyoruz. Siber tehditleri tanımlamak ve engellemek üzere AI/ML teknolojisini kullanan ve güvenlik uzmanlarının siber saldırılara karşı daha hızlı ve etkili bir şekilde savunma yapıp tespit etmesini sağlamak amacıyla giderek daha etkili özellikler ve hizmetler geliştirmek için çalışıyoruz.

Belki de en önemlisi, MDDR boyunca, bireylerin, kurumların ve işletmelerin bu artan dijital tehditlere kendilerini karşı savunmak için atabilecekleri adımlar konusunda en iyi tavsiyemizi sunuyoruz. İyi siber hijyen uygulamalarını benimsemek en iyi savunmadır ve siber saldırı riskini önemli ölçüde azaltabilir.

Siber suçların durumu

Siber suçlular, çok karmaşık kâr amaçlı kurumlar şeklinde faaliyet göstermeye devam ediyor. Saldırganlar, saldırı operasyon altyapısına ilişkin barındırma hizmetinin yeri ve şekline ilişkin karmaşıklığı artırarak uyum sağlıyor ve tekniklerini uygulamakla ilgili yeni yollar buluyor. Aynı zamanda, siber suçlular gittikçe daha tutumlu oluyor. Saldırganlar, genel giderlerini azaltıp meşru görünme çabalarını artırmak adına kimlik avı saldırıları ve malware için barındırma hizmeti almak, hatta bilgi işlem güçlerini kripto para madenciliği yapmak amacıyla kullanmak için iş ağlarını ve cihazlarını tehlikeye atıyor.

Daha fazla bilgi için bkz.sayfa 6

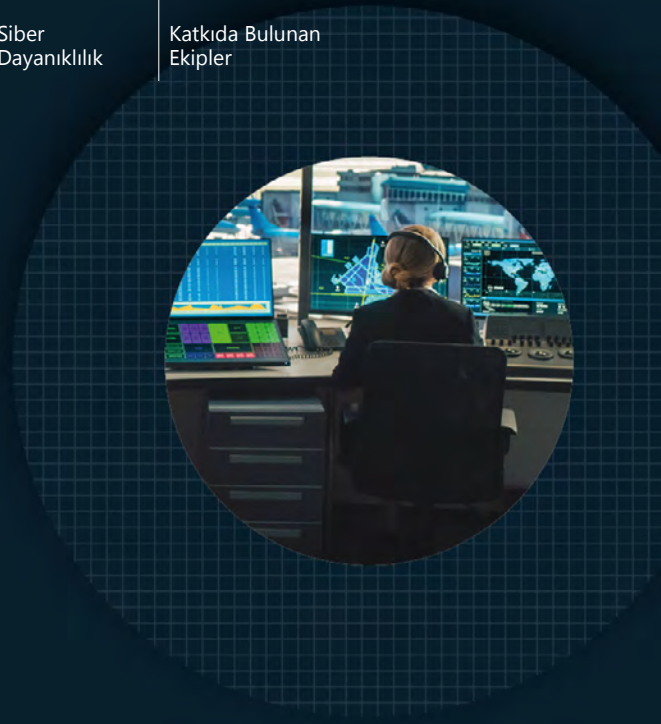
"Ukrayna'daki hibrit savaşta siber silah kullanımının ortaya çıkışı, yeni bir çatışma çağının başlangıcıdır."

Ulus devlet tehditleri

Ulus devlet aktörleri, tespit edilmekten kaçınmak ve kendi stratejik önceliklerini ileriye taşımak üzere tasarlanmış, giderek daha karmaşık hâle gelen siber saldırılar başlatmaktadır. Ukrayna'daki hibrit savaşta siber silah kullanımının ortaya çıkışı, yeni bir çatışma çağının başlangıcıdır. Rusya ayrıca kendi ülkesi, Ukrayna ve dünya genelindeki bakış açısını etkilemek üzere propagandayı kullanarak bilgi etkileme operasyonlarıyla savaşını destekledi. Ukrayna dışında, ulus devlet aktörleri faaliyetlerini artırdı ve daha geniş bir hedef kümesine saldırı düzenlemek için otomasyon, bulut altyapısı ve uzaktan erişim teknolojilerindeki gelişmeleri kullanmaya başladı. Nihai hedeflere erişim sağlayan kurumsal BT tedarik zincirleri sık sık saldırıya uğradı. Aktörlerin, henüz patch uygulanmamış güvenlik açıklarından hızlı bir şekilde yararlanmaları, kimlik bilgilerini çalmak üzere gelişmiş tekniklerin yanı sıra deneme yanılma yöntemlerini kullanmaları ve açık kaynaklı veya yasal yazılımları kullanarak operasyonlarını gizlemeleri ile siber güvenlik hijyeni çok daha kritik bir hâl aldı. Buna ek olarak İran, saldırılarının temel unsuru olarak fidye yazılımları kullanmak da dahil olmak üzere yıkıcı siber silahların kullanımı konusunda Rusya'ya katılıyor.

Bu gelişmeler, insan haklarına öncelik veren ve halkı online ortamda sergilenen sorumsuz devlet davranışlarına karşı koruyan tutarlı, küresel bir çerçevenin acilen benimsenmesini gerektirmektedir. Tüm uluslar, sorumlu devlet davranışına yönelik normları ve kuralları uygulamak için el ele vermelidir.

Daha fazla bilgi için bkz. sayfa 30



Cihazlar ve altyapı

Pandemi, gittikçe artan dijital dönüşümün bir bileşeni olarak internete yönelik her türlü cihazın hızla benimsenmesiyle birleştiğinde dijital dünyamızın saldırıya açık yüzeyini büyük ölçüde genişletti. Sonuç olarak, siber suçlular ve ulus devletler hızla avantaj kazanmaktadır. BT donanım ve yazılımlarının güvenliği son yıllarda güçlenirken, IoT ve OT cihazlarının güvenliği buna ayak uyduramadı. Tehdit aktörleri; ağlara erişim sağlamak ve yanal hareket edebilmek, bir tedarik zincirinde tutunabilmek veya hedef kurumun OT operasyonlarını bozmak amacıyla bu cihazlardan faydalanmaktadır.

Daha fazla bilgi için bkz. sayfa 56

Tom Burt'ün Rapor Tanıtımı

Devamı

Siber etki operasyonları

Ulus devletler, hem yerel hem de uluslararası düzeyde propagandasını yaymak ve kamuoyunu etkilemek amacıyla karmaşık etki operasyonlarını giderek daha fazla kullanıyor. Bu operasyonlar güveni sarsıyor, kutuplaşmayı artırıyor ve demokratik süreçleri tehdit ediyor. Nitelikli İleri Düzeyde Kalıcı Manipülasyon yapan aktörler, operasyonlarının kapsam, ölçek ve verimliliğinin yanı sıra küresel bilgi ekosisteminde sahip oldukları etkiyi büyük ölçüde artırmak için geleneksel medyayı internet ve sosyal medya ile birlikte kullanıyor. Geçen yıl, bu operasyonların Rusya'nın Ukrayna'daki hibrit savaşının bir parçası olarak kullanıldığına şahitlik ettik ancak aynı zamanda Rusya, Çin ve İran'ın da aralarında olduğu diğer ulusların bazı sorunlarla ilgili küresel etkilerini genişletmek amacıyla sosyal medyadan güç alan propaganda operasyonlarını giderek daha fazla kullandıklarını gördük.

Daha fazla bilgi için bkz. sayfa 71

Siber dayanıklılık

Güvenlik, teknolojik başarının kilit unsurlarından biridir. Yenilik ve artırılmış verimlilik, sadece kurumları modern saldırılara karşı mümkün olduğunca dayanıklı hâle getiren güvenlik önlemlerinin uygulanmasıyla gerçeğe dönüşebilir. Pandemi, Microsoft'ta bizi, güvenlik uygulamalarımızı ve teknolojilerimizi, çalışanlarımızın işlerini yaptığı her yerde onları koruyacak şekilde yönlendirmeye zorladı. Geçen yıl tehdit aktörleri, pandemi sırasında ortaya çıkan güvenlik açıklarından ve hibrit çalışma ortamına geçiş durumundan yararlanmaya devam etti. O zamandan beri başlıca sorunumuz, çeşitli saldırı yöntemlerinin yaygınlığını ve karmaşıklığını ve artan ulus devlet faaliyetini yönetmek oldu. Bu bölümde, karşılaştığımız zorlukları ve 15.000'den fazla ortağımızla birlikte bunlara yanıt olarak seferber ettiğimiz savunmaları ayrıntılarıyla açıklayacağız.

Daha fazla bilgi için bkz. sayfa 86

Benzersiz bakış açımız

37 milyar
e-posta tehdidi engellendi

34,7 milyar
kimlik tehdidi engellendi

43 trilyon
sinyal, dijital tehditleri ve suçlu siber faaliyetleri anlamak ve bunlara karşı korunmak için gelişmiş veri analitiği ve yapay zeka algoritmaları kullanılarak günlük olarak sentezlendi.

8.500'den fazla
mühendis, araştırmacı, veri bilimci, siber güvenlik uzmanı, tehdit avcısı, jeopolitik analist, araştırmacı ve ön saftaki müdahale ekibi 77 ülkede faaliyet gösteriyor.

2,5 milyar
uç nokta sinyali günlük olarak analiz edildi

15.000'den fazla
iş ortağı, güvenlik ekosistemimizde müşterilerimiz için siber dayanıklılığı arttırdı.

1 Temmuz 2021 - 30 Haziran 2022

Tom Burt'ün Rapor Tanıtımı

Devamı

Microsoft'un bağımsız bir şekilde ve özel sektör, kamu kuruluşları ve sivil toplumdaki diğer birimlerle kurduğu yakın ortaklıklar aracılığıyla toplumumuzun sosyal dokusunu destekleyen dijital sistemleri koruma ve nerede olursa olsun herkes için güvenli bilgi işlem ortamlarını teşvik etme sorumluluğuna sahip olduğuna inanıyoruz. 2020 yılından bu yana MDDR'yi her yıl yayınlamamızın nedeni işte bu sorumluluktur. Bu rapor, Microsoft'un elindeki devasa verilerin ve yürüttüğü kapsamlı araştırmasının ulaştığı doruk noktasıdır. Dijital tehdit ortamının nasıl evrildiğine ve ekosistemin güvenliğini artırmak için bugün alınabilecek önemli önlemlere ilişkin benzersiz içgörülerimiz paylaşılmaktadır.

Okuyucuların hem burada hem de yıl boyunca yayımladığımız birçok siber güvenlik yayınında sunulan verilere ve içgörülere dayanarak anında harekete geçebilmesi için bir aciliyet duygusu aşılamayı umuyoruz. Dijital ortama yönelik tehdidin ağırlık merkezini ve bunun fiziksel dünyaya olan yansımasını değerlendirirken, hepimizin kendimizi, kurumlarımızı ve işletmeleri dijital tehditlere karşı korumak için harekete geçme gücüne sahip olduğunu aklımızdan çıkarmamız önemlidir.

Bu yılki Microsoft Dijital Savunma Raporu'nu incelemeye zaman ayırdığınız için teşekkür ederiz. Raporda, dijital ekosistemi toplu olarak savunmamıza yardımcı olacak değerli içgörüler ve öneriler bulunduğunu göreceğinizi umuyoruz.

Tom Burt
Müşteri Güvenliği ve Güveni'nden Sorumlu Kurumsal Başkan Yardımcısı

Bu raporla ulaşmak istediğimiz hedef iki yönlüdür:

1. Müşterilerimiz, iş ortaklarımız ve daha geniş bir ekosistemde yer alan paydaşlarımız için her geçen gün evrilen dijital tehdit ortamını hem yeni siber saldırılara hem de tarihsel olarak kalıcı hâle gelmiş tehditlerdeki gelişen trendlere ışık tutarak aydınlatmak.
2. Müşteri ve iş ortaklarımızı siber dayanıklılıklarını geliştirecek ve bu tehditlere yanıt verecek şekilde güçlendirmek.

Siber Suçların Durumu

Siber savunmaların gelişimine ve daha fazla kurumun önlem alma konusunda proaktif bir yaklaşım benimsemesine bağlı olarak saldırganlar da kullandıkları teknikleri uyarlamaktadır.

Siber Suçların

Durumuna genel bakış

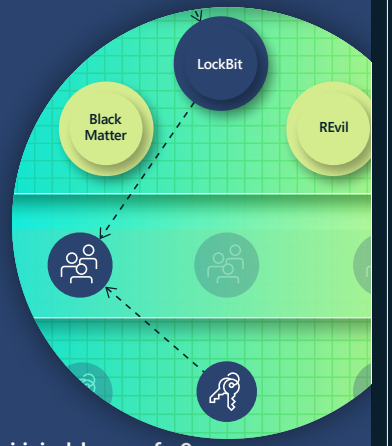
Siber savunmaların gelişimine ve daha fazla kurumun önlem alma konusunda proaktif bir yaklaşım benimsemesine bağlı olarak saldırganlar da kullandıkları teknikleri uyarlamaktadır.

Siber suçlular, çok karmaşık kâr amaçlı kurumlar şeklinde faaliyet göstermeye devam ediyor. Saldırganlar, saldırı operasyon altyapısına ilişkin barındırma hizmetinin yeri ve şekline ilişkin karmaşıklığı artırarak uyum sağlıyor ve tekniklerini uygulamakla ilgili yeni yollar buluyor. Aynı zamanda, siber suçlular gittikçe daha tutumlu oluyor. Saldırganlar, genel giderlerini azaltıp meşru görünme çabalarını artırmak adına kimlik avı saldırıları ve malware için barındırma hizmeti almak, hatta bilgi işlem güçlerini kripto para madenciliği yapmak amacıyla kullanmak için iş ağlarını ve cihazlarını tehlikeye atıyor.

Siber suç ekonomisinin sanayiye dönüşümü, araçlara ve altyapıya daha fazla erişim sağlayarak siber suça girişin önündeki beceri engelini azalttığı için siber suçlar artmaya devam etmektedir.

Daha fazla bilgi için bkz. sayfa 18

Fidye yazılımı ve şantaj tehdidi; kamu kuruluşları, kurumlar ve kritik altyapıyı hedef alan saldırılarla daha cüretkar hâle gelmektedir.

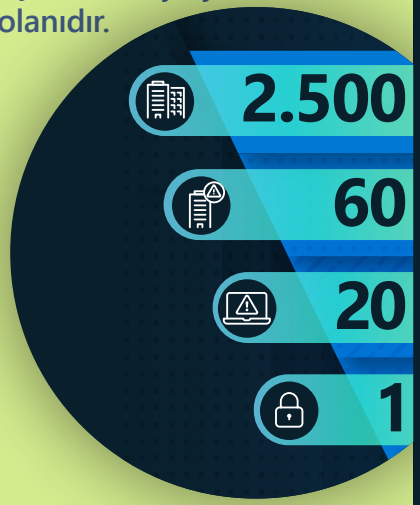


Daha fazla bilgi için bkz. sayfa 9

Saldırganlar, mağdurları fidye ödeme konusunda iknaya çalışırken onları, hassas verileri ifşa etmekle tehdit eder.

Daha fazla bilgi için bkz. sayfa 10

Hedeflerin üçte biri bu saldırıları kullanan suçlular tarafından başarıyla ele geçirildiği ve bunların %5'inden fidye alındığı için, insan tarafından işletilen fidye yazılımları en yaygın olanıdır.

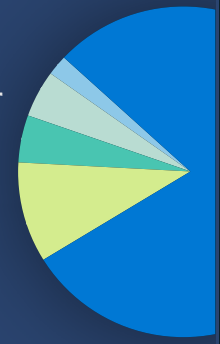


Daha fazla bilgi için bkz. sayfa 9

Fidye yazılımlarına karşı en etkili savunma yönteminde; ağ mimarisi genelinde çok faktörlü kimlik doğrulama, sıklıkla sunulan güvenlik yamaları ve Sıfır Güven ilkeleri yer alır.

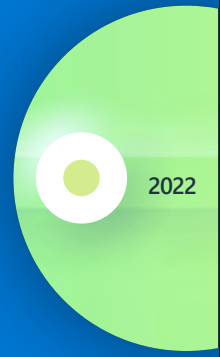
Daha fazla bilgi için bkz. sayfa 13

Tüm gelen kutularını gelişigüzel bir şekilde hedef alan kimlik bilgileri avlama saldırıları artmakta ve fatura dolandırıcılığı dahil kurum e-postalarının ele geçirilmesi, kurumlar için önemli bir siber suç riski oluşturmaktadır.



Daha fazla bilgi için bkz. sayfa 21

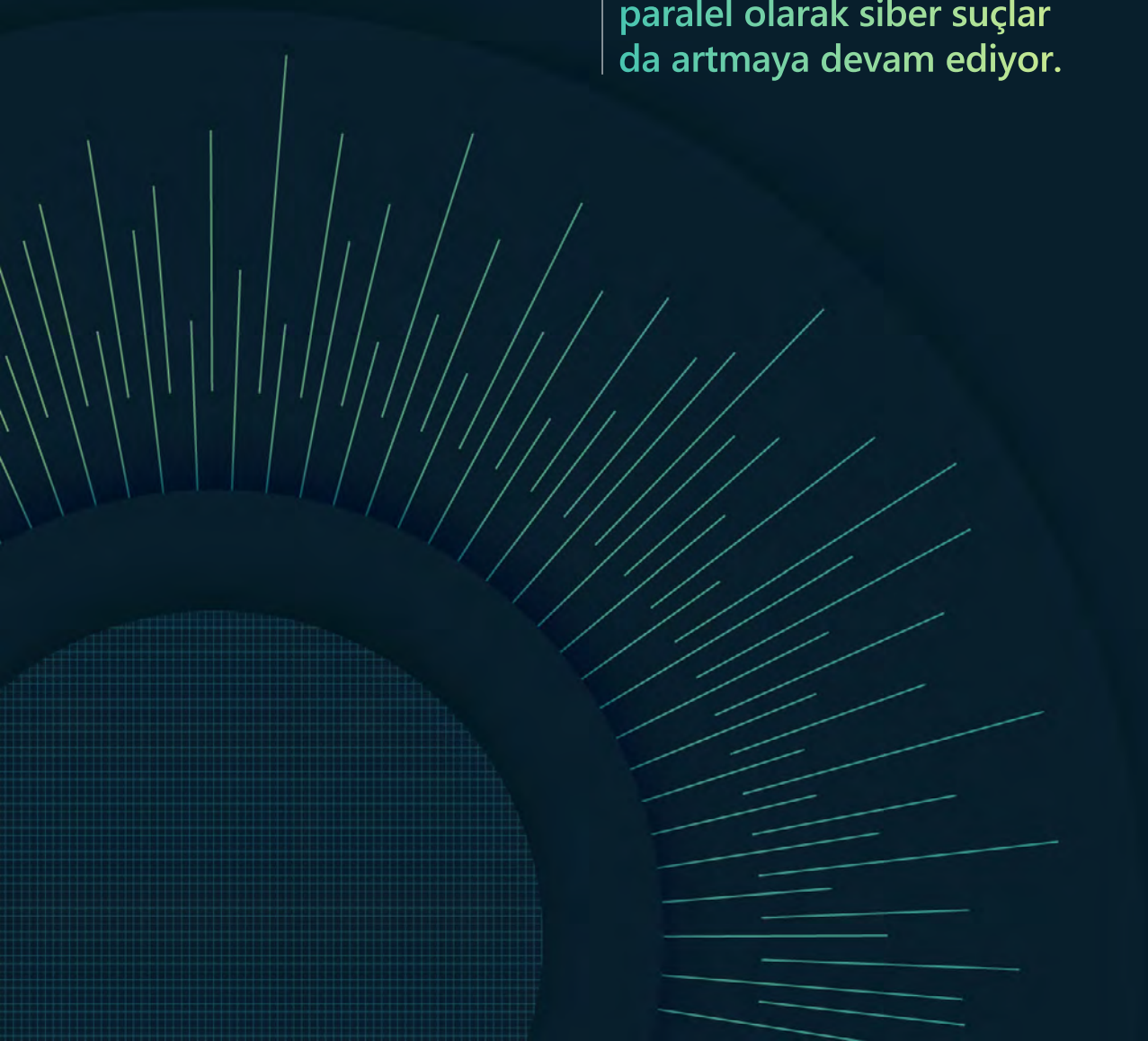
Microsoft, siber suçluların ve ulus devlet aktörlerinin kötü amaçlı altyapılarını durdurmak için yenilikçi yasal yaklaşımlar ile kamu ve özel ortaklıklarımıza güvenmektedir.



Daha fazla bilgi için bkz. sayfa 25

Giriş

Hem rastgele hem de hedefli saldırılardaki artışa paralel olarak siber suçlar da artmaya devam ediyor.



Siber savunmalar geliştikçe ve daha fazla kamu kuruluşu ve işletme önlem alma konusunda proaktif bir yaklaşım benimsedikçe saldırganların, siber suçları kolaylaştırmak için gereken erişimi elde etme aşamasında iki strateji kullandığını görüyoruz. Bu yaklaşımlardan ilki, hacme dayalı geniş hedefleri olan bir operasyondur. Diğeri ise getiri oranını artırmak amacıyla izleme ve daha seçici hedeflemenin kullanımıdır. Jeopolitik amaçlara yönelik ulus devlet faaliyetleri gibi gelir elde etme amacı olmadığında bile hem rastgele hem de hedefli saldırılar kullanılır. Geçtiğimiz yıl siber suçlular, operasyonların başarısını en üst düzeye çıkarmak için sosyal mühendisliği ve güncel konuların istismarı yöntemini kullanmayı sürdürdü. Örneğin, COVID temalı kimlik avı tuzakları daha az kullanılırken, Ukrayna vatandaşlarına destek olmak amaçlı bağış toplama tuzaklarında artış olduğunu gözlemledik.

Saldırganlar, saldırı operasyon altyapısına ilişkin barındırma hizmetinin yeri ve şekline ilişkin karmaşıklığı artırarak uyum sağlıyor ve tekniklerini uygulamakla ilgili yeni yollar buluyor. Siber suçluların artık daha tutumlu hâle geldiğini ve saldırganların teknoloji masraflarını kıstığını gözlemledik. Bazı saldırganlar, genel giderlerini azaltmak ve meşruiyet görünümünü artırmak amacıyla kimlik avı operasyonları ile malware'i barındırmak, hatta kurumların bilgi işlem güçlerini kripto para madenciliği yapmak amacıyla kullanmak üzere kurumların güvenliğini aşmayla giderek daha fazla ilgileniyor.

Bu bölümde, sosyal veya politik hedeflere yönelik siber saldırılar gerçekleştiren özel vatandaşların neden olduğu bir aksaklık olan hacktivizmdeki artışı da inceleyeceğiz. Dünya çapında Şubat 2022'den bu yana, içerisinde hem uzman hem de acemilerin bulunduğu binlerce kişi, Rusya-Ukrayna savaşının bir parçası olarak web sitelerini devre dışı bırakma ve çalınan verileri sızdırma gibi saldırılar başlatmak için harekete geçti. Aktif savaşın sona ermesinden sonra bu trendin devam edip etmeyeceği konusunda tahmin yürütmek için henüz çok erken.

Kurumlar, siber saldırılara karşı savunma yapmak için erişim kontrollerini düzenli olarak gözden geçirip güçlendirmeli ve güvenlik stratejileri uygulamalıdır. Ancak elbette ellerinden gelen tek şey bu değil. Dijital Suçlar Birimimizin (DCU), siber suçlular ve ulus devlet aktörleri tarafından kullanılan kötü amaçlı altyapıyı ele geçirmek üzere hukuk davalarını nasıl kullandığına ilişkin açıklamalar da sunuyoruz. Bu tehdide karşı hem kamu hem de özel ortaklıklar el ele vererek mücadele yürütmeliyiz. Son 10 yılda öğrendiklerimizi paylaşarak, başkalarının kendilerini ve geniş ekosistemi sürekli büyüyen siber suç tehdidine karşı korumak üzere alabilecekleri proaktif önlemleri anlamasına ve değerlendirmesine yardımcı olmaya ümit ediyoruz.

Amy Hogan-Burney
Genel Müdür, Dijital Suçlar Birimi

Fidye yazılımı ve şantaj: Ulus düzeyinde bir tehdit

Fidye yazılımı saldırıları; kritik altyapı, her büyüklükten işletme ve eyalet ile yerel kamu kuruluşlarının, gittikçe büyüyen siber suç ekosisteminden yararlanan suçlular tarafından hedeflenmesiyle tüm bireyler için daha fazla tehlike oluşturmaktadır.

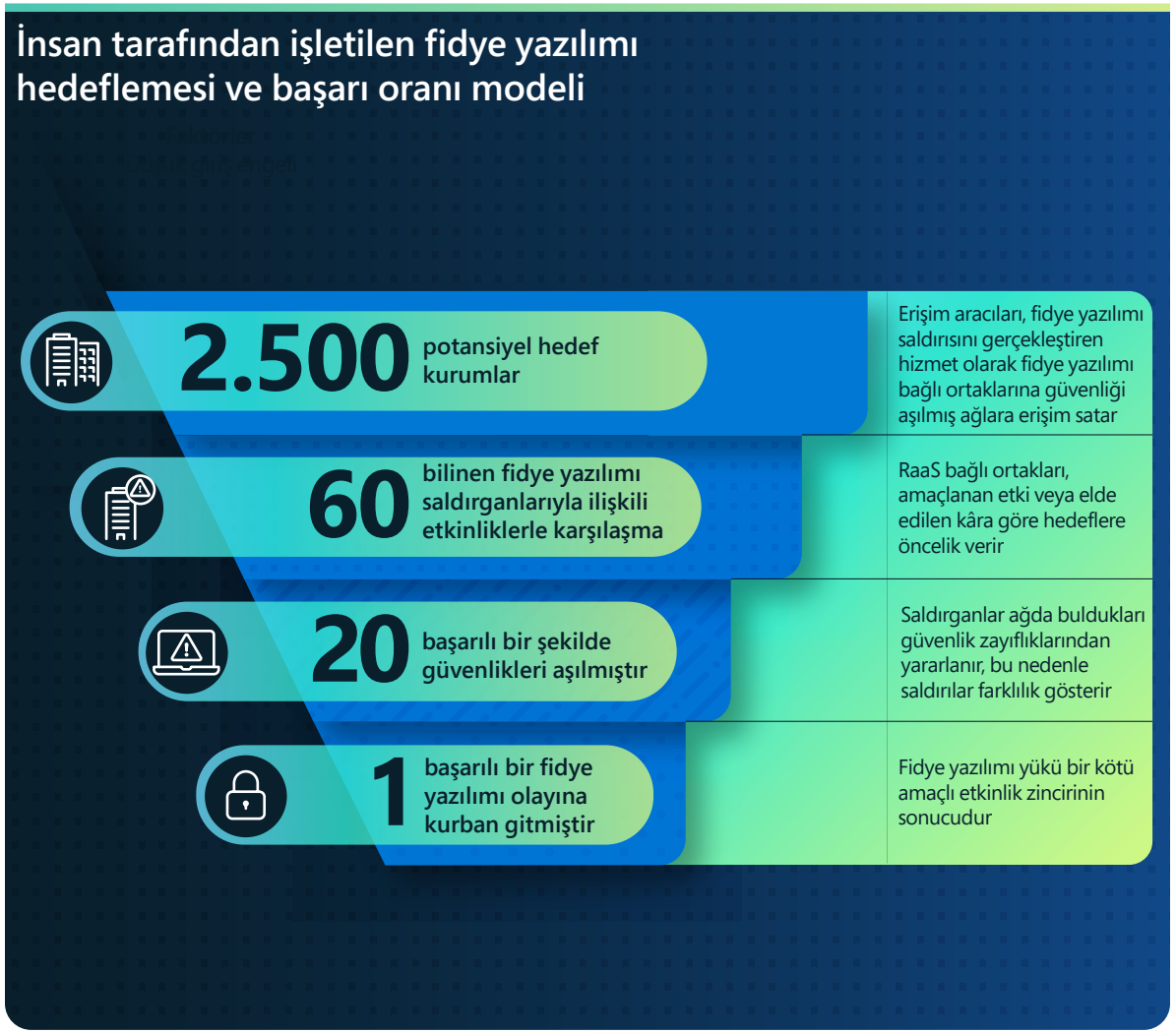
Son iki yılda kritik altyapı, sağlık hizmetleri ve BT hizmet sağlayıcıları gibi yüksek profilli fidye yazılımı olayları, kamuoyunun büyük ilgisini çekmiştir. Fidye yazılımı saldırıları kapsam olarak daha cüretkar hâle geldikçe, etkileri daha geniş bir kesime yayılmaktadır. Aşağıda, 2022 yılında gördüğümüz saldırı örnekleri yer almaktadır:

- Şubat ayında gerçekleştirilen iki kuruma yönelik bir saldırıda, Almanya'nın kuzey bölgesindeki yüzlerce benzin istasyonunun ödeme işleme sistemi etkilenmiştir.[1]
- Mart ayında, Yunanistan'ın posta hizmetine yönelik bir saldırı, posta dağıtımını geçici olarak kesintiye uğratmış ve finansal işlemlerin işlenmesini etkilemiştir.[2]
- Mayıs ayı sonlarında, Kosta Rika devlet kurumlarına yönelik bir fidye yazılımı saldırısında, hastanelerin kapatılması ve gümrük vergileri ile diğer vergi tahsilatının aksaması sonrasında ulusal bir acil durum ilan edilmesi zorunlu hâle gelmiştir.[3]
- Yine Mayıs ayında gerçekleştirilen bir saldırı, Hindistan'ın en büyük havayollarından birinde uçuşlarda gecikme ve iptallere neden olarak yüzlerce yolcunun mağdur olmasına neden olmuştur.[4]

Bu saldırıların başarısı ve gerçek hayattaki etkilerinin boyutu; siber suç ekonomisinin bir endüstri hâline gelmesi, araçlara ve altyapıya erişimin sağlanması ve sisteme girişin önündeki beceri engelleri azaltılarak siber suç yeteneklerinin genişletilmesinin bir sonucu olarak ortaya çıkmaktadır.

Son yıllarda fidye yazılımı, tek bir "çetenin" bir fidye yazılımı yükü geliştirip dağıttığı modelden hizmet olan fidye yazılımı (RaaS) modeline geçiş yapmıştır. RaaS, bir grubun fidye yazılımı yüküne ilişkin geliştirme sürecini yönetmesine ve kârdan pay almak için "ortaklar" olarak anılan diğer siber suçlulara (fiilen fidye yazılımı saldırılarını başlatanlara) veri sızıntısı yoluyla ödeme ve şantaj hizmetleri sağlamasına olanak tanır. Siber suç ekonomisinin bu şekilde marka kiralamasına gitmesi saldırgan havuzunu genişletti. Siber suç araçlarının endüstrileşmesi, saldırganların yetkisiz erişimini, verileri sızdırmasını ve fidye yazılımı kurmasını kolaylaştırdı.

İnsan tarafından işletilen fidye yazılımı[5], Microsoft araştırmacıları tarafından, saldırıların her aşamasında hedeflerinde yer alan ağda tespit ettiklerine dayanarak karar veren ve ticari fidye yazılımı saldırılarından kaynaklanan tehdidi tanımlayan insanlar tarafından yönlendirilen tehditleri tespit etmek için türetilen bir terim olup kurumlar için hala önemli bir tehdit olmaya devam etmektedir.



Uç Nokta için Microsoft Defender (EDR) verilerine dayalı model (Ocak–Haziran 2022).

Fidye yazılımı ve şantaj: Ulus düzeyinde tehdit

Devamı

Çifte şantajla para kazanma stratejisinin benimsenmesi standart bir uygulama halini aldıkça fidye yazılımı saldırıları daha da etkili hâle bürünmüştür. Bu uygulamada; güvenliği aşılmış cihazlardan veri sızdırma, cihazlardaki verileri şifreleme ve ardından mağdurları fidye ödemeye zorlamak için çalınan verileri herkese açık olarak gönderme veya göndermekle tehdit etme yer alır.

Fidye yazılımı saldırganlarının çoğu, fırsatçı olarak eriştikleri ağa fidye yazılımı kursa da, bazıları diğer siber suçlulardan erişim satın alarak erişim aracıları ile fidye yazılımı operatörleri arasındaki bağlantıları kullanır.

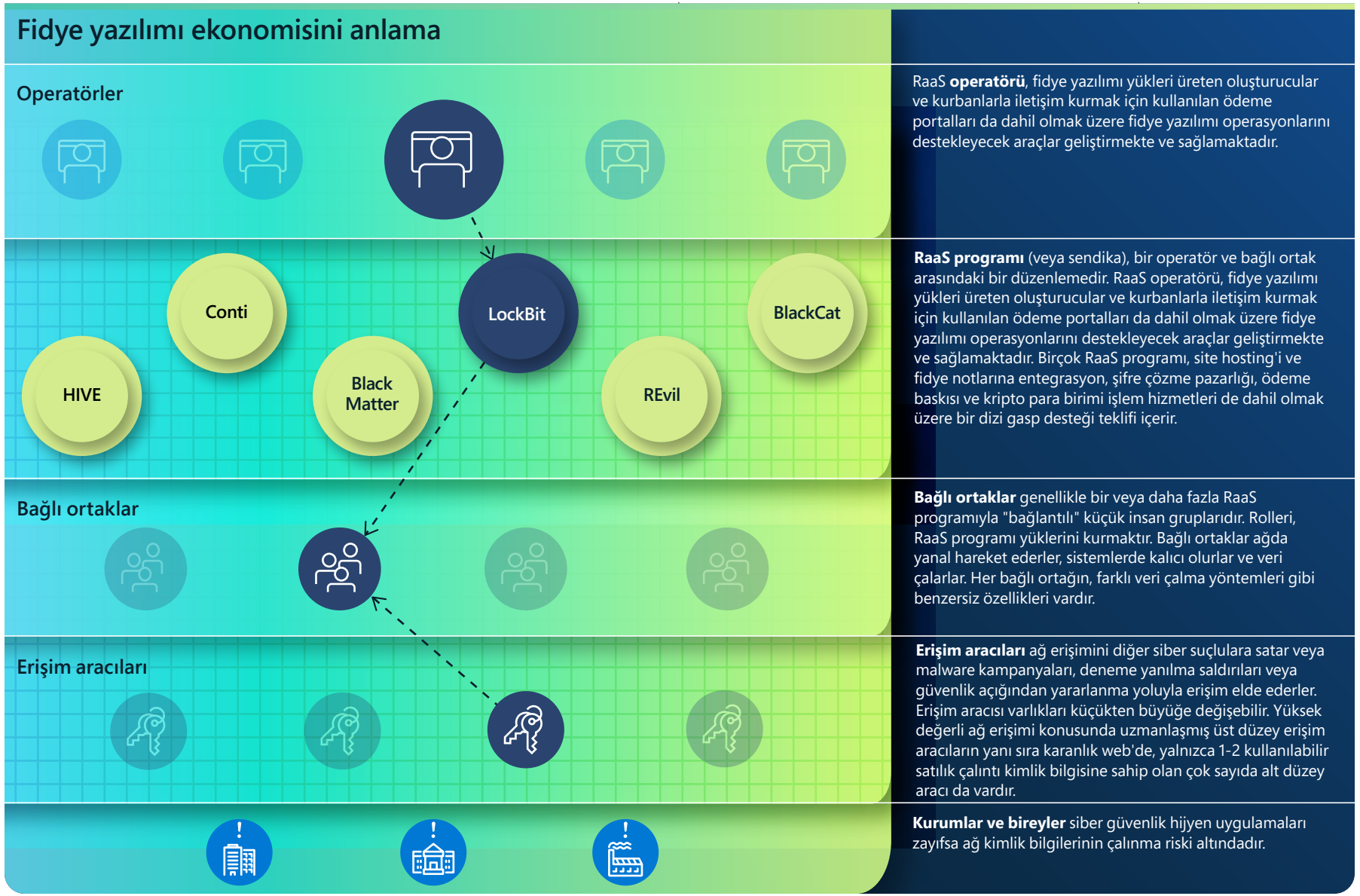
Kimlik bilgileri, e-posta, uç noktalar ve bulut gibi birden çok kaynaktan toplanan benzersiz elektronik istihbarat çeşitliliği, teknik olarak daha az yetenekli saldırganlar için tasarlanmış araçlar içeren bir bağlı kurum sistemiyle birlikte büyüyen fidye yazılımı ekonomisi hakkında içgörü sağlar.

Uzman siber suçlular arasındaki artan ilişkiler, fidye yazılımı saldırılarının hızını, karmaşıklığını ve başarısını artırdı. Bu süreç; siber suç ekosisteminin evrimini, hedeflere, ödeme hizmetlerine ve şifre çözme veya yayımlama araçları ve sitelerine ilk erişimde birbirini destekleyen farklı tekniklere, hedeflere ve becerilere sahip bağlantılı oyunculara doğru yönlendirdi.

Fidye yazılımı operatörleri artık online olarak kurumlara veya kamu kuruluşlarına erişim satın alabilir veya tek amacı yalnızca elde ettikleri erişimden para kazanmak olan aracılarla kişiler arası ilişkiler yoluyla kimlik bilgileri ve erişim elde edebilir.

Operatörler daha sonra satın alınan erişimi, karanlık ağ pazar yerleri veya forumlar üzerinden satın alınan bir fidye yazılımı yükünü kurmak için kullanır. Çoğu durumda, mağdur kişilerle yapılan görüşmeler operatörlerin yerine bizzat RaaS ekibi tarafından yürütülür. Bu suç işlemleri sorunsuz bir şekilde ilerler; karanlık ağın anonimliği ve ulus ötesi yasaların uygulanmasının zorluğu nedeniyle suça karışanların tutuklanma ve suçlanma ihtimali çok düşüktür.

Bu tehdide karşı yürütülen çabanın sürdürülebilir ve başarılı olması için, özel sektörle yakın ortaklık içinde kamu kuruluşları çapında yürütülecek bir strateji olması gerekir.



Fidye yazılımının bazen medyada nasıl gösterildiğinin aksine, tek bir fidye yazılımı biçiminin uçtan uca bir "fidye yazılımı çetesi" tarafından yönetilmesi sıkça karşılaşılan bir durum değildir. Bunun yerine, malware oluşturan, mağdurlara erişim sağlayan, fidye yazılımı kuran ve şantaj görüşmelerini yürüten ayrı oluşumlar vardır. Suç ekosisteminin endüstrileşmesi şunlara ulaşılabilmeyi sağlamıştır:

- İzinsiz erişim (bir hizmet olarak erişim) elde eden ve erişimi dağıtan aracılar.
- Araçların satışını yapan malware geliştiricileri.
- İzinsiz girişleri sağlayan suç operatörleri ve ortakları.
- Ortaklardan (RaaS ile) elde ettikleri geliri devralan şifreleme ve şantaj hizmet sağlayıcıları.

İnsan tarafından işletilen tüm fidye yazılımı operasyonlarında, güvenlik zayıflıklarına ilişkin ortak bağımlılıklar paylaşılır. Spesifik olarak saldırganlar, genellikle bir kurumda patch uygulamalarının sık kullanılmadığı ve çok faktörlü kimlik doğrulamanın (MFA) uygulanamadığı yetersiz siber hijyenden yararlanmaktadır.

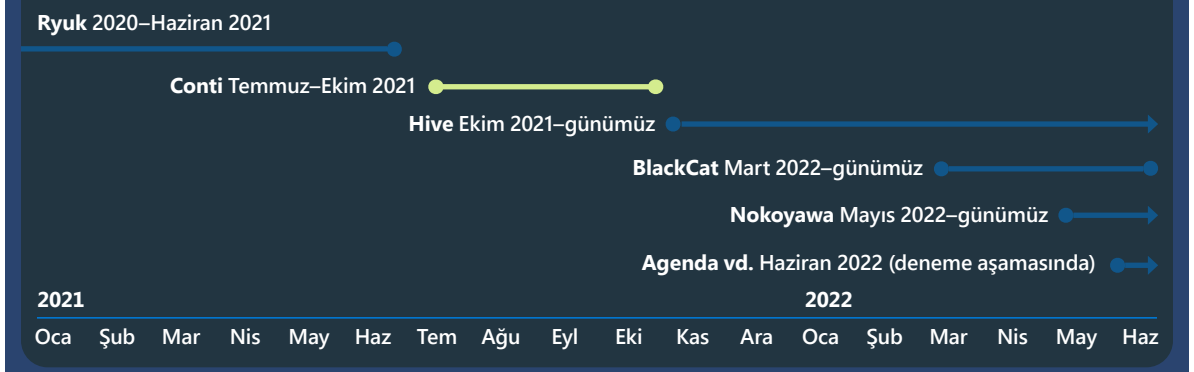
Başarı hikayesi: Conti'nin dağılması

Son iki yılın en iyi fidye yazılımlarından biri olan Conti, Microsoft Tehdit Bilgileri Merkezi'nin (MSTIC) mart sonu ve nisan başında etkinliklerde önemli bir düşüş gözlemlemesiyle 2022'nin ortalarında operasyonlarını durdurma sürecine girdi. En yeni Conti fidye yazılımı kurulum işlemlerini nisan ayı ortasında gözlemledik. Bununla birlikte MSTIC; BlackBasta, Lockbit 2.0, LockbitBlack ve HIVE dahil Conti ortaklarının diğer fidye yazılımı yüklerini kurmaya başladığını gözlemlediği için diğer fidye yazılımı operasyonlarının kapatılmasında olduğu gibi, Conti'nin dağılmasının da fidye yazılımı kurulumları üzerinde önemli bir etkisi olmadı. Bu durum, önceki yıllara ait verilerle tutarlıdır; fidye yazılımı çeteleri çevrimdışı olduğunda, bunların aylar sonra yeniden ortaya çıktığını veya teknik becerilerini ve kaynaklarını yeni gruplara yeniden dağıttıklarını ortaya koymaktadır.

Microsoft'taki tehdit bilgileri ekiplerimiz; fidye yazılımı tehdit aktörlerini, kullandıkları malware'e göre izlemek yerine, kendi özel araçlarına göre ayrı gruplar (DEV'ler olarak etiketlenir) şeklinde izler. Buradan Conti'nin ortakları dağıldığında, diğer araçları veya RaaS kitlerini kullanarak bu DEV'leri izlemeye devam edebileceğimiz anlamı çıkarılabilmekteydi. Örneğin:

- Trickbot'a bağlı DEV-0230, Conti'nin üretken bir kullanıcısıydı. Nisan ayı sonlarında MSTIC bunu QuantumLocker kullanırken gözlemledi.
- DEV-0237, Conti'nin fidye yazılımı kitinden HIVE ve Nokoyawa'ya geçti; buna Kosta Rika kamu kuruluşlarına yönelik 31 Mayıs saldırısında HIVE'ın kullanılması da dahildir.
- Conti fidye yazılımı kitinin bir başka üretken kullanıcısı olan DEV-0506'nın BlackBasta kullandığı gözlemlendi.

RaaS programları arasında hızla geçiş yapan bir ortağa (DEV-0237) ilişkin örnek



Conti gibi bir RaaS programı kapatıldıktan sonra, fidye yazılımı ortağı neredeyse anında başka bir programa (Hive) geçmektedir.

RaaS, fidye yazılımı ekosistemini geliştirir ve ilişkilendirmeyi engeller

İnsan tarafından işletilen fidye yazılımı, kişi operatörler tarafından yönlendirildiği için saldırı modelleri hedefe göre ve saldırı süresi boyunca değişir. Geçmişte, tek bir fidye yazılımı türüyle yapılan tüm operasyonlarda ilk giriş vektörü, araçları ve fidye yazılımı yük seçenekleri arasında yakın bir ilişki olduğunu gözlemlemiştik. Bu durum, ilişkilendirmeyi kolaylaştırdı. Ancak RaaS ortaklık modelinde bu ilişki birbirinden ayrılmaktadır. Sonuç olarak Microsoft, fidye yazılımı yük geliştiricilerini operatör olarak izlemek yerine, belirli saldırılarda yükleri dağıtan fidye yazılımı ortaklarını izlemektedir.

Başka bir deyişle, artık HIVE geliştiricisinin bir HIVE fidye yazılımı saldırısının arkasında yer alan operatör olduğunu düşünmüyoruz; bu operasyonun arkasında bir ortaklığın bulunma olasılığının daha yüksek olduğunu değerlendiriyoruz.

Siber güvenlik endüstrisi, geliştiriciler ile operatörler arasındaki bu durumu yeterli düzeyde yakalamak tespit etmek için çabaladı. Bu endüstride bir fidye yazılımı olayı hala yük adına göre bildirildiğinden, söz konusu fidye yazılımı yükünü kullanan tüm saldırıların arkasında tek bir oluşumun veya fidye yazılımı çetesinin bulunduğu ve bununla ilişkili tüm olaylarda ortak tekniklerin ve altyapının kullanıldığı gibi yanlış bir izlenime varılmaktadır. Ağ savunucularını desteklemek amacıyla farklı ortakların saldırılarından önceki aşamalar (veri hırsızlığı ve ilave kalıcılık mekanizmaları gibi) ile mevcut olabilecek algılama ve koruma fırsatları hakkında daha fazla bilgi edinmek önemlidir.

Saldırganların operasyonlarında başarılı olmak için malware'den ziyade kimlik bilgilerine ihtiyacı vardır. Bir kurumun tamamına, insan tarafından işletilen fidye yazılımının başarılı bir şekilde bulaştırılması, üst düzey ayrıcalıklı bir hesaba erişime bağlıdır.

İnsan tarafından işletilen fidye yazılım saldırılarında öne çıkanlar

Geçtiğimiz yıl Microsoft'taki fidye yazılımı uzmanları, saldırganların tekniklerini izlemek ve müşterilerimiz için nasıl daha iyi koruma sağlayabileceğimizi anlamak için insan tarafından işletilen 100'den fazla fidye yazılımı olayına ilişkin derinlemesine araştırmalar yürüttü.

Burada paylaştığımız analizin yalnızca eklenen ve yönetilen cihazlar için mümkün olduğunu unutmamak önemlidir. Eklenmeyen ve yönetilmeyen cihazlar, bir kurumdaki donanım varlıklarının en az güvenli olan bölümünü temsil eder.

En yaygın fidye yazılımı aşaması teknikleri:

%75
Yönetici araçları kullanır.

%75
Kötü amaçlı yükleri SMB protokolü aracılığıyla yaymak için ele geçirilmiş, yükseltilmiş ve güvenliği ihlal edilmiş bir kullanıcı hesabını kullanır.

%99
İşletim sistemine yerleşik araçları kullanarak keşfedilen güvenlik ve yedekleme ürünlerini bozmaya çalışır.

İnsan tarafından işletilen tipik bir saldırı

İnsan tarafından işletilen fidye yazılımı saldırıları, fidye yazılımı öncesi aşama ve fidye yazılımı kurulum aşaması olarak kategorize edilebilir. Fidye yazılımı öncesi aşamada saldırganlar, kurumun tipolojisini ve güvenlik altyapısını öğrenerek ağa sızmaya hazırlanır.

Saldırganları fidye yazılımı kurulum aşamasına gelmeden durdurun	**Kurulum!**
Fidye yazılımı öncesi	**Fidye Yazılımı**
Bu aşama, birkaç gün ile birkaç hafta veya ay arasında değişebilir. Bununla birlikte, son iki yılda kısalmıştır.	Bu aşama yalnızca birkaç dakika sürebilir
Saldırganlar, topoloji ve güvenlik altyapısı hakkında mümkün olduğunca çok şey öğrenerek ağa sızmaya hazırlanır. Saldırganlar bu aşamada verileri de çalabilir.	Saldırganlar mümkün olduğunca çok veriyi şifrelemeyi hedefler

Araştırmalarımız, insan tarafından işletilen fidye yazılımı saldırılarının arkasındaki çoğu aktörün benzer güvenlik zayıflıklarından yararlandığını ve ortak saldırı modellerini ve tekniklerini paylaştığını ortaya koymuştur.

Dayanıklı bir güvenlik stratejisi

Bu türden saldırılarla mücadele etme ve bunları önleme değerlendirildiğinde, saldırganları fidye yazılımı öncesi aşamadan fidye yazılımı kurulum aşamasına geçmeden önce yavaşlatmak ve durdurmak için gereken kapsamlı korumaya odaklanmak amacıyla kurumun zihniyetinde değişiklik yapılması gereklidir.

Kurumlar, saldırı sınıflarındaki etkiyi azaltmak hedefiyle ağlarında en iyi güvenlik uygulamalarını tutarlı ve hızlı bir şekilde uygulamalıdır. Bu fidye yazılımı saldırıları, insan tarafından karar verilme sürecinin etkisiyle, kolayca kaybolabilen veya zamanında yanıt veremeyen birden çok ve görünüşte birbirinden farklı güvenlik ürünü uyarıları üretebilir. Uyarı karmaşası gerçek olup güvenlik operasyon merkezleri (SOC'ler), daha büyük resmi görebilmeleri için uyarılarındaki eğilimlere bakarak veya uyarıları olaylara göre gruplandırarak işleri kolaylaştırabilir. SOC'ler daha sonra, saldırı yüzeyi azaltma kuralları gibi güçlendirme becerilerini kullanarak uyarıları azaltabilir. Yaygın tehditlere karşı sağlamlaştırma, yalnızca uyarı hacmini azaltmakla kalmaz, aynı zamanda birçok saldırganı ağlara erişmeden önce durdurabilir.

Kurumlar, kendilerini insan tarafından işletilen fidye yazılımı saldırılarına karşı korumak için güvenlik duruşu ve ağ hijyenine ilişkin yüksek standartları sürekli olarak devam ettirmelidir.

Eyleme dönüştürülebilir içgörüler

Fidye yazılımı saldırganları kolay kâr edinme ile motive edilir, bu nedenle güvenlikte sıkılaştırma yoluyla maliyetlerine katkıda bulunmak, siber suçlu ekonomisini bozmanın anahtarıdır.

1. Kimlik bilgileri hijyeni oluşturun. Saldırganların operasyonlarında başarılı olmak için malware'den ziyade kimlik bilgilerine ihtiyacı vardır. Bir kurumun tamamına insan tarafından işletilen fidye yazılımının başarılı bir şekilde bulaştırılması, Etki Alanı Yöneticisi gibi yüksek düzeyde ayrıcalıklı bir hesaba erişime veya Grup İlkesi düzenleme becerilerine bağlıdır.
2. Kimlik bilgilerine erişimi denetleyin.
3. Active Directory güncelleştirmelerinin kurulumuna öncelik verin.
4. Bulut sağlamlaştırmaya öncelik verin.
5. Saldırı yüzey alanını azaltın.
6. İnternete dönük varlıkları sağlamlaştırın ve çevrenizde olup biteni anlayın.
7. Yüksek öncelikli olaylar için hacmi azaltmak ve bant genişliğini korumak üzere ağınızı güçlendirerek SOC uyarı karmaşasını azaltın.

Daha ayrıntılı bilgi için bağlantılar

- RaaS: Siber suç iş gücü ekonomisini ve kendinizi nasıl koruyacağınızı anlamak | Microsoft Güvenlik Blogu
- İnsan tarafından işletilen fidye yazılımı saldırıları: Önlenebilir bir felaket | Microsoft Güvenlik Blogu

Ön saflarda müdahale edenlerin fidye yazılımlarına dair içgörüleri

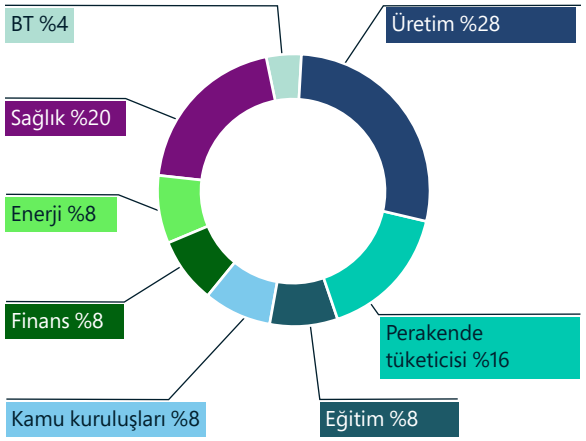
Dünya genelinde kurumlar, 2019 yılından itibaren insan tarafından işletilen fidye yazılımı saldırılarında sürekli bir büyümeyle karşı karşıya kaldı. Ancak, geçen yılki emniyet güçleri operasyonları ve jeopolitik olaylar, siber suç örgütleri üzerinde önemli bir etki yarattı.

Microsoft'un Güvenlik Hizmet Hattı, araştırmadan başarılı bir şekilde kontrol altına alma ve kurtarma etkinliklerine kadar bir siber saldırının başından sonuna müşterileri destekler. Müdahale ve kurtarma hizmetleri, biri araştırmaya ve kurtarma için zemin çalışmasına, ikincisi ise kontrol altına alma ve kurtarmaya odaklanan, son derece entegre iki ekip aracılığıyla sunulur. Bu bölümde, geçtiğimiz yıl boyunca fidye yazılımı etkileşimlerine dayanan bulguların bir özeti sunulmaktadır.

%93

oranında Microsoft araştırma sonucu, fidye yazılımı kurtarma etkileşimleri sırasında ayrıcalık erişiminin ve yanal hareket kontrollerinin yetersiz olduğunu ortaya çıkardı.

Sektöre göre fidye yazılımı olayları ve kurtarma etkileşimleri

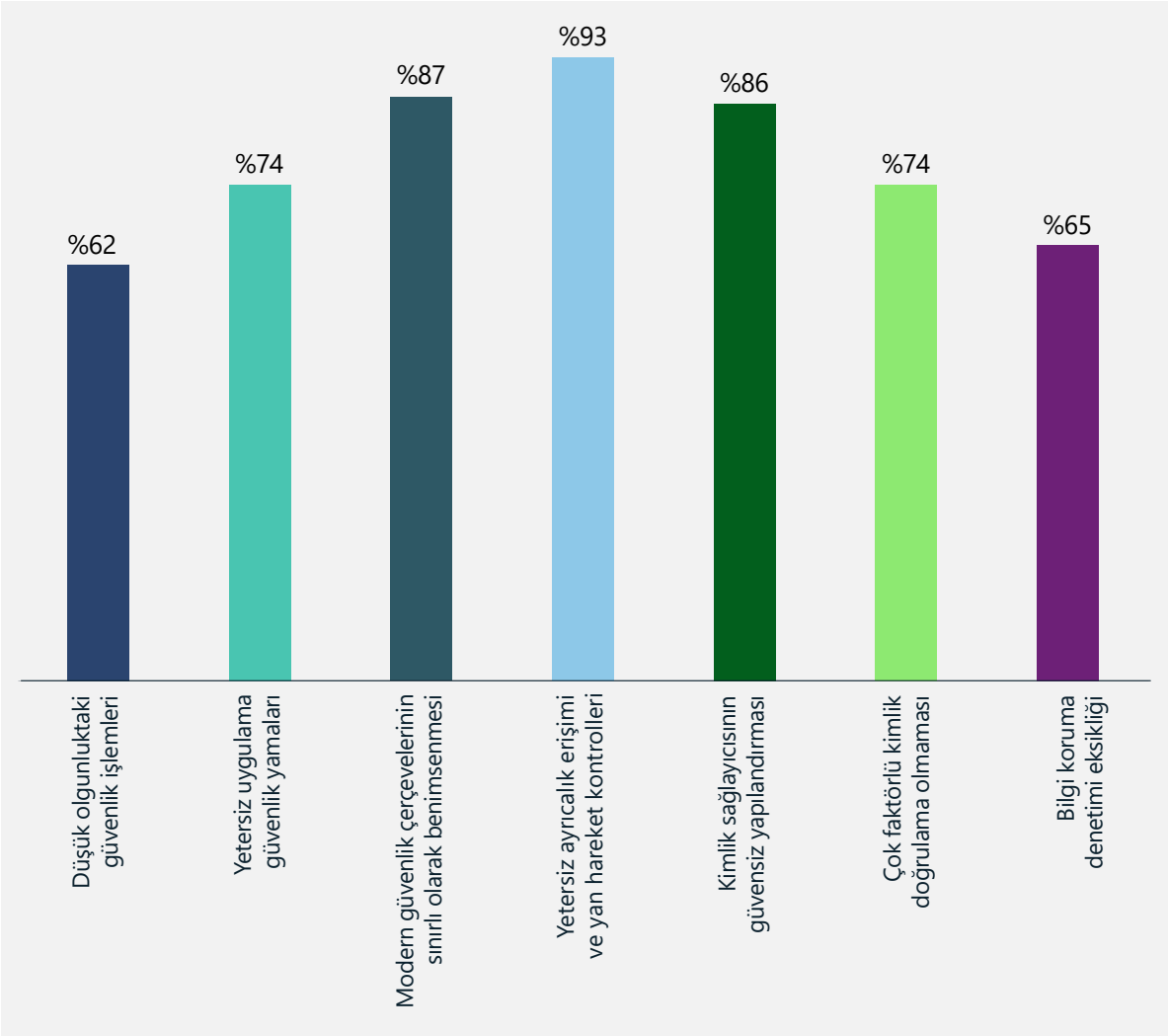


Yeni küçük gruplar ve tehditler ortaya çıktıkça, savunma ekipleri gelişen fidye yazılımı tehditlerinin farkında olmalı ve daha önce bilinmeyen fidye yazılımı malware ailelerine karşı koruma sağlamalıdır. Suç grupları tarafından kullanılan hızlı geliştirme yaklaşımı, kullanımı kolay kitlerde paketlenmiş akıllı fidye yazılımlarının oluşturulmasını sağlamıştır. Bu, daha fazla sayıda hedefe geniş çaplı saldırılar başlatmada daha çok esneklik sağlar.

Aşağıdaki sayfalar, fidye yazılımlarına karşı zayıf korumaya katkıda bulunduğu en sık gözlemlenen faktörlere daha derinlemesine bir bakış sağlar veüç bulgu kategorisine ayrılır:

1. Zayıf kimlik kontrolleri
2. Etkisiz güvenlik operasyonları
3. Sınırlı veri koruması

Fidye yazılımı müdahalesi etkileşimlerindeki en yaygın bulguların özeti



Fidye yazılımı olay müdahalesi etkileşimleri arasında en yaygın bulgu, yetersiz ayrıcalık erişimi ve yanal hareket kontrolleridir.

Ön saflarda müdahale edenlerin fidye yazılımlarına dair içgörüleri

Devamı

Yerinde müdahale etkileşimlerimizde görülen ve saldırıya katkıda bulunan üç ana faktör şunlardır:

① **Zayıf kimlik kontrolleri:** Kimlik bilgisi hırsızlığı saldırıları, saldırıya en çok katkıda bulunan faktörlerden biri olmaya devam etmektedir

② **Etkisiz güvenlik operasyonu** süreçleri, saldırganlar için yalnızca bir fırsat penceresi sunmakla kalmaz, aynı zamanda kurtarma süresini de önemli ölçüde etkiler.

③ Sonunda konunun özeti veridir; kurumlar, iş gereksinimleriyle uyumlu etkili bir **veri koruma stratejisini** uygulamakta zorlanmaktadır

① Zayıf kimlik kontrolleri

İnsan tarafından işletilen fidye yazılımları gelişmeye ve geleneksel olarak hedeflenen saldırılarla ilişkilendirilen kimlik bilgisi hırsızlığı ve yanal hareket yöntemlerini kullanmaya devam etmektedir. Başarılı saldırılar genellikle, insan operatörlerin kimlik bilgilerini çalmasına, sistemlere erişmesine ve ağda kalıcı olarak yerleşmesine imkan tanıyan, Active Directory (AD) gibi kimlik sistemlerinin güvenliğinin aşılmasını içeren, uzun soluklu saldırı kampanyalarının sonucudur.

Active Directory (AD) ve Azure AD güvenliği

%88

oranındaki etkilenen müşteriler, AD ve Azure AD güvenliği için en iyi yöntemleri kullanmıyordu. Saldırganlar, kurumlara daha geniş bir erişim sağlamak ve etki yaratmak için kritik kimlik sistemlerindeki hatalı yapılandırmalardan ve zayıf güvenlik duruşlarından yararlandıkça bu, yaygın bir saldırı vektörü hâline gelmiştir.

En az ayrıcalıklı erişim ve Ayrıcalıklı Erişim İş İstasyonlarının (PAW) kullanımı

Etkilenen kurumların hiçbiri, kritik kimliklerinin ve özel sistemler ve iş açısından kritik uygulamalar gibi yüksek değerli varlıkların yönetimi sırasında, özel iş istasyonları aracılığıyla uygun idari kimlik bilgisi ayrımı ve en az ayrıcalıklı erişim ilkelerini uygulamamıştı.

Ayrıcalıklı hesap güvenliği

%88

oranındaki etkileşimlerde, hassas ve yüksek ayrıcalıklı hesaplar için MFA uygulanmamıştı ve saldırganların, kimlik bilgilerini ele geçirmesi ve meşru kimlik bilgilerini kullanarak daha fazla saldırı gerçekleştirmesi için bir güvenlik boşluğu bırakmıştı.

%84

Kurumların yüzde 84'ünde yöneticiler, ele geçirilen ayrıcalıklı kimlik bilgilerinin daha da fazla kötüye kullanılmasını önlemek için tam zamanında erişim gibi ayrıcalık kimlik kontrollerini kullanmamıştı.

Ön saflarda müdahale edenlerin fidye yazılımlarına dair içgörüleri

Devamı

② Etkisiz güvenlik operasyonları

Verilerimiz, fidye yazılımı saldırılarına uğrayan kurumların güvenlik operasyonlarında, araçlarında ve bilgi teknolojisi varlıklarının yaşam döngüsü yönetiminde önemli boşluklar olduğunu göstermektedir. Mevcut verilere dayanarak en çok aşağıdaki alanlarda boşluklar gözlenmiştir:

Patch uygulama:

%68

oranında etkilenen kurum, etkili bir güvenlik açığı ve yama yönetimi sürecine sahip değildi ve otomatik patch uygulamasına karşı manuel süreçlere yüksek oranda bağımlı olmaları kritik açıklara yol açmıştı. Üretim ve kritik altyapı, eski operasyonel teknoloji (OT) sistemlerinin bakımı ve bunlara patch uygulanmasıyla uğraşmaktadır.

Güvenlik operasyonları araçlarının eksikliği:

Çoğu kurum, güvenlik araçlarının eksikliği veya yanlış yapılandırılması nedeniyle uçtan uca güvenlik görünürlüğü olmadığını ve bunun tespit ve müdahale etkinliğinde azalmaya yol açtığını bildirmiştir.

%60

oranında kurum, tespit ve müdahale için temel bir teknoloji olan EDR[6] aracını kullanmadığını bildirmiştir.

%60

oranında kurumun güvenlik bilgilerine ve olay yönetimi (SIEM) teknolojisine yatırım yapmaması izleme silolarına, uçtan uca tehditleri algılamada sınırlı yeteneğe ve verimsiz güvenlik operasyonlarına yol açmıştı. Otomasyon, SOC araçları ve süreçlerinde önemli bir boşluk olmaya devam ederek, SOC personelini güvenlik telemetrisini anlamlandırmak için saatlerini harcamaya zorlamaktadır.

%84

oranındaki etkilenen kurum, çoklu bulut ortamlarının güvenlik operasyonları araçlarına entegrasyonunu sağlamamıştı.

Müdahale ve kurtarma süreçleri:

%76

Etkilenen kurulumların yüzde 76'sında etkili bir müdahale planının olmadığı gözlemlenmiştir. Bu, kurumun krize uygun şekilde hazırlanmasını engelleyen ve müdahale ile kurtarma sürelerini olumsuz etkileyen kritik bir noktadır.

③ Sınırlı veri koruması

Güvenliği ihlal edilmiş olan birçok kurum, uygun veri koruma süreçlerinden yoksundu. Bu da kurtarma süreleri ve kurum operasyonlarına geri dönme yeteneği üzerinde ciddi bir etkiye yol açıyordu. Karşılaşılan en yaygın eksiklikler arasında şunlar bulunmaktadır:

Sabit yedekleme:

%44

oranında kurumlar, etkilenen sistemler için sabit yedeklemeye sahip değildi. Veriler, yöneticilerin AD gibi kritik varlıklar için yedekleme ve kurtarma planlarına sahip olmadığını da göstermektedir.

Veri kaybını önleme:

Saldırganlar genellikle kurumdaki güvenlik açıklarından yararlanıp sistemlerin güvenliğini aşmanın bir yolunu bularak fidye, fikri mülkiyet hırsızlığı veya gelir elde etme amacıyla kritik verileri sızdırırlar.

%92

oranında saldırılardan etkilenen kurum, kritik veri kaybına yol açan bu riskleri azaltmak için etkili veri kaybı önleme kontrolleri uygulamamıştır.

Fidye yazılımları bazı bölgelerde azalırken bazılarında arttı

Bu yıl, Kuzey Amerika ve Avrupa'daki müdahale ekiplerimize bildirilen fidye yazılımı vakalarının toplam sayısında bir önceki yıla göre bir düşüş gözlemledik. Buna karşılık, Latin Amerika'da bildirilen vakalar arttı.

Bu gözlem, siber suçluların hukuki yaptırımları tetikleme riskinin daha yüksek olduğu düşünülen alanlardan uzaklaşarak daha yumuşak hedeflere yönelmesi olarak yorumlanabilir. Microsoft, dünya çapındaki kurumsal ağ güvenliğinde fidye yazılımlarıyla ilgili destek çağrılarındaki düşüşü açıklayacak önemli bir gelişme gözlemlemediğinden en olası nedenin, 2022'deki bazı jeopolitik olayların yanı sıra 2021 ve 2022'deki suç faaliyetlerinin maliyetini artıran hukuki yaptırımların bir birleşimi olduğunu düşünüyoruz.

En etkili RaaS operasyonlarından biri, 2019'dan beri faaliyet gösteren REvil (Sodinokibi olarak da bilinir) adlı Rusça konuşan bir suç grubuna aittir. Ekim 2021'de REvil'in sunucuları, uluslararası kanun uygulayıcılarının yürüttüğü Operation GoldDust kapsamında çevrimdışına alındı.[7] Ocak 2022'de Rusya, REvil üyesi olduğu iddia edilen 14 kişiyi tutukladı ve bunlarla bağlantılı 25 yere baskın düzenledi.[8] Bu operasyonla Rusya, kendi topraklarında fidye yazılımı operatörlerine karşı ilk kez harekete geçmiş oldu.

2022'de saldırıların sıklığını muhtemelen kanun uygulayıcılarınfaaliyetleri yavaşlatmış olsa da, tehdit aktörleri gelecekte yakalanmamak için yeni stratejiler geliştirebilir.

2 kat

Bazı bölgelerde fidye yazılımı saldırıları azalırken, fidye talepleri iki kattan fazla arttı.

2022'de saldırıların sıklığını muhtemelen kanun uygulayıcıların faaliyetleri yavaşlatmış olsa da, tehdit aktörleri gelecekte yakalanmamak için yeni stratejiler geliştirebilir. Dahası, Rusya ile ABD arasında Rusya'nın Ukrayna'yı işgali nedeniyle yaşanan gerilim, Rusya'nın fidye yazılımlarına karşı küresel mücadelede yeni oluşan işbirliğine son vermiş gibi görünüyor. REvil tutuklamalarının ardından yaşanan kısa bir belirsizlik döneminden sonra ABD ve Rusya, fidye yazılımı aktörlerini takip etme konusundaki işbirliğini durdurdu. Bu da siber suçluların Rusya'yı bir kez daha güvenli bir sığınak olarak görebileceği anlamına gelmektedir.

Geleceğe baktığımızda, fidye yazılımı etkinliklerinin hızının bazı önemli soruların sonucuna bağlı olacağını tahmin ediyoruz:

1. Hükümetler, fidye yazılımı suçlularının kendi sınırları içinde faaliyet göstermesini önlemek için harekete geçecekler mi yoksa aktörlerin yabancı topraklarda faaliyet göstermesini engellemek mi öncelikli amaçları olacak?
2. Fidye yazılımı grupları taktik değiştirerek fidye yazılımlarına olan ihtiyacı ortadan kaldıracak ve şantaj tipi saldırılara yönelecek mi?
3. Kurumlar, BT operasyonlarını suçluların güvenlik açıklarından yararlanabileceğinden daha hızlı bir şekilde modernize edip dönüştürebilecek mi?
4. Fidye ödemelerini izleme ve takip etme konusundaki ilerlemeler, fidye alıcılarının taktik ve müzakerelerini değiştirmeye zorlayacak mı?

Eyleme dönüştürülebilir içgörüler

1. Tüm fidye yazılımı aileleri bir ağı etkilemek için aynı güvenlik zayıflıklarından yararlandığından bütünsel güvenlik stratejilerine odaklanın.
2. Kapsamlı savunma temel koruma düzeyini yükseltmek ve güvenlik operasyonlarını modernize etmek için güvenlik temellerini güncelleştirin ve sürdürün. Buluta geçiş, tehditlerin daha hızlı tespitine ve bunlara daha hızlı müdahale etmenize olanak tanır.

Daha ayrıntılı bilgi için bağlantılar

- Kurumunuzu fidye yazılımlarından koruyun | Microsoft Güvenlik
- Güvenliğin ihlal edilmesine karşı ortamınızı sağlamlaştırmanın 7 yolu | Microsoft Güvenlik Blogu
- İnsan tarafından işletilen fidye yazılımlarını engellemek için yapay zeka tabanlı savunmaları iyileştirme | Microsoft 365 Defender Araştırma Ekibi
- Security Insider: En yeni siber güvenlik içgörülerini ve güncelleştirmelerini keşfedin | Microsoft Güvenlik

Hizmet olarak siber suç

Hizmet olarak siber suç (CaaS), dünya genelinde müşteriler için büyüyen ve gelişen bir tehdittir. Microsoft Dijital Suçlar Birimi (DCU), BEC ve insan tarafından işletilen fidye yazılımları da dahil olmak üzere, çeşitli siber suçları kolaylaştıran ve sayıları giderek artan online hizmetlerle CaaS ekosisteminin büyümeye devam ettiğini gözlemlemiştir. Siber suçlular, hesapları başarıyla çalmak ve çalınan hesaplara erişimi satmaktan önemli bir kazanç elde edebildikleri için kimlik avı tercih edilen bir saldırı yöntemi olmaya devam etmektedir.

Genişleyen CaaS pazarına bir yanıt olarak DCU, dinleme sistemlerini internet, derin web, incelenmiş forumlar,[9] özel web siteleri, online tartışma forumları ve mesajlaşma platformlarının tüm ekosisteminde CaaS tekliflerini tespit edecek ve tanımlayacak şekilde geliştirdi.

Dünyanın farklı yerlerinden ve farklı dilleri konuşan siber suçlular artık belirli sonuçlar elde etmek için işbirliği yapıyor. Örneğin, Asya'daki bir kişi tarafından yönetilen bir CaaS web sitesi, Avrupa'da faaliyetlerini sürdürüyor ve Afrika'da kötü amaçlı hesaplar oluşturuyor. Bu operasyonların birden fazla yargı bölgesini kapsayan yapısı, hukuki karmaşa ve uygulama zorlukları doğuruyor. Buna karşılık DCU, CaaS saldırılarını kolaylaştırmak için kullanılan kötü amaçlı suç altyapısını devre dışı bırakmaya ve suçluları sorumlu tutmak için dünyanın dört bir yanındaki kanun uygulayıcı kurumlarla işbirliği yapmaya odaklanmaktadır.

Siber suçlular erişimi, kapsamı ve kazancı en üst düzeye çıkarmak için analitiği giderek daha fazla kullanmaktadır. Meşru işletmeler gibi, CaaS web siteleri de itibarlarını korumak için ürün ve hizmetlerin geçerliliğini sağlamalıdır. Örneğin, CaaS web siteleri, ele geçirilmiş kimlik bilgilerinin geçerliliğini sağlamak için ele geçirilmiş hesaplara erişimi rutin olarak otomatik hâle getirir. Siber suçlular, parolalar sıfırlandığında veya güvenlik açıkları düzeltildiğinde belirli hesapların satışına son verir. Giderek daha fazla CaaS web sitesinin alıcılara bir kalite kontrol süreci olarak talep üzerine doğrulama sağladığını tespit ettik. Bu, CaaS web sitesinin aktif hesaplar ve parolalar sattığı konusunda alıcıların güven duymasını sağlarken, çalınan kimlik bilgilerinin satıştan önce düzeltilmesi durumunda CaaS satıcısının potansiyel maliyetlerini azaltmaktadır.

DCU ayrıca, alıcılara belirli coğrafi konumlara, belirlenmiş online hizmet sağlayıcılarına ve özellikle de hedeflenen kişilere, mesleklere ve sektörlere ait, ele geçirilmiş hesaplar satın alma seçeneği sunan CaaS web sitelerinin olduğunu da gözlemlemiştir. Sık sipariş edilen hesaplar, CFO'lar veya "Alacak Hesapları" gibi faturalamayı işleyen profesyonellere veya departmanlara odaklanmaktadır. Benzer şekilde, kamu sözleşmelerine katılan sektörler, genellikle kamu ihale süreci aracılığıyla sağlanan bilgilerin miktarı nedeniyle hedef alınır.

DCU'nun CaaS ile ilgili araştırmaları bazı temel eğilimleri ortaya çıkarmıştır:

Hizmetlerin sayısı ve karmaşıklığı artıyor.

Bunun bir örneği, genellikle kimlik avı saldırılarını otomatikleştirmek için kullanılan ele geçirilmiş web sunucularının oluşturduğu web kabuklarının evrimidir. DCU, CaaS satıcılarının özelleştirilmiş web dashboard'ları aracılığıyla kimlik avı kitlerinin veya malware'lerin yüklenmesini basitleştirdiğini gözlemlemiştir. CaaS satıcıları daha sonra genellikle, istenmeyen posta mesaj hizmetleri ve coğrafi konum veya meslek dahil olmak üzere tanımlı niteliklere dayalı özelleştirilmiş istenmeyen posta alıcı listeleri gibi ek hizmetleri dashboard üzerinden tehdit aktörüne satmaya çalışmaktadır. Bazı durumlarda, çoklu saldırı kampanyalarında tek bir web kabuğunun kullanıldığını gözlemledik, bu da tehdit aktörlerinin güvenliği aşılmış olan sunucuya kalıcı erişim sağlayabileceğini düşündürmektedir. CaaS ekosisteminin bir parçası olarak sunulan anonimleştirme hizmetlerinin yanı sıra sanal özel ağlar (VPN) ve sanal özel sunucu (VPS) hesapları için sunulan tekliflerde de bir artış gözlemledik. Çoğu durumda, sunulan VPN/VPS, başlangıçta çalıntı kredi kartları aracılığıyla temin edilmekteydi. CaaS web siteleri, siber suç saldırılarını düzenlemek için bir platform olarak kullanılmak üzere daha fazla sayıda uzak masaüstü protokolü (RDP), güvenli kabuk (SSH) ve cPanel'leri de sunuyordu. CaaS satıcıları, çeşitli türlerdeki siber saldırıları kolaylaştırmak için RDP, SSH ve cPanel'leri uygun araçlar ve kodlarla yapılandırmaktadır.

Homoglif etki alanı oluşturma hizmetleri, kripto para birimi olarak giderek daha fazla ödeme yapılmasını gerektiriyor.

Homoglif etki alanları, görünüşte başka bir karakterle aynı veya neredeyse aynı olan karakterleri kullanarak meşru etki alanı adlarını taklit eder. Amaç, görüntüleyen kişiyi homoglif etki alanının gerçek etki alanı olduğuna inandırmaktır. Bu etki alanları her yerde bulunan bir tehdittir ve daha büyük bir siber suça açılan geçittir. CaaS siteleri artık alıcıların kimliğine bürünmek istedikleri belirli kurum ve etki alanı adlarını talep etmesine olanak tanıyan özel homoglif etki alanı adları satmaktadır. Ödeme alındıktan sonra CaaS satıcıları, etki alanı adını seçmek için bir homoglif oluşturma aracı kullanır ve ardından kötü amaçlı homoglifi kaydeder. Bu hizmetin ödemesi neredeyse tamamen kripto para biriminde yapılır.

2.750.000

site kaydının bu yıl DCU tarafından başarıyla engellenmesi sayesinde suç aktörlerinin bunları küresel siber suçlarda kullanmasının önüne geçildi.

Hizmet olarak siber suç

Devamı

CaaS satıcıları, giderek daha fazla sayıda ele geçirilmiş kimlik bilgisini satışa sunuyor.

Ele geçirilmiş kimlik bilgileri, e-posta mesajlaşma hizmeti, kurumsal dosya paylaşımı kaynakları ve OneDrive İş gibi kullanıcı hesaplarına yetkisiz erişim sağlar. Yönetici kimlik bilgilerini ele geçirilirse yetkisiz kullanıcılar gizli dosyalara, Azure kaynaklarına ve kurumun kullanıcı hesaplarına erişim sağlayabilir. Birçok durumda, DCU araştırmaları, aynı kimlik bilgilerinin birden fazla sunucuda kimlik doğrulamasını otomatikleştirmesi için yetkisiz bir şekilde kullanıldığını tespit etti. Bu model, güvenliği ihlal edilen kullanıcının birden çok kimlik avı saldırısının kurbanı olabileceğini veya botnet tuş kaydedicilerin kimlik bilgilerini toplamasına imkan tanıyan cihaz malware'lerine sahip olabileceğini göstermektedir.

CaaS hizmetleri ve ürünleri tespit edilmelerini önleyecek özelliklerle ortaya çıkıyor.

Bir CaaS satıcısı, tespit ve önleme sistemlerini atlatmak için tasarlanmış, daha fazla karmaşıklık katmanına ve anonimleştirme özelliklerine sahip kimlik avı kitlerini günlük 6 USD gibi düşük bir ücretle sunmaktadır. Hizmet, trafiğin bir sonraki katmana veya siteye gitmesine izin vermeden önce kontroller yapan bir dizi yönlendirme sunar. Bunların biri, cihazın sanal bir makine olup olmadığı, kullanılan tarayıcı ve donanım hakkında ayrıntıların toplanması ve diğer bilgiler dahil olmak üzere, cihazın parmak izini oluşturmak için 90'dan fazla kontrol gerçekleştirir. Tüm kontroller başarılı olursa trafik, kimlik avı için kullanılan bir açılış sayfasına gönderilir.

Uçtan uca siber suç hizmetleri, yönetilen hizmetlere abonelik satıyor.

Operasyonel güvenlik zayıfsa genellikle online bir suç işlenirken gerçekleştirilen herhangi bir adım tehdit aktörlerinin açığa çıkmasına yol açabilir. Hizmetler birden fazla CaaS sitesinden satın alınırsa açığa çıkma ve tanımlanma riski artar. DCU, karanlık web'de, açığa çıkmayı azaltmak için yazılım kodunu anonimleştirmeye ve web sitesi metnini genelleştirmeye yönelik hizmetlerde endişe verici bir artış trendi olduğunu gözlemlemiştir. Uçtan uca siber suç aboneliği hizmet sağlayıcıları, tüm hizmetleri yönetir ve OCN'ye abone olurken açığa çıkma risklerini daha da azaltan sonuçları garanti etmektedir. Azalan risk, bu uçtan uca hizmetlerin popülerliğini de artırır.

Hizmet olarak kimlik avı (PhaaS), uçtan uca siber suç hizmetine bir örnektir. PhaaS, tamamen tespit edilemeyen hizmetler (FUD) olarak bilinen önceki hizmetlerin gelişmiş bir sürümüdür ve abonelik esasına göre sunulur. Genel PhaaS koşulları, kimlik avı web sitelerini bir ay boyunca aktif tutmayı içerir.

DCU ayrıca bir abonelik modeliyle dağıtılmış hizmet reddi (DDoS) sunan bir CaaS satıcısı tespit etmiştir. Bu modelde, saldırılar gerçekleştirmek için gerekli olan botnet'i oluşturma ve bakım işlerini CaaS satıcısı üstlenir. Her DDoS aboneliği müşterisi, operasyonel güvenliği geliştirmek ve bir yıl boyunca 7/24 destek için şifrelenmiş bir hizmet alır. DDoS abonelik hizmeti, farklı mimariler ve saldırı yöntemleri sunar; böylece, hizmeti satın alan kişinin saldırmak için bir kaynak seçmesi yeterli olur ve satıcı, saldırıyı gerçekleştirmek için botnet'inde güvenliği aşılmış olan bir dizi cihaza erişim sağlar. DDoS aboneliğinin maliyeti yalnızca 500 USD'dir.

PhaaS, siber suçlulara tek bir abonelikle birden çok hizmet sunar. Genel olarak, hizmeti satın alan bir kişinin yalnızca üç işlem yapması gerekir:

1. Sunulan yüzlerce hizmet arasından bir kimlik avı sitesi şablonu/tasarımı seçme.
2. Kimlik avı kurbanlarından elde edilen kimlik bilgilerini almak için bir e-posta adresi sağlama.
3. PhaaS satıcısına kripto para birimi ile ödeme yapma.

Bu adımlar tamamlandıktan sonra, PhaaS satıcısı belirli kullanıcıları hedeflemek için üç veya dört yönlendirme katmanına ve barındırma kaynaklarına sahip hizmetler oluşturur. Sonrasında kampanya başlatılır ve kurban kimlik bilgileri toplanır, doğrulanır ve alıcı tarafından sağlanan e-posta adresine gönderilir. Bonus olarak birçok PhaaS satıcısı, herhangi bir tarayıcıdan erişilebilmeleri ve yönlendirmelerin kullanıcıları dağıtılmış defter üzerindeki bir kaynağa götürebilmesi için kimlik avı sitelerini genel blok zincirinde barındırmayı teklif eder.

DCU'nun CaaS siber suçlularını tespit eden ve engelleyen araçlar ve teknikler geliştirme çalışmaları devam etmektedir. CaaS hizmetlerinin gelişimi, özellikle kripto para ödemelerinin engellenmesinde önemli zorluklar ortaya koymaktadır.

Kripto paraların suç amaçlı kullanımı

Kripto para biriminin benimsenmesi ana akım hâline geldikçe, suçlular da bunu giderek artan bir şekilde emniyet güçlerinden ve kara parayla mücadele (AML) önlemlerinden kaçmak için kullanıyor. Bu, emniyet güçlerinin siber suçlulara yapılan kripto para ödemelerini izleme ve takip etme zorluğunu arttırmaktadır.

Blok zinciri çözümlerine dünya çapında yapılan harcamalar son dört yılda yaklaşık yüzde 340 artarken, yeni kripto para cüzdanları yaklaşık yüzde 270 büyüdü. Dünya çapında 83 milyondan fazla benzersiz cüzdan mevcut ve tüm kripto para birimlerinin toplam piyasa değeri 28 Temmuz 2022 itibariyle yaklaşık 1,1 trilyon USD'dir.[10]

Kaynak: Twitter.com—@PeckShieldAlert (PeckShield, Çin merkezli bir blok zinciri güvenlik kurumudur).

Fidye yazılımı ödemelerini izleme

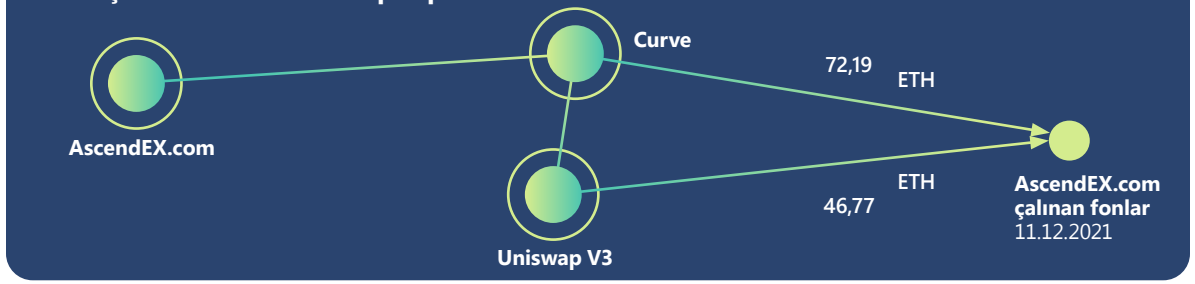
Yasa dışı yollarla elde edilen kripto para biriminin en büyük kaynaklarından biri fidye yazılımıdır. Microsoft DCU, fidye yazılımı saldırılarında kullanılan kötü amaçlı teknik altyapıyı engellemek amacıyla (örneğin, Nisan 2022'de Zloader'ın engellenmesi)[11] kripto para birimi izleme ve kurtarma yeteneklerini sunmak için suç cüzdanlarını izlemektedir.

DCU araştırmacıları, fidye yazılımı aktörlerinin paranın izini gizlemek için kurbanlarla iletişim taktiklerini değiştirdiğini gözlemlemiştir. Başlangıçta, siber suçlular fidye notlarına Bitcoin adreslerini dahil ekliyordu. Ancak bu durum, blok zincirindeki ödeme işlemlerini takip etmeyi kolaylaştırdığından fidye yazılımı aktörleri, cüzdan adreslerini dahil etmeyi bırakıp bunun yerine, kurbanlara fidye ödeme adreslerini iletmek için e-posta adresleri veya sohbet web siteleri bağlantıları eklemeye başladılar. Hatta bazı aktörler, güvenlik araştırmacılarının ve emniyet güçlerinin kurban gibi davranarak suçluların cüzdan adreslerini ele geçirmesini engellemek amacıyla her kurban için benzersiz web sayfaları ve giriş bilgileri oluşturdu. Suçluların izlerini gizleme çabalarına rağmen, bazı fidye ödemeleri, blok zincirindeki hareketi takip edebilen emniyet güçleri ve kripto analiz kurumlarıyla birlikte çalışılarak geri alınabilmektedir.

Popüler: DEX'in yasadışı gelirleri aklaması

Siber suçlular için önemli bir sorun, kripto para biriminin itibari para birimine dönüştürülmesidir. Siber suçluların, her biri farklı derecede risk taşıyan birkaç potansiyel dönüştürme yolu vardır. Riski azaltmak için kullanılan yöntemlerden biri, merkezi borsalar (CEX), eşler arası (P2P) işlemler ve tezgah üstü (OTC) borsalar gibi mevcut para çekme seçenekleri aracılığıyla nakde çevirmeden önce merkezi olmayan bir borsa (DEX) yoluyla gelirleri aklamaktır. DEX'ler, genellikle AML önlemlerine uymadıkları için ilgi çekici bir para aklama merkezidir.

Yasa dışı olarak kazanılan kripto para birimlerini izleme



Kripto para araştırma aracı Chainalysis'i kullanan Microsoft'un Dijital Suçlar Birimi, AcendEX bilgisayar korsanlarının çalıntı fonları Uniswap'e ek olarak Curve adlı daha küçük bir DEX'te takas ettiğini keşfetti. Bu şema, ekibin ortaya çıkardığı aklama yollarını göstermektedir. Her daire, bir cüzdan kümesini ve her bir satırdaki sayılar, aklama amacıyla iletilen toplam Ethereum miktarını temsil eder.

Aralık 2021'de bilgisayar korsanları, küresel kripto para ticaret platformu AscendEx'e saldırdı ve kurumun müşterilerine ait yaklaşık 77,7 milyon USD değerinde kripto parayı çaldı.[12] AscendEx, blok zinciri analiz firmalarıyla işbirliği yaptı ve çalınan kripto paraları alan cüzdanların kara listeye alınabilmesi için diğer CEX'lerle iletişime geçti. Kripto paraların gönderildiği adresler, Ethereum blok zinciri gezgini Etherscan'de de bu şekilde etiketlendi.[13] Bilgisayar korsanları, tespit edilmemek ve kara listeye alınmamak için 18 Şubat 2022'de dünyanın en büyük DEX'lerinden biri olan Uniswap'e 1,5 milyon USD'lik Ethereum gönderdi.[14]

DEX'ler tarafından daha güçlü AML önlemlerinin benimsenmesi, platformlarındaki aklama faaliyetini azaltabilir ve siber suçluları, kripto para karıştırma veya lisanssız borsalar gibi diğer maskeleme yöntemlerini kullanmaya zorlayabilir. Örneğin, Uniswap geçtiğimiz günlerde yasa dışı faaliyetlerde bulunduğu bilinen cüzdanların borsada işlem yapmasını engellemek için kara listeleri kullanmaya başlayacağını duyurdu.[15]

Eyleme dönüştürülebilir içgörüler

1. Bir suçluya kripto para kullanarak ödeme yapmış bir siber suç kurbanıysanız kayıp fonların izlenmesine ve kurtarılmasına yardımcı olabilecek yerel emniyet güçleriyle iletişime geçin.
2. Bir DEX seçerken yürürlükteki ALM önlemlerini öğrenin.

Daha ayrıntılı bilgi için bağlantılar

- Giderek daha karmaşık hâle gelen kötü niyetli kripto madencilerine karşı donanım tabanlı tehdit savunması | Microsoft 365 Defender Araştırma Ekibi

Gelişen kimlik avı tehdit ortamı

Kimlik bilgilerine yönelik kimlik avı dolandırıcılıkları yükselişte ve ayrım gözetmeksizin tüm gelen kutularını hedeflemeleri sebebiyle her yerdeki kullanıcılar için önemli bir tehdit olmaya devam ediyor. Araştırmacılarımızın tespit ettiği ve karşı koruma sağladığı tehditler arasında, kimlik avı saldırılarının hacmi diğer tüm tehditlerden katbekat fazladır.

Office için Defender verilerini kullanarak, kötü amaçlı e-posta ve ele geçirilmiş kimlik etkinliklerini görüyoruz. Azure Active Directory Kimlik Koruması, ele geçirilmiş kimlik olayı uyarıları aracılığıyla daha fazla bilgi sağlar. Defender for Cloud Apps'i kullanarak, ele geçirilmiş kimlik verilerine erişim olaylarını görürüz ve Microsoft 365 Defender (M365D), ürünler arası korelasyon sağlar. Yanal hareket ölçümü, Uç Nokta için Defender (saldırı davranışı uyarıları ve olayları) ile Office için Defender (kötü amaçlı e-posta) ve ürünler arası korelasyon için yine M365D'den gelir.

710 milyon

kimlik avı e-postası haftalık olarak engelleniyor.

1 saat 12 dk

Kimlik avı e-postası kurbanı olursanız bir saldırganın gizli verilerinize erişmesi için gereken ortalama süre.[16]

1 saat 42 dakika

Bir cihazın güvenliği aşıldığında, bir saldırganın kurumsal ağınız içinde yanal olarak hareket etmeye başlaması için geçen ortalama süre.[17]

Microsoft 365 kimlik bilgileri, saldırganlar için en çok aranan hesap türlerinden biri olmaya devam etmektedir. Oturum açma kimlik bilgileri ele geçirildiğinde, saldırganlar diğer eylemlerin yanı sıra malware ve fidye yazılımı bulaşmasını kolaylaştırmak, SharePoint dosyalarına erişerek kurumun gizli verilerini ve bilgilerini çalmak ve Outlook aracılığıyla kötü amaçlı başka e-postalar göndererek kimlik avını yaymaya devam etmek için kuruma bağlı bilgisayar sistemlerinde oturum açabilir.

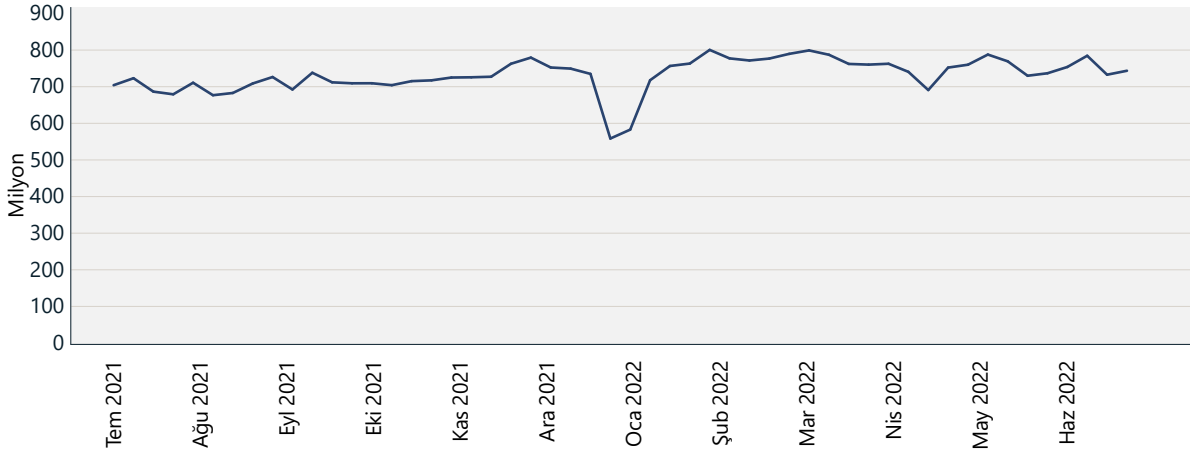
Saldırganlar, daha geniş hedefleri olan kampanyalar ile kimlik bilgileri, bağışlar ve kişisel bilgilere yönelik kimlik avına ek olarak, daha büyük ödemeler için seçtikleri kurumları hedeflemektedir. Mali kazanç için kurumlara yönelik e-posta kimlik avı saldırılarına toplu olarak BEC saldırıları denir. Microsoft, her ay gözlemlenen tüm kimlik avı e-postalarının yüzde 0,6'sına eşdeğer milyonlarca BEC e-postası tespit etmektedir. Mayıs 2022'de yayımlanan IC3[18] raporu, BEC saldırıları nedeniyle maruz kalınan zararlarda bir yukarı yönlü trend olduğunu göstermektedir.

Kimlik avı saldırılarında kullanılan tekniklerin karmaşıklığı artırmaya devam ediyor. Saldırganlar, karşı önlemlere yanıt olarak, tekniklerini uygulamak için yeni yollar benimsemekte ve saldırı operasyon altyapısını barındırma yöntemi ve yerine ilişkin karmaşıklığı artırmaktadır. Bu, kurumların kötü amaçlı e-postaları engellemek ve bireysel kullanıcı hesapları için erişim denetimini güçlendirmek için güvenlik çözümleri uygulama stratejilerini düzenli olarak yeniden değerlendirmeleri gerektiği anlamına gelir.

531.000

Office için Defender tarafından engellenen URL'lere ek olarak Dijital Suçlar Birimimiz, Microsoft dışında barındırılan 531.000 benzersiz kimlik avı URL'sinin kaldırılma sürecini yönetti.

Tespit edilen kimlik avı e-postaları



Haftalık kimlik avı tespitlerinin sayısı artmaya devam etmektedir. Aralık-Ocak aylarındaki düşüş, geçen yılki raporda da bildirilen, beklenen bir mevsimsel düşüştür. Kaynak: Exchange Online Protection sinyalleri.

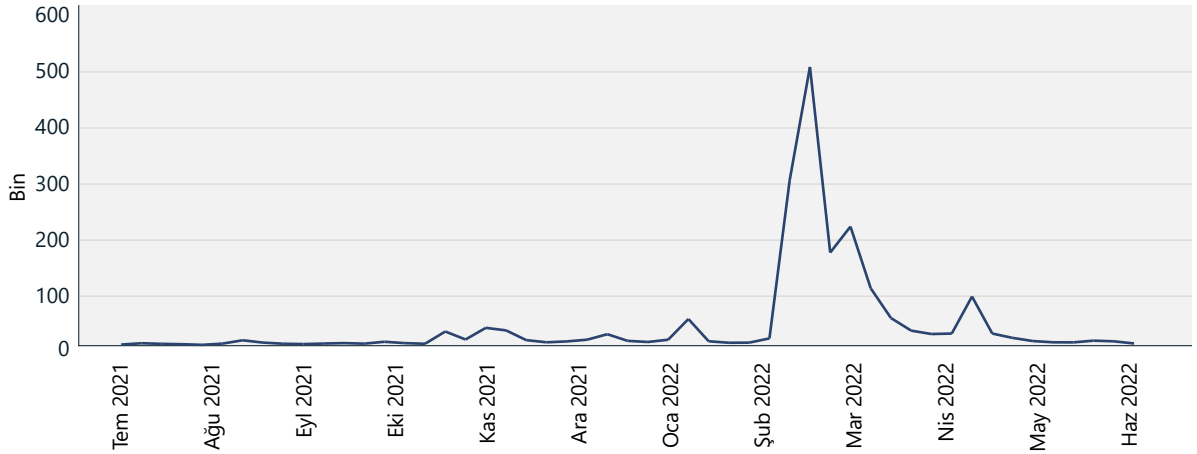
Gelişen kimlik avı tehdit ortamı

Devamı

Kimlik avı e-postalarında yıldan yıla sürekli bir artış gözlemlemeye devam ediyoruz. 2020 ve 2021 yıllarında uzaktan çalışmaya geçiş, değişen çalışma ortamından yararlanmayı amaçlayan kimlik avı saldırılarında önemli bir artışa neden oldu. Kimlik avı operatörleri, COVID-19 salgını gibi büyük dünya olaylarıyla uyumlu yemleri ve Google Drive veya OneDrive dosya paylaşımı gibi işbirliği ve üretkenlik araçlarıyla bağlantılı temaları kullanarak yeni e-posta şablonlarını hızla benimsiyor. COVID-19 temaları azalırken, Ukrayna'daki savaş Mart 2022'nin başlarından itibaren yeni bir cazibe hâline geldi. Araştırmacılarımız, Ukrayna vatandaşlarını desteklemek için Bitcoin ve Ethereum olarak kripto para bağışı talep eden meşru kurumları taklit eden e-postalarda şaşırtıcı bir artış gözlemledi.

Şubat 2022'nin sonlarında Ukrayna'da savaşın başlamasından sadece birkaç gün sonra, kurumsal müşteriler arasında karşılaşılan Ethereum adreslerini içeren kimlik avı e-postalarının sayısı önemli ölçüde arttı. Toplam karşılaşma sayısı, Mart ayının ilk haftasında yarım milyon kimlik avı e-postasının bir Ethereum cüzdan adresi içermesiyle en yüksek seviyeye ulaştı. Savaşın başlamasından önce, kimlik avı olarak tespit edilen diğer e-postalardaki Ethereum cüzdan adreslerinin sayısı, günde ortalama birkaç bin e-posta ile çok daha az sayıdaydı.

Ethereum cüzdan adresleri içeren kimlik avı e-postaları



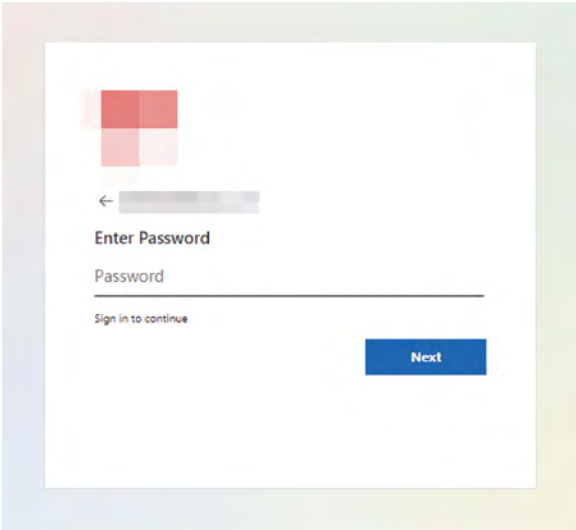
Ethereum cüzdan adresleri içeren ve kimlik avı olduğu tespit edilen toplam e-posta sayısı, Ukrayna-Rusya çatışmasının başlamasıyla artış gösterdi ve ilk artıştan sonra giderek azaldı.

Kimlik avcılarının her zamankinden daha fazla işlem yapmak için meşru altyapıyı kullanmalarıyla kendi altyapılarını satın almak, barındırmak veya işletmek zorunda kalmamaları, bir operasyonun güvenliğini çeşitli yönlerden aşmayı amaçlayan kimlik avı saldırılarında artışa neden olmaktadır. Örneğin, ele geçirilmiş gönderen hesaplarından kötü amaçlı e-postalar gelebilir. Saldırganlar, itibar puanı daha yüksek olan ve yeni oluşturulan hesaplara ve etki alanlarına göre daha güvenilir olarak görülen bu e-posta adreslerinden yararlanır. Daha ileri düzey bazı kimlik avı saldırılarında, saldırganların DMARC'nin[19] yanlış bir şekilde "eylem yok" politikasıyla ayarlandığı etki alanlarından e-posta gönderip kimlik sahtekarlığı yaparak e-posta sahtekarlığına kapı aralamayı tercih ettiğini gözlemledik.

Büyük kimlik avı operasyonları, büyük ölçekli saldırıları işlevsel hâle getirmek için bulut hizmetlerini ve bulut sanal makinelerini (VM'ler) kullanma eğilimindedir. Saldırganlar, bu gerçek hizmetlerin yüksek dağıtılabilirlik hızından ve olumlu itibarından yararlanmak için SMTP e-posta geçişlerini veya bulut e-posta altyapısını kullanarak VM'lerden e-posta dağıtma ve teslim etme sürecini tamamen otomatikleştirebilir. Bu bulut hizmetleri aracılığıyla kötü amaçlıpostaların gönderilmesine izin verilirse savunucuların, e-postaların ortamlarına girmesini engellemek için güçlü e-posta filtreleme özelliklerinden faydalanması gerekir.

Microsoft 365 oturum açma sayfasının kimliğine bürünen çok sayıda kimlik avı açılış sayfasının gösterdiği gibi, Microsoft hesapları kimlik avı operatörleri için önemli bir hedef olmaya devam etmektedir. Örneğin, kimlik avcıları, alıcıya göre özelleştirilmiş benzersiz bir URL oluşturarak kimlik avı kitlerini Microsoft oturum açma deneyimiyle eşleştirmeye çalışmaktadır. Bu URL, kimlik bilgilerini toplamak için geliştirilmiş kötü amaçlı bir web sayfasına yönlendirme yapar ancak URL'deki bir parametre belirli alıcının e-posta adresini içerir. Hedef, sayfaya gittiğinde kimlik avı kiti, kullanıcı oturum açma verilerini ve hedeflenen kurumun özel Microsoft 365 oturum açma sayfasının görünümünü yansıtan, e-posta alıcısına göre özelleştirilmiş bir kurumsal logoyu önceden yerleştirir.

Microsoft oturum açma sayfasını taklit eden, dinamik içeriğe sahip kimlik avı sayfası

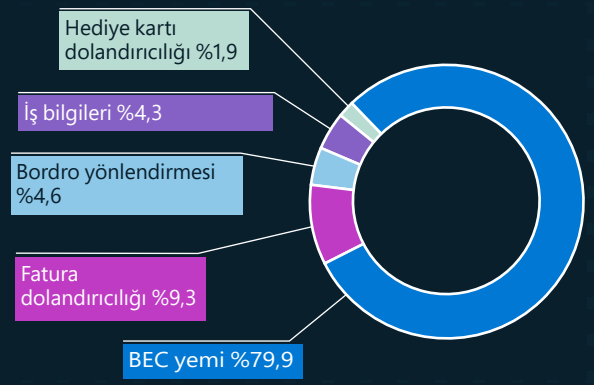


Kurumsal e-posta güvenliğinin ihlaline bakış

Siber suçlular, güvenlik ayarlarını alt etmek ve bireyleri, işletmeleri ve kurumları hedef almak için giderek daha karmaşık planlar ve teknikler geliştiriyor. Yanıt olarak BEC uygulama programımızı daha da geliştirmek için önemli kaynaklara yatırım yapıyoruz.

BEC, 2021 yılında 2,4 milyar USD tutarında olduğu tahmin edilen ayarlanmış kayıpla en maliyetli mali siber suçtur ve dünya çapında en büyük beş internet suçu zararlarının yüzde 59'undan fazlasını temsil eder.[20] Microsoft güvenlik araştırmacıları, kullanıcıları BEC'ye karşı en iyi nasıl koruyabileceklerini ve sorunun kapsamını anlamak için saldırılarda kullanılan en yaygın temaları takip eder.

BEC temaları (Ocak-Haziran 2022)



Meydana gelme yüzdesine göre BEC temaları

BEC trendleri

Bir başlangıç noktası olarak, BEC saldırganları genelde yakınlık kurmak için potansiyel kurbanlarla bir konuşma başlatmaya çalışır. Saldırgan, bir meslektaş veya iş arkadaşı gibi davranarak konuşmayı yavaş yavaş para transferine doğru yönlendirir. BEC yemi olarak takip ettiğimiz tanıtım e-postası, tespit edilen BEC e-postalarının yaklaşık yüzde 80'ini temsil etmektedir. Geçen yıl boyunca Microsoft güvenlik araştırmacıları tarafından belirlenen diğer trendler şunlardır:

- 2022'de gözlemlenen BEC saldırılarında en sık kullanılan teknikler kimlik sahtekarlığı[21] ve kimliğe bürünme[22] olmuştur.
- Kurbanlara en fazla maddi zarar veren BEC alt türü, fatura dolandırıcılığı olmuştur (BEC kampanya araştırmalarımızda görülen hacim ve talep edilen dolar tutarlarına göre).
- Borç hesapları raporları ve müşteri iletişim bilgileri gibi kurumsal bilgilerin hırsızlığı, saldırganların inandırıcı bir şekilde fatura dolandırıcılığı yapmalarına olanak sağlamıştır.
- Çoğu bordro yönlendirme isteği, ücretsiz e-posta hizmetlerinden ve nadiren ele geçirilmiş olan hesaplardan gönderilmiştir. Bu kaynaklardan gelen e-posta hacmi, en yaygın maaş ödeme tarihleri olan her ayın biri ve on beşi civarında artış göstermiştir.
- Dolandırıcılık konusunda iyi bilinen bir yol olmasına rağmen, hediye kartı dolandırıcılıkları, tespit edilen BEC saldırılarının yalnızca yüzde 1,9'unu oluşturmaktaydı.

Eyleme dönüştürülebilir içgörüler

Kimlik avına karşı savunma

Kurumunuzun kimlik avına maruz kalma oranını azaltmak için BT yöneticileri aşağıdaki kuralları ve özellikleri uygulamaya teşvik edilir:

1. Yetkisiz erişimi sınırlamak için tüm hesaplarda MFA'nın kullanılmasını zorunlu kılma.
2. Normalde kurumunuzda trafik oluşturmayan ülkelerden, bölgelerden ve IP'lerden erişimi engellemek için yüksek düzeyde ayrıcalıklı hesaplar için koşullu erişim özelliklerini etkinleştirme.
3. Yöneticiler, ödeme veya satın alma faaliyetlerinde bulunan çalışanlar ve diğer ayrıcalıklı hesaplar için fiziksel güvenlik anahtarları kullanma seçeneğini değerlendirme.
4. URL'leri şüpheli davranışlara karşı analiz etmek için Microsoft SmartScreen gibi hizmetleri destekleyen ve bilinen kötü amaçlı web sitelerine erişimi engelleyen tarayıcıların kullanımını zorunlu kılma.[23]
5. Office 365 için Microsoft Defender gibi, yüksek olasılıklı kimlik avını karantinaya alan ve e-posta gelen kutusuna ulaşmadan önce bir sanal alanda URL'leri ve ekleri engelleyen, makine öğrenimi tabanlı bir güvenlik çözümü kullanma.[24]
6. Kurumunuz genelinde kimliğe bürünme ve kimlik sahtekarlığına karşı koruma özelliklerini etkinleştirme.
7. Saygın gönderenleri yanıltabilecek kimliği doğrulanmamış e-postaların teslim edilmesini önlemek için Etki Alanı Anahtarlarıyla Tanımlanmış E-Posta (DKIM) ve Etki Alanı Tabanlı İleti Kimlik Doğrulaması Raporlama ve Uyumluluk (DMARC) eylem kurallarını yapılandırma.
8. Kiracı ve kullanıcı tarafından oluşturulan izin kurallarını denetleme ve geniş etki alanı ve IP tabanlı özel durumları kaldırma. Bu kurallar genellikle öncelik sahibidir ve e-posta filtreleme yoluyla, bilinen kötü amaçlı e-postalara izin verebilir.
9. Kurumunuzdaki potansiyel riski ölçmek ve kolayca kandırılabilecek kullanıcıları belirleyip eğitmek için düzenli olarak kimlik avı simülatörleri çalıştırma.

Daha ayrıntılı bilgi için bağlantılar

- Çerez hırsızlığından BEC'ye: Saldırganlar, daha fazla finansal dolandırıcılık için başlangıç noktası olarak AiTM kimlik avı sitelerini kullanıyor | Microsoft 365 Defender Araştırma Ekibi, Microsoft Tehdit Bilgileri Merkezi (MSTIC)

Homoglif aldatmacası

BEC ve kimlik avı, yaygın sosyal mühendislik taktikleridir. Sosyal mühendislik, bir hedefi güven kazanarak suçluyla etkileşime girmeye ikna etmesi açısından suçun gerçekleştirilmesinde önemli bir rol oynar.

Fiziksel ticarette ticari markalar, bir ürün veya hizmetin kaynağına olan güveni sağlamak için kullanılır ve sahte ürünler, ticari markanın kötüye kullanılmasıdır. Benzer şekilde siber suçlular, potansiyel kurbanları aldatmak için homoglifleri kullanarak bir kimlik avı saldırısı sırasında hedefe tanıdık bir kişi gibi yaklaşır.

Bir homoglif, BEC'de e-posta iletişimi için kullanılan, hedefi aldatmak için bir karakterin tam olarak veya neredeyse aynısı gibi görünen bir karakterle değiştirildiği bir etki alanı adıdır.

BEC girişimlerinde kullanılan homoglif teknikleri

BEC genellikle iki aşamadan oluşur. Bunlardan ilki kimlik bilgilerinin ele geçirilmesini içerir. Bu tür kimlik bilgisi sızıntıları, kimlik avı saldırılarının veya büyük veri ihlallerinin bir sonucu olabilir. Kimlik bilgileri daha sonra karanlık web'de satılır veya değiş tokuş edilir.

İkinci aşama olan dolandırıcılık aşamasında, saldırganlar karmaşık bir sosyal mühendislikle harekete geçmek için ele geçirilmiş kimlik bilgilerini ve homoglif e-posta etki alanlarını kullanır.

Bir BEC saldırısının ilerleyişi

Teknik	Homoglif tekniğinin görüldüğü etki alanlarının yüzdesi
I harfini I ile değiştirme	%25
i harfini l ile değiştirme	%12
g harfini q ile değiştirme	%7
m harfini rn ile değiştirme	%6
.com uzantısını .cam ile değiştirme	%6
o harfini 0 ile değiştirme	%5
l harfini ll ile değiştirme	%3
i harfini ii ile değiştirme	%2
w harfini vv ile değiştirme	%2
ll karakterlerini l ile değiştirme	%2
a harfini e ile değiştirme	%2
m harfini nn ile değiştirme	%1
I harfini ll ve i harfini I ile değiştirme	%1
u harfini o ile değiştirme	%1

Ocak-Temmuz 2022 arasında 1.700'den fazla homoglif etki alanının analizi. 170 homoglif tekniği kullanılırken etki alanlarının %75'inde yalnızca 14 teknik kullanılmıştır.

Homoglif iş başında

Kurbanın bildiği bir posta etki alanıyla aynı görünen bir homoglif etki alanı, aynı kullanıcı adıyla bir posta sağlayıcısına kayıtlıdır. Ardından, ele geçirilen etki alanından, yeni ödeme talimatlarının yer aldığı bir e-posta gönderilir.

Açık kaynak bilgilerinden ve e-posta dizilerine erişimden yararlanan suçlu, faturalama ve ödemelerden sorumlu kişileri tespit eder. Daha sonra faturaları gönderen kişinin bireysel e-posta adresinin kimliğine bürünürler. Bu kimliğe bürünme, gerçek gönderenin homoglifi olan aynı kullanıcı adı ve posta etki alanından oluşur.

Saldırgan, yasal bir fatura içeren e-posta zincirini kopyalar ve ardından faturayı kendi banka bilgilerini içerecek şekilde değiştirir. Bu yeni, değiştirilmiş fatura daha sonra homoglif kimliğe bürünme e-postasından hedefe yeniden gönderilir. Bağlam anlamlı olduğu ve e-posta orijinal göründüğü için hedef genellikle sahte talimatları uygular.

Eyleme dönüştürülebilir içgörüler

1. Güvenli Bağlantılar ve SmartScreen gibi, URL'lerin şüpheli davranışlarını analiz etmeye yönelik hizmetleri destekleyen ve bilinen kötü amaçlı web sitelerine erişimi engelleyen tarayıcıların kullanımını zorunlu kılma.[25]
2. Yüksek olasılıklı kimlik avını karantinaya alan ve URL'ler ile ekleri, e-posta gelen kutusuna ulaşmadan önce bir korumalı alanda engelleyen, makine öğrenimi tabanlı bir güvenlik çözümü kullanma.

Daha ayrıntılı bilgi için bağlantılar

- İnternet Suçları Şikayet Merkezi (IC3) | Kurumsal E-posta Güvenliğinin Bozulması: 43 Milyar USD'lik Dolandırıcılık
- Kimlik sahtekarlığı bilgisi içgörüsü—Office 365 | Microsoft Docs
- Kimliğe bürünme içgörüsü—Office 365 | Microsoft Docs

Microsoft'un yaptığı işbirliğinin ilk günlerindeki botnet engelleme zaman çizelgesi

On yıldan uzun bir süredir DCU'nun siber suçları proaktif olarak durdurma çalışmaları 26 malware ve ulus devlet engellemesiyle sonuçlanmıştır. DCU ekibi bu yasa dışı operasyonları durdurmak için daha gelişmiş taktikler ve araçlar kullanırken, siber suçluların da bir adım önde kalmak için yaklaşımlar geliştirdiğini görüyoruz. DCU tarafından engellenen botnet'lerin bir örneğini ve Microsoft'un bunları kapatmak için benimsediği stratejileri gösteren bir zaman çizelgesini burada bulabilirsiniz.

2008

Conficker botnet'i

Açıklama: Windows işletim sistemini hedef alan ve ortak bir ağdaki milyonlarca bilgisayarı ve cihazı etkileyen, hızla yayılan bir solucan, dünya çapında ağ kesintilerine neden oldu.

İşbirliği: Bu alandaki ilk konsorsiyum olan Conficker Çalışma Grubu oluşturuldu. Microsoft, botu yenmek için dünya genelinde 16 kurumla ortaklık kurdu.

Microsoft'un yaklaşımı: Grup, birçok uluslararası yargı alanında işbirliği yaptı ve Conficker'ı devirmeyi başardı.

2009

Waledac botnet'i

Açıklama: E-posta adreslerini toplayan ve dünya çapında 90.000'e yakın bilgisayara bulaşarak istenmeyen posta dağıtan, ABD etki alanlarına sahip karmaşık bir istenmeyen posta botnet'i.[26]

İşbirliği: Akademisyenlerle yakın işbirliğine odaklanan başka bir konsorsiyum olan Microsoft Malware'den Koruma Merkezi'nin (MMPC) oluşturulması.[27]

Microsoft'un yaklaşımı: Microsoft, C2'yi kademeli olarak engelleme yaklaşımını kullandı ve ABD merkezli etki alanlarını bildirimde bulunmaksızın ele geçirerek kötü aktörleri şaşırttı.[28] Microsoft, Waledac'ın sunucuları tarafından kullanılan yaklaşık 280 etki alanının geçici sahipliğini aldı.

2011

Microsoft Dijital Suçlar Birimi kuruldu

İşbirliği: Araştırmacılar, avukatlar ve mühendislerden oluşan bir ekip ile sıkı bir entegrasyon içinde Microsoft ekosistemini etkileyen siber suçları engellemek için tasarlandı.

Microsoft'un yaklaşımı: Amaç, çeşitli malware'lerin teknik yönlerini daha iyi anlamak ve etkili bir engelleme stratejisi geliştirmek için bu içgörüleri Microsoft'un hukuk ekibine sağlamaktır.

2013

Rustock botnet'i

Açıklama: İnternet sağlayıcılarını birincil C2'ler olarak kullanan, tıbbi ilaçlar satmak için tasarlanmış bir arka kapı Truva atı istenmeyen posta botudur.

İşbirliği: Microsoft, Rustock tarafından satılan tıbbi ilaçları anlamak için Pfizer Pharmaceuticals ile bir ortaklık kurdu ve Hollandalı emniyet gücü yetkilileriyle yakın bir şekilde çalıştı.[29]

Microsoft'un yaklaşımı: Microsoft, ilgili ülkedeki C2 sunucularını kapatmak için ABD polis şefleri ve Hollanda'daki emniyet güçleriyle birlikte çalıştı. İleriye dönük olarak tüm etki alanı oluşturma algoritmalarını (DGA'lar) kaydetti ve engelledi.

Sirefef / Zero Access botnet'i

Açıklama: Kullanıcıları, malware yükleyecek veya kişisel bilgileri çalacak tehlikeli web sitelerine yönlendirmek için tasarlanmış bir reklamcılık botnet'i iki milyondan fazla bilgisayara bulaştı ve başta ABD ve Batı Avrupa olmak üzere reklamverenlere ayda 2,7 milyon USD'den fazlaya mal oldu.

İşbirliği: Eşler arası altyapıyı çökertmek için FBI ve Europol Siber Suç Merkezi ile yakın bir işbirliği içinde çalışıldı.

Microsoft'un yaklaşımı: Sıfır Erişim ağına katıldı, suçlu C2 sunucularını değiştirdi ve indirme sunucusu etki alanlarını başarıyla ele geçirdi.

2019

Trickbot botnet'i

Açıklama: Finansal hizmetler sektörünü hedef alan, dünya geneline yayılmış parçalı bir altyapıya sahip gelişmiş bir botnet, IoT cihazlarını ele geçirdi.

İşbirliği: Microsoft, Trickbot'u devirmek için Finansal Hizmetler Bilgi Paylaşımı ve Analiz Merkezi (FS-ISAC) ile ortaklık kurdu.[30]

Microsoft'un yaklaşımı: DCU, bot altyapısını tanımlamak ve izlemek için bir sistem oluşturdu ve çeşitli ülkelerdeki belirli yasaları dikkate alarak aktif internet sağlayıcıları için bildirimler oluşturdu.

Engellemeye odaklanılmaya devam edildi

Açıklama: Microsoft, geçen yıl yedi tehdit aktörünün altyapısını bozarak bunların ek malware dağıtmalarını, kurbanlarının bilgisayarlarını kontrol etmelerini ve ek kurbanları hedeflemelerini engelledi.

İşbirliği: İnternet servis sağlayıcıları, hükümetler, emniyet güçleri ve özel sektörle ortaklaşa olarak Microsoft, dünya çapında 17 milyondan fazla malware kurbanına çözüm bulmak için bilgiler paylaştı.

2022

Geleceğe bakış

DCU yeniliklerine devam ediyor ve malware'in ötesine geçen koordineli operasyonlar yürütmek için botnet engellemelerinde elde ettiği deneyimini kullanmayı amaçlıyor. Başarımızın devam etmesi yaratıcı mühendislik, bilgi paylaşımı, yenilikçi yasal teoriler ve kamu ile özel sektör ortaklıklarını gerektirir.

Altyapının siber suç amaçlı kötüye kullanımı

Suç komuta ve kontrol altyapısı olarak internet ağ geçitleri

IoT cihazları, geniş çaplı botnet'leri kullanan siber suçlular için giderek daha popüler bir hedef hâline gelmektedir. Yönlendiricilere patch uygulanmadığında ve bunlar doğrudan internete açık bırakıldığında, tehdit aktörleri ağlara erişim elde etmek, kötü amaçlı saldırılar gerçekleştirmek, hatta operasyonlarını desteklemek için bunları kötüye kullanabilir.

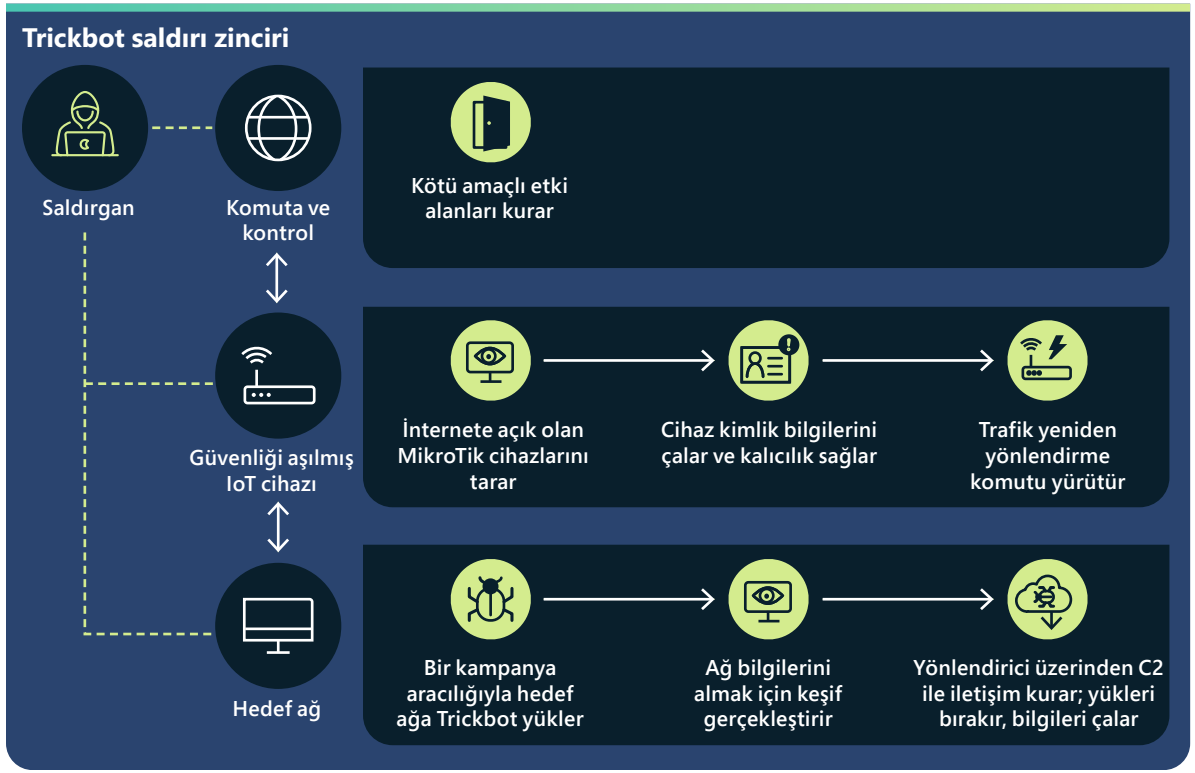
IoT için Microsoft Defender ekibi, eski endüstriyel kontrol sistemi denetleyicilerinden son teknoloji IoT sensörlerine kadar çeşitli ekipmanlar üzerinde araştırmalar yürütmektedir. Ekip, güvenlik ihlali göstergelerinin paylaşılan listesine katkıda bulunmak için IoT ve OT'ye özgü malware'leri araştırmaktadır.

Yönlendiriciler, internete bağlı evlerde ve kurumlarda her yerde bulundukları için özellikle savunmasız saldırı vektörleridir. Konut ve ticari olarak dünya genelinde popüler bir yönlendirici olan MikroTik yönlendiricilerinin etkinliklerini izleyerek, komuta ve kontrol (C2), etki alanı adı sistemi (DNS) saldırıları ve kripto madenciliği amacıyla ele geçirme için nasıl kullanıldığını tespit ediyoruz.

Daha spesifik olarak, Trickbot operatörlerinin güvenliği aşılmış MikroTik yönlendiricilerini nasıl kullandıklarını ve bunları C2 altyapılarının bir parçası olarak hareket edecek şekilde nasıl yeniden yapılandırdıklarını belirledik. Bu cihazların popülerliği, Trickbot tarafından kötüye kullanılmalarının ciddiyetini artırır ve benzersiz donanım ve yazılımları, tehdit aktörlerinin geleneksel güvenlik önlemlerinden kaçmasına, altyapılarını genişletmesine ve daha fazla cihaz ve ağın güvenliğini aşmasına olanak tanır.

İnternete açık yönlendiricilerin potansiyel olarak güvenlik açıklarından yararlanılabilir.

Güvenli kabuk (SSH) komutları içeren trafiği izleyip analiz ederek, saldırganların MikroTik yönlendiricilerini, cihazların meşru kimlik bilgilerini aldıktan sonra Trickbot altyapısıyla iletişim kurmak için kullandığını gözlemledik. Bu kimlik bilgileri deneme yanılma saldırıları üzerinden, halihazırda yamaların bulunduğu, bilinen güvenlik açıklarından yararlanılarak ve varsayılan parolalar kullanılarak elde edilebilir.



MikroTik IoT cihazlarının C2 için proxy sunucuları olarak kullanımını gösteren Trickbot saldırı zinciri.

Bir cihaza erişildiğinde saldırgan benzersiz bir komut göndererek, trafiği yönlendiricideki iki bağlantı noktası arasında yeniden yönlendirir ve Trickbot'tan etkilenen cihazlar ile C2 arasındaki iletişim hattını oluşturur.

Trickbot'un ötesinde MikroTik cihazlarına yönelik çeşitli saldırı yöntemleri hakkındaki bilgilerimizi ve ayrıca bilinen yaygın güvenlik açıkları ve risklerini (CVE'ler) MikroTik cihazları için hazırladığımız, bu cihazlara yapılan saldırılarla ilgili adli yapıları çıkarabilen açık kaynaklı bir araçta topladık.[31]

Malware C2'si için ters proxy görevi gören cihazlar, yalnızca Trickbot ve MikroTik yönlendiricilerine özgü değildir. Microsoft RiskIQ ekibiyle işbirliği içinde, ilgili C2'nin izini sürdük ve SSL sertifikalarını gözlemleyerek etkilenen Ubiquiti ve LigoWave cihazlarını da belirledik.[32] Bu, IoT cihazlarının ülke çapında koordine edilen saldırıların aktif bileşenleri hâline geldiğinin ve yaygın botnet'leri kullanan siber suçlular için popüler birer hedefe dönüştüklerinin güçlü bir göstergesidir.

IoT cihazlarını kötüye kullanan kripto suçl ular

Bilinen güvenlik açıklarının sayısı yıldan yıla istikrarlı bir şekilde arttığından, ağ geçidi cihazları, tehdit aktörleri için giderek daha değerli bir hedef hâline gelmiştir. Bunlar, kripto madenciliği ve diğer kötü amaçlı etkinlikler için kullanılmaktadır.

Kripto para birimi popüler hâle geldikçe, birçok kişi ve kurum, yönlendiriciler gibi cihazlar ile blok zincirinde kripto para madenciliği yapmak için işlem gücü ve ağ kaynaklarına yatırım yaptı. Ancak kripto para madenciliği, başarı olasılığı düşük olan, zaman ve kaynak isteyen bir süreçtir. Madencilik ile kripto para kazanma olasılığını artırmak için madenciler dağıtılmış, işbirliğine dayalı ağlarda bir araya gelirler ve başarılı bir şekilde çıkardıkları kripto paradan bağlı kaynaklarının karma yüzdesine göre pay alırlar.

Geçen yıl Microsoft, kripto para madenciliği çalışmalarını yeniden yönlendirmek için yönlendiricileri kötüye kullanan saldırıların sayısında bir artış gözlemlemiştir. Siber suçlular, madencilik havuzlarına bağlı yönlendiricilerin güvenliğini ihlal etmekte ve madencilik trafiğini, hedeflenen cihazların DNS ayarlarını değiştiren DNS zehirlenmesi saldırılarıyla ilişkili IP adreslerine yönlendirmektedir. Etkilenen yönlendiriciler, belirli bir etki alanı adına yanlış IP adresini kaydederek madencilik kaynaklarını veya karma değerlerini tehdit aktörleri tarafından kullanılan havuzlara gönderir. Bu havuzlar, suç faaliyetleriyle ilişkili anonim kripto paralar çıkarabilir veya madencilerin çıkardıkları kripto paranın bir yüzdesini elde etmek için ürettikleri meşru karmaları kullanarak ödülleri toplayabilir.

2021'de tespit edilen güvenlik açıklarının yarısından fazlası için bir yama bulunmadığından, kurumsal ve özel ağlardaki yönlendiricilerin güncelleştirilmesi ve güvenliğinin sağlanması, cihaz sahipleri ve yöneticileri için önemli bir zorluk olmaya devam etmektedir.

Yasadışı kripto madenciliği için cihazların güvenliğini ihlal etme.

Özgün havuzdaki karmaların bir kısmı tehdit aktörleri tarafından çalınır veya kaynaklar, tehdit aktörlerinin kendi havuzlarına aktarılır ya da yönlendiricilere madencilik için kaynak çalan malware kurulur.

Ağ geçidi cihazlarının DNS zehirlenmesi yaşaması, meşru madencilik faaliyetlerinin güvenliğini ihlal eder ve kaynakları, suçla ilgili madencilik faaliyetlerine yönlendirir.

Suç altyapısı olarak sanal makineler

Siber suçlular, buluta geniş çaplı geçişle birlikte, durumun farkında olmayan kurbanlardan kimlik avı veya kimlik bilgilerini çalan malware'lerin dağıtılması yoluyla elde ettikleri özel varlıklardan da yararlanmaktadır. Birçok siber suçlu, kötü niyetli altyapılarını bulut tabanlı sanal makineler (VM'ler), kapsayıcılar ve mikro hizmetler üzerine kurmayı seçmektedir.

Siber suçlu erişim iznini elde ettiğinde, altyapıyı kurmak için komut dosyası oluşturma ve otomatikleştirilmiş işlemler yoluyla sanal makineler oluşturma gibi bir dizi olay meydana gelebilir. Kod ile yazılan bu otomatikleştirilmiş işlemler, büyük ölçekli istenmeyen posta saldırıları, kimlik avı saldırıları dahil olmak üzere kötü niyetli etkinlikleri ve kötü içerikler barındıran web sayfaları başlatmak için kullanılır. Bu, kripto para birimi madenciliği faaliyetlerinin yürütüldüğü ve kurbana ay sonunda yüz binlerce dolarlık bir faturaya neden olabilen büyük ölçekli bir sanal ortam kurmayı da içerebilir.

Siber suçlular, kötü amaçlı etkinliklerinin tespit edilip kapatılmasından önce sınırlı bir yaşam süresi olduğunu bilir. Bunun sonucunda, ölçeklerini büyütmüşler ve artık olasılıkları göz önünde bulundurarak proaktif bir şekilde çalışmaktadırlar. Ele geçirilmiş hesapları önceden hazırladıkları ve ortamlarını izledikleri gözlemlenmiştir. Bir hesap (yüz binlerce sanal makine kullanılarak kurulmuş) algılanır algılanmaz, komut dosyaları tarafından hemen etkinleştirilmek üzere hazırlanmış olan bir sonraki hesaba geçerler ve kötü amaçlı etkinlikleri çok kısa bir kesintiyle veya hiç kesinti olmadan devam eder.

Bulut altyapısı gibi kurum içindeki altyapı da kurum içindeki kullanıcıların farkında olmadığı sanal yerel ortamlarla yapılan saldırılarda kullanılabilir. Bu, ilk erişim noktasının açık ve erişilebilir kalmasını gerektirir. Kurum içindeki özel varlıklar da siber suçlular tarafından, şüpheli altyapı oluşturma sürecinin tespit edilmesini önlemek için başlangıç noktalarını gizlemek üzere kurulmuş ve ileriye dönük bir bulut altyapısı zinciri başlatmak için suistimal edilmiştir.

Eyleme dönüştürülebilir içgörüler

1. İyi bir siber hijyen uygulayın ve sosyal mühendislikten kaçınmak için çalışanlara rehberlik ederek siber güvenlik eğitimi verin.
2. Bu tür saldırıları azaltmaya yardımcı olmak için geniş ölçekte tespit aracılığıyla, düzenli olarak otomatikleştirilmiş kullanıcı etkinliği anormallik kontrolleri gerçekleştirin.
3. Kurumsal ve özel ağlardaki yönlendiricileri güncelleştirin ve güvenli hâle getirin.

Hacktivizm kalıcı olacak mı?

Hacktivizm yeni bir olgu olmasa da, Ukrayna'daki savaş, gönüllü bilgisayar korsanlarında bir artışa neden oldu; bunlardan bazıları hükümetler tarafından siyasi muhaliflerin, kurumların, hatta ulus devletlerin itibarına veya varlıklarına zarar vermek için siber araçlar kullanmak üzere yönlendirildi.

Şubat 2022'de Ukrayna hükümeti, dünyanın dört bir yanındaki sivil vatandaşları, 300.000 kişilik güçlü "BT Ordusu"nun bir parçası olarak Rusya'ya siber saldırılar düzenlemeye çağırdı.[33] Aynı zamanda Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans ve RaidForum2 gibi köklü bilgisayar korsanlığı grupları Ukrayna'yı desteklemek için saldırılar düzenlemeye başladı. Conti fidye yazılımı çetesinin bir kısmı da dahil olmak üzere diğer gruplar ise Rusya'nın yanında yer aldı.[34]

Takip eden aylarda Anonymous'un faaliyetleri oldukça görünür hâle geldi. Grubun kendisi veya bağlı örgütlerinden biri adına hareket eden bilgisayar korsanları, binlerce Rus ve Belarus web sitesini geçici olarak devre dışı bıraktı, yüzlerce gigabayt çalıntı veriyi sızdırdı, Ukrayna yanlısı içerikler yayınlamak için Rus TV kanallarını ele geçirdi, hatta teslim olacak Rus tankları için Bitcoin ödemeyi teklif etti.

Vatandaş bilgisayar korsanlarının yükselişi

Sosyal medya platformları, DDoS saldırıları gibi kolayca yürütülebilir saldırılar gerçekleştirmeleri için talimatlar alan binlerce sözde vatandaş bilgisayar korsanının hızlı bir şekilde örgütlenebilmesini ve harekete geçebilmesini sağlamıştır. Bu faaliyetleri organize eden kişiler, bilgisayar korsanlarını toplamak, operasyonları organize etmek ve bilgisayar korsanlığı talimat kılavuzlarını yaymak için Twitter, Telegram ve özel forumlardan yararlanmaktadır.

Ancak, bu bilgisayar korsanlarının çoğu, talimatlar sağlanmış olsa bile sınırlı becerilere sahiptir. Bu, iki olası geleceği işaret etmektedir: temel teknik becerilere sahip yüzlerce veya binlerce kişinin, hedeflere karşı gelecekte koordineli veya bireysel hacktivist saldırıları gerçekleştirmek üzere saldırı şablonları kullandığı bir gelecek veya Ukrayna'daki düşmanlıkların nihai olarak sona ermesiyle en azından bir sonraki siyasi veya sosyal sorun onları harekete geçirmeye teşvik edene kadar hacktivizm'i geride bıraktıkları ikinci bir gelecek.

Bilgisayar korsanlarının siyasallaşması

Bu siyasi seferberliğin ortaya çıkardığı daha büyük bir risk ise kendi ulusal önceliklerini desteklemek için kendi başlarına başlattıkları girişimler veya devletlerinin emriyle, yabancı devletlerdeki hedeflerine karşı siber saldırılar düzenlemeye devam edebilecek teknolojiden anlayan bilgisayar korsanlarının yayılmasıdır.

İran, Çin ve Rusya, halihazırda hacktivizm'i devlet bilgisayar korsanlığı gruplarına üye almak için bir ateşleyici olarak kullanıyor. Örneğin, Nisan 2022'de Rus yanlısı bilgisayar korsanlığı grubu Killnet, Çekya savaşa doğrudan dahil olmamasına rağmen Çek demiryollarına, bölgesel havaalanlarına ve Çekya'nın kamu hizmeti sunucusuna karşı DDoS saldırıları başlattı.[35] Aynı zamanda bazı hükümetler, İran'ın İsrail'e karşı faaliyetlerinde olduğu gibi, bilgisayar korsanlığını geleneksel siber casusluk veya sabotaj operasyonları için bir kılıf olarak kullanabilir.

DDoS saldırılarının hacktivizm ile bağlantılı şekilde arttığı bir ortamda teknoloji sektörü, bir web sitesine giden normal ve anormal trafik akışı arasındaki farkı hızlı bir şekilde deşifre etmeye zorlanmaktadır. Microsoft ve iş ortakları, kötü amaçlı DDoS trafiğini ayırt eden ve kaynağına kadar izleyen bir araç koleksiyonu geliştirdi. Buna ek olarak, Microsoft'un Azure platformu, platformda olağanüstü yüksek düzeyde giden trafik üreten makineleri tespit edip bunları kapatabilmektedir.

Protesto yazılımlarının ortaya çıkışı

Protesto yazılımları, Rusya ve Ukrayna arasındaki savaşa verilen duygusal tepkilerin doğrudan bir sonucu olarak ortaya çıktı. Bazı açık kaynaklı yazılım geliştiricileri, yazılımlarının popülaritesini, gelişmekte olan bir jeopolitik duruma karşı sesini yükseltmek veya harekete geçmek için bir araç olarak kullandılar. Bunlar, barış mesajlarını yaymak için bir masaüstünde veya bir tarayıcıda açılan zararsız metin dosyalarını içerdiği gibi, IP adresinin coğrafi konuma göre hedeflenmiş saldırıları ve bir sabit diski silmek gibi yıkıcı eylemleri de içeriyordu. Başka küresel olaylar meydana geldikçe, protesto yazılımlarının gelecekte tekrar ortaya çıkmasını bekleyebiliriz. Bunlar genellikle saygın açık kaynak sağlayıcılarının kendi açık kaynak bileşenlerini kullanarak kişisel beyanlarda bulunmaya karar verdiği durumlar olduğundan, şu anda kaynak dosya paketlerinde bu tür değişikliklerin oluşmasını durduracak herhangi bir koruma bulunmamaktadır ve kullanıcılar olası etkilerin farkında olmalıdır.

> Sosyal medya platformları, DDoS saldırıları gibi kolayca yürütülebilir saldırılar gerçekleştirmeleri için talimatlar alan binlerce sözde vatandaş bilgisayar korsanının örgütlenebilmesini ve harekete geçebilmesini sağlamıştır.

Eyleme dönüştürülebilir içgörüler

1. Teknoloji sektörü, bu yeni tehdide kapsamlı bir yanıt oluşturmak için bir araya gelmelidir.
2. Microsoft da dahil olmak üzere önde gelen teknoloji kurumları, DDoS saldırılarıyla ilişkili kötü amaçlı trafiği belirlemeye ve sorumlu makineleri devre dışı bırakmaya yönelik araçlara sahiptir.
3. Açık kaynak kullanıcıları, jeopolitik sorunların olduğu dönemlerde daha dikkatli olmalıdır.

Son Notlar

1. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2. https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to- ransomware-attack/
3. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4. https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6. Uç nokta algılama ve yanıtlama. https://www.microsoft.com/en-us/security/business/threat-protection/
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. https://www.bbc.com/news/technology-59998925
9. Vetted Forum, mevcut bir üyenin yeni bir üyenin eklenmesi için kefil olunmasını gerektiren bir online tartışma forumudur.
10. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11. https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12. https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/ ; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13. https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14. https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15. https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16. Veri kaynağı: Office için Defender (kötü amaçlı e-posta/ele geçirilmiş kimlik etkinliği), Azure Active Directory Kimlik Koruması (ele geçirilmiş kimlik etkinlikleri/uyarıları), Defender for Cloud Apps (ele geçirilmiş kimlik verilerine erişim etkinlikleri) ve M365D (ürünler arası korelasyon).
17. Veri kaynağı: Uç Nokta için Defender (saldırı davranışı uyarıları/etkinlikleri), Office için Defender (kötü amaçlı e-posta) ve M365D (ürünler arası korelasyon).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Etki Alanı Tabanlı İleti Kimlik Doğrulaması, Raporlama ve Uygunluk: E-posta etki alanı sahiplerine, etki alanlarını yetkisiz kullanıma karşı koruma yeteneği sağlamak için tasarlanmış bir e-posta kimlik doğrulaması, kural ve raporlama protokolü.
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27 vd., No. 1:10CV156, (E.D.Va. 22 Şubat 2010).
27. Bkz. Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27 Eylül 2011.
28. Özellikle, Federal Hukuk Muhakemeleri Usul Kurallarının 65. maddesi, bir tarafın şu durumlarda bu tür bir çözüm aramasına olanak tanımaktadır: 1) yardımın sağlanmaması durumunda taraf ani ve onarılamaz bir zarara uğrayacaksa ve 2) taraf, diğer tarafa zamanında bildirimde bulunmaya çalışıyorsa. Ayrıca yasa, davalının ihbar hakkını kamuya verdiği zararın miktarına karşı dengeleyen bir dengeleme testinin uygulanmasını gerektirmektedir.
29. Microsoft Corporation v. John Does 1-11 vd., No. 2:11cv222, (W.D. Wa. 9 Şubat 2011).
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12 Ağustos 2021).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Güvenliği Aşılmış ve Malware C2 Ters Proxy'si Olarak Kullanılan Ubiquiti Cihazları | RiskIQ Topluluk Sürümü
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

Ulus Devlet Tehditleri

Ulus devlet aktörleri, tespit edilmemek ve kendi stratejik önceliklerini ileriye taşımak için, giderek daha karmaşık hâle gelen siber saldırılar başlatmaktadır.

Ulus Devlet

Tehditlerine genel bakış

Ulus devlet aktörleri, tespit edilmemek ve kendi stratejik önceliklerini ileriye taşımak için, giderek daha karmaşık hâle gelen siber saldırılar başlatmaktadır. Ukrayna'daki hibrit savaşta siber silah kullanımının ortaya çıkışı, yeni bir çatışma çağının başlangıcıdır.

Rusya ayrıca kendi ülkesi, Ukrayna ve dünya genelindeki bakış açısını etkilemek üzere propagandayı kullanarak bilgi etkileme operasyonlarıyla savaşını destekledi. Bu ilk tam ölçekli hibrit çatışma, başka önemli dersler de verdi. İlk olarak, dijital operasyonların ve verilerin güvenliğinin hem siber alanda hem de fiziksel alanda bunların buluta taşınmasıyla en iyi şekilde korunabildiği ortaya çıktı. İlk Rus saldırıları, veri silen malware'lerle kurum içindeki hizmetleri ve fırlatılan ilk füzelerden bir tanesi ile de fiziksel veri merkezlerini hedef aldı.

Ukrayna, iş yüklerini ve verileri hızla Ukrayna dışındaki veri merkezlerinde bulunan hiper ölçekli bulutlara taşıyarak yanıt verdi. İkinci olarak, veri ve ileri düzey yapay zeka ve makine öğrenimi hizmetleriyle desteklenen siber tehdit bilgilerindeki ve uç nokta korumasındaki ilerlemeler, Ukrayna'nın Rus siber saldırılarına karşı kendini savunmasına yardımcı oldu.

Başka yerlerde, ulus devlet aktörleri faaliyetlerini artırdı ve daha geniş bir hedef kümesine saldırı düzenlemek için otomasyon, bulut altyapısı ve uzaktan erişim teknolojilerindeki gelişmeleri kullandı. Nihai hedeflere erişim sağlayan kurumsal BT tedarik zincirleri sık sık saldırıya uğradı. Aktörlerin, henüz patch uygulanmamış güvenlik açıklarından hızlı bir şekilde yararlanmaları, kimlik bilgilerini çalmak üzere gelişmiş tekniklerin yanı sıra deneme yanılma yöntemlerini kullanmaları ve açık kaynaklı veya yasal yazılımları kullanarak operasyonlarını gizlemeleri ile siber güvenlik hijyeni çok daha kritik bir hâl aldı. Ayrıca İran, saldırılarının temel unsuru olarak fidye yazılımları kullanmak da dahil olmak üzere yıkıcı siber silahların kullanımı konusunda Rusya'ya katıldı.

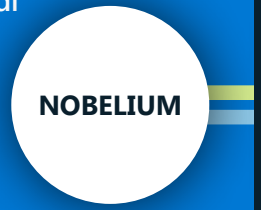
Bu gelişmeler, insan haklarına öncelik veren ve halkı online ortamda sergilenen sorumsuz devlet davranışlarına karşı koruyan tutarlı, küresel bir çerçevenin acilen benimsenmesini gerektirmektedir. Tüm uluslar, sorumlu bir devlet davranışı için üzerinde anlaşmaya varılan normları ve kuralları uygulamak için çalışmalıdır.

Ukrayna'yı Savunmak: Siber Savaştan Çıkarılan İlk Dersler — Microsoft On the Issues

Bilişim sektörü, finansal hizmetler, ulaşım sistemleri ve iletişim altyapısı başta olmak üzere kritik altyapılar giderek daha fazla hedefleniyor.

Daha fazla bilgi için bkz. sayfa 35

BT tedarik zinciri, hedeflere erişmek için bir ağ geçidi olarak kullanılıyor.



Daha fazla bilgi için bkz. sayfa 36

Çin, istihbarat ve rekabet avantajı elde etmek için özellikle Güneydoğu Asya'daki küçük ülkeleri genel olarak hedef alıyor.

Daha fazla bilgi için bkz. sayfa 44

İran, iktidarın el değiştirmesinin ardından giderek daha saldırgan hâle gelerek, fidye yazılımı saldırılarını bölgesel düşmanların ötesine, ABD ve AB'de bulunan kurbanlara kadar genişletti ve yüksek profilli ABD kritik altyapılarını hedef aldı.

Daha fazla bilgi için bkz. sayfa 46

Patch uygulanmamış güvenlik açıklarının tespit edilmesi ve hızla kötüye kullanılması önemli bir taktik hâline geldi. Güvenlik güncelleştirmelerinin hızlı bir şekilde kurulması savunmanın anahtarıdır.

Ayrıntılar için bkz. sayfa 39

Kuzey Kore, rejimin savunma inşa etme, ekonomiyi destekleme ve iç istikrarı sağlama hedeflerine ulaşmak için savunma ve havacılık kurumlarını, kripto para birimini, haber kuruluşlarını, sığınmacıları ve yardım kurumlarını hedef aldı.

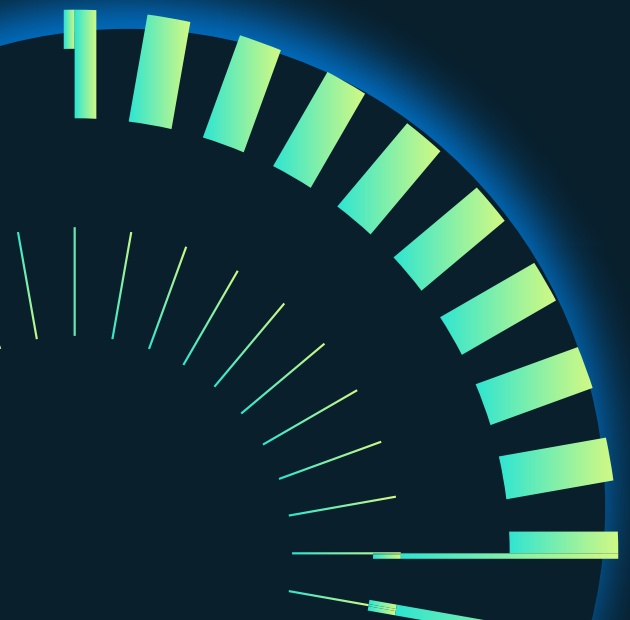
Daha fazla bilgi için bkz. sayfa 49

Siber paralı askerler, müşterilerinin (çoğunlukla hükümetlerin) ağlara ve cihazlara sızmasını sağlamak için ileri düzey araçlar, teknikler ve hizmetler geliştirip satan özel kurumlardan oluşan bu sektörün büyümesiyle, siber alanın istikrarını tehdit ediyor.

Daha fazla bilgi için bkz. sayfa 52

Giriş

2020 ve 2021'deki yüksek profilli saldırıların ardından ulus devlet tehdit aktörleri, karmaşık tehditlere karşı savunma yapmak amacıyla kurumlar tarafından uygulanan yeni güvenlik korumalarına uyum sağlamak için önemli miktarda kaynak harcadı.



Kurumsal organizasyonlara çok benzer şekilde, saldırganlar da saldırılarını daha geniş bir hedef kümesine genişletmek için otomasyon, bulut altyapısı ve uzaktan erişim teknolojilerindeki ilerlemeleri kullanmaya başladı. Bu taktiksel düzenlemeler, kurumsal tedarik zincirlerine karşı yeni yaklaşımlara ve büyük çaplı saldırılara yol açtı. Aktörler, patch uygulanmamış güvenlik açıklarından hızla yararlanmak için yeni yollar geliştirip, kurumsal ağların güvenliğini aşmak üzere tekniklerini genişlettikçe ve açık kaynaklı veya meşru yazılımları kullanarak operasyonlarını gizledikçe BT güvenlik hijyeni daha da önemli hâle geldi. Yeni saldırı teknikleri, bir hedefin ağına erişim sağlamak için yeni ve tespit edilmesi daha zor vektörler sağladı. Son olarak, savaş sırasındaki fiziksel saldırılar arttıkça, siber saldırıların askeri faaliyetlerde önemli bir rol oynadığını gördük.

Ukrayna'daki çatışma, savaş alanındaki askeri çatışmaya paralel olarak siber saldırıların da dünyayı etkilemek için nasıl geliştiğine dair çok net bir örnek sağladı. Güç sistemleri, telekomünikasyon sistemleri, medya ve diğer kritik altyapıların tümü hem fiziksel saldırıların hem de siber saldırıların hedefi hâline geldi. Casusluk ve bilgi sızdırma saldırılarının bir parçası olarak yaygın bir şekilde gözlemlenen ağ güvenliğini aşma girişimleri, hibrit savaşta kritik altyapı sistemlerine yönelik veri silici malware saldırılarına odaklandı. Bu sistemlerin güvenliğini buluta bağlamak, yıkıcı olabilecek bu saldırıların erken tespitini ve engellenmesini mümkün kıldı.[1]

İlk kez büyük bir siber etkinlikte, makine öğreniminden yararlanan davranışsal tespitler, temelde yer alan malware hakkında önceden bilgi sahibi olmadan, hatta insanlar tehditlerin bile farkına varmadan önce, daha sonraki saldırıları başarılı bir şekilde tespit etmek ve durdurmak için bilinen saldırı modellerini kullandı. Ayrıca, tehdit bilgilerini bu sistemleri koruyan savunucularla gerçek zamanlı olarak paylaşmanın değerini gördük ve onlara aktif saldırıları tahmin etmeleri ve bunlara karşı savunmaları için hayati bilgiler sağladık.

Dünyanın dört bir yanındaki ulus devlet tehdit aktörleri, operasyonlarını yeni ve eski yollarla genişletmeye devam ediyor. Çin, Kuzey Kore, İran ve Rusya, Microsoft müşterilerine yönelik saldırılar gerçekleştirdi. Aktörler, odağı birden çok kuruma erişim noktası olabilecek yukarı akış hizmetlerine kaydırdıkça BT hizmetleri tedarik zinciri de ortak bir hedef hâline geldi. Aktörlerin, kurumsal tedarik zincirlerindeki güvenilir ilişkilerden yararlanmaya devam etmelerini beklediğimizden, kimlik doğrulaması kurallarının kapsamlı bir şekilde uygulanmasına, özenli patch uygulamalarına, uzaktan erişim altyapısı için hesap yapılandırmalarına ve gerçekliği doğrulamak üzere ortak ilişkilerinin sık sık denetlenmesinin önemine vurgu yapıyoruz,

Ulus devlet aktörleri, fidye yazılımları ve suç operatörleri gibi, kendini idame ettiren saldırıları gerçekleştirmek için hatalı bir şekilde yapılandırılmış veya patch uygulanmamış kurumsal sistemleri (VPN/VPS altyapısı, kurum içindeki sunucular, üçüncü taraf yazılımlar) hedef alarak artan koruma düzeyine yanıt verdi. Birçoğu, kötü amaçlı faaliyetlerini gizlemek için ticari malware ve açık kaynaklı kırmızı ekip araçlarının kullanımını artırdı. Sonuç olarak, öncelikli patch uygulaması yoluyla güçlü bir BT güvenlik hijyeni temelinin korunması, hileyi önlemeye yönelik özelliklerinin etkinleştirilmesi, bir saldırı yüzeyinin dışarıdan nasıl göründüğünü öğrenmek için RiskIQ gibi saldırı yüzeyi yönetimi araçlarının kullanılması ve kurum genelinde çok faktörlü kimlik doğrulamanın etkinleştirilmesi, birçok ileri düzey aktöre karşı proaktif olarak savunmanın temel unsurları hâline geldi.

Ulus devlet aktörleri, saldırılarında bir taktik olarak fidye yazılımı kullanımını da artırdı ve genellikle saldırılarında bu suç ekosistemi tarafından oluşturulan fidye amaçlı malware'leri yeniden kullandı. Hem İran hem de Kuzey Kore merkezli aktörlerin, genellikle kritik altyapı dahil olmak üzere bölgesel rakiplerinde hedefledikleri sistemlere zarar vermek için ticari fidye yazılımı araçlarından yararlandığını gördük. Son olarak, savunmasız üçüncü taraf çözümlere karşı açıklardan daha fazla yararlanmak için araçlar, teknikler ve hizmetler geliştirip satan siber paralı askerlerin oluşturduğu tehdidin de arttığını gördük. Ulus devlet aktörleri tarafından gerçekleştirilen saldırıların karmaşıklığı ve çevikliği her yıl gelişmeye devam edecektir. Kurumlar, bu aktör değişikliklerinin farkında olarak yanıt vermeli ve buna paralel olarak savunmalar geliştirmelidir.

John Lambert
Kurumsal Başkan Yardımcısı ve Seçkin Mühendis, Microsoft Tehdit Bilgileri Merkezi

Ulus devlet verilerine ilişkin arka plan

Ulus devlet tehditleri, ulusal çıkarları ileriye taşıma amacıyla belirli bir ülkeden yürütülen siber tehdit faaliyetleridir. Ulus devlet aktörleri, fikri mülkiyet hırsızlığı, casusluk, gözetleme, kimlik bilgisi hırsızlığı, yıkıcı saldırılar ve başka alanları da kapsayacak şekilde müşterilerimizin karşılaştığı en ileri düzey ve kalıcı tehditlerden bazılarına neden olmaktadır.

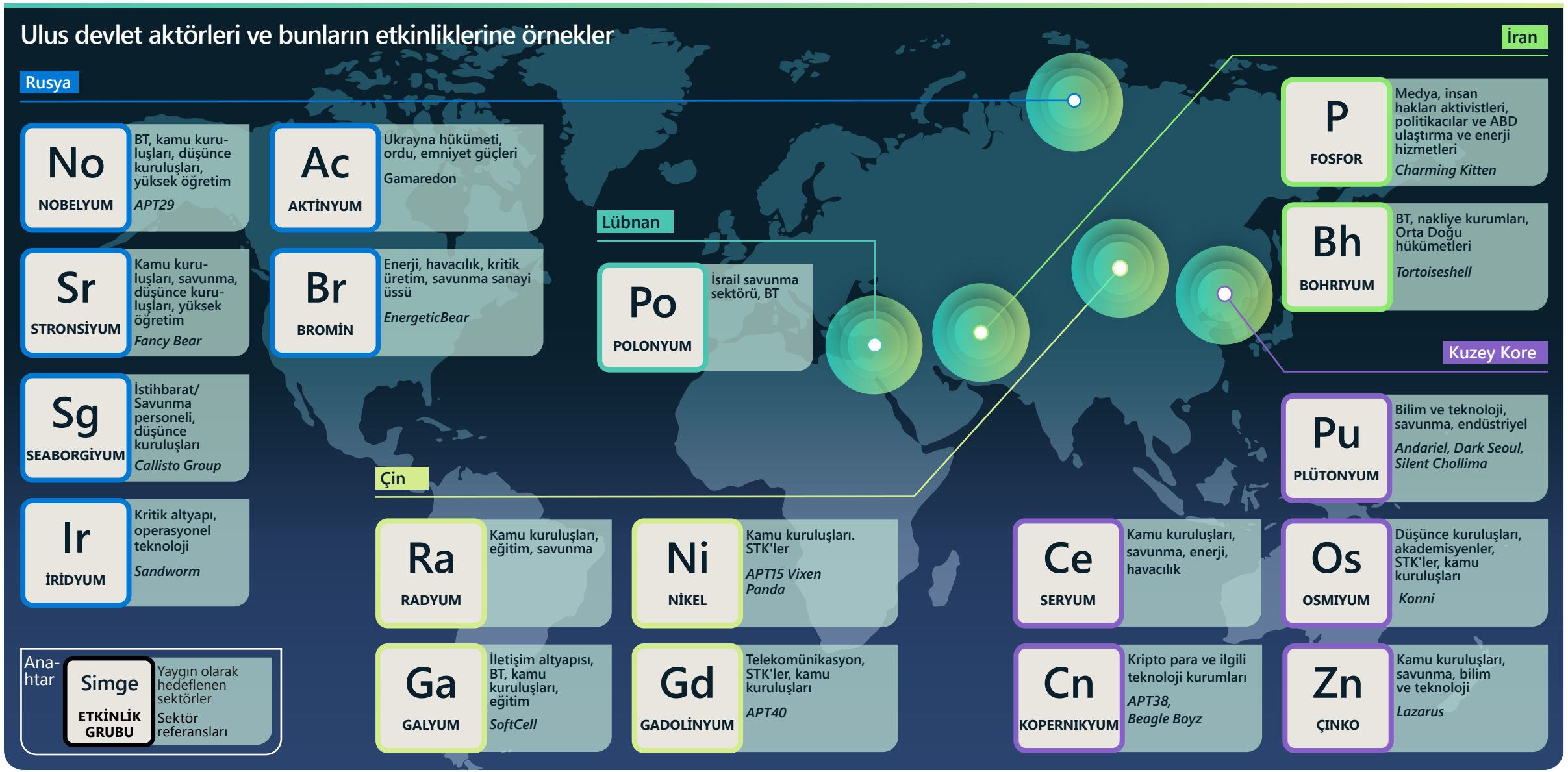
Bu tehditleri keşfetmek, anlamak ve bunlarla mücadele etmek için önemli miktarda kaynak yatırımı yapıyoruz. Bir kurum veya bireysel hesap sahibi, gözlemlenen ulus devlet etkinlikleri tarafından hedef alındığında veya güvenliği aşıldığında Microsoft, doğrudan müşteriye ulus devlet bildirimi (NSN) biçiminde, etkinliği araştırmak için ihtiyaç duydukları bilgileri de içeren bir uyarı gönderir. Haziran 2022 itibarıyla, 2018'de başladığımızdan bu yana 67.000'den fazla NSN gönderdik.

Microsoft NSN uyarı verileri, ölçülebilir etkinliklerin bir görünümünü sağlamak için bu bölümde sunulmuştur. Grafiklerde gösterilen ulus devlet etkinlik düzeyi, müşteri kurumda en az bir hesabı hedef alan veya güvenliğini aşan ulus devlet aktörlerinin tespitine yanıt olarak Microsoft'un müşterilere verdiği NSN sayısını temel almaktadır.

Bu rapora tehdit gruplarını dahil ettiğimiz başlıca dört ulus devlet Rusya, Çin, İran ve Kuzey Kore'dir. Bunlar, geçtiğimiz yıl boyunca en yaygın şekilde Microsoft müşterilerini hedef aldığı gözlemlenen aktörlerin menşe ülkelerini temsil etmektedir. Rapor aynı zamanda, Lübnan'dan ve siber paralı askerlerden veya kiralık özel sektör saldırı aktörlerinden gelen tehdit grupları hakkındaki gözlemlerimizi de içermektedir.

Microsoft, ulus devlet gruplarını, bir kısmı sonraki sayfada gösterilen kimyasal element adlarına (NOBELIUM gibi) göre tanımlamaktadır. DEV-#### gösterimleri bilinmeyen, yeni ortaya çıkan veya gelişmekte olan bir tehdit etkinliği kümesine verilen geçici bir ad olarak kullanılmaktadır ve bu, faaliyetin arkasındaki aktörün menşei veya kimliği hakkında yüksek bir güven düzeyine ulaşana kadar onu benzersiz bir bilgi kümesi olarak izlememize olanak tanır.

Bir DEV, ölçütleri karşıladığında, adlandırılmış yeni bir aktöre dönüşür veya mevcut aktörlerle birleştirilir. Bu kısımda, saldırı hedeflerine, tekniklere ve motivasyonlarının analizine daha derin bir bakış sağlamak için ulus devlet ve DEV gruplarından örnekler vereceğiz. Bu grupların birçoğu siber suçlularla aynı araçları kullansa da özel malware'ler, sıfır gün güvenlik açıklarını keşfetme ve bunlardan yararlanma ve yasal dokunulmazlık biçimlerinde benzersiz tehditlere neden olurlar.


Ulus devlet aktörleri ve bunların etkinliklerine örnekler
Rusya
No
NOBELYUM
BT, kamu kuruluşları, düşünce kuruluşları, yüksek öğretim
APT29
Ac
AKTİNYUM
Ukrayna hükümeti, ordu, emniyet güçleri
Gamaredon
Sr
STRONSİYUM
Kamu kuruluşları, savunma, düşünce kuruluşları, yüksek öğretim
Fancy Bear
Br
BROMİN
Enerji, havacılık, kritik üretim, savunma sanayi üssü
EnergeticBear
Sg
SEABORGİYUM
İstihbarat/ Savunma personeli, düşünce kuruluşları
Callisto Group
Ir
İRİDYUM
Kritik altyapı, operasyonel teknoloji
Sandworm
Lübnan
Po
POLONYUM
İsrail savunma sektörü, BT
İran
P
FOSFOR
Medya, insan hakları aktivistleri, politikacılar ve ABD ulaştırma ve enerji hizmetleri
Charming Kitten
Bh
BOHRIYUM
BT, nakliye kurumları, Orta Doğu hükümetleri
Tortoiseshell
Kuzey Kore
Pu
PLÜTONYUM
Bilim ve teknoloji, savunma, endüstriyel
Andariel, Dark Seoul, Silent Chollima
Çin
Ra
RADYUM
Kamu kuruluşları, eğitim, savunma
Ni
NİKEL
Kamu kuruluşları. STK'ler
APT15 Vixen Panda
Ce
SERYUM
Kamu kuruluşları, savunma, enerji, havacılık
Os
OSMIYUM
Düşünce kuruluşları, akademisyenler, STK'ler, kamu kuruluşları
Konni
Ga
GALYUM
İletişim altyapısı, BT, kamu kuruluşları, eğitim
SoftCell
Gd
GADOLİNYUM
Telekomünikasyon, STK'ler, kamu kuruluşları
APT40
Cn
KOPERNIKYUM
Kripto para ve ilgili teknoloji kurumları
APT38, Beagle Boyz
Zn
ÇINKO
Kamu kuruluşları, savunma, bilim ve teknoloji
Lazarus
Ana-htar
Simge
ETKİNLİK GRUBU
Yaygın olarak hedeflenen sektörler
Sektör referansları

Gelişen tehdit ortamı

Microsoft'un ulus devlet aktörlerinin faaliyetlerini takip etme ve hedeflendiklerini veya güvenliklerinin aşıldığını gördüğünde müşterilerini bilgilendirme görevi, müşterilerimizi saldırılardan koruma misyonumuza dayanmaktadır.

Bu bildirim, gözlemlenen saldırıların güvenlik ürünü korumalarımız tarafından başarıyla engellenip engellenmediği veya saldırıların bilinmeyen güvenlik zaafları nedeniyle etkili olup olmadığı konusunda müşterilere bilgi verme taahhüdümüzün önemli bir parçasıdır. Bildirimleri takip etmek, Microsoft'un zaman içinde aktörlerin neden olduğu gelişen tehdit trendlerini belirlemesine ve ürün korumalarında, bulut hizmetlerimizdeki müşterilere yönelik tehditleri proaktif olarak azaltmaya odaklanmasına yardımcı olur.

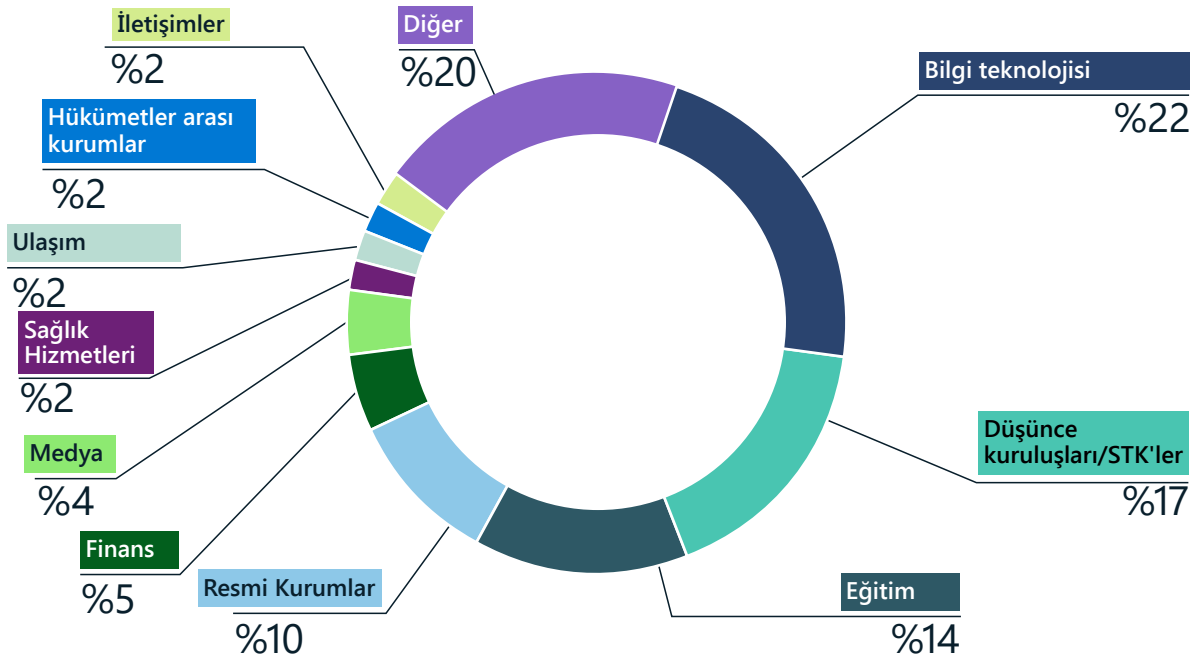
Bu takip, gördüklerimizle ilgili verileri ve içgörüleri paylaşmamıza da olanak tanır. Bu aktörleri gözlemleyen ve saldırılarını takip eden analistler, aktörlerin motivasyonlarını anlamak için teknik göstergeler ve jeopolitik uzmanlığın bir birleşimini kullanarak teknik ve küresel bağlamı yeni içgörülerle bir araya getirir. Bu düzenleme, ulus devlet siber aktörlerinin önceliklerine ve motivasyonlarının, kendilerini görevlendiren ulus devletlerin siyasi, askeri ve ekonomik önceliklerini nasıl yansıtabileceğine dair benzersiz bir görüş sunmaktadır.

Geçen yılki siyasi gelişmeler, dünya çapında devlet destekli tehdit gruplarının önceliklerini ve risk toleranslarını şekillendirdi. Jeopolitik ilişkiler bozuldukça ve bazı ülkelerdeki savaş yanlısı unsurlar daha güçlendikçe, siber aktörler de daha cesur ve saldırgan hâle geldi. Örneğin:

- Rusya, savaş alanındaki askeri harekatını tamamlamak için acımasızca Ukrayna hükümetini ve ülkenin kritik altyapısını hedef aldı.[2]
- İran, ABD'nin liman idareleri gibi kritik altyapılarına agresif bir şekilde girmeye çalıştı.
- Kuzey Kore, finans ve teknoloji kurumlarından kripto para çalmayı amaçlayan saldırılarına devam etti.
- Çin, küresel siber casusluk operasyonlarını genişletti.

Ulus devlet aktörleri teknik olarak gelişmiş ve çok çeşitli taktikler uygulayabiliyor olsalar da, saldırıları genellikle iyi bir siber hijyen ile hafifletilebilir. Bu aktörlerin birçoğu, amaçlarına ulaşmak için özelleştirilmiş güvenlik açığı kodları geliştirmeye yatırım yapmak veya hedeflenen sosyal mühendisliği kullanmak yerine gelişmiş malware'ler sunmak için hedefli kimlik avı e-postaları gibi nispeten düşük teknolojili araçları kullanır.

Ulus devlet aktörlerinin hedef aldığı endüstri sektörleri



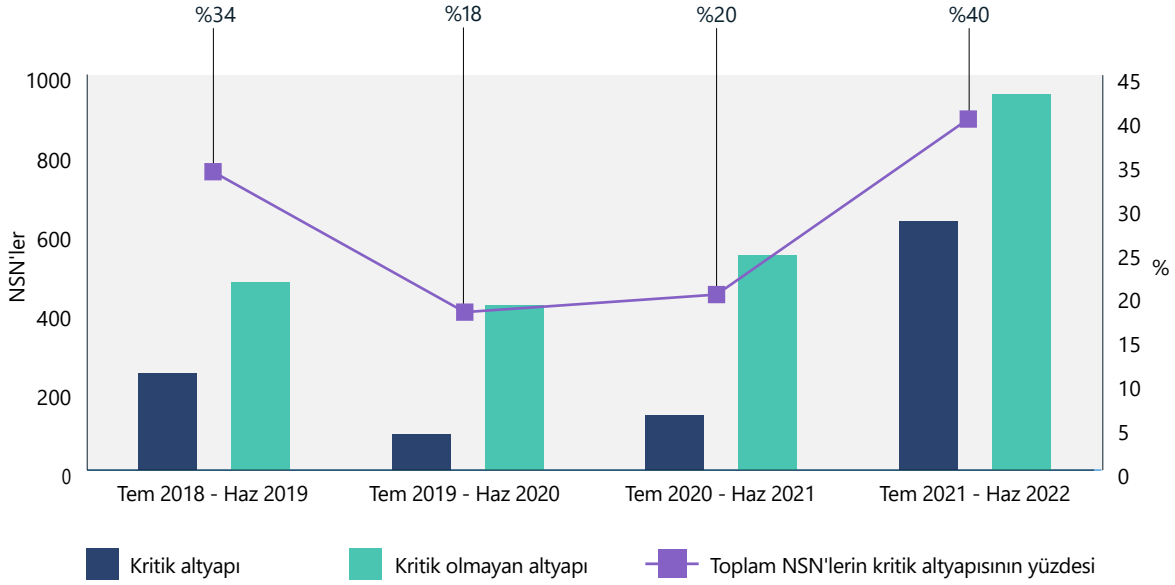
Ulus devlet grupları çeşitli sektörleri hedef almıştır. Rus ve İran devlet aktörleri, BT kurumlarının müşterilerine erişmek için bir araç olarak BT sektörünü hedef almıştır. Düşünce kuruluşları, sivil toplum kuruluşları (STK'ler), üniversiteler ve kamu kuruluşları, ulus devlet aktörlerinin diğer ortak hedefleri olmaya devam etmiştir.

Ulus devlet aktörleri, çeşitli amaçlarına ulaşmak için belirli kurum veya birey gruplarını hedef alabilir. Geçen yıl, özellikle BT kurumlarına odaklanan tedarik zinciri saldırıları artış göstermiştir. Tehdit aktörleri, BT hizmet sağlayıcılarının güvenliğini aşarak, genellikle bağlı sistemleri yöneten kurumla kurulan güvenilir bir ilişki yoluyla asıl hedeflerine ulaşabilmekte veya tek bir saldırıda yüzlerce alt müşterinin güvenliğini ihlal edip potansiyel olarak çok daha büyük ölçekte saldırılar gerçekleştirebilmektedir. Bilişim sektöründen sonra en sık karşılaşılan hedefler düşünce kuruluşları, üniversitelere bağlı akademisyenler ve kamu kuruluşu yetkilileridir. Bunlar, jeopolitik sorunlarda istihbarat toplamak için istenen "yumuşak casusluk hedefleri"dir.

Gelişen tehdit ortamı

Devamı

Kritik altyapı trendleri

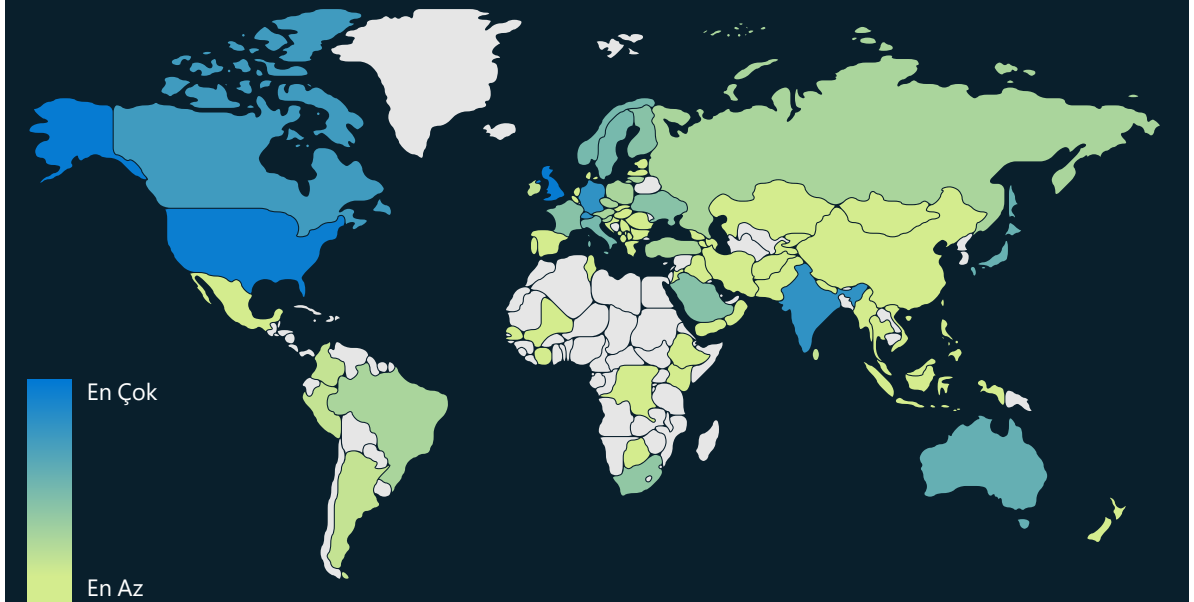


Aktörlerin bilişim sektörü, finansal hizmetler, ulaşım sistemleri ve iletişim altyapısındaki kurumlara odaklanmasıyla, ulus devlet gruplarının kritik altyapıyı hedeflemesi[3] geçen yıl artış gösterdi.

"Ukrayna'nın işgalinden önce hükümetler, verilerin güvende olması için ülke içinde kalması gerektiğini düşünüyorlardı. İşgalden sonra, verileri buluta geçirmek ve bölgesel sınırların dışına taşımak artık dayanıklılık planlamasının ve iyi yönetimin bir parçası hâline geldi."

Cristin Flynn Goodwin,
Baş Hukuk Müşaviri, Müşteri Güvenliği ve Güveni

Ulus devlet aktörlerinin coğrafi hedeflemesi



Ulus devlet gruplarının siber hedeflemesi, geçtiğimiz yıl özellikle ABD ve İngiliz kurumlarına yoğun bir şekilde odaklanarak tüm dünyayı sardı. NSN verilerimize göre İsrail, BAE, Kanada, Almanya, Hindistan, İsviçre ve Japonya'daki kurumlar da en sık hedef alınanlar arasındaydı.

Eyleme dönüştürülebilir içgörüler

1. Ulus devlet gruplarının stratejik öncelikleriyle uyumlu olabilecek, potansiyel olarak yüksek değerli veri hedeflerinizi, risk altındaki teknolojilerinizi, bilgilerinizi ve kurum operasyonlarınızı tanımlayın ve koruyun.
2. Ağınıza yönelik önceden bilinen ve yeni tehditlerin büyük ölçekte tanımlanmasını ve azaltılmasını sağlamak için bulut korumalarını etkinleştirin.

Dijital ekosisteme açılan bir kapı olarak BT tedarik zinciri

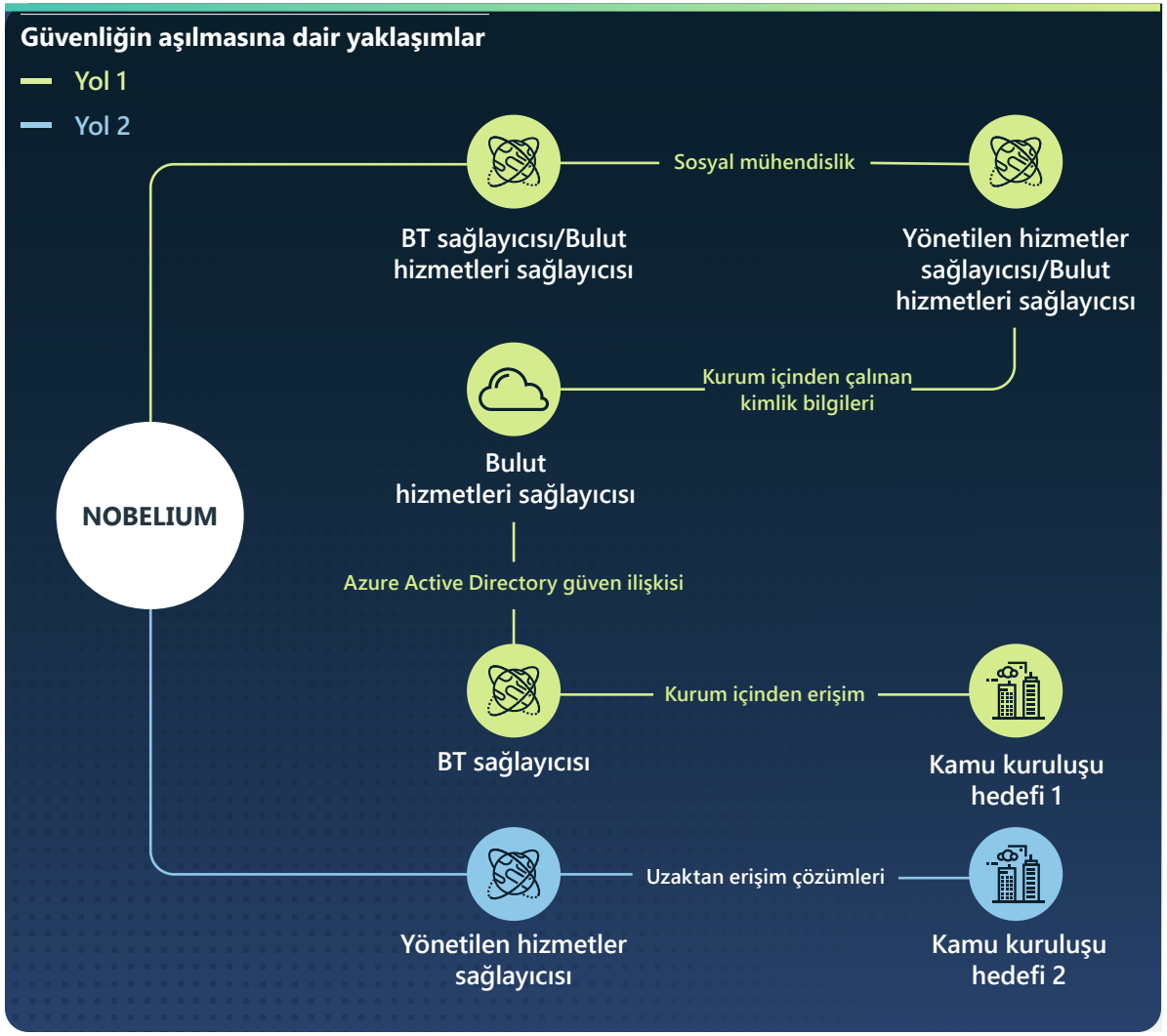
Ulus devlet gruplarının BT hizmet sağlayıcılarını hedeflemesi, tehdit aktörlerinin bu tedarik zinciri sağlayıcılarına duyulan güven ve verilen erişimden yararlanarak diğer ilgili kurumlardan kötü amaçla yararlanmasına olanak sağlayabilir. Geçen yıl ulus devlet siber tehdit grupları, üçüncü taraf hedeflere saldırmak ve kamu kuruluşları, politika ve kritik altyapı sektörlerindeki alt müşterilere erişim elde etmek için BT hizmet sağlayıcılarını hedef aldı.

BT hizmet sağlayıcıları, yabancı istihbarat servislerinin ilgilenebileceği yüzlerce doğrudan ve binlerce dolaylı müşteriye hizmet sundukları için cazip ara hedeflerdir. Kötü amaçla kullanılırsa bu kurumların sahip olduğu rutin iş uygulamaları ve yetki verilen yönetim ayrıcalıkları, uyarılar tetiklenmeden kötü niyetli aktörlerin BT hizmet sağlayıcısı müşteri ağlarına erişmesine ve bunları yönetmesine imkan tanıyabilir.

Geçen yıl NOBELYUM, başta ABD ve Avrupa kamu kuruluşları ve politika müşterileri olmak üzere hedeflenen alt erişimi denemek için bulut çözümlerindeki ve diğer yönetilen hizmet sağlayıcılarındaki ayrıcalıklı hesapların güvenliğini aşmaya ve bunlardan yararlanmaya çalıştı.

NOBELYUM, "birden çok hesabın güvenliğini aşmak için birinin güvenliğini aş" yaklaşımının nasıl tespit edilen bir jeopolitik düşmana karşı yönlendirilebileceğini gösterdi. Geçtiğimiz yıl tehdit aktörü, Rus hükümetinin varoluşsal bir tehdit olarak algıladığı Kuzey Atlantik Antlaşması Örgütü'nün (NATO) üye devletlerinde bulunan hassas kurumlara yapılan hem üçüncü taraf hem de doğrudan izinsiz girişlerin peşine düştü. Temmuz 2021 ile Haziran 2022'nin başları arasındaki dönemde, Microsoft'un online hizmet müşterilerine yönelik Rus tehdidi etkinliklerine dair müşteri bildirimlerinin yüzde 48'i, muhtemelen ara erişim noktaları olarak görülen, NATO üyesi ülkelerdeki BT sektörü firmalarına gitti. Genel olarak, aynı dönemde Rus tehdit faaliyetleriyle ilgili bildirimlerin yüzde 90'ı, BT, düşünce kuruluşları ve sivil toplum kuruluşları (STK'ler) ve kamu sektörleri başta olmak üzere NATO üyesi devletlerde bulunan müşterilere gitti. Bu durum, bu hedeflere ilk erişim için birden fazla yol izleme stratejisinin izlendiğini gösteriyordu.

Alt müşterilere ulaşmak amacıyla bulut çözümlerini ve yönetilen hizmet sağlayıcılarını hedeflemek için yazılım tedarik zincirini kötüye kullanmaktan BT hizmetleri tedarik zincirini kötüye kullanmaya bir geçiş yaşandı.



Bu şema, NOBELYUM'un nihai hedeflerinin güvenliğini aşmaya yönelik çok vektörlü yaklaşımını ve yol boyunca diğer kurbanlara verdikleri ek hasarı göstermektedir. Yukarıda gösterilen eylemlere ek olarak NOBELYUM, dahil olan kurumlara karşı parola spreyi ve kimlik avı saldırıları düzenledi, hatta başka bir potansiyel güvenlik ihlali yolu olarak en az bir devlet çalışanının kişisel hesabını da hedef aldı.

Dijital ekosisteme açılan bir kapı olarak BT tedarik zinciri

Devamı

Yıl boyunca Microsoft Tehdit Bilgileri Merkezi (MSTIC), giderek artan sayıda İran devleti ve İran bağlantılı aktörün BT kurumlarının güvenliğini tehlikeye attığını tespit etti. Birçok durumda, aktörlerin, istihbarat toplamaktan misilleme amaçlı yıkıcı saldırılara kadar bir dizi hedefe yönelik alt müşterilere erişim sağlamak amacıyla oturum açma kimlik bilgilerini çaldığı tespit edildi.

- Temmuz ve Ağustos 2021'de DEV-0228, daha sonra İsrail savunma, enerji ve hukuk sektörlerindeki alt müşterilerin güvenliklerini aşmak için bir İsrailli ticari yazılım sağlayıcısının güvenliğini aştı.[4]
- Microsoft, Ağustos ile Eylül 202 arasında İran devlet aktörlerinin Hindistan merkezli BT kurumlarını daha fazla hedef aldığını tespit etti. Böyle bir değişime yol açabilecek baskılayıcı jeopolitik sorunların olmaması, bu hedeflemenin Hindistan dışındaki yan kuruluşlara ve müşterilere dolaylı erişim için olduğunu göstermektedir.
- Ocak 2022'de, İran hükümetine bağlı olduğunu düşündüğümüz DEV-0198 grubu, İsrailli bir bulut çözümü sağlayıcısının güvenliğini aştı. Microsoft, aktörün muhtemelen bir İsrail lojistik kurumunda kimlik doğrulaması yapmak için sağlayıcının ele geçirilmiş kimlik bilgilerini kullandığını düşünmektedir. MSTIC, aynı aktörün ocak ayının sonlarında lojistik kurumuna karşı yıkıcı bir siber saldırı gerçekleştirmeye çalıştığını gözlemledi.
- Nisan 2022'de, İran devlet gruplarıyla BT tedarik zinciri teknikleri konusunda işbirliği yaptığını düşündüğümüz Lübnan merkezli bir grup olan POLONYUM, İsrail savunma ve hukuk kurumlarına erişim elde etmek için başka bir İsrailli BT kurumuna erişim sağladı.[5]

Geçtiğimiz yıl gerçekleştirilen etkinlikler, NOBELYUM ve DEV-0228 gibi tehdit aktörlerinin bir kurumun güvenilir ilişkilerini kurumların kendilerinden daha iyi tanımaya başladığını gösteriyor. Bu artan tehdit, kurumların dijital varlıklarının sınırlarını ve giriş noktalarını anlama ve sağlamlaştırma ihtiyacını vurgulamaktadır. Ayrıca, BT hizmet sağlayıcılarının kendi siber güvenlik durumlarını titizlikle izlemelerinin öneminin altını çizmektedir. Örneğin, kurumlar, kötü niyetli aktörlerin ayrıcalıklı hesapları ele geçirmesini veya bir ağa yayılmasını zorlaştıran çok faktörlü kimlik doğrulama ve koşullu erişim kuralları uygulamalıdır.

İş ortağı ilişkilerinin kapsamlı bir incelemesini ve denetimini yürütmek, kurumunuz ile üst sağlayıcıları arasındaki gereksiz izinleri en aza indirmeye ve alışılmadık görünen tüm ilişkilere erişimi anında kaldırmaya yardımcı olur. Etkinlik günlüklerinin daha iyi anlaşılması ve mevcut etkinliğin gözden geçirilmesi, daha fazla araştırmayı tetikleyebilecek anormalliklerin tespit edilmesini kolaylaştırır.

> Ulus devletlerin üçüncü tarafları hedeflemesi, bir tedarik zincirindeki güven ve erişimden yararlanarak hassas kurumlardan yararlanmalarına olanak tanır.

Eyleme dönüştürülebilir içgörüler

1. Gereksiz izinleri en aza indirmek için üst ve alt hizmet sağlayıcı ilişkilerini ve yetki verilen ayrıcalık erişimlerini gözden geçirin ve denetleyin. Bilmediğiniz veya henüz denetlenmemiş tüm iş ortağı ilişkilerinin erişimini kaldırın.[6]
2. Gerçekliği onaylamak ve anormal etkinliği araştırmak üzere, tek faktörlü kimlik doğrulama ile yapılandırılmış hesaplara odaklanarak, uzaktan erişim altyapısı ve sanal özel ağlar (VPN'ler) için günlüğe kaydetmeyi etkinleştirin ve tüm kimlik doğrulama etkinliğini gözden geçirin.
3. Tüm hesaplar (hizmet hesapları dahil) için MFA'yı etkinleştirin ve MFA'nın tüm uzak bağlantılar için zorunlu kılındığından emin olun.
4. Hesapların güvenliğini sağlamak için parolasız çözümleri kullanın.[7]

Daha ayrıntılı bilgi için bağlantılar

- NOBELYUM, daha geniş çaplı saldırıları kolaylaştırmak için yetki verilen yönetici ayrıcalıklarını hedefliyor | Microsoft Tehdit Bilgileri Merkezi (MSTIC)
- İran'ın BT sektörü giderek daha fazla hedeflemesi | Microsoft Tehdit Bilgileri Merkezi (MSTIC), Microsoft Dijital Güvenlik Birimi
- İsrail kurumlarını hedef alan POLONYUM'un faaliyetleri ve altyapısı ifşa oldu | Microsoft Tehdit Bilgileri Merkezi (MSTIC)

Güvenlik açığından hızla yararlanma

Kurumlar siber güvenlik duruşlarını güçlendirdikçe ulus devlet aktörleri, saldırılar gerçekleştirmek ve tespit edilmemek için yeni ve benzersiz taktikler geliştirerek karşılık verir. Sıfır gün güvenlik açıkları olarak bilinen ve önceden bilinmeyen güvenlik açıklarının tanımlanması ve açığa çıkarılması, bu çabadaki önemli bir taktiktir.

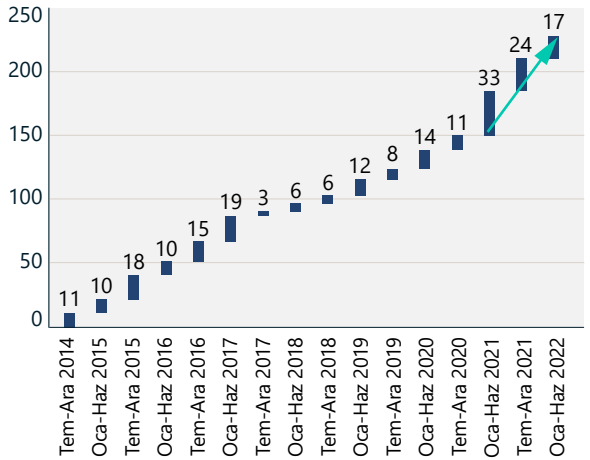
Sıfır gün güvenlik açıkları, güvenlik açığından ilk olarak yararlanma için özellikle etkili bir araçtır ve bir kez kamuya açıklandığında güvenlik açıkları, diğer ulus devletler ve suç aktörleri tarafından hızla yeniden kullanılabilir. Bir önceki yıl kamuya açıklanan sıfır gün güvenlik açıklarının sayısı rekor kırmıştı, ancak bu yıl kaydedilen sayı da buna eşittir.

Hem ulus devlet hem de suçlu siber tehdit aktörleri bu güvenlik açıklarından yararlanma konusunda ustalaştıkça, bir güvenlik açığının duyurulması ile bu güvenlik açığının metalaştırılması arasındaki sürenin kısaldığını gözlemledik. Bu, kurumların açıklardan yararlanma sistemlerine hemen patch uygulanmasını gerekli kılar. Benzer şekilde, yeni güvenlik açıklarını ortaya çıkaran kurumların veya bireylerin, koordineli güvenlik açığı kamuya açıklama prosedürlerine uygun olarak bunları sorumlu bir şekilde etkilenen satıcılara mümkün olan en kısa sürede açıklaması veya bildirmesi kritik öneme sahiptir.

Bu, güvenlik açıklarının tanımlanmasını ve müşterileri önceden bilinmeyen tehditlerden korumak için patch'lerin zamanında geliştirilmesini sağlamaktadır.

Birçok kurum, güvenlik açığı yönetimi ağ güvenliğiyle tümleşikse sıfır gün açıklarından yararlanma saldırılarının kurbanı olma olasılıklarının daha düşük olduğunu varsayar. Ancak, açıkların metalaştırılması, saldırıların çok daha hızlı bir şekilde başlarına gelmesine yol açmaktadır. Sıfır gün güvenlik açıkları genellikle diğer aktörler tarafından keşfedilir ve kısa bir süre içinde geniş çapta yeniden kullanılır ve patch uygulanmamış sistemleri risk altında bırakır. Sıfır gün güvenlik açıklarından yararlanmayı tespit etmek zor olsa da, aktörlerin güvenlik açığını keşfettikten sonraki eylemlerini tespit etmek genellikle daha kolaydır ve patch'lerin tam olarak uygulandığı bir yazılımdan geliyorsa bir güvenlik ihlali uyarısı olarak işlev görebilir.

Sıfır gün güvenlik açıkları için yayınlanan yamalar



Yaygın Güvenlik Açıkları ve Açıklamaları Listesi'nden (CVE'ler) kamuya açıklanan sıfır gün güvenlik açıklarının sayısı.

Bir güvenlik açığı kamuya açıklandıktan sonra bu açıktan yararlanan bir yöntemin kullanıma sunulması ortalama olarak yalnızca 14 gün sürmektedir. Bu görünümde, sıfır gün güvenlik açıklarından yararlanma zaman çizelgelerinin yanı sıra söz konusu açıktan yararlanmaya karşı savunmasız ve ilk kez kamuya açıklanma anından itibaren internette aktif olan sistemlerin sayısının bir analizi sağlanmaktadır.

> Sıfır gün güvenlik açığı saldırıları başlangıçta sınırlı sayıda kurumu hedef alma eğilimindeyken, hızla daha büyük tehdit aktörü ekosistemi tarafından benimsenmiştir. Bu, tehdit aktörleri için, potansiyel hedefler yamaları yüklemeden önce güvenlik açığından olabildiğince geniş bir şekilde yararlanma yarışını başlatır.

Pek çok ulus devlet aktörünün bilinmeyen güvenlik açıklarından yararlandığını gözlemlesek de, Çin merkezli ulus devlet tehdit aktörleri sıfır gün açıklarını keşfetme ve geliştirme konusunda özellikle yetkindir. Çin'in güvenlik açığı raporlama yönetmeliği Eylül 2021'de yürürlüğe girdi ve dünyada ilk kez bir devlet, güvenlik açıklarının ürün veya hizmet sahibiyle paylaşılmadan önce incelenmesi amacıyla bir devlet idaresine bildirilmesini zorunlu kıldı. Bu yeni düzenleme, Çin hükümetindeki unsurların, rapor edilen güvenlik açıklarını silaha dönüştürmek için hazır hâle getirmesini sağlayabilir. Geçtiğimiz yıl boyunca Çin merkezli aktörlerin sıfır gün açıklarını daha fazla kullanması, muhtemelen Çin'in Çin güvenlik topluluğundan güvenlik açıklarını açıklama zorunluluklarını getirmesinin ilk tam yılını ve sıfır gün açıklarından yararlanmayı bir devlet önceliği olarak kullanmasına yönelik büyük bir adımı yansıtmaktadır. Aşağıda açıklanan güvenlik açıkları, keşfedilip daha büyük bir tehdit ekosistemindeki diğer aktörler arasında yayılmadan önce ilk olarak Çin merkezli ulus devlet aktörleri tarafından saldırılarda geliştirilmiş ve dağıtılmıştır.

Güvenlik açığından hızla yararlanma

Devamı

Ulus devlet tehdit aktörlerinin saldırılarının hedefinde olmayan kurumlar bile, daha geniş aktör ekosistemi güvenlik açıklarından yararlanmadan önce, etkilenen sistemlerdeki sıfır gün güvenlik açıklarına yama uygulamak için sınırlı bir süreye sahiptir.

Yeni tanımlanan güvenlik açıklarına ilişkin bu örnekler, kurumların bir güvenlik açığına yama uygulanmasından ve bir kavram kanıtı (POC) kodunun online olarak kullanıma sunulmasından ve genellikle diğer aktörler tarafından yeniden kullanılmak üzere alınmasından itibaren ortalama 60 günü olduğunu göstermektedir. Benzer şekilde, kurumların Metasploit gibi otomatik güvenlik açığı tarama ve açıklardan yararlanma araçlarında bir güvenlik açığının kullanıma sunulmasından önce ortalama 120 günü vardır. Bir güvenlik açığının böyle bir araçta sunulması, genellikle açıktan devasa ölçekte yararlanılmasına neden olur. Bu, ulus devlet tehdit aktörlerinin hedefi olmayan kurumların bile, daha geniş aktör ekosistemi güvenlik açıklarından yararlanmadan önce, etkilenen sistemlerdeki sıfır gün güvenlik açıklarına yama uygulamak için sınırlı bir süreye sahip olduklarını göstermektedir.

CVE-2021-35211 SolarWinds Serv-U

Temmuz 2021'de SolarWinds, CVE-2021-35211 için Microsoft'un bildirimine güvenerek bir güvenlik danışma belgesi yayınladı.[8] O sırada, ulus devlet bağlantılı tehdit aktörü DEV-0322'nin SolarWinds Serv-U güvenlik açığından aktif olarak yararlandığını keşfetmiştik. RiskIQ ekibimiz, 15 Haziran ile 9 Temmuz arasında etkilenen cihazların internete bağlı sürümlerini barındıran 12.646 IP adresini gözlemlemişti.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

Eylül 2021'de araştırmacılarımız, Çin bağlantılı aktörlerin ABD merkezli bazı kurumlarda Zoho ManageEngine güvenlik açığından yararlandığını gözlemledi. Güvenlik açığı, kurumların genellikle parola sıfırlama işlemlerini gerçekleştirmek için kullandığı CVE-2021-40539 Zoho ManageEngine ADSelfService Plus olarak 6 Eylül'de kamuoyuna duyuruldu.[9] DEV-0322, Eylül ayının sonlarında bu güvenlik açığını ağlarda bir yer edinmek için başlangıç vektörü olarak kullandı ve kimlik bilgileri dökümü, özel ikili dosyaların yüklenmesi ve kalıcılığı sürdürmek için malware'ler bırakma gibi ek eylemler gerçekleştirdi. Açıklama sırasında, RiskIQ bu sistemlerin 4.011 örneğinin aktif ve internette mevcut olduğunu gözlemledi.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

Ekim 2021'in sonlarında, varlık yönetimine sahip bir BT yardım masası yazılımı ve ikinci bir Zoho ManageEngine ürünü olan ServiceDesk Plus'ta DEV-0322'nin bir güvenlik açığından (CVE-2021-44077) yararlandığını gözlemledik. DEV-0322 bu güvenlik açığını sağlık, bilgi teknolojisi, yüksek öğretim ve kritik üretim sektörlerindeki varlıkları hedef almak ve bunların güvenliklerini ihlal etmek için kullanıyordu. 2 Aralık'ta Federal Soruşturma Bürosu (FBI) ve Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), güvenlik açığından yararlanan ulus devlet tehdit aktörleri hakkında kamuya tavsiye niteliğinde ortak bir uyarı yayınladı. Açıklama sırasında, RiskIQ bu sistemlerin 7.956 örneğinin aktif ve internette mevcut olduğunu gözlemledi.

CVE-2021-42321 Microsoft Exchange

16 ve 17 Ekim 2021 tarihlerinde Çin'in Chengdu kentinde düzenlenen uluslararası bir siber güvenlik zirvesi ve bilgisayar korsanlığı yarışması olan Tianfu Cup sırasında bir Exchange güvenlik açığı (CVE-2021-42321) için sıfır gün açığından yararlanıldığı ortaya çıktı. Microsoft'taki güvenlik araştırmacıları, güvenlik açığının ortaya çıkmasından yalnızca üç gün sonra, 21 Ekim'de kontrolsüz kullanım ile Exchange güvenlik açığından yararlanıldığını gözlemlediler. Açıklama sırasında, RiskIQ bu sistemlerin 61.559 örneğinin aktif ve internette mevcut olduğunu gözlemledi. 2021 Kasım'ına kadar güvenlik açığından yararlanma faaliyetlerini gözlemlemeye devam ettik.

CVE-2022-26134 Confluence

Çin bağlantılı bir aktör, Confluence güvenlik açığı (CVE-2022-26134) için sıfır gün güvenlik açığından yararlanma koduna, muhtemelen güvenlik açığı 2 Haziran'da kamuya açıklanmadan dört gün önce sahip olmuştu ve büyük olasılıkla bunu ABD merkezli bir kuruma karşı kullandı. Açıklama sırasında RiskIQ, internette savunmasız Confluence sistemlerinin 53.621 örneğinin mevcut olduğunu gözlemledi.

Güvenlik açıkları, devasa ölçekte ve giderek daha kısa zaman dilimlerinde tespit ediliyor ve kullanılıyor.

Eyleme dönüştürülebilir içgörüler

1. Sıfır gün güvenlik açıkları yayımlandıktan hemen sonra patch uygulamaya öncelik verin; patch yönetimi döngüsünün kurulumunu beklemeyin.
2. Riski belirlemek ve patch'ler üzerinde ne zaman harekete geçileceğini hızlı bir şekilde belirlemek için tüm kurumsal donanım ve yazılım varlıklarını belgeleyin ve envanterini çıkarın.

Rus devlet aktörlerinin savaş zamanı Ukrayna ve ötesini tehdit eden siber taktikleri

Bu yıl, Rus devlet aktörlerinin, Rusya'nın Ukrayna'yı işgali sırasında askeri eylemleri tamamlamak için siber operasyonlar başlattığı ve genellikle Ukrayna dışındaki hedeflere karşı uygulanan aynı taktik ve teknikleri kullandığı görüldü. Dünya çapındaki kurumların, Rusya bağlantılı tehdit aktörlerinden kaynaklanan dijital tehditlere karşı siber güvenliği güçlendirmek için önlemler alması kritik önem taşımaktadır.

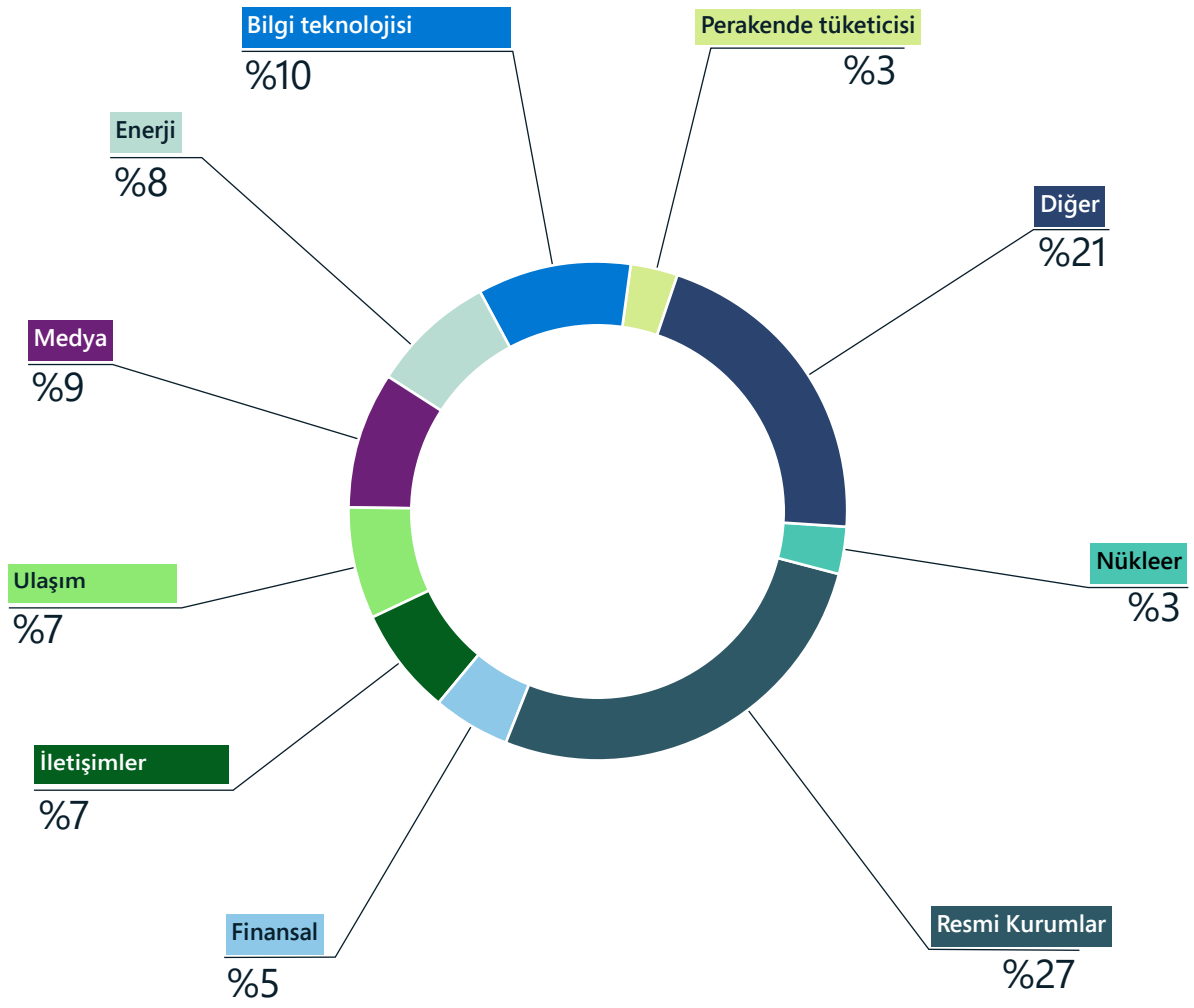
Askeri çatışma devam ettikçe sahadaki durum değişiklik göstermeye devam etmektedir ve Ukrayna ile müttefikleri de, Rus devlet siber operatörlerinin askeri amaçlar doğrultusunda izinsiz girişlerinin sıklığını veya yoğunluğunu artırması durumunda kendilerini savunmaya hazırlıklı olmalıdır. Savaşın ilk dört ayında Microsoft, Rus ordusuyla ilişkili tehdit aktörlerinin yaklaşık 50 farklı Ukrayna kurumuna ve kuruluşuna karşı çok sayıda yıkıcı siber saldırı dalgası ve birçoğuna karşı casusluk odaklı izinsiz girişler başlattığını gözlemledi. Çevrimiçi hizmet müşterilerine yönelik operasyonlar hariç, Rusya'nın bilinen hedeflere yönelik tehdit faaliyetinin yüzde 64'ü, Şubat sonu ile Haziran arasında Ukrayna merkezli kurumlara yönelikti.

Her operasyonda Rus tehdit aktörleri, işgalden önce hem Ukrayna içindeki hem de dışındaki hedeflere karşı kullanıldığını gözlemlediğimiz birçok taktik, teknik ve prosedürü (TTP) kullandı. Bu aktörler, çatışmanın ilk döneminde verileri yok etmeyi ve Ukrayna devlet kurumlarının dengesini bozmayı amaçladılar. O zamandan beri Ukrayna'ya askeri ve insani yardım ulaşımını ortadan kaldırmaya, halkın hizmetlere ve medyaya erişimini engellemeye ve Rusya'ya uzun vadeli istihbarat veya ekonomik değeri olan bilgileri çalmaya çalıştılar.

Ulaşımı hedeflemek, çatışmada hayatta kalmaya çalışan Ukrayna vatandaşları için kritik öneme sahip bir alanı tehdit etmektedir. Mayıs ayında yapılan UNICEF sponsorluğundaki bir ankete göre, çatışmalardan etkilenen kentsel bölgelerdeki kişiler en çok ulaşım ve yakıt, tedarik kesintileri, güvenlik ve gıda, tıbbi hizmetler ve finansal hizmetlere sınırlı erişim konusunda endişeliydi.[10] Haziran ayında BM Ukrayna Kriz Koordinatörü, Ukrayna'da en az 15,7 milyon kişinin acil insani yardıma ihtiyacı olduğunu ve savaş devam ettikçe sayının artacağını söyledi.[11]

Microsoft, Ukrayna dışında Şubat sonu ile Haziran arasında 42 ülkedeki 128 kurumun ağına yönelik Rusya tarafından izinsiz giriş çabaları tespit etti. ABD, Rusya'nın bir numaralı hedefi oldu. Ukrayna'ya yapılan uluslararası askeri ve insani yardımın çoğunun üzerinden geçtiği Polonya da bu dönemde önemli bir hedefti. Rus devletine bağlı tehdit aktörleri, Nisan ve Mayıs aylarında ise Baltık devletlerindeki kurumlar ile Danimarka, Norveç, Finlandiya ve İsveç'teki bilgisayar ağlarının peşine düştü.

İşgalden bu yana Ukrayna'da en çok hedef alınan endüstri sektörleri



Ukrayna'daki federal, eyalet ve yerel kamu kuruluşları, çatışma boyunca Rus devleti ve devlete bağlı tehdit grupları için öncelikli hedefler olmaya devam etti. Ulaştırma, enerji, finans ve medya sektörü kurumlarına odaklanılması, bu siber operasyonların Ukrayna vatandaşlarının güvendiği hizmetlere yönelik oluşturduğu riski öne çıkarmaktadır.

Rus devlet aktörlerinin savaş zamanı Ukrayna ve ötesini tehdit eden siber taktikleri

Devamı

NATO ülkelerinin dışişleri bakanlıklarını hedef alan benzer faaliyetlerde artış olduğunu gözlemledik.

Rus devleti tehdit grupları, geçtiğimiz yıl hem Ukrayna içinde hem de dışında kritik altyapıyı tehlikeye atmakla ilgilenmeye devam etti. IRIDIUM, Industroyer2 malware'ini Ukrayna'da milyonlarca insanı elektriksiz bırakma amacıyla başarısız bir şekilde dağıttı. BROMINE, 2022'nin başlarında Ukrayna dışında imalat ve endüstriyel kontrol sistemleriyle ilgili kuruluşlara yetkisiz erişimler gerçekleştirdi.

Rus devleti ve devlete bağlı aktörler, bu yıl aşağıdaki TTP'lerin birçoğunu kullanarak Ukrayna'ya, müttefiklerine ve istihbarat değeri olan diğer hedeflere yönelik siber operasyonlar yönetti:

Kötü amaçlı ekler veya bağlantılarla hedef odaklı kimlik avı

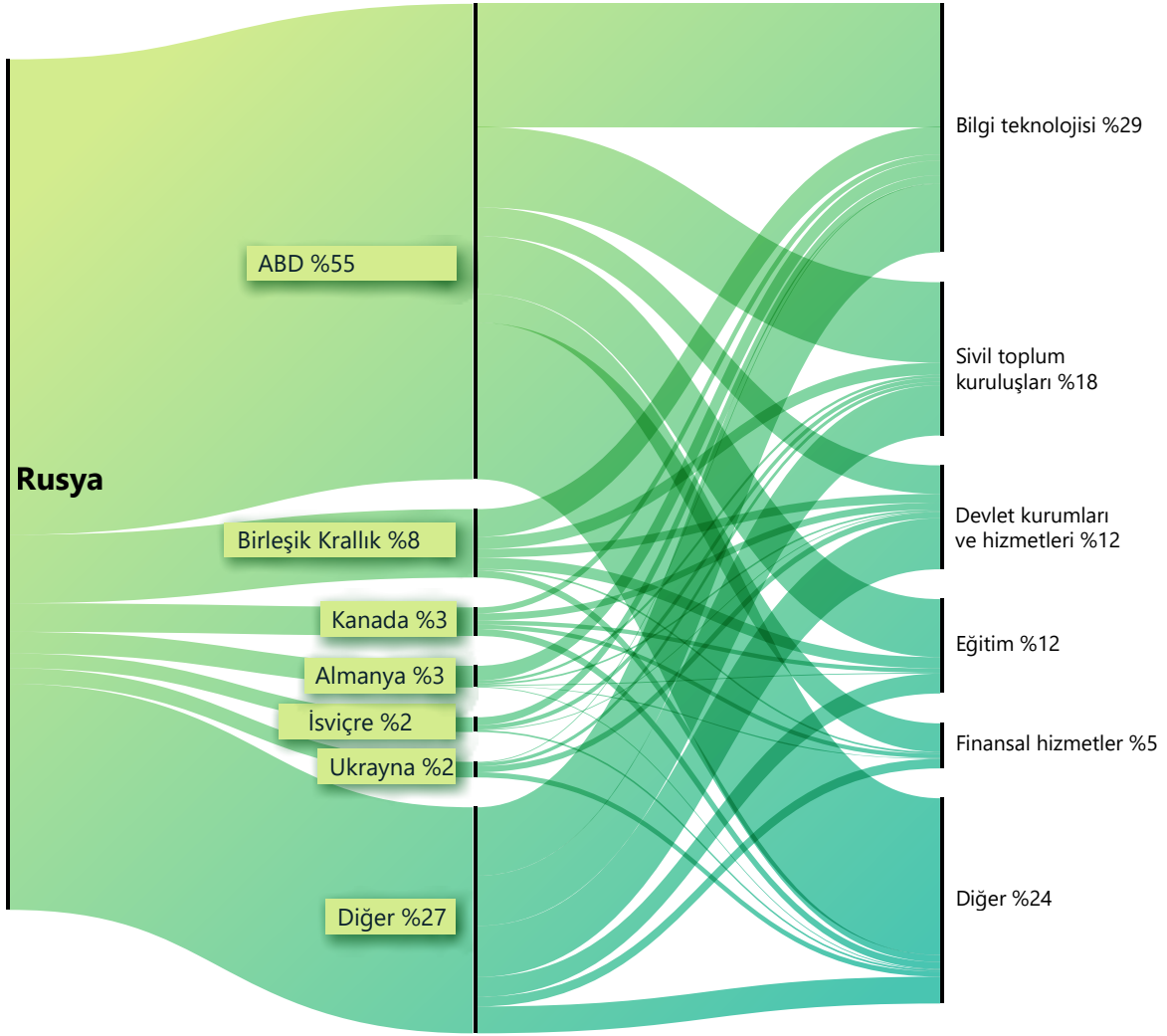
Rus devleti ve ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM ve IRIDIUM gibi Rusya'ya bağlı grupların tümü, Ukrayna içindeki ve dışındaki kurumlarda istenen hesaplara ve ağlara ilk erişimi elde etmek için kimlik avı saldırılarını kullandı. Birçok saldırıda, hedeflenen kurumlardaki veya aynı sektördeki güvenliği aşılmış ve sahte hesaplar ile ilgi çekici temaları kullanarak kurbanları cezbetti. NOBELIUM, dünyanın dört bir yanındaki dışişleri bakanlığı çalışanlarına diplomatik iletişim kılığındaki kimlik avı e-postalarını göndermek için güvenliği ihlal edilmiş diplomatik hesapları kullandı. STRONTIUM, Amerika Birleşik Devletleri'nde bulunan düşünce kuruluşlarındaki hesap sahiplerinin herkese açık adlarını kullanan sahte hesaplar oluşturdu ve bu düşünce kuruluşlarındaki hesaplara erişim elde etmek için kimlik avı mesajları gönderdi. SEABORGIUM, İskandinav ülkelerinde bulunan uluslararası ilişkiler düşünce kuruluşlarındaki hesaplara ilk erişimi elde etmek için Ukrayna'daki çatışmayla ilgili rapor tuzaklarını kullanarak kimlik avı yaptı.

Alt müşterileri etkilemek için BT hizmetleri tedarik zincirinin kullanılması

2021'in sonlarında, Rus devlet aktörleri BT hizmet sağlayıcılarının güvenliğini ihlal etti ve erişimi, web sitesi tahrifatlarını ve Ocak ayında DEV-0586 tarafından Whispergate zararlı malware'inin kurulumunu kolaylaştırmak için kullandı.[12] DEV-0586, Ukrayna Savunma Bakanlığı ve iletişim ve ulaşım sektörlerindeki diğer kurumlar için kaynak yönetim sistemleri oluşturan bir BT firmasının ağını da ele geçirdi ve bu, grubun bu sektörlerde de üçüncü taraf saldırı seçeneklerini araştırdığını gösterdi.

NOBELIUM, dünya çapında, ancak özellikle Amerika Birleşik Devletleri ve Batı Avrupa'da, 2021-2022 yılları arasında hükümete ve diğer hassas ağlara erişim elde etmek için BT hizmet sağlayıcılarını hedef aldı (bu bölümün başlarındaki tedarik zinciri güvenlik açıklarının açıklamasına göz atın).

Rusya: En çok hedeflenen ülkeler ve endüstri sektörleri



2022'nin başlarından beri Ukrayna merkezli kurumlara yoğun bir şekilde odaklanılmasına rağmen, Kuzey Amerika ve Batı Avrupa merkezli işletmeler, Rus aktörlerin en çok hedef aldığı çevrimiçi hizmet müşterileri olmaya devam ediyor. NOBELIUM'un bilişim sektörüne yönelik saldırısı, bu sektörü geçen yıl en çok hedeflenen sektör hâline getirdi.

Rus devlet aktörlerinin savaş zamanı Ukrayna ve ötesini tehdit eden siber taktikleri

Devamı

Ağlara ilk erişimi elde etmek için genel kullanıma yönelik uygulamaların kullanılması

En az 2021'in sonlarından bu yana STRONTIUM, bilgi çalmak için Microsoft Exchange sunucuları gibi genel kullanıma yönelik hizmetlerden yararlanma becerilerini geliştirmek ve iyileştirmek için çabaladı. STRONTIUM, Ukrayna hükümeti hesaplarının yanı sıra Amerika Birleşik Devletleri, Lübnan, Peru ve Romanya'daki askeri ve savunma endüstrisiyle ilgili kurumlar ile Ermenistan, Bosna, Kosova ve Malezya merkezli diğer devlet kurumlarına erişmek için patch uygulanmamış Exchange sunucularından yararlandı. Ayrıca Rus ordusuna bağlı DEV-0586, Ukrayna ve diğer Doğu Avrupa ülkelerindeki hükümet ve BT sektörü kurumlarına ilk erişim elde etmek için Confluence sunucusunun güvenlik açıklarından yararlandı.

Rus devleti ve ona bağlı tehdit aktörleri, aynı TTP'lerin birçoğunu savaş ve barış zamanlarında ilgili kurumların güvenliğini ihlal etmek için kullanıyor.

Ağ keşfi ve yanal hareket için yönetim hesapların ve protokoller ile yerel yardımcı programların kullanımı

Bir ağa ilk erişimi sağladıktan sonra Microsoft, Rus devlet aktörlerinin, tespit edilmekten olabildiğince uzun süre kaçınmak amacıyla temel bakım görevlerini gerçekleştirmek için meşru hesaplardan ve yazılım yardımcı programlarından yararlandığını gözlemledi. Otomatik izlemenin ve ağ savunucularının dikkatini anında çekmeden ağlar içinde yatay olarak hareket etmek için yönetim yeteneklerine ve geçerli yönetim protokollerine, araçlarına ve yöntemlerine sahip güvenliği ihlal edilmiş kimliklere güvendiler.

Temel siber hijyen ve uç nokta algılama ve müdahale araçlarının kullanılması, savaş zamanlarının yanı sıra barış zamanında da bu tür operasyonların olumsuz etkilerinin azaltılmasına yardımcı olabilir.

Devam eden çatışmanın öngörülemezliği, dünya çapındaki kurumların Rus devleti ve Rusya bağlantılı tehdit aktörlerinden kaynaklanan dijital tehditlere karşı siber güvenliği güçlendirmek için önlemler almasını gerektiriyor.

Eyleme dönüştürülebilir içgörüler

1. MFA kimlik koruma araçlarını uygulayarak ve en hassas ve ayrıcalıklı hesapların ve sistemlerin güvenliğini sağlamak için en az ayrıcalıklı erişimi zorunlu kılarak kullanıcılarınızın kimlik korumasını sağlayarak, kimlik bilgisi hırsızlığını ve hesap kötüye kullanımını en aza indirin.
2. Tüm sistemlerinizin mümkün olan en kısa sürede en yüksek düzeyde korumaya sahip olmasını ve güncel kalmasını sağlamak için güncelleştirmeleri uygulayın.
3. Kurumunuz genelinde malware'dan koruma, uç nokta algılama ve kimlik koruma çözümlerini kurun. Eğitimli ve yetenekli personelle birlikte kapsamlı savunma güvenlik çözümlerinin bir kombinasyonu, kurumunuzu etkileyen izinsiz girişleri belirleme, tespit etme ve önleme konusunda kurumunuzu güçlendirebilir.
4. Kritik sistemleri yedekleyerek ve günlüğe kaydetmeyi etkinleştirerek, ortamınıza yönelik bir tehdit algıladığınızda veya bir tehdit bildirimi aldığınızda araştırma ve kurtarmayı etkinleştirin. Bir olay müdahale planının oluşturulması şiddetle tavsiye edilir.

Daha ayrıntılı bilgi için bağlantılar

- Ukrayna'yı Savunmak: Siber Savaştan Çıkarılan İlk Dersler | Microsoft On the Issues
- Ukrayna'daki hibrit savaş | Microsoft On the Issues
- Ukrayna'da siber tehdit etkinliği: analiz ve kaynaklar| Microsoft Güvenlik Yanıt Merkezi (MSRC)
- Ukrayna'yı hedef alan siber saldırıları engellemek | Microsoft On the Issues
- Ukrayna hükümetini hedef alan malware saldırıları | Microsoft On the Issues
- MagicWeb: NOBELIUM'un herhangi biri olarak kimlik doğrulaması için gizlilik ihlali sonrası hilesi | Microsoft Tehdit İstihbarat Merkezi (MSTIC), Tespit ve Müdahale Ekibi (DART), Microsoft 365 Defender Araştırma Ekibi

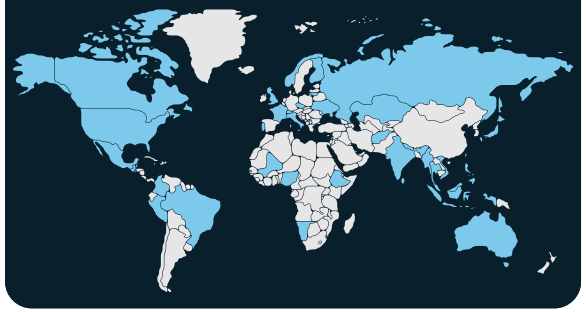
Rekabet avantajı açısından küresel hedeflemeyi genişleten Çin

Günümüzün karmaşık jeopolitik ikliminde, siber operasyonlar yürüten Çin devleti ve devlete bağlı tehdit aktörleri, Çin'in rekabet avantajı elde etme hedefinin bir parçası olarak genellikle ülkenin stratejik olarak askeri, ekonomik ve dış ilişkiler hedeflerini ilerletmeyi amaçlıyor. Geçen yıl Microsoft, dünyanın dört bir yanındaki ülkeleri hedef alan yaygın bir Çin tehdidi faaliyeti gözlemledi.

2021'in ortalarından bu yana Çin, son iki yıldaki en kötü COVID-19 artışının ortasında ekonomik ve finansal istikrarını sağlamak için manevralar yapıyor.[13] Çin, Rusya ile olan "sınırsız" ortaklığını dengeleme mücadelesi gibi jeopolitik olaylardaki konumunu dengelemeye[14] ve dünya sahnesindeki konumunu korumaya devam ediyor.[15] Ayrıca Çin'in Tayvan ve Güney Çin denizi konusunda ABD ve müttefiklerine karşı tutumu[16] birçok ülke ile dış ilişkileri germeye devam ediyor.[17]

Çin devleti ve devlete bağlı tehdit grupları, tüm cephelerde rekabet avantajı elde etmek için Güneydoğu Asya'ya odaklanarak dünya genelinde daha küçük ulusları hedeflemeyi artırdı.

Çin devleti ve devlete bağlı gruplar tarafından hedef alınan ülkeler

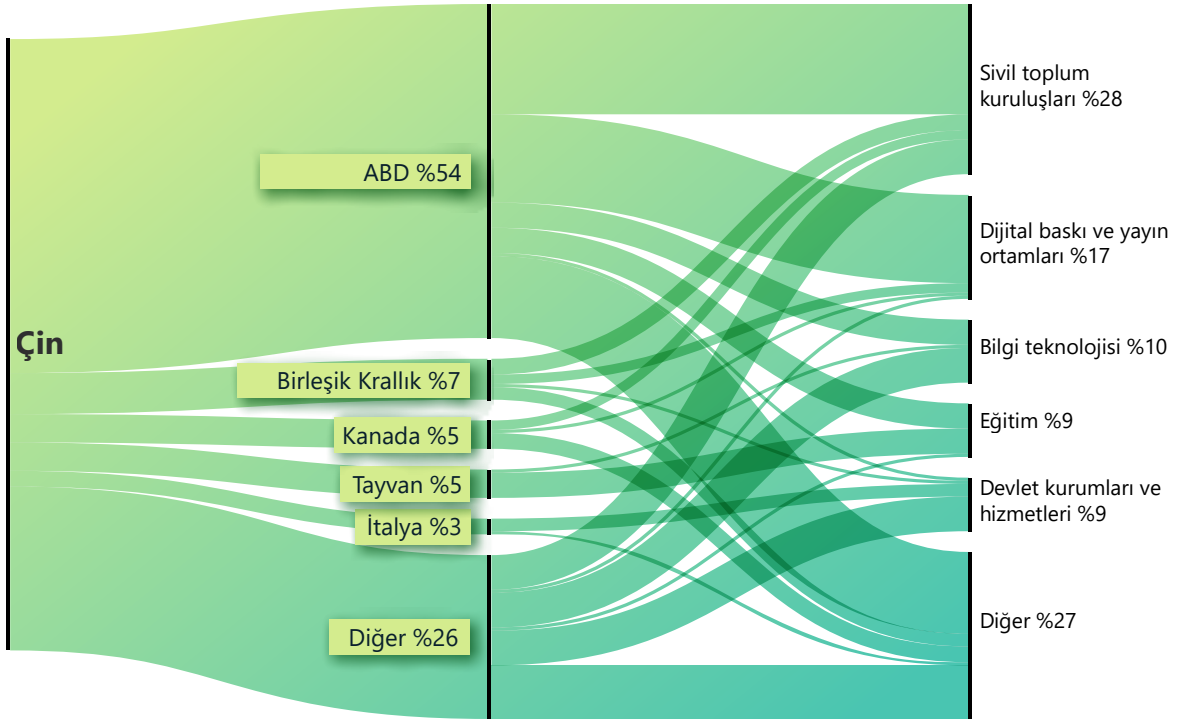


Çin ayrıca, AB ile kapsamlı bir yatırım çerçevesini yeniden canlandırma girişiminde bulunan[18] ve Asya Pasifik'te Bölgesel Kapsamlı Ekonomik Ortaklık olarak bilinen 15 ülkeyle yeni bir bölgesel ticaret anlaşması müzakere eden, daha önce kurulmuş olan Kuşak ve Yol Girişimi (BRI) aracılığıyla ekonomik etkisini küresel olarak genişletmeye devam etti.[19] Microsoft, gözlemlenen siber operasyonlar ve hedeflenen kurumların genişliği nedeniyle Çin'in stratejik siyasi, askeri ve ekonomik hedeflerini ilerletmeye yardımcı olacak bir araç olarak siber koleksiyonu kullanmaya devam edeceği değerlendirmesinde bulunuyor.

Siber hedefleme muhtemelen ekonomik ve askeri çıkarları ilerletecektir.

Microsoft, Çin devleti ve devlete bağlı tehdit grupları tarafından dünyanın dört bir yanındaki küçük ulusların yaygın şekilde hedeflendiğini gözlemledi ve bu da Çin'in küresel ekonomik ve askeri etkisinin bir bileşeni olarak siber casusluğu kullanılmış olabileceğini öne sürdü.

Çin: En çok hedeflenen ülkeler ve endüstri sektörleri



Düşünce kuruluşları/STK'lar, medya, BT, hükümet ve eğitim sektörleri, muhtemelen kalıcı istihbarat toplama ve keşif için Çin merkezli tehdit grupları tarafından en çok hedef alınan sektörler arasındaydı.

Hedeflerin kapsamı, bunlarla sınırlı olmamak üzere Afrika, Karayipler, Orta Doğu, Okyanusya ve Güney Asya'daki ülkeleri içermekte olup, özellikle Güneydoğu Asya ve Pasifik Adaları'ndaki ülkelere odaklanmaktadır.

Çin'in Kuşak ve Yol stratejisine uygun olarak, Çin merkezli tehdit grupları Afganistan, Kazakistan, Mauritius, Namibya ve Trinidad ve Tobago'daki varlıkları hedef aldı.[20] Örneğin, Trinidad ve Tobago, 2018'de Çin'in Kuşak ve Yol stratejisini onaylayan ilk Karayip ülkesi olduğu için Çin, onu bölgede önemli bir ortak olarak görmektedir. NICKEL, 2021'den beri Trinidad ve Tobago'yu hedef alan sürekli ağ operasyonları gerçekleştirdi. Örneğin, Mart 2022'de NICKEL, muhtemelen istihbarat toplama amacıyla bir devlet kurumunu hedef alan keşif faaliyetleri yürüttü.

Rekabet avantajı açısından küresel hedeflemeyi genişleten Çin

Devamı

Bu arada Microsoft, Çin devleti ve devlete bağlı tehdit gruplarının ağ operasyonlarının Güneydoğu Asya'daki varlıklara odakladığını ve Çin'in askeri ve ekonomik önceliklerini ABD'nin bölgeye yeniden ilgisinin getirdiği zorluklarla başa çıkmak için değiştirmesi sebebiyle Pasifik Ada ülkelerine doğru genişlediğini gözlemledi. Ocak 2022'de Microsoft, RADIUM'un Vietnam'da bir enerji kurumunu, enerjiyle bağlantılı bir devlet kurumunu ve bir Endonezya devlet kurumunu hedef aldığını gözlemledi. RADIUM'un faaliyetleri muhtemelen Çin'in Güney Çin Denizi'ndeki stratejik hedefleriyle uyum içindeydi.[21] Şubat sonu ve Mart başında GALLIUM, Güneydoğu Asya bölgesindeki önde gelen bir hükümetler arası kuruluşa (IGO) bağlı 100'den fazla hesabı ele geçirdi. GALLIUM'un bölgedeki IGO'yu hedeflemesinin zamanlaması, ABD ile bölgesel liderler arasında planlanmış bir toplantı duyurusu ile aynı zamana denk geldi. GALLIUM aktörleri, muhtemelen etkinlikten önce iletişimi izlemek ve istihbarat toplamakla görevlendirilmişti.

Çin, Pasifik Ada ülkelerindeki etkisini genişletirken, Çinli tehdit gruplarının faaliyetleri de bunu takip etti. Nisan ayında Çin ve Solomon Adaları, "barışı ve güvenliği teşvik etmeyi" amaçlayan bir güvenlik anlaşması imzaladı. Anlaşma potansiyel olarak Çin'in Solomon Adaları'na silahlı polis ve ordu konuşlandırmasına izin verir.[22] Mayıs ayında Çin, Fiji'de ikinci Çin-Pasifik Ada Ülkeleri (PIC) Dışişleri Bakanları Toplantısına ev sahipliği yaptı ve siyasi, kültürel, sosyal, güvenlik ve iklim değişikliği çıkarlarını ilerletmek ve ayrıca salgınla mücadele etmek için "kapsamlı bir stratejik ortaklık" geliştirmeyi önerdi.[23] Mayıs ayının aynı döneminde Microsoft, GADOLINIUM'un Solomon Adaları hükümet sistemlerindeki malware'larını tespit etti. RADIUM ayrıca Papua Yeni Gine'deki bir telekomünikasyon kurumunun sistemlerinde kötü amaçlı bir kod çalıştırdı. Bu faaliyetlerin, Çin'in genel bölgesel stratejisini desteklemek amacıyla istihbarat toplamak için olabileceği değerlendirmesini yapıyoruz.

Microsoft, NİKEL operasyonlarını engellese de,tehdit grubu ısrarını sürdürüyor.

Aralık 2021'de Microsoft Dijital Suçlar Birimi (DCU), NICKEL tarafından kontrol edilen 42 komuta ve kontrol (C2) etki alanını ele geçirmek için yetki talep eden ABD Virginia Doğu Bölgesi Bölge Mahkemesine dilekçe verdi. Bu C2 etki alanları, Eylül 2019'dan bu yana Orta ve Güney Amerika, Karayipler, Avrupa ve Kuzey Amerika'da hükümetlere, diplomatik kuruluşlara ve STK'lara yönelik operasyonlarda kullanıldı.[24] NICKEL, bu operasyonlar aracılığıyla çeşitli kuruluşlara uzun vadeli erişim sağladı ve 2019'un sonlarından bu yana bazı kurbanlardan sürekli olarak veri sızdırdı.

Çin daha fazla ülkeyle ikili ekonomik ilişkiler kurmaya devam ettikçe (genellikle BRI ile ilgili anlaşmalarda), Çin'in küresel etkisi artmaya devam edecektir. Çin devleti ve devlete bağlı tehdit aktörlerinin, muhtemelen ekonomik casusluk veya geleneksel istihbarat toplama hedefleri peşinde, yeni içgörüler elde etmek için hükümet, diplomasi ve STK sektörlerindeki hedefleri takip edeceklerini değerlendirmesinde bulunduk. Microsoft'un engellemesinden bu yana NICKEL, büyük olasılıkla kaybedilen erişimi yeniden kazanmaya çalışan birkaç devlet kurumunu hedef aldı. Mart sonu ile Mayıs 2022 arasında NICKEL dünya çapında en az beş devlet kurumunun güvenliğini yeniden ele geçirdi. Bu, grubun bu varlıklara ek giriş noktalarına sahip olduğunu veya yeni C2 etki alanları aracılığıyla yeniden erişim elde ettiğini göstermektedir. NICKEL'in küresel olarak aynı devlet kurumlarını defalarca tehlikeye atma konusundaki ısrarı, görevin öneminin üst düzeyde olduğunu gösteriyor.

Çin, dış politikada konusundaki duruşuyla daha iddialı bir konumda. Siber destekli ekonomik casusluğun ve istihbarat toplamanın devam etmesini bekliyoruz.

Eyleme dönüştürülebilir içgörüler

1. Siber tehditleri proaktif olarak azaltmak için siber savunmayı artırın. Çinli tehdit aktörlerinin ısrarı, kurumların olası izinsiz girişleri zamanında belirlemesini, korumasını, tespit etmesini ve yanıt vermesini gerektirmektedir.
2. Tehdit aktörleri, sık kullanılan bir ısrar ve savunmadan kaçma yöntemi olarak zamanlanmış görevleri kullanır.[25] Ortamınızın bu yaygın tekniğe karşı koruma sağlamak için ek güvenlik yönergeleri kullandığından emin olun.[26]
3. Hedeflenen ağlarda ilk vektör olarak web kabuklarının kullanıldığını gözlemlemeye devam ediyoruz.[27] Kurumlar, saldırganların uzaktan komut çalıştırma erişimi sağlayabilen web kabukları saldırılarına karşı sistemlerini güçlendirmelidir.[28]

Daha ayrıntılı bilgi için bağlantılar

- NİKEL, Latin Amerika ve Avrupa'daki devlet kurumlarını hedef alıyor | Microsoft Tehdit İstihbarat Merkezi (MSTIC), Microsoft Dijital Güvenlik Birimi (DSU)
- İnsanları son siber saldırılardan koruma | Microsoft On the Issues

İktidarın el değiştirmesinin ardından giderek daha saldırgan hâle gelen İran

Microsoft, İran devlet gruplarının ve bağlantılı aktörlerin İsrail'e yönelik siber saldırıların hızını ve kapsamını artırdığını, fidye yazılımı saldırılarını bölgesel düşmanların ötesine geçerek ABD ve AB kurbanlarını kapsayacak şekilde genişlettiğini ve potansiyel olarak yıkıcı siber saldırılar için en azından önceden konumlanmak üzere yüksek profilli ABD kritik altyapısını hedef aldığını gözlemledi.

İran devlet aktörlerinin artan siber saldırganlığı, cumhurbaşkanlığı yetkilerinin el değiştirmesini takiben başladı. 2021 yazında, katı Cumhurbaşkanı İbrahim Raisi, ılımlı Cumhurbaşkanı Hassan Rouhani'nin yerini aldı. Yüce Lider'in himayesi ve İslam Devrim Muhafızları Ordusu'nun (IRGC) yakın bir müttefiki olan Raisi'nin tam aksine, eski Cumhurbaşkanı Ruhani'nin diplomasi tutkusu, onu Yüce Lider ve Devrim Muhafızları'nın üst düzey liderleriyle sık sık anlaşmazlığa düşürdü.[29] Raisi yönetiminin savaş yanlısı görüşleri, İran'la nükleer anlaşmayı yeniden canlandırmak için diplomatik etkileşimlerin yeniden başlamasına rağmen, İranlı aktörlerin İsrail, Batı ve özellikle ABD'ye karşı daha cesur adımlar atma isteğini artırmış görünüyor.

İran'ın İsrail'e yönelik siber saldırılarının artan hızı ve kapsamı

Raisi'nin dış politika ekibinin oluşumunu tamamlamasından birkaç hafta sonra,[30] İran devlet aktörleri İsrail'e yönelik yıkıcı siber saldırıları önceki yıla göre daha hızlı bir şekilde yeniden başlattı. Bu fidye yazılımı ile korsanlık ve sızdırma saldırıları, Eylül ayından itibaren birkaç haftada bir gerçekleştirildi ve İran'la bağlantılı en az üç aktörün dahil olması, saldırıların İsrail'e karşı ülke çapında bir misilleme saldırısının parçası olabileceğini düşündürdü. Microsoft, en az bir vakada, 2021'in sonlarında bir İsrail kurumuna yönelik bir fidye yazılımı saldırısının, aslında bir veri silme saldırısını gizleme amaçlı olduğu değerlendirmesinde bulundu. Microsoft malware analizi, kurbana teslim edilen fidye yazılımının şifrelemenin ardından veri silen malware'ları çalıştırmak üzere programlandığını belirledi.

2022 itibarıyla İran siber saldırıları, hedef seçimi ve saldırı biçimleri açısından arttı. Şubat ayında DEV-0198, İsrail'in kritik altyapısına karşı yıkıcı bir saldırı gerçekleştirmeye çalıştı. Microsoft ayrıca, Haziran ayında İsrail'de acil durum roket sirenlerini muhtemelen IP ağları üzerinden sesi ayarlayan bir yazılım kullanarak başlatan karmaşık bir siber saldırıdan büyük olasılıkla İran bağlantılı bir aktörün sorumlu olduğunu değerlendirdi.

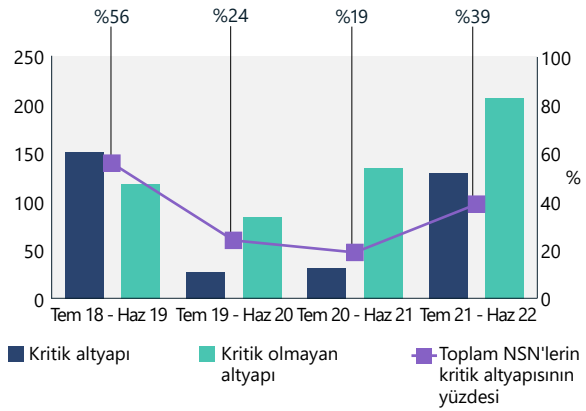
İran'ın ABD ve İsrail'in kritik altyapısına yönelik tehdidi yıl boyunca arttı

Microsoft'un IRGC'ye bağlı olduğu değerlendirmesinde bulunduğu İran devlet aktörleri (PHOSPHORUS ve DEV-0198), 2021'in sonlarından 2022'nin ortalarına kadar yüksek profilli ABD ve İsrail kritik altyapısını hedef aldı. Muhtemel amaç, Tahran'a, üst düzey Devrim Muhafızları yetkililerinin ABD ve İsrail'i İran'da kesintiye uğratmakla suçladıkları sektörlere misilleme yapma seçeneği sağlamaktı.[31] Bu etkinliğin, rejim içindeki diğer etkili isimlerin ABD ve İsrail tarafından İran'ın limanlarına, demiryollarına ve yakıt istasyonlarına siber saldırılar düzenlediği yönündeki suçlamalarını yineleyen İran'ın Pasif Savunma Örgütü başkanı Devrim Muhafızları Generali Gholamreza Jalali'nin Ekim 2021'in sonlarında yaptığı açıklamalara bağlı olduğunu değerlendiriyoruz.[32] Celali, cuma namazı hutbesi sırasında "ABD" kelimelerini vuran bir füze görüntüsünün olduğu sahnede yaptığı hazırlık konuşmasında ikinci kez bu suçlamayı dile getirdi ve üst düzey yöneticilerinin de aynı görüşte olduğunu ima etti.[33]

PHOSPHORUS, yama uygulanmamış Fortinet ve ProxyShell güvenlik açıkları için Ekim 2021'de ABD kurulumlarına yönelik geniş çapta bir tarama başlattı. Bu yamasız sistemlerin güvenliğinin iptal edildiği birkaç durumda, Amerika Birleşik Devletleri ve diğer Batılı ülkelerdeki kritik altyapıya karşı fidye yazılımı saldırıları gerçekleştirmek için kullanıldı. Bunlar, İran devletinin Orta Doğu dışındaki fidye yazılımı saldırılarının ilk doğrulanmış vakaları oldu. Ekim ayı sonlarında İran'ın benzin istasyonlarına yönelik siber saldırının ardından Microsoft, İran'ın ABD kurumlarına yönelik fidye yazılımı saldırılarında olası bir korelasyona işaret eden bir artış gözlemledi.

Aynı zamanda, PHOSPHORUS, büyük limanlar ve ülkeye giriş havaalanları, transit sistemler, kamu hizmeti kurumları ve petrol ve gaz kurumları dahil olmak üzere yüksek profilli ABD kritik altyapı kurumlarını, genellikle hedef odaklı kimlik avı yoluyla, yönlendirilmiş hedeflemeye geçti. Genellikle hedef odaklı kimlik avı yoluyla gerçekleştirilen bu hedefleme, 2022'nin ortalarına kadar sürdü. Hedefler, Tahran'ın ABD ve İsrail'i İran'a saldırmakla suçladığı sektörlerle doğrudan uyuşmaktadır ve muhtemelen İran'a misilleme seçenekleri sağlamıştır. Neredeyse aynı hedeflerin güvenlik ihlali, suçu kabul etmeden saldırıların nedenini işaret ederek artışı önlemeye çalışırken, gelecekteki bu tür saldırıları caydırmak için bir fırsat sağlayacaktır.

İran'ın tekrar altyapıyı hedef almaya başlaması



İran'ın kritik altyapıyı hedef alması, 2018'in sonlarından 2019'un başlarına kadar gözlemlenen en yüksek seviyelere yükseldi. Bir kurumun kritik altyapı kriterlerine uyup uymadığını belirlemek için ABD Başkanlık Politika Direktifi 21'i (PPD-21) kullandık. (Temmuz 2021–Haziran 2022).

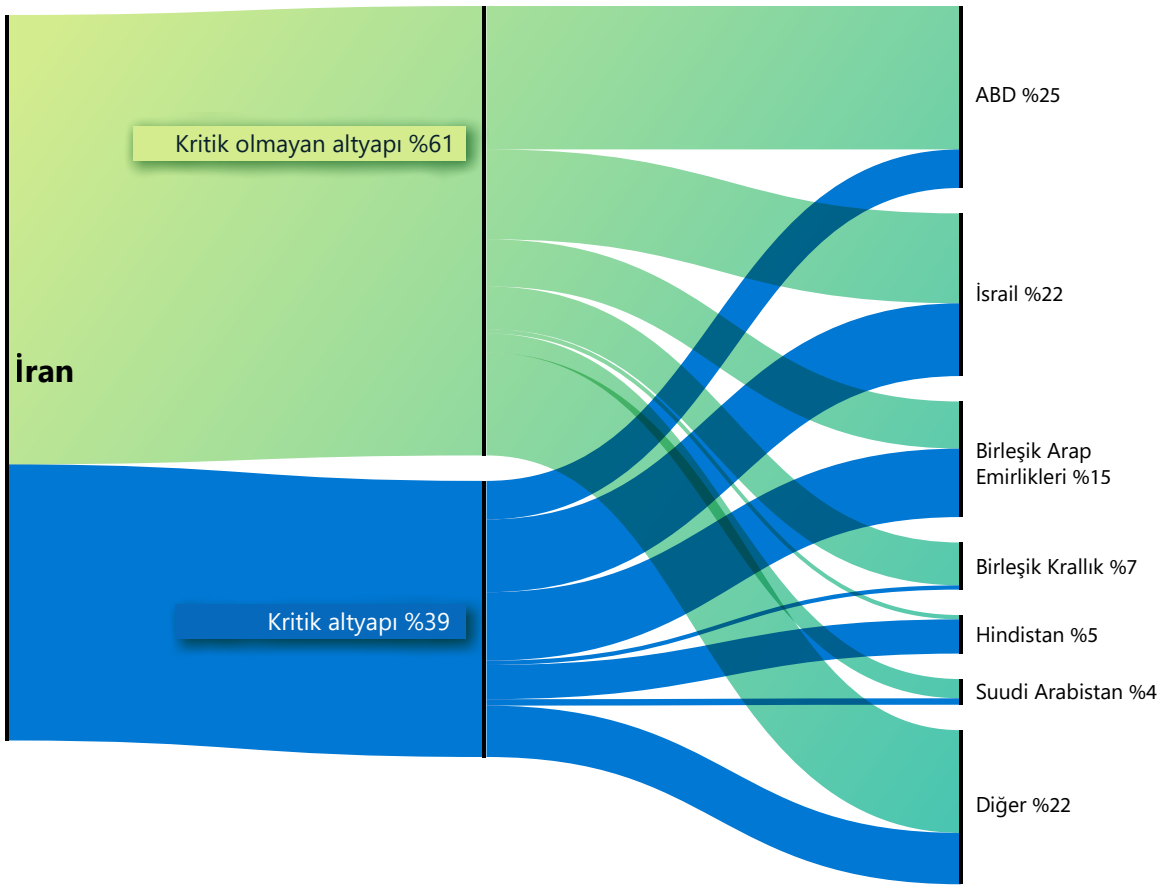
İktidarın el değiştirmesinin ardından giderek daha saldırgan hâle gelen İran

Devamı

İsrail'de DEV-0198, benzin istasyonlarına odaklanarak İsrail demiryollarını, lojistik kurumlarını, lojistik kurumlarının yazılım sağlayıcılarını ve akaryakıt kurumlarını hedef aldı. 2022'nin başlarında grup, büyük bir İsrail lojistik kurumunun ağına yıkıcı bir saldırı düzenledi ve bu saldırı, kurumu saldırıyı kontrol altına almak için bilgisayarlarını ve bazı operasyonlarını kapatmaya zorladı. Başka bir olayda, grubun çalınan veya yeniden kullanılan kimlik bilgileriyle büyük bir İsrail ulaşım sağlayıcısının ağına erişmeye çalıştığını gözlemledik. Bu sırada, savunma, deniz taşımacılığı ve uydu görüntü kurumlarını hedeflemesi Devrim Muhafızları ile bağlantıları olduğunu düşündüren başka bir İranlı aktör olan DEV-0343, 2021'in başlarında İsrail ulaşım ve limanla ilgili kurumlarındaki hesaplarını ele geçirdi.

İranlı tehdit grupları, özellikle İran nükleer anlaşmasını yeniden canlandırmaya yönelik diplomatik çabalar zayıflarken ve Washington, Tel Aviv ve Tahran tavizleri kaldırmak için zorlayıcı alternatif yöntemler ararken, ABD ve İsrail ulaşım ve enerji kurumları için bir tehdit olmaya devam edecek gibi görünüyor.

Ülkelere göre İran kritik altyapı hedeflemesi



İran'ın kritik altyapıyı hedef alması, en belirgin şekilde İsrail, Birleşik Arap Emirlikleri ve ABD kurumlarına karşı gerçekleşti.

İranlı aktörlerin önümüzdeki yıl ABD ve İsrail ulaşım ve enerji kurumları için bir tehdit olmaya devam etmesi muhtemel.

İranlı gruplar, fidye yazılımı saldırılarını bölgesel düşmanların ötesine genişletti ve yüksek profilli ABD ve İsrail kritik altyapı hedeflerine yöneldi.

Eyleme dönüştürülebilir içgörüler

1. MFA gibi parolasız çözümlere olanak tanıyarak ve potansiyel kimlik bilgisi güvenlik ihlallerini azaltmak için tüm uzaktan bağlantılarda bu çözümlerin kullanılmasını zorunlu kılarak kurumunuz genelindeki siber hijyeni iyileştirin.
2. Gönderen adresinin meşru olduğundan emin olmak için tüm gelen e-posta trafiğinin orijinalliğini değerlendirin.
3. Erken ve sık aralıklarla yama yapın.[34]
4. Kurumunuz ve yukarı akış sağlayıcıları arasındaki gereksiz izinleri en aza indirmek için hizmet sağlayıcılarıyla iş ortağı ilişkilerinizi gözden geçirin ve denetleyin. Microsoft, yabancı görünen veya henüz denetlenmemiş tüm iş ortağı ilişkilerine erişimin hemen kaldırılmasını önerir.[35]

Daha ayrıntılı bilgi için bağlantılar

- İran'ın artan BT sektörü hedeflemesi | Microsoft Tehdit İstihbarat Merkezi (MSTIC), Microsoft Dijital Güvenlik Birimi (DSU)
- İran bağlantılı DEV-0343 savunma, CBS ve denizcilik sektörlerini hedefliyor | Microsoft Tehdit İstihbarat Merkezi (MSTIC), Microsoft Dijital Güvenlik Birimi (DSU)

İsrail'i hedef alan İran bağlantılı ve Lübnan merkezli grup

Microsoft, platform, hedeflenen kurban veya coğrafi bölge ne olursa olsun siber tehdit etkinliklerini izler. Müşterilerimiz için daha iyi tespitler kaleme almak için dünya çapında görünürlüğümüzü sürdürerek aktif tehdit avcılığı yapıyoruz.

Rusya, Çin, İran ve Kuzey Kore'den gelen tehditler, gözlemlediğimiz ulus devlet aktörü faaliyetlerimizin çoğunluğunu oluştursa da, NATO üyesi ülkeler ve demokratik ülkelerden gelen tehditleri de takip ediyor ve bunlar hakkında bilgi veriyoruz. Geçen yıl Türkiye merkezli bir aktörün (SILICON) ve Vietnam merkezli bir aktörün (BISMUTH) faaliyetlerine yer verdik. Bu yıl, daha önce kamuya açıkladığımız Lübnan merkezli bir grubun ayrıntılarını detaylandırıyoruz.[36]

Microsoft, İran'ın İstihbarat ve Güvenlik Bakanlığı'na (MOIS) bağlı aktörlerle koordineli olarak faaliyet gösterdiğini orta düzeyde emin olarak değerlendirdiğimiz, daha önce belgelenmemiş Lübnan merkezli bir grubu ortaya çıkardı. Tahran'dan gelen bu tür bir işbirliği veya yönlendirme, 2020'nin sonlarından bu yana İran Hükümeti'nin siber operasyonlar yürütmek için üçüncü tarafları kullandığına dair ifşaatla uyumlu olacak ve bu da muhtemelen İran'ın olası inkarının gerçekliğini artıracaktır.

Gözlemlenen etkinlikte POLONIUM, Microsoft etkinliğini kesintiye uğratıp kamuya açıklamadan önce Şubat ve Mayıs 2022 arasında iki düzine İsrail merkezli kurumu ve Lübnan'da operasyonları olan bir IGO'yu hedef aldı veya tehlikeye attı. İsrail örgütlerinin neredeyse yarısının İsrail savunma endüstrisinin bir parçası olması veya İsrail merkezli savunma kurumlarıyla bağlantıları olması, grubun İsrail hakkında istihbarat toplama ve/veya doğrudan İsrail'e karşı koyma konusunda İran'la benzer çıkarları olduğunu gösteriyor.[37]

POLONIUM'un MOIS gruplarıyla değerlendirilen bağlantıları, gözlemlenen kurban çakışmalarına ve araç ve tekniklerin ortak yönlerine dayanmaktadır.

- Kurban çakışması: Microsoft'un MERCURY olarak takip ettiği, İran'ın MOIS gruplarıyla bağlantılı bir İran devlet grubu, daha önce birden fazla POLONIUM kurbanını tehlikeye atarak, görev gereksinimlerinin bir uyumluluk gereksinimine veya kurbanların gruplar arasında olası bir "aktarılma" durumuna işaret ediyor.
- Yaygın kullanılan araçlar ve teknikler: POLONIUM'a benzer şekilde MSTIC, DEV-0588'in (CopyKittens olarak da bilinir) operasyonları için yaygın olarak AirVPN kullandığını ve DEV-0133'ün (Lyceum[38] olarak da bilinir) C2 ve veri hırsızlığı için OneDrive kullandığını gözlemledi. İran devlet aktörlerine benzer şekilde POLONIUM, bir İsrail havacılık kurumunu ve hukuk firmasını tehlikeye atmak için bir bulut hizmeti sağlayıcısı kullandı..[39]

POLONIUM, C2 ve veri hırsızlığı için bulut hizmetlerini (özellikle OneDrive ve DropBox) kullanan bir dizi özel implant kurdu. POLONYUM genellikle tespit edilmekten kaçınması muhtemel hedefler için benzersiz OneDrive uygulamaları oluşturmuştur.

Haziran 2022 itibarıyla Microsoft, POLONIUM tarafından oluşturulan 20'den fazla OneDrive uygulamasına erişimi askıya aldı, etkilenen kurumları bilgilendirdi ve POLONIUM tarafından geliştirilen araçları karantinaya almak için bir dizi güvenlik istihbaratı güncellemesi kurdu.

Microsoft, POLONIUM'un OneDrive'ı C2 olarak kötüye kullanmasını başarıyla tespit etti ve devre dışı bıraktı.

Eyleme dönüştürülebilir içgörüler

1. İlgili göstergeleri algılamak için virüsten koruma araçlarını güncelleyin[40] ve bulut korumasının[41] açık olduğundan emin olun.
2. Hizmet sağlayıcı ilişkisi olan müşteriler için, kurumunuz ile yukarı akış sağlayıcıları arasındaki gereksiz izinleri en aza indirmek için tüm iş ortağı ilişkilerinin gözden geçirildiğinden ve denetlendiğinden emin olun.[42] Bilmediğiniz veya denetlenmemiş tüm iş ortağı ilişkilerine erişimi hemen kaldırın.

Daha ayrıntılı bilgi için bağlantılar

- İsrail kurumlarını hedef alan POLONIUM faaliyetini ve altyapısını ifşa etmek | Microsoft Tehdit İstihbarat Merkezi (MSTIC), Microsoft Dijital Güvenlik Birimi (DSU)
- MERCURY, İsrail kurulumlarını hedef almak için yamasız sistemlerdeki Log4j 2 güvenlik açıklarından yararlanıyor | Microsoft Tehdit İstihbarat Merkezi (MSTIC), Microsoft 365 Defender Araştırma Ekibi, Microsoft Defender Tehdit İstihbaratı

Rejimin üç ana hedefine ulaşmak için Kuzey Kore tarafından kullanılan siber yetenekler

Kuzey Kore'nin son bir yılki siber öncelikleri,hükümetin belirtilen küresel önceliklerini yansıtmaktaydı. Kim Jong Un, birkaç önemli adreste savunma kapasitesi oluşturma, ülkenin zor durumdaki ekonomisini destekleme ve iç istikrarı sağlama şeklindeki üç önceliği vurguladı.[43] Kuzey Kore devlet aktörlerinin attığı adımlar, siber teknolojinin bu üç amaca ulaşmak için kullanıldığını açıkça göstermektedir.

Kuzey Kore devlet aktörleri, dünyanın dört bir yanındaki havacılık ve uzay kurumlarına sızmaya çalışmak için çeşitli taktikler kullandı.

Başta CERIUM ve ZINC olmak üzere Kuzey Kore devlet tehdit grupları, dünya çapındaki savunma ve havacılık kurumlarının ağlarına sızmak için çeşitli taktikler kullandı. Kuzey Kore, 2022'nin ilk yarısında şimdiye kadarki en agresif füze testi dönemine girerken, Kuzey Koreli araştırmacıların yerli savunma sistemleri geliştirmede avantaj elde etmelerine ve rakiplerinin kaydettiği ilerlemelere karşı önlemler almalarına yardımcı olmak için siber casusluğu kullandı.

COPERNICIUM'un, Kuzey Kore'nin zor durumdaki ekonomisini desteklemeye yardımcı olmak için dünya çapında çeşitli kripto para birimiyle ilgili kurumları hedeflediğini gözlemledik. Grubun bir uzlaşmanın ardından para çalıp çalmadığını doğrulayamasak da, COPERNICIUM'un diğer kripto para kurumlarından yapılan tekliflermiş gibi görünen kötü amaçlı belgeler göndererek düzinelerce makineye bulaştığını gözlemledik.

Son olarak, Microsoft'un izlediği bir grup olan DEV-0215, Kuzey Kore sorunları hakkında haber yapan haber kurumlarını hedef alarak Kuzey Kore'de istikrar ve sadakati korumak için çalıştı. Bu kurumların hem Kuzey Kore'de hem de Pyongyang'ın varoluşsal bir tehdit olarak gördüğü sığınmacı topluluklarında kaynakları vardır. Buna ek olarak, grup, Kuzey Kore'ye karşı açık sözlü olma eğiliminde olan ve Kuzey Koreli sığınmacılarla aktif olarak çalışan Korece konuşan Hıristiyan grupların ağlarına erişim elde etmek için çalıştı.

Savunma ve havacılık kurumlarının hedef alınması

CERIUM ve ZINC liderliğindeki Kuzey Kore devlet aktörleri, savunma ve havacılık kurumlarına sızmayı amaçlayan taktikler geliştirmek için önemli bir çaba sarf etti. CERIUM, istemcileri indirerek ve zayıflıkları arayarak Güney Kore sanal özel ağlarını (VPN'ler) defalarca araştırdı. Ayrıca, büyük olasılıkla güvenlik açıklarını arayan Güney Kore ordusu ve hükümet müşterileri tarafından kullanılan yaygın uygulamaları da indirdi. Grup, güncel olayları yakından takip etti ve malware'a sahip yürütülebilir dosyalara ve bağlantılara tıklamaya teşvik etmek için yüksek profilli konuları yem olarak kullanan yeni yem belgeleri yazdı.

ZINC de CERIUM da, saldırılarda sosyal medyayı ve sosyal mühendisliği kullandı. ZINC, operatörlerinin büyük savunma ve havacılık kurumları için işe alım görevlileri gibi göründüğü LinkedIn ve diğer profesyonel sosyal medya sitelerinde sahte profiller oluşturmakta özellikle uzmandı. Bu profiller ile, sosyal medya veya e-posta üzerinden doğrudan mesajlar göndererek potansiyel kurbanlara bağlantılar veya kötü amaçlı dosya ekleri gönderdiler.

CERIUM, kurum çalışanlarına ek olarak, hem Güney Kore askeri akademilerine hem de akademide çalışan askeri üyelere özel ilgi göstererek, kapsamlı bir şekilde Güney Kore ordusu üyelerini hedef aldı.

Kayıpları dengelemek için kripto para birimini hedef alma

2016'da BM yaptırımlarının uygulanmasından bu yana, sel[44] ve kuraklık[45] gibi doğal afetlerin yanı sıra 2020'nin başlarında COVID-19 salgınının başlamasından ile sınırların ithalata neredeyse tamamen kilitlenmesi sonucunda Kuzey Kore ekonomisi daralmaya devam etti.[46] Kuzey Kore, 2022'nin başlarında Çin ile ticaret için sınırlarını kısa bir süreliğine açsa da kısa süre sonra tekrar kapatıldı.[47] Mayıs ortasında, Kuzey Kore ilk yerel COVID-19 vakasını bildirdi.[48] O zamandan beri, Kuzey Kore'nin zaten kırılgan olan ekonomisini olumsuz etkileyen virüsle savaşmak için Çin tarzı bir "sıfır COVID" toplu karantina stratejisi uyguladı.

Kuzey Kore devlet grubu COPERNICIUM, ağlarına nüfuz edebildiği herhangi bir kurumdan, genel olarak kripto para birimi biçiminde, para çalarak, kaybedilen gelirin bir kısmını telafi etmeye çalıştı. Amerika Birleşik Devletleri, Kanada, Avrupa ve Asya genelinde kripto para birimi ile ilişkili kurumlara ait düzinelerce makinenin ele geçirildiğini gördük. COPERNICIUM, hem anakarada hem de Hong Kong'da Kuzey Kore'nin en güçlü müttefiki olan Çin'deki kripto para birimiyle ilişkili kurumlara ait makineleri bile ele geçirdi. Grup, erken keşifleri ve hedeflere yaklaşımları için büyük ölçüde sosyal medyaya güvendi. Aktörler, kripto para birimi ile ilişkili işletmelerde geliştirici veya kıdemli memurmuş gibi davranan profiller oluşturdular. Daha sonra da, sektördekilerle ilişkiler ve yakınlık kurduktan sonra kötü amaçlı bağlantılar veya dosyalar gönderdiler.

Rejimin üç ana hedefine ulaşmak için Kuzey Kore tarafından kullanılan siber yetenekler

Devamı

PLUTONIUM ile ilişkili bir grup fidye yazılımı geliştirip dağıtıyor

Microsoft'un DEV-0530 olarak izlediği Kuzey Kore kökenli bir grup aktör, Haziran 2021'de fidye yazılımı geliştirmeye ve saldırılarda kullanmaya başladı. Kendilerine H0lyGh0st adını veren bu grup, saldırıları için aynı adı taşıyan bir fidye yazılımı yükü kullandı ve Eylül 2021 gibi bir tarihte birden fazla ülkedeki küçük işletmeleri başarıyla ele geçirdi.

Microsoft, DEV-0530'un PLUTONIUM (DarkSeoul veya Andariel olarak da bilinir) olarak izlenen Kuzey Kore merkezli başka bir grupla bağlantıları olduğu değerlendirmesinde bulundu. H0lyGh0st fidye yazılımının saldırılarda kullanımı DEV-0530'a özgü olsa da, MSTIC, PLUTONIUM tarafından özel olarak oluşturulan araçları kullanarak iki grup arasındaki iletişimleri ve DEV-0530'u gözlemledi.

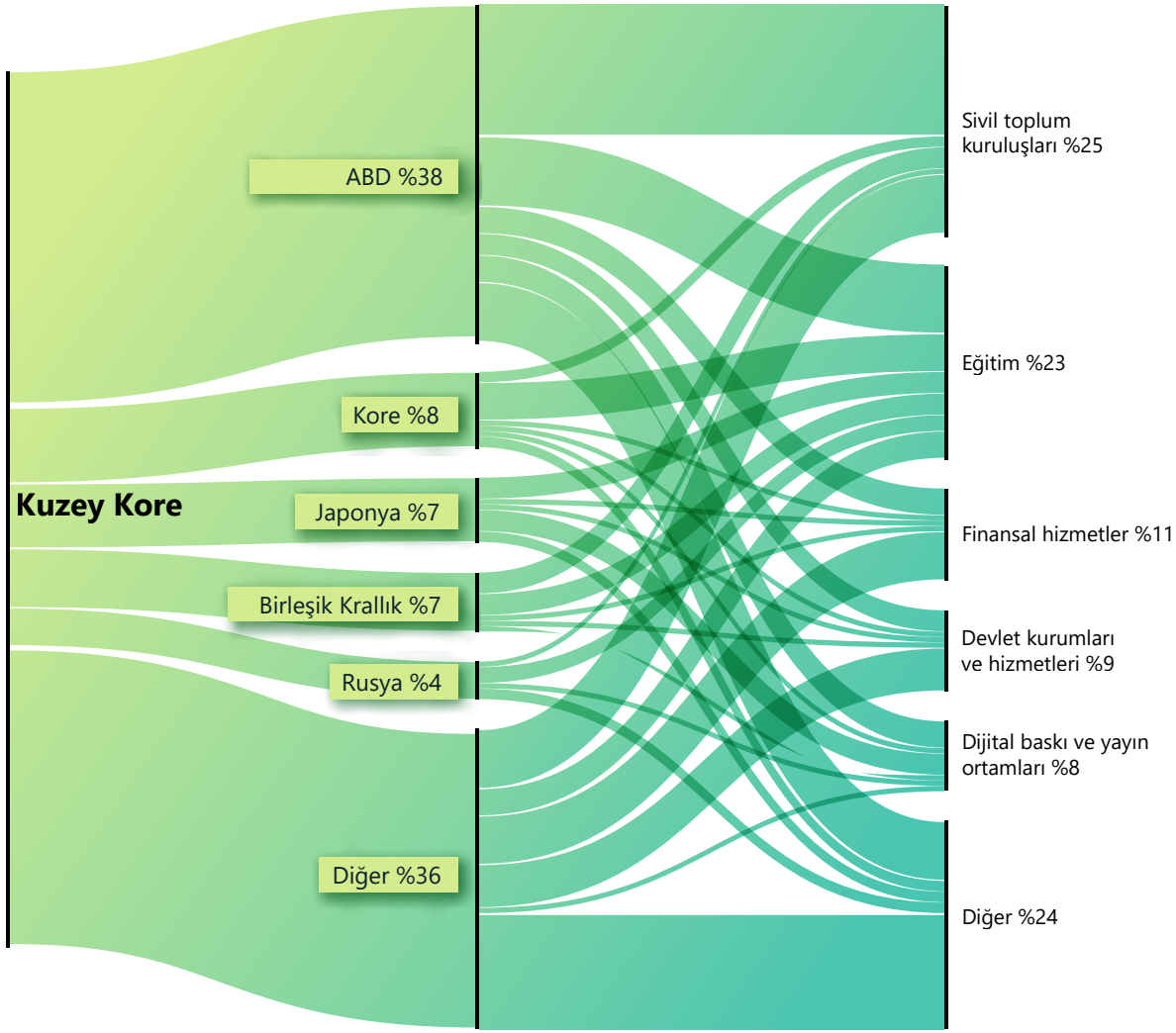
DEV-0530 etkinliğinin devlet destekli olup olmadığı kesin olarak bilinmemektedir. Fidye yazılımı saldırıları, kripto para kurumlarına karşı hırsızlık yapılmasına destek olunmasıyla aynı nedenle devlet tarafından emredilmiş olabilse de, DEV-0530'un arkasındaki aktörlerin kendileri adına para kazanmak için bağımsız hareket etmeleri de mümkündür. Bunu yapanlar bağımsız çalışan Kuzey Koreli bilgisayar korsanları olsaydı, bu, kripto para kurumlarına karşı devlet destekli hırsızlık operasyonlarına kıyasla etkinliğin neden yaygın olmadığını açıklardı.

Kuzey Kore haber kurumlarının, sığınmacıların, dini grupların ve yardım kuruluşlarının hedef alınması

Geçen yıl, Yüce Lider Kim Jong Un, kamuoyunda füzeler ve nükleer silahlardan çok iç güvenlik ve sadakate odaklandı. Bu kaygıyı iç meselelerle birlikte yansıtan en az iki Kuzey Kore devlet grubu, rejimin iç tehdit olarak göreceği yönlere odaklandı.

İlki, Microsoft'un DEV-0215 adıyla izlediği ve Kuzey Kore haberlerini yakından takip eden medya kurumlarını hedefleyen bir gruptu. Bu hedeflemenin olası nedenlerinden biri, bu medya kurumlarının haberlerini dış dünyayla iletişim kurmak için çeşitli yöntemler kullanan Kuzey Kore kaçaklarından, Kuzey Kore ile yakın bir şekilde çalışan Çin vatandaşlarından ve hatta ülke içinde yaşayan bazı Kuzey Kore vatandaşlarından almasıdır. Kuzey Kore hükümeti, bu grupları, özellikle de Kuzey Kore'de hain ve casus olarak görülebilecek vatandaşları, hayatta kalması için varoluşsal bir tehdit olarak görmektedir. DEV-0215 muhtemelen, olası bilgi sızıntılarını etkisiz hâle getirebilmek için bu çıkış noktalarının kaynaklarını belirlemeye çalıştı.

Kuzey Kore: En çok hedeflenen ülkeler ve endüstri sektörleri



Kuzey Kore, ABD, Güney Kore ve Japonya'yı birincil düşmanları olarak görür. Rusya uzun süredir müttefikleri olsa da, Kuzey Koreli tehdit aktörleri, Rus düşünce kuruluşlarını, akademisyenleri ve diplomatik yetkilileri Rusya'nın küresel ilişkiler hakkındaki görüşleriyle ilgili istihbarat elde etmek için hedef almaktadır.

Rejimin üç ana hedefine ulaşmak için Kuzey Kore tarafından kullanılan siber yetenekler

Devamı

Microsoft ayrıca DEV-0215'in Korece konuşan Hıristiyan topluluklarını hedef aldığına dair kanıtlar gördü. Protestan Hıristiyan Kore kiliseleri, Kuzey Kore ile etkileşimi destekleyen Kuzey Kore ve Güney Kore hükümetlerini eleştirme eğilimindedir. Bu kiliselerin büyük olasılıkla amacı amacı bazıları Kuzey Kore ile insani yardım çalışmaları yürütürken ,sığınmacılara yardım etmektir. Kuzey Kore onları bir tehdit olarak görür çünkü salgın sırasında Kuzey Kore'den gelen sığınmacı yoğunluğu neredeyse tamamen durmuşken,[49] bu Hıristiyan gruplar genellikle kaçan sığınmacıların kaçmasına yardım etmede kritik bir rol oynadılar. DEV-0215, grubu hedef almak ve ilticaların organize edilmesine kimin yardım ettiğini keşfetmek için yem olarak Korece konuşanlara yönelik Hıristiyan konferansları ile ilgili sahte belgeler oluşturdu.

Son olarak OSMIUM devlet grubu, geçmişte Kuzey Kore'ye yardım etmiş kurumlar da dahil olmak üzere yıl boyunca uluslararası yardım kuruluşlarına sürekli olarak ilgi gösterdi. Kuzey Kore, özellikle COVID-19'un patlak vermesinden bu yana, ülke dışından gelen yardım tekliflerinden genel olarak kaçınsa da,[50] yardım tekliflerini kabul etmeyi değerlendiriyor olabilir, ancak yabancı yardım görevlilerinin ülkeye girmesine ilişkin güvenlik sonuçları konusunda temkinli olması olasıdır. Kuzey Kore, bu tür bir yardımın kendi ülkelerine girmesine izin verip vermeyeceğini belirlemek için dünya çapındaki yardım kurumlarının ağlarına sızıyor olabilir.

Eyleme dönüştürülebilir içgörüler

1. Kuzey Kore devlet aktörleri yetenekli, amansız ve yaratıcı olsa da, kurumlar onlara karşı savunma yapabilir.
2. Başarılı saldırıların çoğu, iki faktörlü kimlik doğrulama veya sanal ortamda bilinmeyen kişilerden gelen eklerin açılmaması gibi temel bir siber hijyen ile durdurulabilir.

Daha ayrıntılı bilgi için bağlantılar

- Kuzey Koreli tehdit aktörü, H0lyGh0st fidye yazılımı ile küçük ve orta ölçekli işletmeleri hedefliyor | Microsoft Tehdit İstihbarat Merkezi (MSTIC), Microsoft Dijital Güvenlik Birimi (DSU)

Kuzey Kore uzmanları arasında, Kuzey Kore hükümetinin kamuya yaptığı açıklamalarda ciddi olup olmadığı veya etkileri için sahte bir tutum sergileyip sergilemediği konusunda uzun süredir tartışmalar mevcut. Siber saldırıların Kuzey Kore'nin duyurulan öncelikleriyle uyumlu hâle getirilmesi, Kuzey Kore'nin hedeflerini kamuya açıklarken söylediklerinin inandırıcılığını doğrulamaktadır.

Siber paralı askerler siber uzaydaki istikrarı tehdit ediyor

Genellikle hükümetler olmak üzere müşterilerinin, ağlara, bilgisayarlara, telefonlara ve internete bağlı cihazlara girmesine olanak tanıyan araçlar, teknikler ve hizmetler geliştirip satan özel kurumlardan oluşan, büyüyen bir sektör mevcut. Ulus devlet aktörleri için bir varlık olan bu oluşumlar genellikle muhalifleri, insan hakları savunucularını, gazetecileri, sivil toplum savunucularını ve diğer vatandaşları tehlikeye atar. Bu oluşumları siber paralı askerler veya özel sektör saldırı aktörleri olarak adlandırırız.

Özel sektördeki kurumların siber silahlar üretip sattığı bir dünya tüketiciler, her büyüklükteki işletme ve hükümetler için fazlasıyla tehlikelidir. Bu saldırı araçları, iyi yönetişim ve demokrasinin normları ve değerleriyle tutarsız şekillerde kullanılabilir. Microsoft, insan haklarının korunmasının temel bir yükümlülük olduğuna inanmaktadır ve dünya genelinde "bir hizmet olarak gözetim" anlayışını azaltarak ciddiyetimizi göstermekteyiz.

Microsoft, demokratik ve otoriter rejimlerdeki belirli devlet aktörlerinin "bir hizmet olarak gözetim" teknolojisinin geliştirilmesi veya kullanılması için dış kaynaklar kullandığını değerlendirdi. Bu şekilde sorumluluk ve gözetimden kaçınmanın yanı sıra yerel olarak geliştirilmesi zor olan yetenekler kazanırlar.

> Bu siber silahlar, ulus devletlere tek başlarına geliştiremeyecekleri izleme yetenekleri sağlar.

Siber paralı askerlerin faaliyet gösterdiği pazar şeffaf değildir. Yine de, bu grupların hiçbir kurban etkileşimi gerektirmeyen sıfır gün açıkları ve hatta sıfır tıklama açıkları kullandığını ve bir hizmet olarak gözetime olanak sağladığını gözlemlemeye devam ediyoruz.

Microsoft kısa bir süre önce DSIRF adındaki Avusturya merkezli bir PSOA olan KNOTWEED olarak adlandırdığımız bir Avrupa özel sektör saldırı aktörünü duyurdu. Çok sayıda haber, kurumu Subzero adlı bir malware araç setinin geliştirilmesi ve satılmaya çalışılmasıyla ilişkilendirdi.[51] Kurbanlar arasında Avusturya, İngiltere ve Panama gibi ülkelerdeki hukuk firmaları, bankalar ve stratejik danışmanlıklar yer almaktadır.[52]

Bu saldırı gözetim yetenekleri artık savunma ve istihbarat teşkilatları tarafından oluşturulan çok gizli yetenekler değil, kurumlara ve bireylere sunulan ticari ürünler olduğu için, siber silahlara yönelik herhangi bir düzenleyici rejimin ihracat kontrolünün ötesine geçmesi gerekiyor. Bu siber silahların etkisi yıkıcı olabilir.

Bir siber paralı asker, bir ürün veya hizmetteki bir güvenlik açığından yararlandığında, tüm bilişim ekosistemini riske atar. Güvenlik açıkları kamuya açık olarak tanımlandığında, kurumlar geniş tabanlı saldırılar gerçekleşmeden önce koruma yayınlamak için zamana karşı bir yarış içine girerler (daha önceki güvenlik açığı istismarları tartışmamıza bakın). Bu, hem (amaca uygun bir şekilde yamalar geliştirmesi gereken) yazılım geliştiricileri hem de (yamaları hemen uygulaması gereken) ürün tüketicileri için tehlikeli ve zor bir döngüdür.

150'den fazla teknoloji kurumunu bir araya getiren önde gelen bir ittifak olan Cybersecurity Tech Accord'un[53]kurucu üyesi olarak Microsoft, çevrimiçi saldırı operasyonlarına katılmama taahhüdünde bulunmuştur. Bu taahhüdümüzün ve bu alandaki insan hakları sorumluluklarımızın arkasında duruyoruz. Siber paralı askerlerin sunduğu hizmetlerin neden olduğu olumsuz etkileri vurgulamak için çabalarken teknik aksamalar ve yasal zorluklarla karşı karşıya kalsak da, gördüğümüz her kötüye kullanımda müşterilerimizi korumaya devam edeceğiz.

> Siber paralı askerler, gelişmiş malware'lar ve bir dizi teknik dahil olmak üzere teknolojik olarak sofistike ve yaygın olarak bulunan "bir hizmet olarak gözetim" özellikleri oluşturur ve sağlar.

Hükümetler için eyleme dönüştürülebilir içgörüler

1. ABD'nin, Varlık Listesindeki kurumları Ticaret Bakanlığı ile listelerken yaptığı gibi, bu saldırgan aktörlerin yasaklanması da dahil olmak üzere, özellikle tedarikte bir hizmet olarak gözetime ilişkin şeffaflık ve denetim gerekliliklerini uygulayın.
2. Bu sektördeki eski çalışanlar için istihdam sonrası kısıtlamalar oluşturun.
3. "Müşterinizi tanıyın" yükümlülüklerini uygulamayı hedefleyin ve kurumları insan hakları taahhütlerini yerine getirmeye teşvik edin.

Daha ayrıntılı bilgi için bağlantılar

- KNOTWEED'i Çözmek: 0 gün açıklarını kullanan Avrupalı özel sektör saldırı aktörü | Microsoft Tehdit İstihbarat Merkezi (MSTIC), Microsoft Güvenlik Yanıt Merkezi (MSRC), RiskIQ (Microsoft Defender Tehdit İstihbaratı)
- Özel sektör siber silahlarıyla mücadeleye devam | Microsoft On the Issues

Siber uzayda barış ve güvenlik için siber güvenlik normlarını operasyonel hâle getirme

insan haklarına öncelik veren ve halkı online ortamda sergilenen sorumsuz devlet davranışlarına karşı koruyan tutarlı, küresel bir çerçeveye acilen ihtiyacımız vardır. Bu, hiçbir yerde Ukrayna'da devam eden savaştan daha net bir şekilde ortaya çıkmadı. Küresel bir stratejik çabaya ek olarak, hükümetler anında olumlu bir etki yaratmak için hemen şimdi harekete geçebilirler.

Beş yıl önce Microsoft, çevrimiçi barışı ve güvenliği savunmak için sektörler arasında sorumlulukları ve yükümlülükleri geliştirmek üzere bir "Dijital Cenevre Sözleşmesi" çağrısında bulundu. Siber uzay, barış zamanlarında bile saldırıların daha yaygın hâle gelmesiyle, devletler arasında ayrı ve değişken bir çatışma ve rekabet alanı olarak ortaya çıkıyordu.

Bugün, Rusya'nın işgalinin bir parçası olarak Ukrayna'ya yönelik Rus siber saldırılarının kanıtladığı gibi, böyle bir çerçeveye hala açık bir ihtiyaç mevcut. Bu savaş, daha önce bildiklerimizden önemli ölçüde farklı yeni bir cephe oluşturdu.

Siber uzaya istikrar getirmek, amaca uygun hâle getirmek için küresel yönetişim kurumlarının güçlendirilmesini ve yeniden tasarlanmasını gerektirecektir. Siber uzay temelde diğer alanlardan farklıdır; sınırsızdır, sentetiktir ve büyük ölçüde özel sektör tarafından sürdürülür. Bu, teknoloji sektöründen hem ürün ve hizmetlerin güvenliği hem de daha geniş bir dijital ekosistem için daha fazla sorumluluk almasını istemek anlamına gelmektedir. Tüm ön saflarda kayda değer bir ilerleme kaydedilmiş olsa da, zorluklar da önemli ölçüde arttı.

Siber uzayın güvenliğini savunmak için ortak çabaları iki katına çıkarmalıyız. Online olarak beklediğimiz hak ve özgürlükleri almış gibi davranamayız. Biz zorlukların üstesinden gelmek için mücadele ederken, kötü niyetli aktörler yapay zekayı kullanarak, dezenformasyondan yararlanarak ve yeni gelişen meta evrenine zarar vermenin yollarını bularak bir sonraki adımda nasıl ve nereye saldıracaklarını planlıyorlar. İnsan hakları savunucuları, teknoloji sektörü ve haklara saygı gösteren hükümetler, güvenli ve emniyetli bir online dünya için olumlu bir vizyon doğrultusunda birlikte çalışmalıdır. Önümüzdeki yol uzun olsa da, hükümetlerin siber güvenlik ekosistemlerini anında iyileştirmek için şu anda yapabilecekleri şeyler mevcut:

- Tespitlerde normları, yasaları ve sonuçları belirtin. Son beş yıldaki önemli iyileştirmelerden biri, hükümetin siber saldırıları tespitlerinin hızı ve koordinasyonu olmuştur. Basitçe ad koymanın ve kınamanın ötesinde, bu beyanların uluslararası beklentilerin tanınmasını güçlendirmeye yardımcı olmak için hangi uluslararası yasaların veya normların ihlal edildiğini ve ne tür sonuçların dayatılacağını vurgulaması gerekir.
- Uluslararası hukuk yorumunu online olarak netleştirin. Hükümetler, uluslararası hukukun online olarak uygulandığı konusunda hemfikir olsa da, belirli durumlarda nasıl uygulanacağı konusunda soru işaretleri devam etmektedir. Bu durum, özellikle Ukrayna'nın işgalinin ardından geçerli olmuştur. Hükümetler, uluslararası hukuk kapsamındaki yükümlülüklerini nasıl anladıklarını belirterek beklentileri belirlemek, yanlış anlamaları önlemek ve güven oluşturmak konusunda uzun bir yol kat edebilirler.
- Diğer paydaşlara danışın. Uluslararası forumlar sağlam çok paydaşlı katılımı kolaylaştırmanın en iyi yollarını tespit etmeye devam ettikçe, hükümetler iletişimde öncelikli uzmanlığa sahip olan kişilerden faydalanılmasını sağlamak için çok paydaşlı topluluklara, özellikle teknoloji sektörüne danışılarak bilgi paylaşılan iletişimleri destekleyebilir.
- Siber uzayda sorumlu devlet davranışını desteklemek için daimi bir yapı oluşturun. Sorumlu devlet davranışını online olarak ilerletmek için uluslararası diplomatik forumlardaki çalışmalar hiç bu kadar önemli olmamıştı. Siber uzayı bir çatışma alanı olarak ele almak için kalıcı bir BM mekanizmasına açıkça ihtiyaç duyulur.
- Gelişen tehditler için yeni normlar tanımlayın. Siber uzay tehditleri, teknolojideki yeniliklerle birlikte sürekli olarak gelişmektedir. Uluslararası normların teknolojiden bağımsız olması gerekirken, tehdit ortamındaki değişikliklere ve teknolojiyi nasıl kullandığımıza bağlı olarak güncellenmeleri ve hafifletilmeleri gerekir. Bugün bile, mevcut uluslararası çerçevedeki boşlukların kötüye kullanıldığını görüyoruz. Devletler, dijital ekosistemin temelini oluşturan yazılım güncelleme süreci gibi temel süreçleri korumayı açıkça taahhüt etmelidir. Ayrıca, belirli alanlar ek korumayı hak eder. Örneğin, pandemi sırasında öğrendiğimiz gibi, sağlık hizmetlerinin korunmasına yönelik normlar çok önemlidir.

Ulus devlet aktörleri ve saldırıları, hacim ve karmaşıklık açısından artmakta ve savunulmaz bir durum yaratmaktadır.

Acil eylem zorunludur - siber uzayda devlet davranışlarına ilişkin üzerinde anlaşmaya varılan normları ve kuralları uygulamak ve ortaya çıkan boşlukları gidermek için daha geniş çok paydaşlı bir toplulukla çalışmak dahil olmak üzere, hükümetlerin siber güvenlik ekosistemini hemen iyileştirmek için yapabilecekleri şeyler vardır.

Çok yönlü kurumlar, ulus devlet siber saldırılarının yarattığı baskıya çözüm bulmak için yeniden tasarlanmalıdır.

Daha ayrıntılı bilgi için bağlantılar

- Hesaplaşma anı: Güçlü ve küresel bir siber güvenlik yanıtına duyulan ihtiyaç | Microsoft On the Issues
- Sağlık hizmetlerini hedef alan siber saldırılar durdurulmalı | Microsoft On the Issues
- Birleşmiş Milletler'de siber diplomasinin bir sonraki bölümü başlıyor | Microsoft On the Issues

Son Notlar

1. https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3. Bu bölümdeki kritik altyapı, Başkanlık Politika Direktifi 21 (PPD-21), Kritik Altyapı Güvenliği ve Dayanıklılığı (Şubat 2013) tarafından tanımlanmıştır.
4. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6. https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8. https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10. https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11. https://news.un.org/en/story/2022/06/1119672
12. https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14. https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15. https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16. https://twitter.com/MoNDefense
17. https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18. https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19. https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20. https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22. https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25. https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26. https://attack.mitre.org/techniques/T1053/
27. https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28. https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29. https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30. https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

Son notların devamı

31. https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.
32. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/
33. https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general
34. Özellikle, ProxyShell güvenlik açıkları için Exchange sunucularına patch uygulayın (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 ve CVE-2021-27065, CVE-2021-34473). Ayrıca, güvenlik açıkları için Fortinet FortiOS SSL VPN cihazlarına patch uyguladığınızdan emin olun.
35. https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide
36. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
37. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
38. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
39. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
40. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide
41. https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus
42. https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide
43. https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
    https://www.bbc.com/news/world-asia-59845636
    https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/
44. https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods
45. https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html
48. https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html
49. https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades
50. https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms
51. Jan-Philipp Hein, In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin, FOCUS Online, (2022), https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy, We unveil the "Subzero" state trojan from Austria, Europe-cities (2021), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; Andre Meister, We unveil the state Trojan "Subzero" from Austria, Netzpolitik.org (2022), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.
52. Teknik blogumuzda belirtildiği gibi, uluslararası hedefleme yaygın olduğu için, bir ülkedeki hedeflerin tanımlanması bir DSIRF müşterisinin aynı ülkede ikamet ettiği anlamına gelmez.
53. Ana Sayfa | Cybersecurity Tech Accord (cybertechaccord.org)

Cihazlar ve Altyapı

Dijital dönüşümün ivme kazanmasıyla birlikte dijital altyapının güvenliği her zamankinden daha önemli hâle geldi.

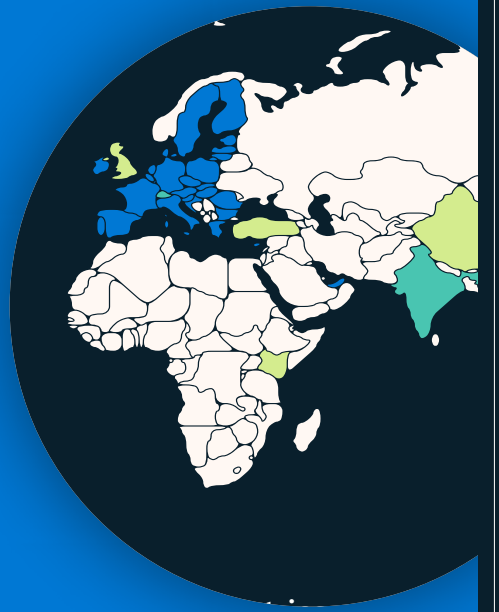
Cihazlar ve

Altyapıya genel bakış

Pandemi, gittikçe artan dijital dönüşümün bir bileşeni olarak internete dönük her türlü cihazın hızla benimsenmesiyle birleştiğinde dijital dünyanın saldırıya açık yüzeyini büyük ölçüde genişletti.

Siber suçlular ve ulus devletler hızla avantaj kazanıyor. BT donanım ve yazılımlarının güvenliği son yıllarda güçlenirken, Nesnelerin İnterneti (IoT) ve Operasyonel Teknoloji (OT) cihazlarının güvenliği buna ayak uyduramadı. Tehdit aktörleri; ağlara erişim sağlamak ve yanal hareket edebilmek, bir tedarik zincirinde tutunabilmek veya hedef kurumun OT operasyonlarını bozmak amacıyla bu cihazlardan faydalanmaktadır.

Dünya çapında hükümetler, IoT ve OT güvenliğini iyileştirerek kritik altyapıyı korumak için harekete geçiyor.

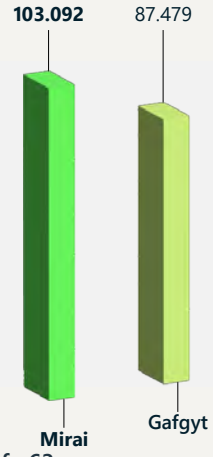


Daha fazla bilgi için bkz. sayfa 59

Kapsamlı bir şekilde benimsenmeyi sağlamak için küresel olarak tutarlı ve birlikte çalışabilir güvenlik politikalarına ihtiyaç vardır.

Daha fazla bilgi için bkz. sayfa 59

Bir hizmet olarak malware, kurumsal ağların yanı sıra altyapı ve yardımcı programlarda açığa çıkan IoT ve OT'ye karşı büyük ölçekli operasyonlara taşındı.



Daha fazla bilgi için bkz. sayfa 63

Uzaktan yönetim cihazlarına yönelik saldırılar, Mayıs 2022'de gözlemlenen 100 milyondan fazla saldırı ile son bir yılda beş kat arttı.

Daha fazla bilgi için bkz. sayfa 62

Saldırganlar, kurumsal ağlara sızmak ve yıkıcı saldırılar başlatmak için IoT cihazlarının üretici yazılımındaki güvenlik açıklarından giderek daha fazla yararlanıyor.

Daha fazla bilgi için bkz. sayfa 65

Analiz edilen ürün yazılımı görüntülerinin %32'si en az 10 bilindik kritik güvenlik açığı içeriyordu.

Daha fazla bilgi için bkz. sayfa 66

Giriş

Dijital dönüşümün hızlanması, kritik altyapıların ve siber-fiziksel sistemlerin siber güvenlik riskini artırmıştır.

Son birkaç yılda dijital dünyada benzeri görülmemiş bir değişim yaşandı. Kurumlar, hem akıllı bulut hem de akıllı uçtaki bilişim yeteneği gelişmelerinden yararlanmak için gelişiyor. Varlıkları hayatta kalmak için dijitalleşmeye zorlayan pandeminin ve dünya çapındaki sektörlerin internete yönelik cihazları benimseme hızının bir sonucu olarak, dijital dünyanın saldırı yüzeyi katlanarak büyüyor.

Bu hızlı geçiş, güvenlik camiasının adaptasyon yeteneğini geride bıraktı. Geçtiğimiz yıl geleneksel BT ekipmanlarından operasyonel teknoloji (OT) denetleyicilerine ve basit Nesnelerin İnterneti (IoT) sensörlerine kadar kurumun dört bir yanında cihazların kötüye kullanıldığı tehditleri gördük. BT ekipmanlarının güvenliği son yıllarda artmış olsa da IoT ve OT cihaz güvenliği aynı hızda ilerleme kaydetmedi. Tehdit aktörleri, ağlara erişim sağlamak ve yanal olarak hareket edebilmek veya kurumun OT operasyonlarını aksatmak için bu cihazlardan faydalanır. Elektrik şebekelerine yönelik saldırılar, OT operasyonlarını aksatan fidye yazılımı saldırıları, IoT yönlendiricilerinin uzun süreli etki için kullanılması ve ürün yazılımındaki güvenlik açıklarının hedef alındığı saldırıları gördük.

IoT ve OT güvenlik açıklarının yaygınlığı tüm kurumlar için bir zorluk yaratırken, tehdit aktörleri kritik hizmetleri devre dışı bırakarak güçlü bir nüfuz elde edebildiğini öğrendiğinden kritik altyapı daha çok risk altındadır. Colonial Pipeline Company'nin 2021 yılında uğradığı fidye yazılımı saldırısında, suçluların daha fazla fidye ödemesi alabilmek için kritik bir hizmeti nasıl bozabildiği görüldü. Öte yandan Rusya'nın Ukrayna'ya karşı yürüttüğü siber saldırılar, bazı ulus devletlerin kritik altyapıya yönelik siber saldırıları askeri hedeflerine ulaşmak için kabul edilebilir bir sabotaj olarak gördüğünü ortaya koyuyor.

Ancak tünelin ucunda bir umut ışığı var. Kural koyucular ve ağ savunma uzmanları, güvendikleri IoT ve OT cihazları gibi kritik altyapıların siber güvenliğini artırmak için gerekli adımları atıyor. Politika yapıcılar, kamunun kritik altyapı ve cihazların siber güvenliğine duyduğu güvenini pekiştirmek üzere yasa ve yönetmelik düzenlemelerini hızla hayata geçiriyor.

Microsoft, siber güvenliği artırma fırsatından yararlanmak için dünya genelindeki kamu kuruluşlarıyla iş ortaklığı yapıyor ve başka kuruluşların katılımını memnuniyetle karşılıyor. Öte yandan yetersiz güvenlik kaynaklarını birbirine benzer sertifikalara uyum için kullanılmasına ayırmak suretiyle tutarsız, ısmarlama veya karmaşık gerekliliklerin, çeşitli durumlarda güvenliği sekteye uğratmak gibi istenmeyen etkiler bırakmasından endişe ediyoruz.

Ağ savunma uzmanları, güvenlik operasyonu konusunda kurumlarının IoT/OT güvenlik duruşunu iyileştirmek için farklı yaklaşımlar benimsiyor. IoT ve OT cihazlarını sürekli takip etmek de bu yaklaşımlardan biridir. Diğer bir yaklaşım ise "sola kaydırma kültürü", yani IoT ve OT cihazları için daha iyi siber güvenlik uygulamalarını talep etmek ve hayata geçirmektir. Üçüncü yaklaşım, hem BT hem de OT ağlarını kapsayan bir güvenlik izleme çözümünü hayata geçirmektir. Bu bütünsel yaklaşım, OT ile BT arasındaki "siloları kırmak" gibi kritik organizasyonel süreçlere katkıda bulunarak önemli bir avantaj daha sunar; böylece kurumu, iş hedeflerini karşılarken ileri seviye bir güvenlik seviyesine ulaştırır.

Michal Braverman-Blumenstyk
Kurumsal Başkan Yardımcısı, Teknolojiden Sorumlu Başkan, Bulut ve Yapay Zeka Güvenliği

Kamu kuruluşları, kritik altyapı güvenliğini ve esnekliğini iyileştirmek üzere harekete geçiyor

Dünya genelindeki kamu kuruluşları, kritik altyapıların siber güvenlik riskini yönetmek üzere politikalar geliştiriyor ve hayata geçiriyor. Birçok kuruluş, IoT ve OT cihaz güvenliğini iyileştirmek için de kurallar hazırlıyor. Dünya çapında yükselen bu politika dalgası, siber güvenliği artırma yolunda önemli bir fırsat teşkil ederken, ekosistemdeki paydaşların yoluna da birtakım zorluklar çıkarıyor.

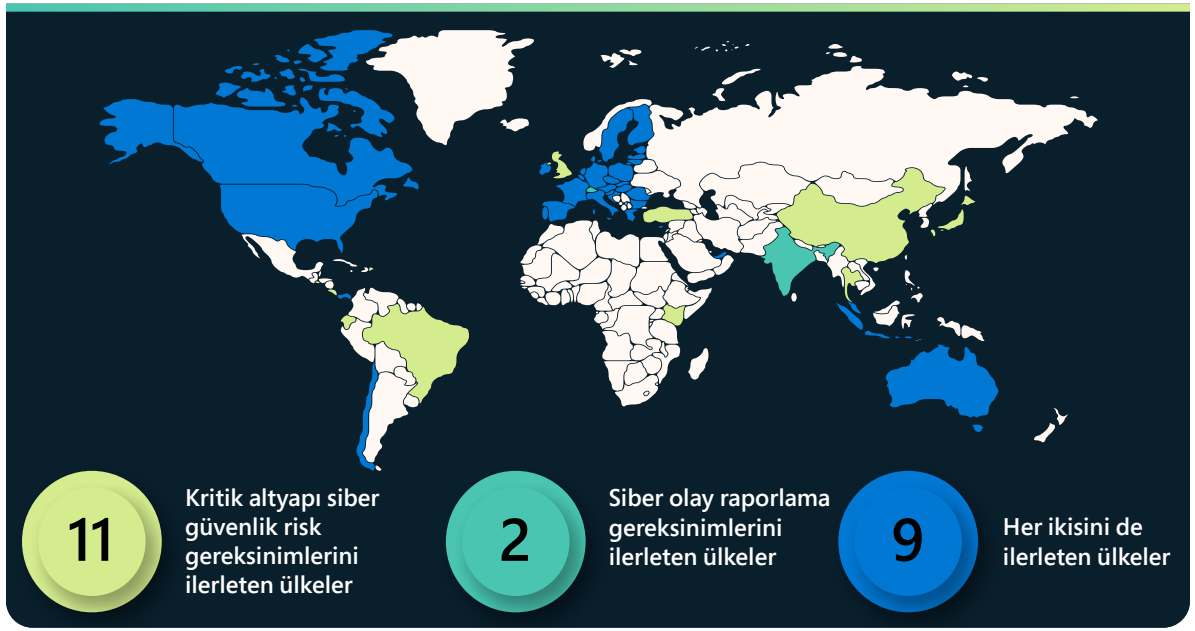
Kritik altyapılarda siber riski yönetmek için bütünsel bir vizyon geliştirmek, özellikle teknolojiler ve küresel tedarikçiler arasındaki bağlantının derecesi, teknoloji kullanım oranları, ilişkili riskler ve hem kısa hem de uzun vadeli stratejilere yatırım yapma ihtiyacı göz önüne alındığında çok önemli ancak karmaşık yapılıdır. Tekrara dayalı öğrenme ve iyileştirmeler ile küresel ve sektörler arası ortak çalışmaları destekleyen, kapsamı etkin biçimde belirlenmiş politikalar, karmaşayı yönetmeye yardımcı olabilir ve güvenlik odağı daha yüksek bir dijital dönüşüm sunar. Ancak, mevzuat konusunda parçalı bir yaklaşım benimsemek, yasal şartlarda bir takım çakışmalara ve tutarsızlıklara neden olabilir. Bu da kaynakları etkileyebilir ve eninde sonunda güvenlik hedeflerini sekteye uğratabilir. Örneğin, kurumlar kaynaklarını yenilik ve güvenlik konuları yerine formalite uyumluluk çalışmalarına yönlendirebilir.

Microsoft, kritik altyapılarda etkin siber güvenlik kurallarını hayata geçirmek, zorlukların ve fırsatların daha iyi anlaşılmasını sağlamak ve ortak risk duruşunu iyileştirme çalışmalarını desteklemek üzere dünya genelindeki kamu kuruluşlarıyla iş ortaklığı yapmayı hedefliyor.

Kritik altyapılara yönelik siber güvenlik risk yönetiminde politika gelişmeleri

Geçtiğimiz yıl Avustralya, Şili, Avrupa Birliği (AB), Japonya, Singapur, Birleşik Krallık ve Amerika Birleşik Devletleri gibi bazı ülkeler ve bölgeler, sektörler arası veya sektörlere özgü siber güvenlik gerekliliklerini hazırlamış, güncellemiş veya hayata geçirmiştir.[1] Bu devletlerin birçoğu ve Hindistan [2] ve İsviçre [3] gibi diğer bazı ülkeler de altyapı ve temel hizmet sağlayıcılara yönelik siber güvenlik olaylarını raporlama gerekliliklerini bundan da önce hayata geçirmişti ya da halen geliştirmeye devam etmektedir.[4]

Geçtiğimiz yıl Avustralya, AB, Endonezya ve ABD'de bazı önemli politika gelişmeleri yaşandı. Avustralya, kritik altyapılarda sektörler arası siber güvenlik risklerini yönetmeye yardımcı olacak iki yasa çıkardı. Öte yandan bu yasalar, kritik altyapıların bulunduğu yeni sektörleri belirlemekte, risk yönetim planlarının geliştirilmesini gerektirmekte, siber güvenlik olaylarını raporlamayı zorunlu tutmakta ve kritik bir altyapı operatörünün bir olaya karşılık vermekte isteksiz kaldığını veya yeterli biçimde karşılık veremediğini tespit ederse kamu kuruluşlarına müdahale etme yetkisi vermektedir.



AB, üye ülkelerin ekonomileri ve toplumlarının işleyişi açısından kritik olduğu düşünülen teknoloji hizmetleri ve ürünlerle ilgili yasal düzenlemelere yönelik bir çerçeve sunan 2016 NIS Direktifine güncelleme getirmek üzere çalışmalar yaptı. Teklif edilen NIS 2, yeni bir kritik dijital altyapı kategorisi oluşturacak, siber olayları raporlamaya yönelik gereklilikleri artıracak ve başka siber güvenlik risk yönetimi gerekliliklerini hayata geçirecek revizyonları kapsamaktadır. AB ayrıca, Dijital Operasyonel Dayanıklılık Yasası (DORA) için güncelleme teklif etti. Buna göre finansal hizmetler sektöründe kullanılan bilgi iletişim teknolojilerine yeni gereklilikler getirilecek.

Mayıs ayında Endonezya, hayati öneme sahip bilgi altyapısının ("IIV") korunmasıyla ilgili olarak, Mayıs 2024'te yürürlüğe girecek ve enerji, ulaştırma, finans ve sağlık gibi sektörleri kapsayacak bir cumhurbaşkanlığı yönetmeliği yayımladı. Endonezya bu yönetmelikte, IIV uygulamasının sürekliliğini korumayı, siber saldırıları önlemeyi ve siber olayların yönetimine ilişkin hazırlıklı olma düzeyini artırmayı hedefliyor. IIV sağlayıcılarının sorumluluğu; güvenli ve güvenilir bir koruma sağlamak, etkili bir siber risk yönetimi uygulamak ve siber risk sonuçlarını ilgili kamu kuruluşlarına bildirmek olacak. Yönetmelikte siber olayların 24 saat içinde bildirilmesi zorunluluğu yer alıyor.

Kamu kuruluşları, kritik altyapı güvenliğini ve esnekliğini iyileştirmek üzere harekete geçiyor

Devamı

ABD Kongresi; Siber Güvenlik ve Altyapı Güvenlik Kurumu'nu (CISA), kritik altyapı operatörlerinin siber güvenlik olaylarını raporlamasını zorunlu hâle getiren yönetmelikleri hayata geçirmesine yetki veren bir yasa çıkardı; ABD Ulaştırma Güvenliği Dairesi (TSA) ulaştırma sektörüne özgü yeni siber güvenlik gerekliliklerini belirledi. 2021 yılında TSA, Colonial Pipeline Company'nin uğradığı fidye yazılımı saldırısına yanıt olarak tehlikeli sıvı ve doğal gaz boru hattı işletmecilerine yönelik iki güvenlik direktifi yayımladı:

- İlk direktife göre işletmecilerin bir siber güvenlik koordinatörü belirlemesi, siber olayları 12 saat içinde haber vermesi ve sistemlerindeki güvenlik açıkları için değerlendirme yapması gerekiyordu.
- TSA'nın 2022 yılında revize ettiği ikinci direktifte ise bu işletmecilerin fidye yazılımı saldırılarının yanı sıra BT ve OT sistemlerine yönelik bilinen diğer tehditlere karşı koruma sağlamak üzere belirli hafifletici önlemleri hayata geçirmeleri, 30 gün içinde bir siber güvenlik acil durum ve müdahale planı geliştirmeleri ve uygulamaları ve her yıl bir siber güvenlik mimari tasarım değerlendirmesinden geçmeleri gerekiyordu.

TSA, boru hatlarına ilişkin yönetmeliklere dayanarak 2021 yılının sonraki dönemlerinde demiryoluyla yük taşıma, yolcu taşıma veya demiryolu transit sistemleri için siber güvenlik gerekliliklerini içeren iki güvenlik direktifi daha yayımladı. Bu direktiflere göre ilgili işletmecilerin bir siber güvenlik koordinatörü görevlendirmesi, 24 saat içinde siber güvenlik olaylarını bildirmesi, bir siber güvenlik olayı müdahale planı geliştirip hayata geçirmesi ve bir siber güvenlik açığı değerlendirmesi yapması gerekiyordu. TSA, aynı zamanda havacılık güvenlik programlarını güncellediğini, havayolu ve yolcu taşımacılığı işletmecilerinin ilk iki hükmü hayata geçirerek bir koordinatör görevlendirmesi ve olayları 24 saat içinde bildirmesi gerektiğini açıkladı.

IoT ve OT cihaz güvenliğindeki kural geliştirmeleri

Onlarca ülkede kamu kuruluşları, IoT ve OT cihazları dahil çeşitli bilgi ve iletişim teknolojisi (ICT) ürünlerine ve hizmetlerine yönelik siber güvenliği artırıcı gereklilikleri geliştirme konusunda etkin bir rol oynamaktadır. ICT ürünleri ve hizmetleriyle ilgili en büyük endişe kaynağı, yazılım tedarik zinciri güvenliği ve IoT güvenliğidir.

- Avrupa Komisyonu; bağımsız yazılımlar, bağlı cihazlar ve yan hizmetler için siber güvenlik gerekliliklerini ortaya koyan Siber Dayanıklılık Yasasını teklif etti.[5] Yazılım tedarikçilerini ilgilendiren uygulamalar arasında, güvenli bir yazılım geliştirme yaşam döngüsü kullanma[6] ve Yazılım Ürün Listesi'ni sağlama var.[7] Yeni güvenlik gereklilikleri, bağlı cihazlar için geçerli olacak ve tüm üreticiler, piyasaya sunulan ürünler için güvenlik açığı duyurusunu koordineli olarak yönetme görevini[8] üstlenecek.

Kural koyucular aynı zamanda IoT cihazlarının ve ağa bağlı OT cihazlarının yaygınlaşmasını sürdürmeye odaklanıyor.

- Birleşik Krallık'ta Ürün Güvenliği ve Telekomünikasyon Altyapısı Yasa Tasarısı, akıllı televizyonlar gibi tüketicinin kendi başına bağlanabileceği ürünlerin üreticilerine, güvenlik açığını ifşa kuralı belirleme (örneğin, güvenlik kusurları hakkında bildirim alma gibi) ve güvenlik güncellemelerini en az ne kadar süreyle daha sağlayabilecekleri hakkında şeffaf hareket etme yükümlülüğünü getirecek.[9]
- AB'de, kablosuz cihazlarla ilgili olan ve ağ dayanıklılığını iyileştirmeyi, tüketicilerin gizliliğini korumayı ve parasal dolandırıcılık riskini azaltmayı amaçlayan Radyo Ekipmanları Direktifi'ne devredilen bir yasa dahil farklı yasal araçlarla yeni güvenlik standartları veya gereklilikleri uygulanıyor.[10] Buna ek olarak, şu anda 2019 tarihli AB Siber Güvenlik Yasası'nın sonucu olan[12] bir bulut sertifika düzeninin kullanılması[12] da gerekebilir.

Tutarlılık ihtiyacı

Birçok durumda bölgeler, sektörler, teknolojiler ve operasyonel risk yönetimi alanlarında farklı faaliyetler eş zamanlı olarak sürdürülüyor; bu durum, yönlendirmeden yararlanmak veya uygunluğunu göstermek isteyen kurumlar için kapsam, gereklilikler ve karmaşa bakımından çakışmalara veya tutarsızlıklara neden olabilmektedir. Evrensel ölçekte kabul görmüş bir IoT tanımı olmadan, özellikle IoT ve OT cihazlara yönelik yasal düzenlemeler için kapsam belirlemek zordur. Yukarıdaki örnekler "bağlı ürünler ve yan hizmetler", "tüketicinin bağlayabileceği ürünler" ve "kablosuz cihazlar" için geçerli olabilir. Aynı zamanda birçok kamu kuruluşu, kurumların ve ürünlerin mevcut, yeni gelişmekte olan ve değişen gereklilikleri karşılayıp karşılamadığını ve ne şekilde karşıladığını daha iyi anlamak üzere daha güçlü değerlendirme rejimlerini hayata geçirmeyi amaçlıyor. Bu eğilimler yaygınlaştıkça karmaşa daha da artacaktır. Neyse ki AB Siber Dayanıklılık Yasası ile ilgili istişarede tartışılan sorularla, yeni düzenlemenin mevcut siber güvenlik yönetmeliğiyle nasıl etkileşime girebileceği anlaşıldı; bu durum, siber güvenlik gereklilikleri arasında çakışmanın önlenmesinin amaçlandığı göstermektedir.

Risk temelli ve sonuç odaklı ya da süreç odaklı (uygulamaya özel olanla karşılaştırıldığında) yinelemeli yaklaşımlar, siber güvenlikte ilerlemeyi ve sürekli iyileştirmeyi destekleyebilir. Aynı şekilde sektörler, bölgeler ve politika alanları arasında ortak çalışma atmosferini sağlamaya odaklanmak, birbirine bağlı küresel tedarik zincirleri arasında siber güvenliği tutarlı bir şekilde artırabilir.

Kamu kuruluşları, kritik altyapı güvenliğini ve esnekliğini iyileştirmek üzere harekete geçiyor

Devamı

Bölgeler, sektörler ve konu alanlarında geliştirme aşamasındaki kritik altyapı siber güvenliği kuralları gittikçe karmaşık bir hâl almaktadır. Bu durum büyük fırsatlar sunarken beraberinde önemli zorluklar da getirmektedir. Kamu kuruluşlarının süreci devam ettirme şekli, dijital dönüşüm ve ekosistem genelinde güvenliğin geleceği için hayati önemde olacaktır.

Ekosistem genelinde yazılım tedarik zinciri güvenliğine ve Sıfır Güven mimarisine dönük yatırımların hızlandırılması

Siber güvenliğin iyileştirilmesine ilişkin 14028 sayılı ABD Başkanlık Emri (EO), Microsoft'un kendi güvenliğimize ve ekosistem genelindeki tedarik zinciri güvenliğine yatırım yapma ve müşterilerimizin Sıfır Güven hedeflerini karşılamaları adına devam eden girişimlerini hızlandırmak için bir itici güç olmuştur.

Uzun bir süredir yazılım tedarik zincirini iyileştirmek için yaklaşık 15 yıl önce Microsoft'un Güvenlik Gelişimi Yaşam Döngüsü açıklamasından başlayarak öğrenilenleri ve en iyi uygulamaları paylaşmanın gerekli olduğuna inanıyoruz.

Buna ek olarak, hem kurum içinde uygulanan Sıfır Güven Mimarisine ilişkin yaklaşımları göstermek için Ulusal Siber Güvenlik Mükemmellik Merkeziyle yakın iş birliği yapıyor, hem de hibrit ve çoklu bulut ortamlarına yönelik kimlik avı dolandırıcılığına karşı dayanıklı kimlik doğrulamasını uygulayabilme gibi yeni ürün özelliklerini de geliştiriyoruz.

Bugün, EO'nun yazılım tedarik zinciri güvenlik gerekliliklerine uygun hareket etme ve Yazılım Ürün Listesi (SBOM) bilgilerini iki şekilde temin etme gerekliliklerini fazlasıyla yerine getiriyoruz.

1. İlk olarak, Windows, Linux, Mac, iOS ve Android platformlarında derlemeleri destekleyen CI/CD işlem hatlarıyla kolayca entegre etmek üzere oluşturduğumuz SBOM üreteci aracımızın açık kaynaklı bir sürümünü paylaşıyoruz.[13]
2. İkinci olarak, Tedarik Zinciri Bütünlüğü, Şeffaflığı ve Güveni (SCITT) için sektör standartlarının geliştirilmesine katkıda bulunuyoruz. Bu sayede EO'nun yazılım tedarik zinciri kılavuzundakiler gibi gerekliliklere karşı uyumluluğu gösteren eserler dahil olmak üzere doğrulanabilir tedarik zinciri bilgilerinin otomatik değişimi mümkün olacak.

Eyleme dönüştürülebilir içgörüler

1. Çok yönlü kurumlar, ulus devlet siber saldırılarının yarattığı baskıya çözüm bulmak için yeniden tasarlanmalıdır.
2. Bölgeler, sektörler ve konu alanlarında tutarlı ve bir arada çalışabilir siber güvenlik kuralları geliştirme.

Daha ayrıntılı bilgi için bağlantılar

- Siber güvenliği desteklemek için tedarik zinciri güvenliğine devam eden yatırımlar | Microsoft Teknoloji Topluluğu
- ABD Hükümeti Sıfır Güven mimari stratejisini ve gerekliliklerini ortaya koyuyor | Microsoft Güvenlik Blogu
- SİBER EO | Microsoft Federal
- Tedarik Zincir Bütünlüğü, Şeffaflığı ve Güveni | github.com
- Sıfır Güven Mimarisini Uygulama | NCCoE (nist.gov)

Savunmasız IoT ve OT: Eğilimler ve saldırılar

Giderek daha fazla birbirine bağlı hâle gelen dijital dünyada cihazlar hızla çevrimiçi hâle geliyor, daha büyük sistemlerle iletişim kuruyor, veri topluyor ve önceden belirsiz kalan alanlarda görünürlük sağlıyor. Bu durum hem kurumlar hem de tehdit aktörleri için bir fırsat yaratırken, siber suçlar açısından milyar dolarlık bir endüstri ve risk yaratıyor.

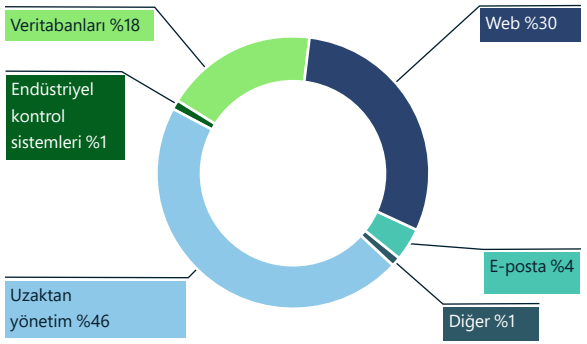
IoT cihazları (yazıcılardan web kameralarına, klima kontrol cihazlarından bina erişim denetimlerine kadar her şey dahil) kişiler, kurumlar ve ağlar için benzeri olmayan güvenlik riskleri oluşturur. Birçok kurumdaki operasyonlar için kritik olmakla birlikte, bunlar bir çırpıda sorumluluk ve güvenlik riskine dönüşebilir. IoT çözümlerinin hemen hemen her sektörde hızla benimsenmesi, saldırı vektör sayısını ve kurumların maruz kaldığı riskleri artırmıştır.

Hizmet olarak malware, kurumsal ağların yanı sıra devlet altyapısı ve kamu hizmetlerine (hastaneler, petrol ve doğal gaz, elektrik şebekeleri, ulaşım hizmetleri ve diğer kritik altyapılar dahil) karşı büyük ölçekli operasyonlara dönüşmüştür. Tehdit aktörlerinin, işletim ortamları ile yerleşik IoT ve OT cihazlarının yapılandırmasını açığa çıkarmak ve kötüye kullanmak için önemli araştırmalar yapmaları gerekiyor.

IoT cihazları, ağ içindeki giriş ve döngü noktaları olarak benzeri olmayan güvenlik riskleri taşımaktadır. Milyonlarca IoT cihazı yama uygulanmamış veya savunmasız durumda kullanılmaktadır.

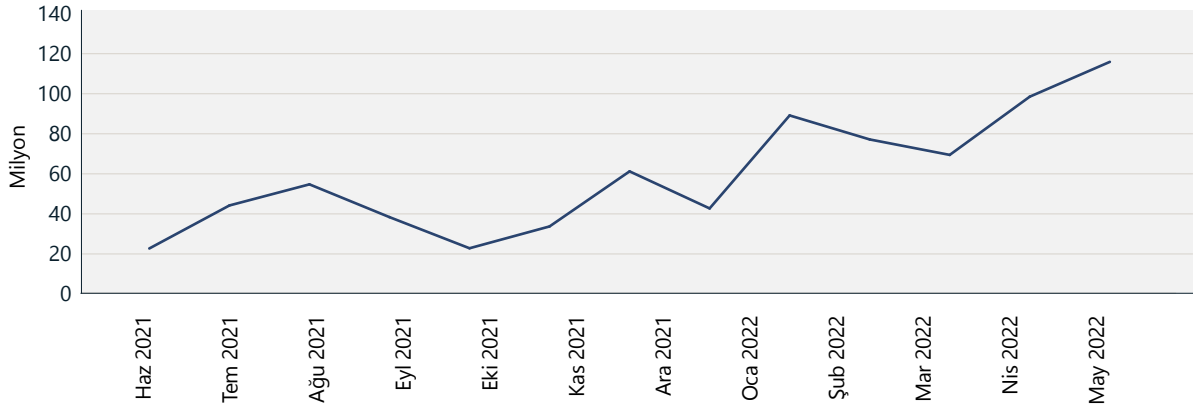
Tehdide açık cihazlar, açık ağ bağlantı noktalarını dinleyen hizmetleri tanımlayarak internet arama araçları üzerinden tespit edilebilir. Bu bağlantı noktaları cihazların uzaktan yönetimi amacıyla yaygın şekilde kullanılmaktadır. Güvenlik doğru bir şekilde sağlanmadığı takdirde, yetkisiz kullanıcılar bağlantı noktalarına uzaktan erişim sağlayabildiğinden savunmasız bir IoT cihazı kurumsal ağın başka bir katmanına dönüş noktası olarak kullanılabilir. Kameralar, yönlendiriciler ve termostatlar gibi internette riske açık farklı cihazlarda tehdit aktörlerinin güvenlik açıklarından yararlanmaya çalıştığını gördük. Ancak bu riske rağmen milyonlarca cihaz yamasız veya savunmasız bir halde kullanılmaktadır.

IoT/OT'deki saldırı türleri özeti



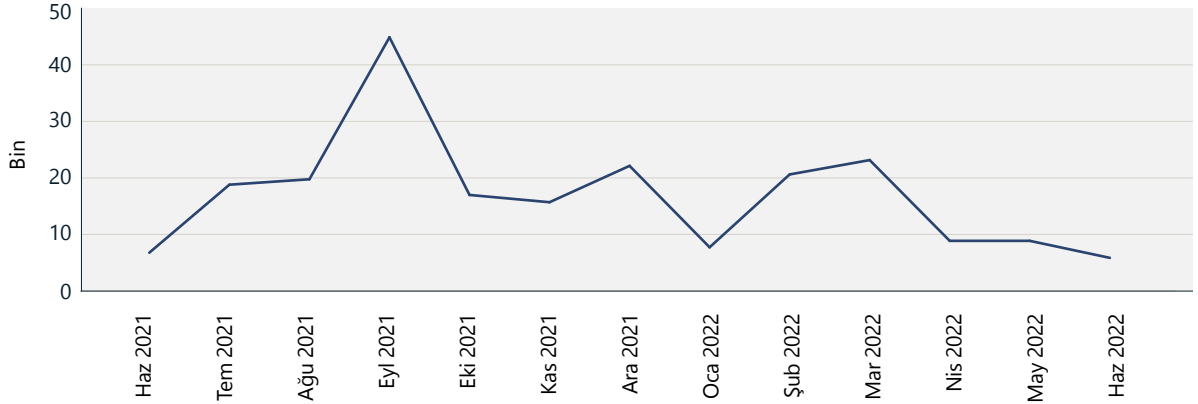
MSTIC sensör ağı üzerinden gözlemlenen saldırı türleri. En yaygın olanları uzaktan yönetim cihazlarına yönelik saldırılar, web üzerinden yapılan saldırılar ve veri tabanlarına yönelik saldırılar oldu (kaba kuvvet veya kötüye kullanma).

Uzaktan yönetim cihazlarına yönelik saldırılar



MSTIC sensör ağı üzerinden görüldüğü üzere, uzaktan yönetim bağlantı noktalarına yapılan saldırıların zaman içinde artması.

IoT ve OT'ye yönelik web saldırıları



MSTIC sensör ağı üzerinden görüldüğü gibi zaman içindeki web saldırısı hacmi. Doğrudan web'e bağlı cihazların sayısı düşmeye devam ettikçe, saldırganların bunları araştırma olasılığı da daha düşük kalabilir.

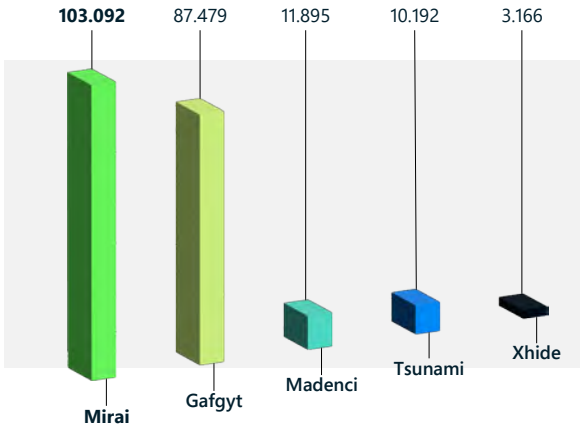
Savunmasız IoT ve OT: Eğilimler ve saldırılar

Devamı

Yenilenmiş malware yardımcı programı

Siber suç gruplarıyla birlikte malware kurulumu ve seçilen hedefler de değişti. Geçtiğimiz yıl, yaygın IoT protokollerine (Telnet gibi) yönelik saldırıların bazı vakalarda yüzde 60'a kadar ciddi şekilde düştüğünü gözlemledik. Öte yandan botnet'ler de siber suç örgütleri ve ulus devlet aktörleri tarafından farklı amaçlara uygun şekilde yeniden tasarlandı. Mirai gibi malware yazılımlarının kalıcılığı, dikkatleri bu saldırıların modülerliğine ve mevcut tehditlerin uyarlanabilirliğine çekmektedir.

Gerçek hayatta en çok algılanan IoT malware yazılımları



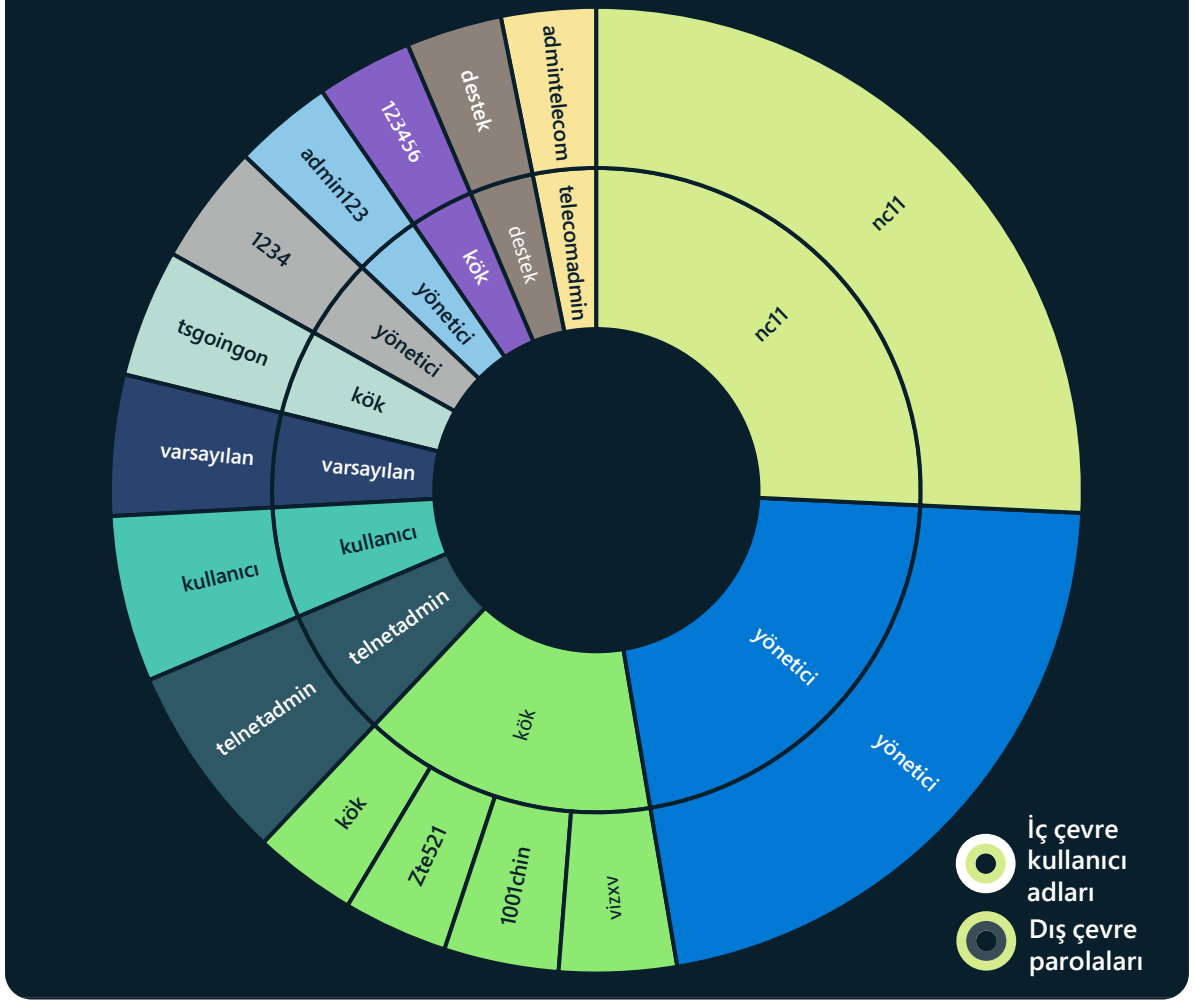
Mirai, internet protokol kameraları, güvenlik kamerası dijital video kayıt cihazları ve yönlendiriciler gibi farklı IoT cihazlarına virüs bulaştıracak şekilde geliştirildi. Eski güvenlik denetimlerini atlatan saldırı vektörleri diğer güvenlik açıklarından yararlanarak ve yanlamasına hareket ederek ağ içindeki uç noktalar için risk oluşturmaktadır. Mirai, farklı mimarilere uyum sağlayabilen ve yeni saldırı vektörlerini tehlikeye atmak için hem bilinen hem de sıfır gün güvenlik açıklarından yararlanan varyantlarla birçok kez yeniden tasarlandı.

Mirai'nin kullanımı geçtiğimiz yıl hem 32 hem de 64 bit x86 CPU mimarileri artış gösterdi; malware'e kazandırılan yeni özellikler, ulus devletler ve suç örgütleri tarafından hızla benimsendi. Ulus devletler, artık yabancı düşmanlara yönelik dağıtılmış hizmet engelleme (DDoS) saldırılarında mevcut botnet'lerin yeni varyantlarından yararlanıyor.

IoT cihazlarına yönelik saldırıların elde edilen gelir 2022 yılında gerilerken, bazı tehdit aktörü gruplarının sunucular gibi cihazlara yönelik kötü amaçlı bir yük göndermek, bu cihazlara bulaştırmak ve bunları, DDoS saldırılarını gerçekleştiren büyük botnet'lere almak için Log4j ve Spring4Shell gibi güvenlik açıklarından yararlandığını gözlemledik. Yanal hareket ek yüklere ve ağlardaki diğer cihazlara izinsiz erişim geçiş noktalarını açığa çıkarabildiğinden, güvenlik açığı bulunan IoT cihazlarını hedef almak üzere tasarlanan yenilenmiş malware'ler hem kurumlar hem de uluslar için ciddi etkiler doğurmaktadır.

Birçok endüstriyel kontrol sistemi protokolü takip edilmediği için bu sistemler OT'ye özel saldırılara açık durumdadır. Bu durum, kritik altyapılar için daha fazla risk anlamına gelmektedir.

45 günlük sensör sinyallerine göre IoT/OT cihazlarında görülen kullanıcı adı ve parola çiftlerinin göreceli yaygınlığı



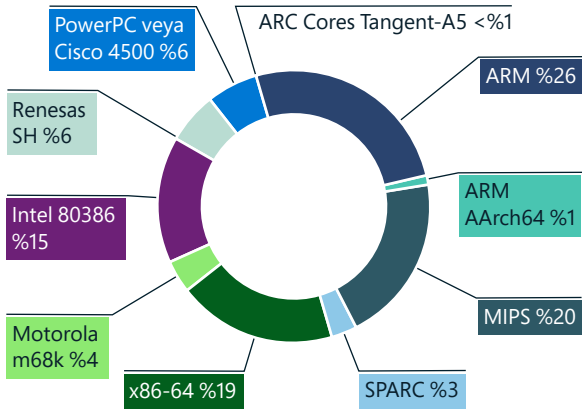
Yaygın kullanıcı adı ve parola çiftlerinin kullanılması, güvenlik ihlali riskini artırır. 39 milyondan fazla IoT ve OT cihazından oluşan örneklem büyüklüğüne bakıldığında, aynı kullanıcı adı ve parolayı kullananların oranı yüzde 20 civarındadır.

Savunmasız IoT ve OT: Eğilimler ve saldırılar

Devamı

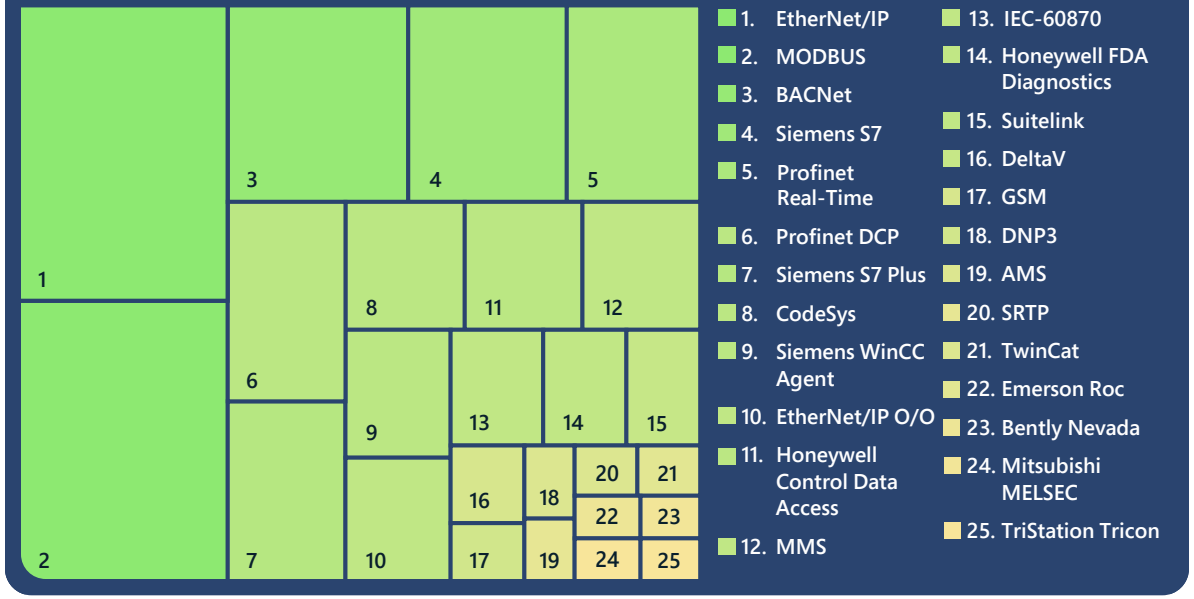
Zayıf yapılandırmalar ve varsayılan kimlik bilgileri, ağlar açısından hala bir risk unsuru olmakla birlikte Microsoft, birçok web tabanlı kötüye kullanım örneğinde HTTP kullanıldığını gözlemlemiştir. Eski botnet'leri kullanan web tabanlı hizmetlere yönelik saldırılarda bu artışı gözlemledik. Öte yandan internetteki açık telnet bağlantı noktalarının sayısında bir azalma oldu; bu durum, eskiden bu yana cihazlara yönelik risk taşıyan botnet'lerin artık ilgi düzeyini kaybettiğine dair ağ güvenliğiyle ilgili pozitif bir göstergedir. Açık telnet bağlantı noktalarındaki bu azalmaya rağmen sensör ağlarında kalıcı botnet'leri görmeye devam ettik.

CPU mimarisine göre IoT malware dağılımı



Microsoft, ARM'de çalışan IoT cihazlarının en çok malware, daha sonra MIPS, X86-64 ve Intel 80386 CPU tarafından hedeflendiğini gözlemledi.

Endüstriyel kontrol sistemi protokolü yaygınlığı



Endüstriyel kontrol sistemi protokolündeki güvenlik açıkları

Buluta bağlı sensörlerimizden gelen OT verilerini inceleyerek en yaygın endüstriyel kontrol sistemi (ICS) protokollerini ortaya çıkardık. Bu protokollerde, bu cihazların yapısı ve saldırı yüzeyleri hakkında bilgi verilmektedir. Bu, özellikle kritik altyapının güvenliğiyle ilgilidir. Öğrenilen bazı önemli bilgiler şunlardır:

1. Sunulan protokollerin çoğu özeldir; bu nedenle standart BT izleme araçlarında bu cihazlar ve protokoller arasında yeterli güvenlik görünürlüğü yoktur. Sonuç olarak, ağlar izleme işlemine tabi tutulmadığından OT'ye özgü saldırılara karşı daha savunmasız durumdadır.
2. Tedarikçiye özel çok çeşitli protokoller söz konusudur. Yani tedarikçiye özel güvenlik çözümleri, ağın tamamını yeterli düzeyde kapsayamaz. Microsoft, birçok farklı cihazda güvenlik kapsamı sağlamak üzere belirli bir tedarikçiye bağlı olmadan çalışmaya öncelik vermektedir.
3. Kurumlar, bu protokollerin kendi ağlarından doğrudan internete açık olmamasını sağlamalıdır. Bu durum, güvenlik açıkları ve bu protokollerin güvensiz olması nedeniyle ciddi bir güvenlik riski teşkil edebilir.

Mirai gibi malware'ler yeni yetenekler kazanarak kalıcılığını sürdürür, siber suç grupları ve ulus devlet aktörleri tarafından benimsenerek yabancı düşmanlara düzenlenen DDoS saldırılarında mevcut botnet'lerin yeni varyantlarından yararlanır.

Eyleme dönüştürülebilir içgörüler

1. Düzeltme yamalarını uygulayarak, varsayılan parolaları ve varsayılan SSH bağlantı noktalarını değiştirerek cihazların güvenli olduğundan emin olun.
2. Gereksiz internet bağlantılarını ve açık bağlantı noktalarını ortadan kaldırarak, bağlantı noktalarını engellemek suretiyle uzaktan erişimi kısıtlayarak, uzaktan erişimi reddederek ve VPN hizmetlerini kullanarak saldırı yüzeyini azaltın.
3. Cihazları, bilinmeyen ana bilgisayarlarla iletişim kurmak gibi olağan dışı veya yetkisiz davranışlara karşı izlemek için bir IoT/OT'ye duyarlı ağ algılama ve yanıt (NDR) çözümü ile bir güvenlik bilgileri ve olay yönetimi (SIEM)/güvenlik düzenleme ve yanıt (SOAR) çözümü kullanın.
4. Saldırganın ilk izinsiz girişten sonra yanal hareket etme ve varlıkların güvenliğini tehlikeye atma kabiliyetini sınırlamak için ağları segmentlere ayırın. IoT cihazları ve OT ağları, güvenlik duvarları ile kurumsal BT ağlarından izole edilmelidir.
5. ICS protokollerinin doğrudan internete açık olmadığından emin olun.

Tedarik zinciri ve üretici yazılımı korsanlığı

Neredeyse internete bağlı her cihazda, donanımına veya devre kartına gömülü halde bir üretici yazılımı vardır. Son birkaç yıl içinde, yıkıcı saldırılar başlatmak amacıyla üretici yazılımlarının daha çok hedef alındığını gördük. Üretici yazılımları, tehdit aktörleri için değerli birer hedef olma niteliğini koruduğundan kurumların, üretici yazılımı korsanlığına karşı kendilerini koruması gerekir.

Üretici yazılımı bir ağa bağlanma veya veri depolama gibi bir cihazın temel işlevlerinden sorumludur. Üretici yazılımı, kritik altyapılarda kullanılan endüstriyel kontrol ekipmanlarıyla (OT) birlikte İşletmelerde kullanılan yönlendiriciler, kameralar, televizyonlar ve diğer cihazlarda (IoT) bulunur. Üretici yazılımları, eskiden bu yana cihazın kontrolünü devralmak veya üretici yazılımının içine kötü amaçlı kod yerleştirmek üzere kullanılabilen ciddi güvenlik açıkları ortaya çıkaran güvenli olmayan kodlarla yazılmıştır.

Bu risk, tedarik zinciri söz konusu olduğunda artış gösterir. Çoğu cihaz, açık kaynak kitaplıkların yanı sıra çok sayıda üreticiye ait yazılım ve donanım bileşenleri kullanılarak geliştirilir. Çoğu zaman cihaz operatörleri, kendi ağlarındaki cihazların tedarik zincir riskini değerlendirmek için donanım ve yazılım ürün listesi (H/SBOM) hakkında yeterli bilgi sahibi değildir. Haziran 2020'de, tüketici ve endüstri ekipmanları alanında yüz milyonlarca IoT cihazının etkilendiği, birçok farklı üretici tarafından kullanılan bir ağ yığınında güvenlik açıkları tespit edildi.[14] Bazı örneklerde bu ağ yığını diğer satıcılar tarafından marka yenileme işlemine tabi tutulmuştu ve bir cihazın savunmasız olduğuna dair hiçbir işaret mevcut değildi. IoT/OT cihazlarında ait bu yazılım ve donanım tedarik zincirini hedef alarak kurumları tehlikeye sokan kötü amaçlı aktörlerin sayısının arttığını gözlemliyoruz.

Üretici yazılımı güncelleme işlemi, cihazlar arasında ciddi farklılıklar gösterir ve bu işlemi gerçekleştirmenin karmaşıklığı ve lojistik zorluğu, güncelleme sıklığını da etkiler. Bir cihazda en güncel üretici yazılımının çalışıp çalışmadığını belirlemek her zaman mümkün değildir. Bu durum, güvenlik profesyonellerinin IoT ve OT cihazlarındaki güvenlik duruşunu izlemesini ve garanti etmesini zorlaştırır. Buna ek olarak, bazı cihazlarda şifreli olarak imzalanmamış ve kullanıcı tarafından doğrulama yapılmadan güncelleştirmelere izin veren üretici yazılımları bulunur. Bu zayıflıklar, cihazları üretim ve dağıtım zincirinde tedarik zinciri saldırılarına karşı daha da savunmasız hâle getirir.

Bu tehditleri ele almak için Microsoft, tedarik zincirinin farklı aşamalarında ilerlerken üretici yazılımının güvenliğinin ve bütünlüğünün sağlanmasına ve istediği bir zamanda, alım sırasında veya süreç içerisinde bir değişiklik yapılmadığının kanıtlanmasına yönelik ciddi yatırımlar yapar. Bu sayede her bir işlem hattı segmenti arasındaki güveni doğrulayabilir ve müşterilere gönderdiğimiz her bileşen için sertifikalı ve kanıtlanabilir uçtan uca bir gözetim zincirleri sunabiliriz. Yongadan buluta kadar olan bu güvenliği, kurum ve OT ağındaki tüm cihazlara ulaştırmak için iş ortaklarımızla birlikte çalışıyoruz.

"ICT altyapı tedarikçileri, tek bir saldırının yaygınlaşarak tekrar etmesine olanak sağladıkları için giderek daha çok hedef oluyor. Aynı zamanda, tedarik zinciri güvenliği ve dayanıklılığına ilişkin küresel mevzuat, düzenleme ve müşteri talepleri artarken genellikle bunlarla ilgili gereklilikler de farklılık gösteriyor.

Çözüm, ortaklıkta yatıyor. Tedarikçiler ve dünyadaki kamu kuruluşlarıyla birlikte Microsoft, tedarik zinciri ekosistemimizde, müşterilerden ve düzenleyicilerden gelen artan taleplere bağlı olarak güvenlik konusunu ele almaya kararlıdır. Bunun için tedarik zincirinde esnek bir şekilde kurulan güvenlik ve operasyonel dayanıklılık konusunda kapsamlı bir yaklaşım uyguluyoruz.

Tasarımdan cihazın işleyişine kadar üretici yazılımında bütünlüğü sağlamak, bu ortak yaklaşımımızın kilit unsurudur. Tedarikçilerin SDL süreçlerini sağlamak ve donanım güven köküne ilişkin yeniliği kurmak, tedarik zinciri bütünlüğünü nasıl oluşturabileceğimize dair örneklerdir.

Topluluğumuz, sürekli izleme ve anomali algılamayla birlikte değişiklik yapmayı önleyici yeni teknikleri ve şifreleme mekanizmalarını kapsayan toplu araştırma ve geliştirmelerden yararlanmaktadır. Hep birlikte, bir saldırı yüzeyi olarak tedarik zincirinin çekiciliğini en aza indirmeye devam ediyoruz."

Edna Conway,
Başkan Yardımcısı, Güvenlik ve Risk Sorumlusu, Bulut Altyapısı

Üretici yazılımlarında güvenlik açıklarında öne çıkanlar

Saldırganlar, kurumsal ağlara sızmak için IoT cihazlarının üretici yazılımındaki güvenlik açıklarından giderek daha fazla yararlanıyor. Zayıflıkları belirlemek için XDR temsilcilerini kullanan geleneksel BT uç noktalarının tam tersine, IoT/OT cihazlarındaki güvenlik açıklarını tanımlamak çok daha zordur.

Microsoft ve Ponemon Institute tarafından yürütülen yakın tarihli bir ankette, bir işletmedeki IoT/OT cihazlarının hem fırsat hem de güvenlik sorununu öne çıkardığı anlaşıldı.[15] Katılımcıların yüzde 68'i IoT/OT kullanımının, kendi stratejik dijital dönüşümleri için kritik öneme sahip olduğunu düşünürken, yüzde 60'ı IoT/OT güvenliğinin IT/OT altyapısının en güvensiz taraflarından biri olduğunu kabul ediyor.

Bir ağa sızmak amacıyla IoT cihazı üretici yazılımındaki güvenlik açıklarını kullanan saldırganlara ilişkin bir örnekte ise Trickboat Truva atı, kurumsal savunma sistemlerini atlatmak üzere Mikrotik yönlendiricilerindeki[16] varsayılan parolalar ve güvenlik açıklarından yararlandı. IoT cihazı üretici yazılımıyla ilgili en temel zorluk, cihazların güvenlik duruşu ve güvenlik açıkları konusunda bilgi eksikliğidir.

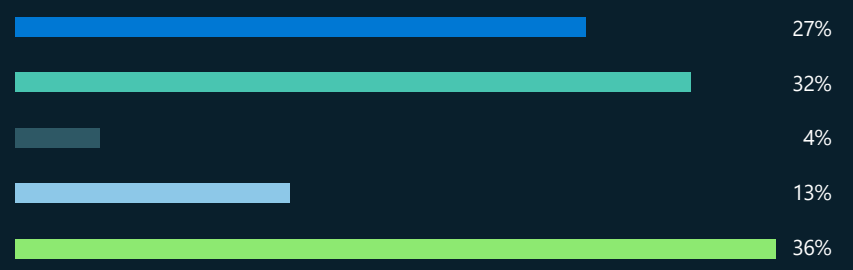
Cihazları güvenli tutmak için kullanılabilecek çözümler olmasına karşın önceden satışı yapılmış ve işletmelere kurulmuş halde milyarlarca cihaz bulunmaktadır. Bunlar, kahverengi alan cihazları olarak bilinir. 2021 yılında Microsoft, kahverengi alan cihaz güvenliğine ışık tutmak ve cihaz imalatçılarının, ürün güvenliğini iyileştirmelerini sağlamak için ReFirm Labs'ı satın aldı. ReFirm Labs, bir cihazın ikili üretici yazılımı imajını analiz eder ve olası güvenlik zayıflıkları hakkında ayrıntılı bir rapor oluşturur.[17] Bu teknoloji, IoT için Microsoft Defender'ın gelecekteki bir sürümüne eklenmektedir.

Geçtiğimiz yıl müşterilerimizin taradığı benzersiz üretici yazılımının sonuçlarını topluca inceledik. Bulunan her zayıflık kötüye kullanılamasa da cihaz üretici yazılımı güvenliğiyle ilgili temel zorluğa dikkat çekiyor.

IoT/OT cihazlarında bulunan zayıflık türlerinin, geleneksel Windows veya Linux uç noktalarında hiçbir zaman kabul edilemeyeceğine dikkat edin.

- Zayıf parolalar: Taranan üretici yazılımı imajlarının yüzde yirmi yedisi, zayıf algoritmalar (MD5/DES) kullanılarak kodlanan ve saldırganlar tarafından kolayca kırılan parolalara sahip hesaplardan oluşuyordu.

Üretici yazılımı imajlarındaki güvenlik zayıflıkları analiz edildi



- Bilinen güvenlik açıkları: Diğer sistemler gibi IoT/OT cihazı üretici yazılımında da açık kaynak kitaplıklardan kapsamlı şekilde yararlanılmıştır. Ancak cihazlar alıcıya genellikle bu bileşenlerin güncel olmayan sürümleriyle gönderilir. Analizimizde, imajların yüzde 32'sinde kritik (9,0 veya üstü) olarak değerlendirilen en az 10 bilinen güvenlik açığı (CVE) vardı. Yüzde dördünde altı yıldan daha eski en az 10 kritik güvenlik açığı vardı.
- Süresi dolmuş sertifikalar: Sertifikalar, bağlantıları ve kimlikleri doğrulamak ve hassas verileri korumak için kullanılır ancak analiz edilen imajların yüzde 13'ünde, üç yıldan uzun bir zaman önce süresi dolmuş en az 10 sertifika vardı.
- Yazılım bileşenleri: İmajların yüzde otuz altısında, Microsoft'un saldırı zincirinin parçası olarak ağ keşfi için kullanılabilen paket yakalama araçları (tcpdump, libpcap) gibi IoT cihazlarından çıkarılmasını önerdiği yazılım bileşenleri bulunmaktadır.

Gerçek hayattaki üretici yazılım saldırıları

Viasat: Uydu iletişimini hedef almak amacıyla üretici yazılımı güvenlik açıklarını kullanma

Şubat 2022'de yaşanan bir uydu ağı olayında, stratejik bir iletişim ağının bağlantısı kesildi ve oluşturduğu etkiler tüm Avrupa'da hissedildi. Viasat'ın KA-SAT sistemi, birçok modemin bağlantısını kesen yüksek miktarda trafik aldı ve ağa yönelik bir hizmet engelleme saldırısı başlatıldı. Sabit geniş bant kesintiye uğradığı için operatörler binlerce rüzgar türbinine uzaktan erişemez hâle geldi, kötü amaçlı wiper malware, etkilenen modemlere kuruldu. Bu aksaklıktan, şirketlerin ve kurumların iletişim için kullandığı 30.000'den fazla uydu terminali etkilendi.

Cyclops Blink: Güvenlik duvarı ağ geçitlerini hedefe almak için üretici yazılımı tedarik zinciri saldırısı kullanma

Tehdit aktörleri için komuta ve kontrol (C2) ve saldırı altyapısının geliştirilmesi ve genişletilmesi, önemli bir başarı bileşenidir. Kararlı bir C2 altyapısına duyulan ihtiyaç arttıkça yönlendiriciler, nadir patch uygulamaları ve kapsamlı güvenlik çözümlerinden yoksun olmalarından dolayı iştah kabartan bir saldırı vektörü hâline geldi.

Microsoft, cihaz güvenliği hakkında daha derinlemesine bilgi sahibi olmak ve yaşam döngüsü boyunca cihaz üreticileri ve operatörleri için güvenliği sağlamak üzere üretici yazılımı analiz teknolojisi konusunda kamu kuruluşları e sektörle iş ortaklığı yapıyor.

Haziran 2019'dan bu yana bir ulus devletle bağlantılı ileri düzey kalıcı tehdit (APT) grubu, kötü amaçlı üretici yazılım güncelleştirmeleri yürüterek ve bunları büyük bir botnet'e dâhil ederek savunmasız WatchGuard güvenlik duvarı cihazlarını ve ASUS yönlendiricilerini hedef aldı ve Cyclops Blink modüler malware'i kullandı. Bu malware, ayrıcalık yükselmesine izin veren bilinen bir güvenlik açığından yararlanarak cihazlara başarılı bir şekilde bulaşmakta ve bu sayede tehdit aktörlerinin cihazı yönetmesine olanak tanımaktadır. MAlware bulaştıktan sonra başka modüllerin yüklenmesine izin verir ve üretici yazılımı güncelleştirmelerini atlatır. Güvenliği risk altına sokulan cihazların, diğer WatchGuard cihazlarında barındırılan C2 sunucularına bağlandığı gözlemlendi. Çeşitli TCP bağlantı noktalarında yer alan kendi C2'leri için birçok SSL sertifikası veren Cyclops Blink operatörleri, kötü amaçlı üretici yazılım güncelleştirmelerini yürüterek ve tarama gibi geleneksel güvenlik yöntemlerini atlatarak ağlara uzaktan ayrıcalıklı olarak erişim olanağı elde etti.

Microsoft tedarik zinciri güvenliğini nasıl iyileştiriyor?

Microsoft, bu IoT ve OT cihazı güvenlik sorunlarını çözmek için kamu kuruluşları ve sektörle iş ortaklığı yapmaktadır (sayfa 6'daki tartışmaya bakın6). Verdiğimiz katkı doğrultusunda, cihaz operatörlerine kendi ağlarındaki cihazların güvenlik duruşu hakkında görünürlük sağlamak üzere üretici yazılımı analiz teknolojisini sunacağız. Bu sayede müşteriler ek koruma, yükseltme veya değiştirme ihtiyacı olan cihazları belirleyip bunlara öncelik verecek. Bunun sonucunda da cihaz üreticilerinin cihaz güvenliğine yatırım talebi artacaktır. Aynı zamanda, kapsamlı çözümlere sahip üreticileri güvenli cihazlar tasarlaması ve güvenli geliştirme yaşam döngülerini benimsemesi konularında destekliyoruz.

Diğer bir önemli nokta ise güvenlik sorunları ortaya çıkarılıp çözüldükçe cihaz üretici yazılımının güncelleştirilmesi için üreticilere ve operatörlere sağlam bir altyapı sağlamaktır. Microsoft, IoT ve OT cihaz güvenliğinin bütün yaşam döngüsüne yönelik bir çözüm sağlamak üzere IoT Hub için Cihaz Güncelleştirmesi ile üretici yazılımı analizini ve IoT için Defender'ı bir araya getiriyor. Bunlar, IoT ve OT çözümlerine yönelik Sıfır Güven yaklaşımını destekleyen cihazların benimsenmesiyle müşterilerin altyapıyı güvence altına almasına ilişkin vizyonumuzu gerçekleştirme yolunda önemli adımlardır.[18]

Saldırganlar, kurumsal ağlara sızmak için IoT cihazlarının üretici yazılımındaki güvenlik açıklarını giderek daha fazla hedef almaktadır.

Eyleme dönüştürülebilir içgörüler

1. Ağınızdaki IoT/OT cihazlarıyla ilgili daha derinlemesine bilgi edinin ve güvenliklerinin risk altında olması halinde bu cihazlara, işletme açısından oluşturacakları riske göre öncelik verin.
2. Olası güvenlik zayıflıklarını anlamak için üretici yazılımı tarama araçlarını kullanın ve yüksek riskli cihazların risklerini nasıl azaltacağınızı anlamak için tedarikçilerle birlikte çalışın.
3. Tedarikçilerinizin güvenli geliştirme yaşam döngüsü en iyi uygulamalarını benimsemesini zorunlu tutarak IoT/OT cihazlarının güvenliğini olumlu yönde etkileyin.

Daha ayrıntılı bilgi için bağlantılar

- ABD Bilgi ve İletişim Teknolojisi Sektörünü Destekleyen Kritik Tedarik Zincirlerinin Değerlendirilmesi

Keşif tabanlı OT saldırıları

Karmaşık tedarik zincirlerinde, gerçek sistemi planlamak için belirli tasarım bilgileri kullanılır. Bu tasarım bilgilerini oluşturan sayısız varlıktan en hassas olanı, ortamı ve içindeki varlıkları tanımlayan proje dosyasıdır. Bu dosya, tamamen ortama özel olarak uyarlanmış erişim elde etmek ve başarılı bir saldırı gerçekleştirmek isteyen tehdit aktörleri için önemli bir stratejik hedeftir.

Operasyonel süreçleri kesintiye uğratmak amacıyla endüstriyel sistemlerin hedeflenmesi iki adımdan oluşur.

1. İlk olarak, saldırganın OT ağına erişmesi gerekir. Bu, ağın kurumsal tarafındaki IoT cihazlarından (Purdue Model Seviyesi 4) girilerek ve geleneksel olarak güvenlik duvarları ve ağ iletişim ekipmanıyla ayrılmış olan IT-OT sınırının çalışma ve kontrol düzeylerine geçiş yapılmasıyla yapılabilir.
2. İkinci olarak, ağ cihazlarının tanımlanması gerekir. Endüstriyel sistemlerde, kendi ortamlarına özgü olarak tasarlanmış özel mimariler içinde standart cihazlar ve bileşenler kullanılır. Bu standart cihazlardan biri de programlanabilir mantık denetleyicisidir (PLC). Her üretici, endüstriyel sistemlerin önemli bir bileşeni olan PLC'leri için benzersiz arabirimler ve işlevler geliştirir; bu cihazlar, müşteriye ait ortamlara özgü tasarlanmış özel şemalarla daha fazla yapılandırılır.

Her bir PLC'nin benzersiz yapılandırması; ortam ve içindeki varlıkların tanımını, merdiven mantığını ve diğer konuları içeren proje dosyasında açıklanmaktadır.

Yapılan analize göre, bir saldırıya ilişkin kanıt gösteren pek çok ortamda, saldırıdan önceki zaman çizelgesinin saldırının kendisinin uzunluğunu çok daha fazla aştığını gösterir. Tehdit aktörleri, ortamı ve içindeki varlıkları uzaktan simüle etmek için aylarını harcayarak bir model inşa etmek ve hedeflenen saldırılarına hazırlanmak için birçok kez girişimde bulunur. Ortamlar sürekli değişkenlik gösterir ve yeni cihazları entegre ederken, özellikle proje ve yapılandırma dosyalarındaki verilerle ilgili güvenlik açıkları ortaya çıkar. Bir proje dosyasının çalınması, saldırıyı haftalara veya aylara yayabilir ve saldırganların hedef ortamı hızlı ve doğru bir şekilde modellemesini sağlayarak kötü amaçlı etkinlikleri tespit etmeyi daha da zorlaştırabilir.

Industroyer ve Incontroller

Modüler malware ve saldırı çerçeveleri kullanan devlet destekli aktörler tarafından kurumlara, kritik altyapılara ve kamu kuruluşları hedeflerine yönelik saldırıların arttığını gözlemledik. Ukrayna'daki kritik operasyonlara müdahale etmeye yönelik yeni girişimler, hedef ortamlarına özel olarak yüksek düzeyde uyarlanmış keşif tabanlı OT saldırı tehditlerinin arttığına dikkat çekmektedir. Ulus devlet siber aktörler tarafından yürütülen genişletilmiş keşif ve araştırma aşamalarına bakıldığında, karma siber-kinetik operasyonlar ve politik strateji açısından belirli stratejik veya operasyonel hedeflere ulaşmaya yönelik altyapıyı uzaktan bozucu siber savaş stratejisinin kullanıldığı anlaşılmaktadır.

Hedef ortamlarına göre özel olarak yüksek düzeyde uyarlanmış, keşif tabanlı OT saldırıları tehdidinin arttığını gözlemledik.

Keşif tabanlı OT saldırıları

Devamı

2022'nin başlarında, iki farklı uyarlanabilir kritik OT saldırısı tespit edildi. 2016 yılında kurulumu yapıldıktan sonra Ukrayna'da elektrik kesintilerine neden olduğu bilinen bir malware olan Industroyer'ın bir varyantının da aralarında bulunduğu özelleştirilmiş bir malware ile Ukrayna'daki elektrik trafo merkezlerine ve koruma rölelerine siber-fiziksel saldırı düzenlendi.

Industroyer2, kötü amaçlı OT saldırı malware'inin yeni bir hedefe yeniden kurulumuna ilişkin ilk örnek olarak karşımıza çıkmaktadır. Bu malware, Industroyer için geliştirilen ve çoğunlukla ABB RTU540/560 model numaralı PLC benzeri uzak terminal birimlerini hedefleyen IEC104 protokolü (güç sistemi izleme ve kontrolüne ilişkin standart protokol) eklentisini kullanmıştır. Bu malware'in yazarı, önceden belirlenmiş çıktılara tekrar tekrar komutlar göndermek için mağdurun ortamına ilişkin bilgileri kullanarak bunların manuel olarak etkinleştirilemeyeceğinden emin oldu. Bu durum, elektrik kesintilerinin uzamasına ve daha fazla zarara neden olan bir etkiye neden oldu.

Aynı dönemde tespit edilen modüler bir saldırı çerçevesi olan Incontroller, eski güvenlik çözümlerini atlatarak OT cihazlarına nüfuz etme ve saldırma süresini önemli ölçüde azaltan modüler bir araç setidir. Genel amaçlı araç seti, farklı ortamlar için üst düzeyde özelleştirilebilir veri toplama, keşif ve saldırı özelliklerine sahiptir; öte yandan bir OT saldırısına yönelik araştırma aşamasını büyük ölçüde etkileyerek keşif yapma için gereken süreyi kısaltır, cihazlar ve cihaz yapılandırmaları hakkındaki bilgileri ayıklayarak ortamların simülasyonunu destekler.

Incontroller çerçevesi, Schneider Electric ve Omron PLC'lerine yönelik protokolleri destekler ve üretici yazılımı sürümü, model türü ve bağlı cihazlar gibi bilgileri toplar. Bu araç seti, yapılandırmaları değiştirme, çıktıları açma ve kapatma komutlarını verebilir. Bir ortama erişim sağlandığında çerçeve, daha fazla yük getirmek için cihazlara arka kapı eklentisi yerleştirmeyi, erişim noktalarını artırmak için güvenlik açıkları oluşturmayı, merdiven mantığını yüklemeyi ve DoS saldırılarını başlatma yeteneğini destekler. Bu araç setinin genel yapısı, bir tehdit aktörünün her PLC veya konum için yeni saldırılar yazmasına gerek kalmadan bir ortama hızlı bir şekilde saldırı düzenlemesini mümkün kılar. Böylece aktörün birçok sektörde potansiyel olarak yer alan farklı türdeki makinelerle kolayca etkileşim kurmasını sağlanmış olur.

Eyleme dönüştürülebilir içgörüler

1. Sistem tanımlarını içeren dosyaları güvenli olmayan kanallar üzerinden veya bunları alması zorunlu olmayan personele aktarmaktan kaçının.
2. Bu tür dosyaları aktarmak kaçınılmaz olduğunda, ağdaki etkinliği takip ettiğinizden ve varlıkların güvende olduğundan emin olun.
3. EDR çözümleriyle izlemeyerek mühendislik istasyonlarını koruyun.
4. OT ağları için olay yanıtını proaktif bir şekilde gerçekleştirin.
5. IoT için Defender benzeri sürekli izleme mekanizmaları kurun.

Son Notlar

1. Bkz. Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au); Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance; Japan passes economic security bill to guard sensitive technology | The Japan Times; Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg); Proposal for legislation to improve the UK's cyber resilience—GOV.UK (www.gov.uk); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework—Journey To CSF 2.0 | NIST
2. Cert-In—Ana Sayfa
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Bkz. başlıksız (house.gov)
5. Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
6. Bkz. Microsoft Güvenlik Geliştirme Yaşam Döngüsü
7. Bkz. Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft—Engineering@Microsoft; ayrıca bkz. The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Bkz. https://www.microsoft.com/en-us/msrc/cvd
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill—product security factsheet—GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe — ENISA (europa.eu)
12. Sertifikasyon - ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool" GitHub - microsoft/sbom-tool: The SBOM tool is a highly scalable and enterprise ready tool to create SPDX 2.2 compatible SBOMs for any variety of artifacts.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. IoT/OT Innovation Critical but Comes with Significant Risks (Dec 2021): https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/
16. Uncovering Trickbot's use of IoT devices in C2 Infrastructure (Mart 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. IoT Show on Channel 9 Episode on IoT Firmware Scanning (Mayıs 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. How to apply a Zero Trust approach to your IoT solutions (Mayıs 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Siber Etki Operasyonları

Günümüzde dış kaynaklı operasyonlarda yeni yöntemler ve teknolojiler kullanılıyor.Böylece güveni sarsmak üzere tasarlanan bunlara ait işlemler daha etkili ve verimli bir hâl alıyor.

Siber Etki

Operasyonlarına genel bakış

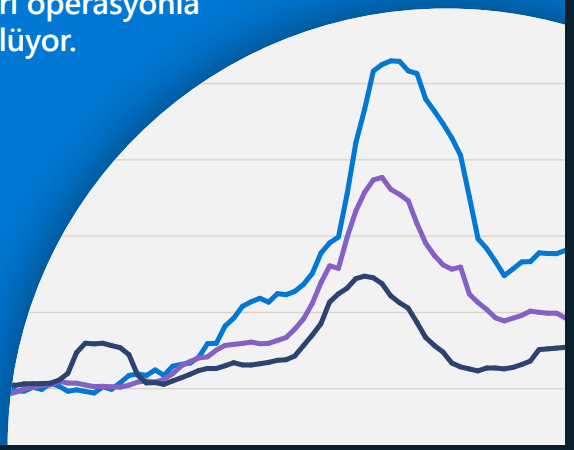
Günümüzde dış kaynaklı operasyonlarda yeni yöntemler ve teknolojiler kullanılıyor. Böylece güveni sarsmak üzere tasarlanan bunlara ait işlemler daha etkili ve verimli bir hâl alıyor.

Ulus devletler, hem yerel hem de uluslararası düzeyde propagandasını yaymak ve kamuoyunu etkilemek amacıyla karmaşık etki operasyonlarını giderek daha fazla kullanıyor. Bu operasyonlar güveni sarsıyor, kutuplaşmayı artırıyor ve demokratik süreçleri tehdit ediyor. Nitelikli İleri Düzeyde Kalıcı Manipülasyon yapan aktörler, operasyonlarının kapsam, ölçek ve verimliliğinin yanı sıra küresel bilgi ekosisteminde sahip oldukları etkiyi büyük ölçüde artırmak için geleneksel medyayı internet ve sosyal medya ile birlikte kullanıyor. Geçen yıl, bu operasyonların Rusya'nın Ukrayna'daki hibrit savaşının bir parçası olarak kullanıldığına şahitlik ettik ancak aynı zamanda Rusya'nın ve Çin ile İran'ın da aralarında olduğu diğer ulusların küresel etkilerini genişletmek amacıyla sosyal medyadan güç alan propaganda operasyonlarını giderek daha fazla kullandıklarını gördük.

Daha fazla kamu kuruluşu ve ulus devlet; görüşleri şekillendirmek, düşmanları itibarsızlaştırmak ve anlaşmazlığı teşvik etmek amacıyla siber etki operasyonları kullandığı için bu operasyonlar daha da karmaşık bir hâle geliyor.

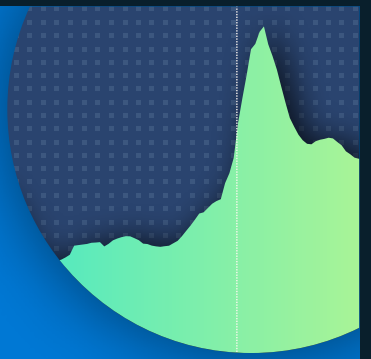
Daha fazla bilgi için bkz. sayfa 74

Rusya'nın Ukrayna işgalinde, siber etki operasyonlarının etkiyi en üst düzeye çıkarmak için daha fazla geleneksel siber saldırı ve kinetik askeri operasyonla entegre edildiği görülüyor.



Daha fazla bilgi için bkz. sayfa 76

Rusya, İran ve Çin, COVID-19 salgınında genellikle daha geniş siyasi hedeflere ulaşmak için stratejik bir araç olarak propaganda ve etki kampanyalarını kullandılar.



Daha fazla bilgi için bkz. sayfa 76

Sentetik medya, son derece gerçekçi yapay görüntü, video ve sesleri kolayca oluşturup yayan araçların popüler hâle gelmesiyle daha çok kullanılmaktadır. Medya varlığının kökenini onaylayan dijital kaynak teknolojisi, yanlış kullanıma karşı mücadeleyi amaçlar.

Daha fazla bilgi için bkz. sayfa 80

Siber etki operasyonlarına karşı korunmaya yönelik bütünsel yaklaşım

Microsoft, siber etki operasyonlarıyla mücadele etmek için yeterli olgunluğa ulaşmış siber tehdit istihbarat altyapısına güveniyor. Stratejimiz, yabancı saldırganların propaganda kampanyalarını tespit etmek, bozmak, bunlara karşı savunmada bulunmak ve caydırmaktır.

Daha fazla bilgi için bkz. sayfa 83

Giriş

Demokrasinin gelişmesi için güvenilir bilgiler gereklidir. Ulus devletler tarafından geliştirilen ve icra edilen etki operasyonları, Microsoft için önemli bir odak alanıdır. Bu operasyonlar güveni sarsıyor, kutuplaşmayı artırıyor ve demokratik süreçleri tehdit ediyor.

Yabancı etki operasyonları bilgi ekosistemi için her zaman bir tehdit olmuştur. Öte yandan internet ve sosyal medya çağında operasyonların kapsamı, ölçeği ve etkinliği büyük ölçüde artarak farklılık gösteriyor; bunlar dünyadaki bilgi ekosisteminin sağlığı üzerinde büyük bir etki oluşturabilir.

Asırlık "Gerçek, ayakkabılarını giymeden yalan dünyayı üç kez dolaşır" özdeyişi artık veri konusunda gerçeğe dönüşüyor. Massachusetts Institute of Technology (MIT) tarafından yapılan bir çalışmada[1] yalan bilginin retweet edilme olasılığının gerçek bilgiye kıyasla yüzde 70 daha yüksek olduğu ve ilk 1.500 kişiye altı kat daha hızlı ulaştığı tespit edildi. Propaganda kampanyaları internette ve sosyal medyada yankı bulup geleneksel haberlere duyulan güveni baltalarken, bilgi ekosistemi de giderek daha belirsiz hâle gelmektedir. 2021 yılında yapılan bir çalışmada[2] ABD'deki yetişkinlerin yalnızca yüzde yedisi gazete, televizyon ve radyo haberlerine "büyük" güven duyduklarını söylerken, yüzde 34'ü "hiçbirine" güvenmediğini ifade etti.

Microsoft, yabancı siber etki alanındaki ana aktörleri, tehditleri ve taktikleri belirlemek ve öğrenilen dersleri paylaşmak için çaba sarf ediyor. Bu yılın Haziran ayında, Ukrayna'dan çıkarılan dersler hakkında Rusya'nın siber etki operasyonlarına dair ayrıntılı bilgi sunan kapsamlı bir rapor yayımladık.[3]

Ayrıca, derin sahtecilik gibi ileri düzey teknolojilerin nasıl kötüye kullanılabileceğini ve gazetecilerin güvenilirliğinin nasıl zayıflatabileceğini de inceliyoruz. Ek olarak yalan bilgileri tespit edebilen yapay zeka (AI) sistemleri gibi sentetik medyayı belirlemeye ve güveni yeniden sağlamaya yönelik daha iyi yolları bulmak için sektör, kamu kuruluşları ve akademi kurumlarıyla birlikte çalışıyoruz.

Etki operasyonlarıyla geleneksel siber saldırıların iç içe geçmesi ve demokratik seçimlere yapılan müdahaleler dahil, bilgi ekosisteminin ve ulus devletlerin online propagandasının niteliğinin hızla değişmesi sonucunda demokrasiye yönelik hem online hem de çevrimdışı tehditleri hafifletmeye yönelik, toplumun bütününü kapsayan bir yaklaşım gerekli hâle geldi.

Microsoft, güvenilir haberlerin ve bilgilerin paylaşıldığı sağlıklı bir bilgi ekosistemini desteklemek için kararlı bir şekilde çalışmaktadır. Ulus devletlerin etkisiyle şekillenen operasyonların getirdiği artan ve büyüyen risklerle mücadele etmeye yönelik araçlar ve tehdit algılama yetenekleri geliştiriyoruz. Bu çalışmaları uygulamaya koymak için yakın zamanda Miburo Solutions'ı satın aldık; Global Dezenformasyon Endeksi ve NewsGuard gibi üçüncü taraf doğrulayıcılarla ortaklık yapıyoruz, İçerik Kaynağı ve Gerçekliği Koalisyonu (C2PA) dahil olmak üzere, çok sayıda paydaştan oluşan ortaklıklara katılıyor ve zaman zaman liderlik ediyoruz. Demokratik süreçleri ve kurumları zayıflatmaya çalışanları, ancak hep birlikte çalışarak bozguna uğratabiliriz.

Teresa Hutson

Başkan Yardımcısı, Teknoloji ve Kurumsal Sorumluluk

Siber etki operasyonlarındaki trendler

Teknoloji gelişirken siber etki operasyonları da giderek daha karmaşık hâle geliyor. Siber etki operasyonlarına uygulanan geleneksel siber saldırılarda kullanılan araçların çakıştığını ve genişlediğini görüyoruz. Buna ek olarak, ulus devletler arasındaki koordinasyon ve güç birliğinde de bir artış göze çarpıyor.

Microsoft, bu yıl yabancı etki operasyonlarının analizi konusunda uzman bir kurum olan Miburo Solutions'ı satın alarak yabancı etki operasyonlarıyla mücadeleye yatırım yaptı. Microsoft, bu analistleri kendi tehdit analistleriyle bir araya getirerek Dijital Tehdit Analiz Merkezini (DTAC) kurdu. DTAC, hem siber saldırılar hem de etki operasyonları dahil ulus devletlerden gelen tehditleri analiz edip raporluyor; bilgiler ve tehdit istihbaratını jeopolitik analizle bir araya getirip içgörü sağlayarak etkili müdahalelerde bulunuyor ve gerekli korumayı sağlıyor.

Dünyadaki insanların dörtte üçünden fazlası bilginin kötüye kullanılmasından endişe duyduklarını ifade ediyor[4] ve verilerimiz de bu endişeleri destekliyor. Microsoft ve iş ortakları, ulus devlet aktörlerinin stratejik hedeflerine ve siyasal hedeflerine ulaşmak için etki operasyonlarını nasıl kullandıklarını yakından takip ediyor. Otoriter rejimler yıkıcı siber saldırılar ve siber casusluk çalışmalarına ek olarak, görüş şekillendirmek, düşmanları itibarsızlaştırmak, korkuyu salmak, anlaşmazlığı teşvik etmek ve gerçekleri çarpıtmak için siber etki operasyonlarını gittikçe daha fazla kullanıyor.

Bu yabancı siber etki operasyonları genellikle üç aşamalıdır:

Önceden konumlandırma

Malware'in bir kurumun bilgisayar ağına önceden konumlandırılması gibi, yabancı siber etki operasyonları da yanlış bilgileri internette herkesin kolay erişebileceği şekilde önceden konumlandırır. Önceden konumlandırma taktiği uzunca bir süredir, özellikle BT yöneticileri en son ağ etkinliğini taradığı daha fazla sayıda geleneksel siber etkinliğe ön ayak olmuştur. Bir ağda uzunca bir süre uykuda olan malware, bir sonraki kullanımda daha yüksek etki oluşturabilir. İnternette dikkat çekmeyen yanlış bilgiler, daha sonra bunlara yapılan atıfların daha güvenilir görünmesine neden olabilir.

Başlatma

Genellikle aktörün hedeflerine ulaşması için en çok kullanılan yöntem, hükümet destekli ve kamuoyunda etkili olan medya organları ve sosyal medya kanalları aracılığıyla yalan bilgiyi yaymak üzere eşgüdümlü bir kampanya başlatmaktır.

Güçlendirme

Son olarak, ulus devletlerin kontrolündeki medya organları ve aracıları hedef kitlelerin arasında bu söylemleri güçlendirir. Çoğu zaman yalan bilginin farkında olmayan teknoloji önderleri, bu söylemlerin daha geniş kesimlere ulaşmasına ön ayak olur. Örneğin online reklamcılık, finansal faaliyetlerin ve eşgüdümlü içerik sunum sistemlerinin arama motorlarını doldurmasına yardımcı olabilir.

Bu üç adımlı yaklaşım, 2021 yılının sonlarına doğru Ukrayna'da bulunduğu öne sürülen biyolojik silahlara ve biyoloji laboratuvarlara dair Rusya'nın yalan bilgilerini desteklemek amacıyla kullanıldı. Bu söylem ilk defa 29 Kasım 2021 tarihinde, Moskova'da yaşayan bir Amerikalının İngilizce dilinde yayın yaptığı bir YouTube kanalına, ABD tarafından finanse edilen Ukrayna'daki biyoloji laboratuvarlarının biyolojik silahlarla ilişkili olduğunu iddia ettiği bir videonun yüklenmesiyle başladı. Bu iddia çok uzun bir süre dikkat çekmedi. 24 Şubat 2022 tarihinde, tıpkı Rus tanklarının sınırı geçmesi gibi bu söylem de savaş ortamına gönderildi. Microsoft'taki bir veri analitiği ekibi, 24 Şubat'ta "geçen yılki rapora" işaret eden ve buna güvenilirlik kazandırmak isteyen haberleri eş zamanlı olarak paylaşan Rusya kontrolünde veya etkisi altındaki 10 haber sitesini belirledi. Buna ek olarak, Rusya Dışişleri Bakanlığı yetkilileri, bilgi ortamında yer alan ABD biyoloji laboratuvarlarına dair yanlış iddiaları daha da körükleyen basın toplantıları düzenledi. Daha sonra Rusya destekli ekipler, sosyal medya ve internet sitelerindeki söylemi daha geniş kitlelere yaymaya çalıştı.

Dünya çapındaki otoriter rejimlerin bilgi ekosistemini karşılıklı çıkarları için kirletmek üzere birlikte çalıştığını görüyoruz. Örneğin, COVID-19 salgınında Rusya, İran ve Çin, demokrasileri hedef almak ve diğer jeopolitik hedeflere odaklanmak üzere açık, yarı açık ve gizli dağıtım yöntemlerini kullanarak propaganda ve etki operasyonlarını uyguladı.(Konuyla ilgili ayrıntılar için bkz. sayfa 76). Bu üç rejim, seçtikleri iddiaları desteklemek için birbirlerinin mesajlaşma ve bilgi ekosistemlerinde faaliyet gösterdi. Bu haberlerin büyük bir kısmında, kendi COVID-19 aşılarının ve müdahalelerinin Amerika Birleşik Devletleri'nden ve diğer demokrasilerden daha üstün olduğunu öne sürüp resmi açıklamalarında Amerika Birleşik Devletleri ve müttefikleri hakkında eleştiriler ve komplo teorilerine yer verdiler. Devletçe işletilen medya organları, birbirlerine güç katmak suretiyle, demokrasilere ilişkin olumsuz haberlerin paylaşıldığı (veya Rusya, İran ve Çin hakkında pozitif haberlerin paylaşıldığı) ve bir devlet destekli medya organının haberinin, diğerleri tarafından güçlendirildiği bir ekosistem oluşturdu.

ABD biyoloji laboratuvarları ve biyolojik silahlarla ilgili söylemlerin, birçok yabancı etki operasyonunun üç kapsamlı aşaması (önceden konumlandırma, başlatma ve güçlendirme) üzerinden nasıl yayıldığına ilişkin görsel.

Siber etki operasyonlarındaki trendler

Devamı

Özel sektör teknoloji varlıkları farkında olmadan bu kampanyalara aracı olmak suretiyle bu zorluğa katkıda bulunabilir. Bunun olmasını sağlayanlar arasında internet etki alanlarını kaydeden, web sitelerini barındıran, sosyal medya ve arama sitelerinde ürün tanıtan, trafiği yönlendiren ve dijital reklamcılık yoluyla bu çalışmalar için ödeme yapılmasına yardımcı olan kurumlar vardır. Kurumlar, siber etki operasyonları için otoriter rejimlerin kullandığı araç ve yöntemlerden haberdar olmalıdır. Bu şekilde kampanyaların yayılmasını tespit edip önleyebilirler. Ayrıca, tüketicilerin yabancı etki operasyonlarını belirleyip bunlardaki söylem veya içeriklerle etkileşimi sınırlayabilmek anlamında daha karmaşık bir yetenek geliştirmelerine yardımcı olmak, gittikçe daha önemli bir ihtiyaç hâline geliyor.

Otoriter propaganda dahil siber etki operasyonları; güveni sarstığı, kutuplaşmayı artırdığı ve demokratik süreçleri tehdit ettiği için dünya demokrasilerine yönelik bir tehdit olarak karşımıza çıkmaktadır.

Şeffaflığı artırmak, bu etki kampanyalarını gün yüzüne çıkarıp sekteye uğratmak için devlet, özel sektör ve sivil toplum arasında koordinasyon ve bilgi paylaşımının artması gerekiyor.

Dünya genelinde insanların dörtte üçünden fazlası bilginin bir silah hâline getirilmesinden endişe ediyor.

COVID-19 ve Rusya'nın Ukrayna'yı işgali sırasındaki etki operasyonlarında öne çıkanlar

Pandemide ve Rusya'nın Ukrayna'yı işgali sırasında bilgi ortamını kontrol etmeye çalışan ulus devletler, otoriter rejimlerin siber ve bilgi operasyonlarını nasıl harmanladığına ilişkin çok açık örnekler sunuyor.

COVID-19 propagandası

Rusya, İran ve Çin, COVID-19 pandemisinde propaganda ve etki kampanyalarından yararlandı. COVID-19 bu kampanyalarda başlıca iki şekilde öne çıktı:

1. Bizzat pandemiyle ilgili sunumlar.
2. Daha geniş siyasi hedeflere ulaşmak üzere COVID-19'un stratejik bir araç olarak kullanıldığı kampanyalar.

Bu tür kampanyaların geniş çerçevedeki amacı iki yönlüdür: Birincisi, demokrasileri, demokratik kurumları ve ABD ile müttefiklerinin dünya arenasındaki imajını baltalamak; ikincisi ise yurt içinde ve dışında kendi konumlarını güçlendirmek.

Rus hükümetinin COVID-19 aşısı ve salgının ciddiyeti hakkında kendi halkıyla iletişim kurma şekline karşı İngilizce bilen okuyucuları hedefleyen, bilinen Rus hesapları ve medya kuruluşları tarafından verilen mesajlarda buna ilişkin örneklere rastlamaktayız.

RT.com'da en çok görüntülenen 10 koronavirüs haberinde yer alan konular (Ekim 2021–Nisan 2022)

Aşı karşıtı propaganda Rus olmayan okuyucuları hedef alıyor

Rusça (İngilizce çevirisi aşağıdadır)	İngilizce
"Kapanmalar ve hatırlatma dozları, bulaşı engelliyor"	"Aşılar bulaşmanın önüne geçemiyor ve yeni varyantlara karşı etkisiz"
"Rusya'da kamuya mal olmuş pek çok kişinin COVID testi pozitif çıkıyor"	"Pfizer aşısının tehlikeli yan etkileri var"
"Rusya'da vaka ve ölüm sayısı artış gösteriyor"	"Kitlesel aşılama siyasi amaçlıdır"
"Sputnik V aşısı son derece etkili"	"Pfizer ve Moderna mevzuata uygun olmayan denemeler yapıyor"
"Toplu taşımada aşı belgesi gerekli"	

Rusça yazılan COVID-19 mesajları dile göre farklılık gösteriyor.

COVID-19 virüsünün kaynağını başka şekilde yansıtmaya çalışan kampanyalar ise başka bir örnek olarak alınabilir. Pandeminin başlangıcından beri Rusya, İran ve Çin'in COVID-19 propagandasında, bu ana temaların etkisini güçlendirmeye yönelik diğerlerinden gelen haber yorumlara daha çok yer verildi. Bu haberlerin çoğu, Amerika Birleşik Devletleri hakkındaki eleştirileri veya komplo teorilerini desteklemekten ibaretti. Devletçe işletilen medya organları, birbirlerine güç katmak suretiyle, demokrasilere ilişkin olumsuz haberlerin paylaşıldığı (veya Rusya, İran ve Çin hakkında pozitif haberlerin paylaşıldığı) ve bir devlet destekli medya organının haberinin, diğerleri tarafından güçlendirildiği bir ekosistem oluşturdu.

Rusya ve İran devlet medyasının COVID-19'un ABD tarafından geliştirilen bir biyolojik silah olabileceği yönündeki iddiaları ise buna ilişkin bir başka örnektir. Bu iddia, pandeminin başlarında COVID-19'un bir silah olarak geliştirildiğini iddia eden bir hukuk profesörüyle yapılan röportajın ardından, diğer komplo web sitelerinde dolaştı.[6] Bu röportaj, sınırlı erişimi olan birkaç web sitesinde paylaşıldıktan sonra, haber devlete ait medya organları tarafından alındı. İran hükümeti tarafından desteklenen, İngilizce ve Fransızca dillerinde yayın yapan PressTV,[7] Şubat 2020'de "Koronavirüs, Francis Boyle'un inandığı gibi ABD'nin bir biyolojik savaş silahı mı?" başlıklı İngilizce bir haber yayımladı. Bu makalede COVID-19 salgınının arkasında ABD'nin olduğunu öne sürülerek, "Tüm ABD savaşlarında radyolojik, kimyasal, biyolojik ve yasaklanmış diğer silahlar kullanılıyor ve hedeflenen bölgelerdeki insanlar çok büyük zarar görüyor." ifadeleri kullanıldı.[8] Rus devlet medya organları ve Çin hükümetine ait hesaplar da bu ifadeyi dillendirdi. Kremlin'in propagandasının yayılmasındaki rolüyle bilinen devlete ait bir yayın kuruluşu olan Russia Today (RT),[9] İranlı yetkililerin COVID-19'un "ABD'nin İran'a ve Çin'e yönelik 'biyolojik saldırısının' bir ürünü" olabileceğini iddia eden açıklamalarını destekleyen en az bir haber yayınladı[10] ve öte yandan buna dikkat çeken sosyal medya paylaşımlarında bulundu. Örneğin, RT'nin 27 Şubat 2020 tarihli tweet'inde şöyle bir ifade yer almaktadır: "Ellerinizi kaldırın, bir gün #coronavirus'ün biyolojik silah olduğu ortaya çıkarsa kimler şaşırmayacak?"[11]

Ukrayna'daki savaş: propagandanın savaş silahı olarak kullanımı

Rusya'nın Ukrayna'yı işgali, siber etki operasyonlarının tesirini en üst düzeye çıkarmak için daha geleneksel siber saldırılar ve karada yürütülen askeri operasyonlarla nasıl birleştirilebileceğine dair apaçık bir örnek sunmaktadır.

Microsoft'taki tehdit bilgileri analistleri, Ukrayna'nın işgaline giden yolda Rusya ile yakın ilişkileri olan en az altı farklı aktörün Ukrayna'ya karşı 237'den fazla siber saldırı düzenlediğini tespit etti. Bu operasyonlar; hizmetleri ve kurumları bozmayı, Ukraynalıların güvenilir bilgiye erişimini engellemeyi ve ülkenin yönetimi hakkında şüpheler duymalarını amaçlıyordu.

COVID-19 ve Rusya'nın Ukrayna'yı işgali sırasındaki etki operasyonlarında öne çıkanlar

Devamı

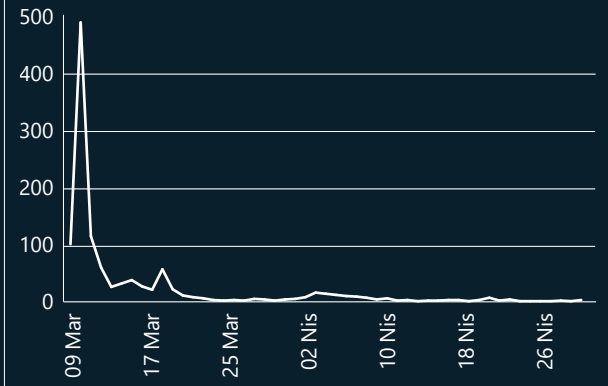
Microsoft'un Nisan 2022'de yayınlandığı raporda, Rusya'nın Kiev'deki bilgi ortamını kontrol altına almak üzere açık bir girişimde bulunduğunu, Ukrayna'nın önde gelen medya kurumuna karşı yıkıcı bir malware başlattığı gün Kiev'deki bir televizyon kulesine de füze saldırısı düzenlediğini ortaya çıkardık.[12]

Siber saldırıların ve etki operasyonlarının nasıl ayarlandığına dair başka bir örnekte, bir Rus tehdit aktörü Ukrayna vatandaşlarına Mariupol sakinlerinden geldiği iddia edilen e-postalar göndererek, Ukrayna hükümetini savaşı tırmandırmaktan sorumlu tuttu ve vatandaşlarını hükümete karşı geri adım atmaya çağırdı. Bu e-postalar, özel olarak e-postayı alan kişilere adlarıyla hitap ediyordu; bu durum bilgilerin daha önceki bir casusluk siber saldırısında çalınmış olabileceğini gösteriyor. Hiçbir kötü amaçlı bağlantının bulunmaması, buradaki niyetin tamamen etki operasyonları gerçekleştirmek olduğunu gösteriyor.

Bilgisayar korsanlığı ile ele geçirilen, sızdırılan veya başka bir şekilde edinilen, hassas olduğu iddia edilen materyalleri yayınlamak Rus aktörlerin etki operasyonlarında yaygın şekilde kullandığı bir taktiktir. Ukrayna'daki savaş süresince Rusya yanlısı sosyal medya kanalları, Ukrayna kaynaklarından sızdırıldığını ya da başka bir şekilde edinildiğini iddia ettikleri hassas materyallerin tanıtımını yaptı. Sızdırılan veya hassas nitelikteki materyaller, Rusya yanlısı sosyal medya kanalları ve kuruluşları tarafından, kurumlara olan güveni azaltmak ve ana akım söylemlere karşı şüphe düşürmek için daha geniş bir etki stratejisinin parçası olarak kullanılıyor. Bu bilgiler, Ukrayna ve Batı'yı hedef alan propaganda oluşturmak, dijital güvenliğe olan güveni azaltmak ve Batı'nın Ukrayna'ya yaptığı yardıma verilen desteği sekteye uğratmak için manipüle edilebilir.

Rusya, sahadaki olaylardan sonra gerçekleri karartmak veya zedelemek için başka bilgi saldırılarını kullanarak kamuoyunu şekillendirdi. Örneğin, 7 Mart tarihinde Rusya, Birleşmiş Milletler (BM) nezdinde yaptığı bir başvuruyla Ukrayna'nın Mariupol kentindeki bir kadın doğum hastanesinin boşaltıldığına ve askeri bir alan olarak kullanıldığına dair bir söylemi önceden konumlandırdı. 9 Mart tarihinde Rusya bu hastaneyi bombaladı. Bombalama haberinin ardından Rusya'nın BM temsilcisi Dmitry Polyanskiy, bombalama haberlerinin "sahte haber" olduğuna dair tweet attı ve bu hastanenin alan olarak kullanıldığına ilişkin Rusya'nın daha önceki iddialarına atıfta bulundu. Rusya daha sonra bu söylemi, hastaneye yapılan saldırının ardından iki hafta boyunca Rus destekli web sitelerinde geniş çapta dile getirdi.

Trafik bilgisi içeren etki alanları
(9Mart 2022 - 30 Nisan 2022)



Propaganda web siteleri, 1 Nisan 2022 tarihinde başlayan kısa bir yeniden gösterimle birlikte yaklaşık iki hafta boyunca kadın doğum hastanesi hakkında hikayeler paylaştı. Kaynak: Microsoft AI for Good Lab.

Şubat ve Mart 2022'de Mariupol'daki bir doğum hastanesine ait uydu görüntüleri

Microsoft'un kendi uydu görüntüsü analizinde doğum hastanesinin bombalandığı görüldü. İlk fotoğraf 24 Şubat 2022, ikincisi ise 24 Mart 2022 tarihlidir. Fotoğraf kaynağı: Planet Labs.

Rusya'nın vahşeti örtbas etmesi, savaşın ilerleyen safhalarında da devam etti. Örneğin, 2022'nin Haziran ayının sonlarına doğru Rus medya organları ve etki sahibi kişiler, bir alışveriş merkezinin bombalanmasını haklı bir gerekçeymiş gibi göstererek, yalan bilgiler üreterek bu binanın bir alışveriş merkezi olarak kullanılmadığını, bunun yerine Ukrayna bölge savunma güçlerinin cephaneliği olarak kullanıldığını iddia etti.[13] Telegram'da Kremlin yanlısı birkaç blog yazarı "sahte bayrak" söylemini destekleyen içerikler yayınladı ve iddialarını güçlendirdi. Blog yazarları, olay yerinden gelen görüntülerde askeri üniforma giyen insanların varlığı[14] ve görüntülerde kadınların olmaması gibi uydurma verilere işaret etti.[15] Rusya, dışarıda oluşturulan propaganda habercileri ve ortamlarından oluşan bir sistemi etrafında şekillenen kampanyalar başlattı. Bu hikayelerin internet online olarak güçlendirilmesi, Rusya'ya uluslararası arenada suçu saptırma ve hesap verme sorumluluğundan kaçma imkanı sağlıyor.

Rusya gibi ulus devletler, kamuoyundaki algıyı etkilemek için kapalı kaynaklardan elde edilen bilgileri kullanmanın, karşı söylemleri yaymak ve güvensizlik oluşturmak için "korsanlık ve sızdırma" operasyonlarını kullanmanın değerinin farkında.

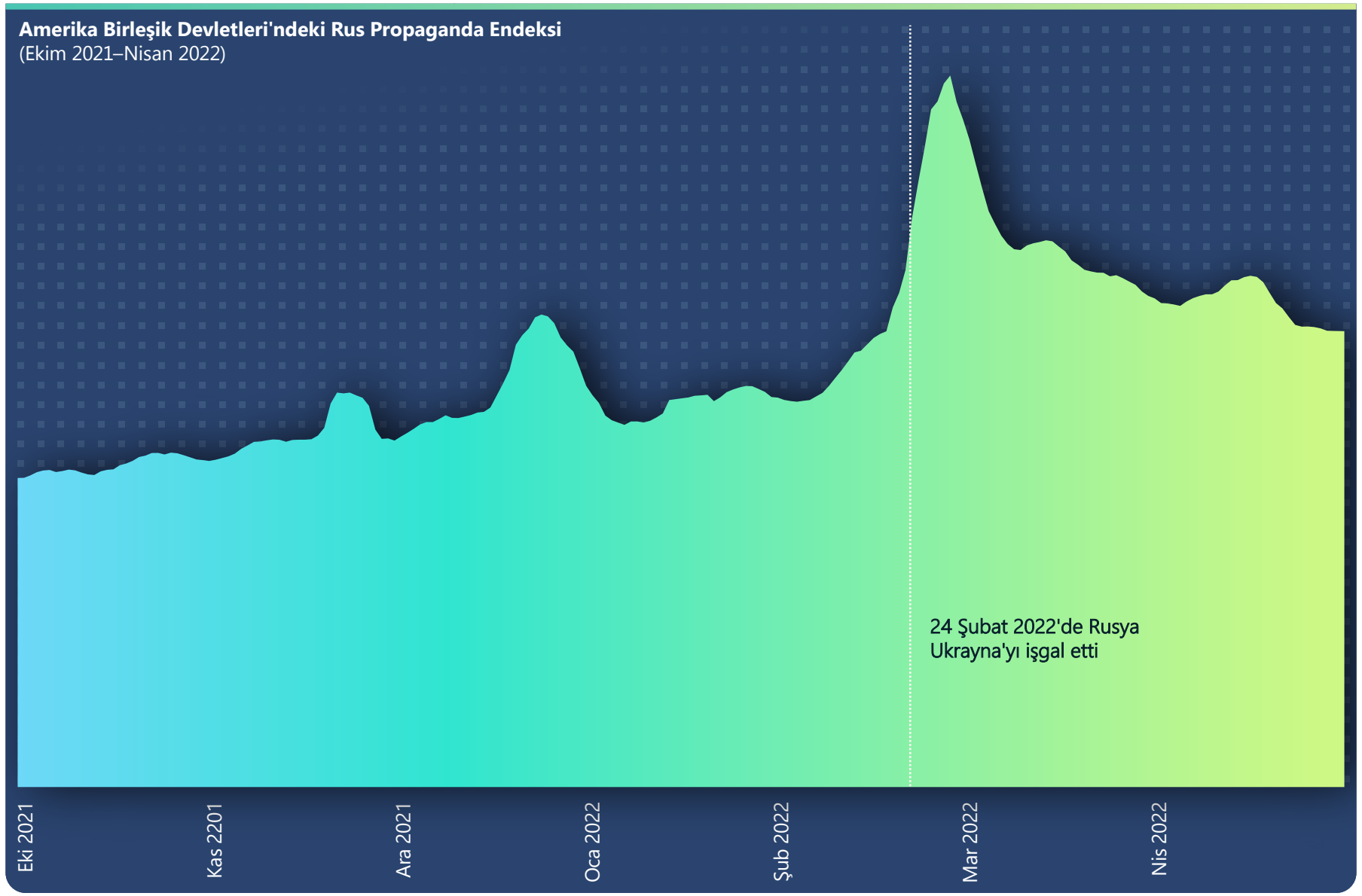
Daha ayrıntılı bilgi için bağlantılar

- Ukrayna'yı Savunmak: Siber Savaştan Çıkarılan İlk Dersler | Microsoft On the Issues
- Rusya'nın Ukrayna'daki siber saldırı faaliyetlerine genel bir bakış | Microsoft Özel Raporu
- Ukrayna'yı hedef alan siber saldırıları engellemek | Microsoft On the Issues

Rus Propaganda Endeksini izleme

Ocak 2022'de bin kadar ABD web sitesi trafiği, Rus propaganda web sitelerine yönlendiriliyordu. ABD'li bir kitleyi hedef alan Rus propaganda web sitelerinin paylaştığı en yaygın konular; Ukrayna'daki savaş, ABD iç siyaseti (Trump yanlısı veya Biden yanlısı), COVID-19 ve aşılarla ilgili söylemlerdi.

Rus Propaganda Endeksi (RPI), Rusya devlet kontrolündeki ve sponsorluğundaki haber kuruluşları ve destekleyici güçlerden gelen haber akışını internetteki genel haber trafiğine oranlayarak takip eder. RPI, internetteki ve farklı coğrafyalardaki Rus propagandası kullanımını kesin bir zaman çizelgesinde grafik şeklinde göstermek için kullanılabilir. Ancak Microsoft, sadece daha önceden belirlenmiş web sitelerinde yayınlanan Rus propagandasını gözlemleyebileceğimize dikkat çekiyor. Güvenilir haber web siteleri, tanımlanmamış web siteleri ve sosyal medya grupları gibi diğer türlerdeki web sitelerinde yapılan propagandalar hakkında bir içgörümüz yok.



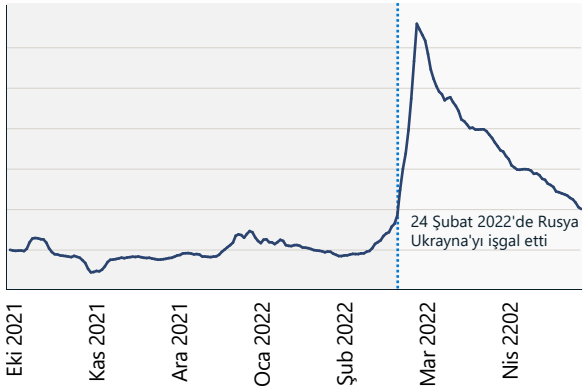
Rus Propaganda Endeksini izleme

Devamı

Rus Propaganda Endeksi: Ukrayna

Ukrayna savaşı başladığında, Rus propagandasında yüzde 216'lık bir artış gözlemledik; bu artış 2 Mart'ta zirve noktasına ulaştı. Aşağıdaki grafikte, bu ani yükselişin işgalle aynı zaman denk geldiği görülüyor. Bu iki grafik, işgal başladıktan kısa bir süre sonra Rus propagandasındaki artışı gösteriyor.

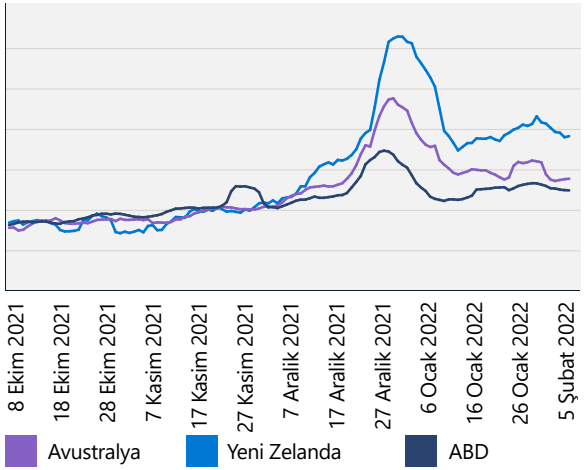
RPI, Ukrayna
(7 Ekim 2021–30 Nisan 2022)



Rus Propaganda Endeksi: Yeni Zelanda, Avustralya ve Amerika Birleşik Devletleri

Yeni Zelanda'daki RPI değerlendirmesi, 2021 yılının COVID-19 propagandasıyla ilgili artışı ortaya koydu. Yeni Zelanda'daki Rus propaganda kullanımındaki bu artış, 2022 yılının başlarında Wellington'daki halk protestolarının başlamasından önce kaydedildi. İkinci artış, açık bir şekilde Rusya'nın Ukrayna'yı işgaliyle ilgiliydi ve Avustralya ile ABD'nin RPI'larını geride bıraktı.

RPI, Yeni Zelanda, Avustralya ve Amerika Birleşik Devletleri



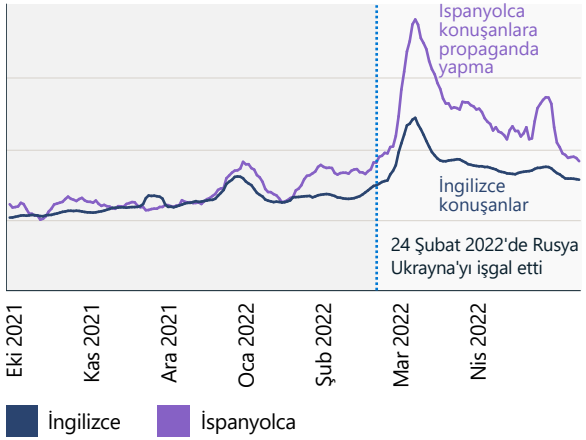
Yeni Zelanda'daki Rus propaganda kullanımı, 2021 Aralık ayının ilk haftasına kadar Avustralya'dakine benzer. Aralık ayından sonra Yeni Zelanda'daki Rus propaganda kullanımı, Avustralya ve Amerika Birleşik Devletleri'ndeki kullanıma göre yüzde 30'un üzerinde artış gösterdi.

Amerika Birleşik Devletleri'nde Rus Propaganda Endeksi: İngilizce ve İspanyolca

RPI, propagandayı ayrıca diller bazında da takip eder. RT ve Sputnik News gibi farklı medya organları 20'den fazla dilde yayın yapmaktadır. Bu diller arasında İngilizce, İspanyolca, Almanca, Fransızca, Yunanca, İtalyanca, Çekçe, Lehçe, Sırpça, Letonca, Litvanca, Moldovaca, Beyaz Rusça, Ermenice, Osetçe, Gürcüce, Azerice, Arapça, Türkçe, Farsça ve Darice var.

Aşağıdaki grafikte, Amerika Birleşik Devletleri'ndeki İspanyolca haberlere ilişkin RPI'ının İngilizce haberler için olandan çok daha yüksek olduğu görülüyor.

Rus propaganda kullanımı İspanyolca konuşanlar arasında 2 kat daha yüksek



Amerika Birleşik Devletleri'ndeki Rus propaganda kullanımı, İspanyolca konuşanlar arasında iki kat daha fazla.

Latin Amerika'da Rus propagandası çok fazla

İspanyolca yayın yapan RT, en fazla sayfa görüntüleme ve Facebook takipçisi olan uluslararası haber kanalıdır.

Kaynak: Microsoft AI for Good Research Lab

Sentetik medya

Yapay zeka destekli medya oluşturma ve manipülasyonu bakımından altın bir çağa giriyoruz. Microsoft analistleri, bunun iki ana eğilim etrafında şekillendiğine dikkat çekiyor: son derece gerçekçi sentetik görüntü, video, ses ve metinler oluşturmak için kullanımı kolay araçların ve hizmetlerin yaygınlaşması ve belirli kitleler için optimize edilmiş içeriği hızla yayma yeteneği.

Bu gelişmelerin hiçbiri, yapısı gereği tek tek ele alındığında sorunlu değildir. Yapay zeka tabanlı teknoloji, ister tamamen sentetik isterse mevcut materyali geliştiriyor olsun, eğlenceli ve heyecan verici dijital içerik oluşturmak maksadıyla kullanılabilir. Bu araçlar, işletmeler tarafından reklam ve iletişim amacıyla ve bireyler tarafından takipçilerine ilgi çekici içerikler oluşturmak amacıyla yaygın olarak kullanılıyor. Ancak sentetik medya zarar verme niyetiyle oluşturulup ve dağıtıldığında bireylere, şirketlere, kurumlara ve topluma ciddi zararlar verebilir. Microsoft, bu zararları sınırlamak için hem kurum içinde hem de daha geniş çerçevedeki medya ekosisteminde teknolojiler ve uygulamalar geliştirme yönünde itici bir güç olmuştur.

Bu bölümde, zararlı sentetik içerik oluşturmaya yönelik mevcut en son teknolojiye ilişkin Microsoft analizinden elde edilen içgörüler, bu içeriğin geniş çapta yayılması durumunda ortaya çıkabilecek zararlar ve sentetik medya tabanlı siber tehditlere savunmada kullanılabilecek teknik etki hafifletme adımları inceleniyor.

Sentetik medya oluşturma

Bir zamanlar sadece büyük film stüdyolarındaki devasa bilişim kaynaklarıyla mümkün olan teknikler artık telefon uygulamalarına kolayca entegre edildiğinden, sentetik metin ve medya alanı inanılmaz bir ivmeyle ilerliyor. Aynı zamanda, araçlar da daha kolay kullanılabilir hâle geliyor ve adli medya uzmanlarını bile yanıltabilecek düzeyde gerçekçi içerikler üretebiliyor. Artık bir kişinin herhangi bir şeyi söylediği veya yaptığı sentetik videolar oluşturmamıza çok az zaman kaldı. Dijital ortamda gördüğümüz içeriğin önemli bir kısmının yapay zeka teknikleriyle tamamen veya kısmen sentetik yapıya büründürüldüğü bir çağa girdiğimizi söylesek yanlış olmaz.

> Daha karmaşık, kullanımı kolay ve yaygın bulunan araçların geliştirilmesiyle beraber sentetik içerik oluşturma trendi yükselişe geçti; çok yakında bunları gerçek bilgiden ayırt etmek güç olacak.

Halen kullanımda olan birçok yüksek kaliteli ücretsiz ve ticari resim, video ve ses düzenleme aracı var. Bu araçlar; yanıltıcı metin ekleme, yüz değiştirme ve bağlamı kaldırma veya değiştirme gibi dijital içeriklerde basit ama potansiyel olarak zarar verici değişiklikler yapmak amacıyla kullanılabilir. Bu tür "ucuz sahte üretimler"; kötü içeriği yaymak, siyasi ideolojileri desteklemek ve itibara zarar vermek için yaygın olarak kullanılıyor. 2019 yılında[16] ABD Temsilciler Meclisi Başkanı Nancy Pelosi'nin konuşmasını geveleyerek ve sarhoşmuş gibi yaptığını gösteren video, bunun en iyi bilinen örneğidir. Bu efekti vermek için videonun yavaşlatıldığı çabucak tespit edilmiş olsa da, orijinal video ve bağlam ortaya çıkmadan önce bu "ucuz sahte üretim" çok büyük yankı buldu.

Medya içeriğini değiştirmeye yönelik daha karmaşık yaklaşımlar arasında; (a) tamamen sentetik medya oluşturmak ve (b) mevcut medyada daha karmaşık düzenlemeler yapmak için ileri düzey yapay zeka tekniklerinin uygulanması yer alıyor. Derin sahtecilik terimi genellikle son teknoloji yapay zeka tekniklerinden yararlanılarak oluşturulan sentetik medya için kullanılır (bu ad, bazen ara sıra kullanılan derin sinir ağlarından geliyor). Bu teknolojiler; bağımsız uygulamalar, araçlar ve hizmetler şeklinde geliştiriliyor, yerleşik ticari ve açık kaynaklı düzenleme araçlarına entegre ediliyor.

Bu gibi teknolojiler, kişilere ve kurumlara zarar vermeyi amaçlayan kötü aktörler tarafından bir silah gibi kullanılmaktadır. Derin sahtecilik tekniklerine ilişkin örnekler:

- **Yüz değiştirme (video, görüntü):** bir videodaki yüzü bir başkasının yüzüyle değiştirme. Bu teknik; bir kişi, kurum veya kuruluşa şantaj yapmak veya kişileri utanılacak konuma veya duruma sokmak için kullanılabilir.
- **Kuklacılık yapma (video, görüntü):** hareketsiz bir görüntü veya ikinci bir video ile animasyon yapmak üzere video kullanma. Böylece bir kişinin utanç verici veya yanıltıcı bir şey söylediği izlenimi verilebilir.
- **Çekişmeli üretici ağlar (video, görüntü):** fotogerçekçi görüntüler oluşturmak için kullanılan teknikler grubu.
- **Dönüştürücü modeller (video, görüntü, metin):** metin açıklamalarını kullanarak zengin görüntüler oluşturma.

Bu tür ileri düzey yapay zeka tabanlı teknikler, günümüzde siber etki kampanyalarında henüz yaygın olarak kullanılmamakla birlikte, bu araçların kullanımı daha kolay ve daha yaygın hâle geldikçe bu sorunun büyümesini bekliyoruz.

Sentetik medya manipülasyonunun etkisi

Zarar vermek veya etkiyi genişletmek amacıyla bilgi operasyonlarının kullanılması yeni bir olgu değildir. Bununla birlikte, bilginin yayılma hızı ve gerçeği kurgudan hemen ayırma yeteneğimizin olmayışı, Pelosi örneğinde oldu gibi, sahte ve sentetik olarak oluşturulmuş diğer kötü niyetli medya materyallerinin yol açtığı etki ve zararın çok daha büyük olabileceği anlamına gelir.

Dikkate alınacak birkaç zarar kategorisi bulunmaktadır: piyasa manipülasyonu, ödeme dolandırıcılığı, sesli kimlik avı, başka birinin kimliğine bürünme, marka zararı, itibar zedelemesi ve botnet'ler. Bu kategorilerin birçoğunda, gerçeği kurgudan ayırmamızı zora sokabilecek gerçek hayattan örnekler kapsamlı olarak rapor edildi.

Gördüklerimize ve duyduklarımıza artık güvenemediğimizde, neyin doğru neyin yanlış olduğunu ayırt edememek daha uzun vadeli ve sinsi bir tehdittir. Bu nedenle, bir kamu figürünün veya özel şahsiyetin itibarını zedeleyen görüntü, ses veya video sahte olduğu gerekçesiyle reddedilebilir; bu durum Yalancının Yanına Kâr Kalma olarak bilinen bir sonuçtur.[17] Yakın zamanda yapılan bir araştırma[18] diğer birçok kötüye kullanım senaryosu akla yatkın görünse de, bu teknolojinin kötüye kullanımının finansal sistemlere saldırmak amacıyla zaten kullanıldığını göstermektedir.

Sentetik medya

Devamı

Sentetik medyayı tespit etme

Sentetik medyayı tespit etmek, etkisini azaltmak ve güveni yeniden tesis etmeye yönelik daha iyi yollar geliştirmek üzere sektör, kamu kuruluşları ve akademi düzeyinde çalışmalar devam etmektedir. İleriye dönük umut verici birkaç yol olmasına karşın, bazı engellerin de dikkate alınması gerekiyor.

Saldırgan yapay zeka sistemlerine karşı koymak için esasen "savunma amaçlı" yapay zeka sistemleri olan sahte içerikli tespit edebilen yapay zeka tabanlı sistemler oluşturmak da bir diğer yaklaşımdır. Bu, sentetik ses ve video oluşturmaya yönelik mevcut sistemlerin, medya alanında eğitimli adli analistler ve otomatik araçlar tarafından fark edilebilecek, bariz izler bıraktığı aktif bir araştırma alanıdır.

Mevcut sahte içeriklerde belirgin kusurlar olsa da, ne yazık ki kesin yapıtlar belirli bir araca veya algoritmaya özgü olabiliyor. Buradan, derin sahtecilik görüntü dedektörleri oluşturmaya yönelik 2020 yılında düzenlenen bir açık yarışmada gösterildiği gibi, bu sahte içeriklere ilişkin eğitimin genellikle diğer algoritmalara genellenmediği anlamı çıkarılabilir.[19] Daha ileri düzey dedektörler geliştirmeye yönelik yatırımı artırmak cazip olabilir ancak Microsoft'un bunun iki nedenden dolayı anlamlı iyileştirmeleri beraberinde getireceğine dair şüpheleri vardır:

İlk olarak, gerçek dünyayı yansıtan mükemmel fiziksel modellerimiz var. Mevcut sahte içerik geliştiriciler işin kolayına tespit edilebilir yapıtlar ortaya koyuyor ancak daha yeni modellerin şu ana kadar olanlara göre daha gerçekçi olacağı değerlendiriliyor. Bir fotoğraf makinesi ile yakalanmış, bilgisayar tarafından modellenemeyen gerçek hayattaki bir sahne için, yapısı gereği özel bir şey yoktur.

İkincisi, ileri düzey sahte üretim algoritmalarında, üretim işleminin bir parçası olarak Çekişmeli Üretici Ağlar (GAN'lar) adı verilen bir teknik kullanılır. Bir GAN, sahte içerik oluşturmak için bir üreteç ve sahte görüntüleri tespit edip üreteci eğitmek için ise bir ayrıştırıcı kullanarak iki yapay zeka sistemini birbirine karşı oynatır. Daha iyi bir dedektör geliştirmek için yapılan yatırımlar, üretecin yalnızca daha iyi kalitede sahte içerikler oluşturmasını sağlayacaktır.

Sentetik medya

Devamı

Dijital varlıkların kaynağı

Sahte içeriklerin tespiti güvenilir olmadığında, sentetik medyanın zararlı kullanımlarına karşı koruma sağlamak için ne yapılabilir? Gelişmekte olan önemli bir teknoloji de dijital kaynaktır. Bu, dijital medya geliştiricilerine bir varlığı sertifikalandırma olanağını sağlayan ve tüketicilerin dijital varlığa müdahale edilip edilmediğini belirlemelerine yardımcı olan bir mekanizmadır. Dijital kaynak, içeriğin internette dolaşım hızı ve kötü aktörlerin içeriği kolayca manipüle etme imkanı düşünüldüğünde, günümüzdeki sosyal medya ağları açısından özellikle önemlidir.

%900

2019 yılından bu yana derin sahteciliğin kullanımında görülen yıllık artış.[20]

Dijital Kaynak Teknolojisi, bugünkü web ortamından geçen nesnelerin kaynağını yakalamak, geçmişini düzenlemek ve meta verilerini almak için tasarlanmış şifreli belge imzalamanın modern bir sürümüdür. Uçtan uca kurcalamaya karşı korumalı bu medya sertifikasyon türünü etkinleştirmeye dair vizyon ve teknik yöntemler, Microsoft'taki araştırmacı ve bilim insanlarından oluşan bir ekip tarafından geliştirildi. Project Origin'de (Microsoft, BBC, CBC/Radio-Canada ve New York Times tarafından kurulmuştur) medya kaynağı teknolojisini hayata geçirmeyi amaçlayan, sektörler arası bir ortaklığa öncülük ediyoruz ve Content Authenticity Initiative (Adobe tarafından) ile yakın iş birliği içindeyiz. Microsoft, İçerik Kaynağı ve Gerçekliği Koalisyonu (C2PA)'yı kurmak için teknoloji ve medya hizmetleri alanındaki iş ortaklarıyla da çalıştı. C2PA, yakın zamanda görüntü, video, ses ve metin gibi medya varlıklarından yararlanmak için en ileri düzey dijital kaynak şartnamesini yayımlayan bir standartlar kurumudur.

C2PA etkin bir nesne üzerinde, nesne ve meta verilerin kurcalamaya karşı korunduğuna ilişkin bir bildiri bulunur; yanında verilen sertifika yayımcıyı tanımlar.

Sentetik medya ilk başta zarar verme amacıyla tasarlanmamış olsa da kötü aktörler tarafından şahıslara ve kurumlara duyulan güveni zedelemek için kötüye kullanılıyor.

Dijital kaynak, bir medya varlığının kökenini doğrulayarak insanların çevrimiçi medya içeriğine olan güvenini geri kazanmalarına yardımcı olma potansiyeline sahip, gelecek vaat eden bir teknolojidir.

C2PA belirtimine dayanan genel kullanıma açık çözümler, mevcut ürünlerde veya yeni bağımsız uygulama ve hizmetlerde yeni bir özellik olarak göze çarpmaktadır. Yaygın olarak kullanılan yakalama, düzenleme ve yazma araçlarının çoğunun birkaç yıl içinde C2PA etkin olmasını bekliyoruz. Bu durum, kurumlara dijital kaynak ihtiyaçlarını ve kullanımlarını bugün belirleme ve mevcut iş akışlarında kullandıkları araçlarda bu ek koruma katmanını zorunlu tutma fırsatını sunar.

Eyleme dönüştürülebilir içgörüler

1. Halkla ilişkiler ve iletişim yanıtlarınızı proaktif bir şekilde değerlendirerek kurumunuzu yanlış bilgi tehditlerine karşı korumak için proaktif adımlar atın.
2. Resmi iletişimi korumak için kaynak teknolojisini kullanın.

Daha ayrıntılı bilgi için bağlantılar

- Dezenformasyon konusunda gelecek vaat eden bir adım | Microsoft On the Issues
- Bir Dönüm Noktasına Ulaşıldı, 31 Ocak 2022
- Project Origin | Microsoft ALT Yeniliği
- İçerik Kaynağı ve Gerçekliği Koalisyonu (C2PA)
- Project Origin'in medya kimlik doğrulaması için kullandığı sistemle ilgili teknik ayrıntıları öğrenin | Microsoft ALT Yeniliği

Siber etki operasyonlarına karşı korunmaya yönelik bütünsel yaklaşım

Microsoft, siber etki operasyonlarına yönelik daha geniş ve kapsayıcı bir yaklaşım geliştirmek için halihazırda olgunlaşmış siber tehdit analizi altyapısını temel alıyor.

Operasyonların neden olduğu tehditle başa çıkmak için önerilen, dört ana başlığa ayrılan (algılama, bozma, savunma ve caydırma) yanıt ve etki azaltma stratejileri için bir çerçeve kullanıyoruz.

Ayrıca Microsoft, çalışmalarımızı bu alana sabitlemek için dört ilke benimsedi. Birincisi, ifade özgürlüğüne saygı gösterme ve platformlarımız, ürünlerimiz ve hizmetlerimiz aracılığıyla müşterilerimizin bilgi oluşturma, yayınlama ve arama yeteneğini destekleme taahhüdüdür. İkincisi, platformlarımızın ve ürünlerimizin yabancı siber etki sitelerini ve içeriğini güçlendirmek için kullanılmasını önlemek üzere proaktif bir şekilde çalışmadır. Üçüncüsü, yabancı siber etki içeriğinden veya aktörlerinden kasıtlı olarak yararlanmamaktır. Son olarak, ürünlerimiz hakkında kurum içi ve güvenilir üçüncü taraf verilerini kullanarak yabancı siber etki operasyonlarına karşı koymak amacıyla görünür içeriklere öncelik veriyoruz.

Sapta

Siber savunmada olduğu gibi, yabancı siber etki operasyonlarına karşı koymanın ilk adımı, bunları saptama kapasitesini geliştirmektir. Hiçbir kurum veya kuruluşun, ihtiyaç duyulan ilerlemeyi tek başına yapması beklenemez. Siber etki operasyonlarını analiz etme ve raporlamadaki ilerlemeyle beraber akademik kurumlar ve kâr amacı gütmeyen kuruluşlar da dahil olmak üzere sivil toplumun rolüne dayalı olarak teknoloji sektöründe yeni ve daha kapsamlı bir iş birliği çok önemli olacaktır.

Princeton Üniversitesi'nde, bu rolün farkında olan araştırmacılar Jake Shapiro ve Alicia Wanless ile Carnegie Uluslararası Barış Vakfı, yeni "Bilgi Ortamı Araştırma Enstitüsü"nü (IRIE) başlatma planlarını sırasıyla oluşturdu. Microsoft, the Knight Foundation ve Craig Newmark Philanthropies'in desteğiyle IRIE, Avrupa Nükleer Araştırmalar Kurumundan (CERN) modellenen kapsayıcı ve çok paydaşlı bir araştırma kurumu oluşturacak. Bu alandaki yeni keşifleri hızlandırmak ve ölçeklendirmek üzere veri işleme ve analiz uzmanlığını bir araya getirecek. Bulgular; kural koyucular, teknoloji kurumları ve tüketicileri daha kapsamlı bir şekilde bilgilendirmek üzere paylaşılacak.

Savun

İkinci stratejik ana başlık, yatırım ve yenilik ihtiyacında uzun sürredir bir öncelik olan demokratik savunmaları desteklemek. Burada teknolojinin demokrasi üzerinde yarattığı zorluklar ve teknolojinin demokratik toplumları daha etkin bir şşekilde savunmak için sunduğu fırsatlar dikkate alınmalıdır.

Microsoft'un strateji çerçevesi; sektörler arası paydaşların, özellikle yabancı saldırganların yürüttüğü kampanyalar olan propagandayı saptamasına, bozmasına, buna karşı savunma yapmasına ve bunu caydırmasına yardımcı olmayı amaçlıyor.

Çağımızın en büyük teknolojik açmazlarından biri olan internetin ve dijital reklamcılığın, geleneksel gazetecilik üzerindeki etkisiyle başlamak daha doğru olur. 1700'lerden bu yana, özgür ve bağımsız bir basın yeryüzündeki tüm demokrasileri desteklemek, yolsuzlukları açığa çıkarmak, savaşları belgelemek, bugünün ve her dönemin en büyük toplumsal zorluklarına ışık tutmak bakımından özel bir rol oynamıştır. Ancak internet, reklam gelirlerini artırarak ve ücretli aboneleri çekerek yerel haberlerin içini boşalttı. Birçok yerel gazete battı. En son çalışmalarımızdan edindiğimiz çok sayıdaki içgörüden biri, gazete eksikliği yaşayan şehirlerin bilmeden ve kaçınılmaz olarak ortalamadan daha fazla yabancı propagandaya maruz kaldığıdır. Bu nedenlerden ötürü demokrasinin en kritik savunma etkinliklerinden birinin, özellikle yerel düzeyde geleneksel gazeteciliği ve özgür basını desteklemesi gerekir. Bunun için farklı ülkelerin ve kıtaların yerel ihtiyaçlarını yansıtması gereken sürekli yatırımlar ve yenilikler yapılmalıdır. Bu sorunların çözümü kolay değildir; Microsoft ve diğer teknoloji kurumlarının her geçen gün desteğini artırdığı çok paydaşlı yaklaşımların benimsenmesi gerekiyor.

Kamu politikasında, kamu önceliği olması gereken yeniliklere de ihtiyacımız var. Bunların arasında, yayıncıların teknoloji kurumlarıyla toplu olarak reklam geliri pazarlığı yapmalarını sağlayan yasalar ve istihdam ettikleri gazetecilerin bordrolarındaki vergilerin bir kısmı için yerel haber kanallarına vergi indirimleri sağlayan düzenlemeler çıkarılabilir. Gazeteciler, içeriklerin meşru ve dolandırıcılık amaçlı kaynaklardan gelip gelmediğini ayırma becerisi gibi kendi uzmanlık alanları için başka birçok araca ihtiyaç duymaktadır.

Ayrıca her geçen gün, tüketicilerin ulus-devlet destekli bilgilendirme operasyonlarını belirleme konusunda daha ileri düzeyde bir yetenek geliştirmesine yardımcı olmaya daha fazla ihtiyaç duyuluyor. Bu durum göz korkutucu gibi görünse de, esasen teknoloji sektörünün diğer siber tehditlerle mücadele etmek için uzun bir süredir yaptığı çalışmalara benziyor. Tüketicilerin istenmeyen postaları ve diğer sahte iletişimleri daha iyi tespit etmelerine yardımcı olabilmek için, bir e-posta adresini daha dikkatli inceleyecek şekilde eğitim alması gerektiğini göz önünde bulundurun. Haber Okuryazarlığı Projesi ve Güvenilir Gazetecilik gibi ABD'de bu konudaki girişimler.

Gördüklerimize ve duyduklarımıza artık güvenemediğimizde, neyin doğru neyin yanlış olduğunu ayırt edememek daha uzun vadeli ve sinsi bir tehdittir.

Siber etki operasyonlarına karşı korunmaya yönelik bütünsel yaklaşım

Devamı

Program: haberler ve bilgilendirme konusunda tüketicilerin daha çok bilgi sahibi olmasına yardımcı oluyoruz. Dünya çapında NewsGuard tarayıcı eklentisi gibi yeni teknolojiler bu çabayı çok daha hızla geliştirmeye yardımcı olabilir.

Bu ayrıca bize, demokrasinin temelinin biraz da yurttaşlık eğitimiyle ilgili olduğunu hatırlatmalıdır. Her zaman olduğu gibi, bu çalışmanın okullarda başlaması gerekiyor. Ancak yaşamımız boyunca sürekli vatandaşlık eğitimi almamız gereken bir dünyada yaşıyoruz. Stratejik ve Uluslararası Çalışmalar Merkezi tarafından öncülük edilen, Microsoft'un imza sahibi ve iş ortağı olduğu İş Yerinde Yurttaşlık Eğiti adlı yeni taahhüt, kurumsal topluluklar içinde vatandaşlık okuryazarlığını yeniden canlandırmayı amaçlıyor. Bu, demokratik değerlerimizi güçlendirmeye yönelik fırsat genişliğine iyi bir örnektir.

Boz

Son yıllarda Microsoft'un Dijital Suçlar Birimi (DCU) fidye yazılımlarından botnet'lere ve ulus devlet saldırılarına kadar değişen siber tehditleri ortadan kaldırmak için taktikler tasarladı ve araçlar geliştirdi. Farklı siber saldırı türleriyle mücadelede aktif bozma rolünden başlamak üzere birçok kritik ders çıkardık.

Siber etki operasyonlarına karşı koymayı düşünürken, bozma unsuru çok daha önemli bir rol oynayabilir ve bozma ile ilgili en iyi yaklaşım daha net hâle gelir. Geniş kapsamlı aldatmacanın en etkili panzehiri şeffaflıktır. Bu nedenle Microsoft, yabancı siber etki operasyonlarına yönelik tespit ve müdahale alanında uzmanlaşmış önde gelen bir siber tehdit analizi ve araştırma kurumu olan Miburo Solutions'u satın alarak ulus devletlerin etki operasyonlarını tespit etme ve ortadan kaldırma kapasitesini artırdı.

Deneyimlerimiz; kamu kuruluşları, teknoloji kurumları ve STK'ların siber saldırılarla dikkatlice ve bol miktarda kanıtla ilgilenmesi gerektiğini bize gösterdi. Böyle bir bozma unsurunun etkisini anlamak çok önemlidir ve siber etkinin ortadan kaldırılmasına daha da yardımcı olabilir. ABD hükümetinin Rusya'nın Ukrayna'yı işgaline giden yolda şeffaflığı etkin eyleme dönüştürdüğü bilgi paylaşımına (sahte bir grafik video kullanma planı gibi belirli kampanyaları içeren Rus planlarını ifşa etmek gibi) tanık olduk.

Ukrayna'nın içinde ve dışında devam eden siber saldırılarla ilgili olarak Cenevre'deki CyberPeace Institute'un geçen yıl yaz aylarında paylaşılan yayınında gösterildiği gibi, farklı sivil toplum ve özel sektör kurumlarının siber etki operasyonlarıyla ilgili şeffaflığı ilerletme fırsatı bulunuyor. Yeni ortaya çıkarılan ve yeterli ölçüde belgelenmiş operasyonlara ilişkin güvenilir raporlar, halkın özellikle internette okuduklarını, gördüklerini ve duyduklarını daha iyi değerlendirmesine yardımcı olabilir. Bu amaçla Microsoft, mevcut siber raporları temel alıp kapsamını genişletecek ve uygun olduğunda ilişkilendirme beyanları dahil siber etki operasyonları hakkında öğrendiğimiz bilgilerle ilgili yeni raporlar, veriler ve güncellemeler paylaşacak. Kurum genelinde yabancı bilgi operasyonlarının yaygınlığını ve kademeli şekilde iyileştirmenin sağlanması için atılacak adımları incelemek üzere veri odaklı bir yaklaşım doğrultusunda bir yıllık bir rapor yayımlayacağız. Ayrıca, bu şeffaflık çerçevesinde diğer adımları da değerlendireceğiz.

Örneğin, reklamcılık, aynı anda yabancı destekli propaganda siteleri için meşru bir görünüm yaratırken, yabancı operasyonların finanse edilmesine yardımcı olabileceğinden dijital reklamcılığın rolü özellikle önemlidir. Bu finansal akışları bozmak için yeni çalışmalar yapılmalıdır.

Caydır

Son olarak, uluslararası kuralları ihlal etmenin bir sorumluluğu yoksa uluslardan davranış değişikliğinde bulunmalarını bekleyemeyiz. Bu tür bir sorumluluğun uygulanması tamamen devletin görevidir. Ancak çok paydaşlı bir eylem, giderek artan şekilde uluslararası normların güçlendirilmesi ve genişletilmesinde önemli bir rol oynar. Sayısı 30'dan fazla olan online platform, reklamcı ve yayıncı (Microsoft dahil), Avrupa Komisyonu'nun yeni güncellenen Dezenformasyon Uygulama Kuralları belgesine imza koyarak her geçen büyüyen bu zorlukla mücadeleye olan bağlılıklarını güçlendirme konusunda mutabık kaldı. Son Paris Çağrısı, Christchurch Çağrısı ve İnternetin Geleceği Deklarasyonu gibi çok taraflı ve çok paydaşlı eylemler de demokratik ülkelerdeki kamu kuruluşlarını ve kamuoyunu bir araya getirebilir. Kamu kuruluşları daha sonra dünya demokrasilerinin ihtiyaç duyduğu ve hak ettiği hesap verebilirlik sorumluluğunu ileri düzeye taşımak amacıyla bu norm ve yasaları temel alabilir.

Demokratik devletler ve toplumlar, hızlı ve radikal şeffaflık yoluyla ulus devlet saldırılarının kaynağını ilişkilendirerek, halkı bilgilendirerek ve kurumlara duyulan güveni artırarak kampanyaları etkin bir şekilde azaltabilir.

Dış etki operasyonlarını saptayıp bozmaya yönelik teknik kapasitemizi artırdık ve siber saldırılara ilişkin raporlarımız gibi bu operasyonlar hakkında şeffaf raporlama yapmayı amaçlıyoruz.

Eyleme dönüştürülebilir içgörüler

1. Kurumunuzda güçlü dijital hijyen uygulamalarını kullanın.
2. Çalışanlarınızın veya iş uygulamalarınızın istemeden siber etki kampanyalarını kolaylaştırmasını azaltmanın yollarını düşünün. Bilinen yabancı propaganda sitelerine olan bilgi beslemesi de buna dahildir.
3. Toplumların propaganda ve dış etkilere karşı korunmasına yardımcı olacak temel bileşenler olarak bilgi okuryazarlığı ve toplum etkileşimi kampanyalarını destekleyin.
4. Etki operasyonlarını yönetmek için çaba harcayan sektörünüzle ilgili gruplarla doğrudan etkileşime geçin.

Son Notlar

1. https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3. Ukrayna'yı Savunmak: Siber Savaştan İlk Dersler (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Rusya Dışişleri Bakanlığı Sözcüsü Maria Zakharova: https://tass.com/politics/1401777; Lavrov: https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. Rusya'nın Kremenchuk İddiaları ve Kanıtlar: bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Bilgi teyidi: "Sarhoş" Nancy Pelosi videosu manipüle edildi | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. Derin Sahtecilik Algılama Zorluğunun Sonuçları: Yapay zekayı geliştirmeye yönelik açık bir girişim (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas, and Kristjan Peterson, Ekim 2020

Siber Dayanıklılık

Modernleşmenin risklerini ve getirilerini anlamak, dayanıklılığa bütünsel bir yaklaşım geliştirmek açısından çok önemlidir.

Siber Dayanıklılığa genel bakış

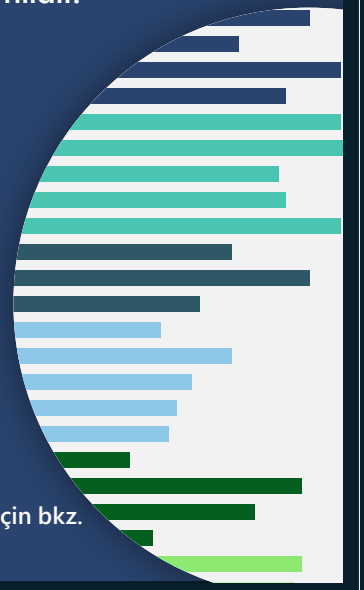
Siber güvenlik, teknolojik başarının kilit unsurlarından biridir. Yenilik ve artırılmış verimlilik, sadece kurumları modern saldırılara karşı mümkün olduğunca dayanıklı hâle getiren güvenlik önlemlerinin uygulanmasıyla gerçeğe dönüşebilir.

Pandemi, bizi güvenlik uygulamalarımızı ve teknolojilerimizi, Microsoft çalışanlarının işlerini yaptığı her yerde onları koruyacak şekilde yönlendirmeye zorladı. Geçen yıl tehdit aktörleri, pandemi sırasında ortaya çıkan güvenlik açıklarından ve hibrit çalışma ortamına geçiş durumundan yararlanmaya devam etti. O zamandan beri başlıca sorunumuz, çeşitli saldırı yöntemlerinin yaygınlığını ve karmaşıklığını ve artan ulus devlet faaliyetini yönetmek oldu.

Etkili siber dayanıklılık; temel hizmetler ve altyapıya yönelik değişen tehditlere karşı koymak için bütüncül ve uyarlanabilir bir yaklaşım gerektirir.

Daha fazla bilgi için bkz. sayfa 89

Modernize edilmiş sistemler ve mimari, hiper bağlantılı bir dünyada tehditleri yönetmek anlamında önemlidir.

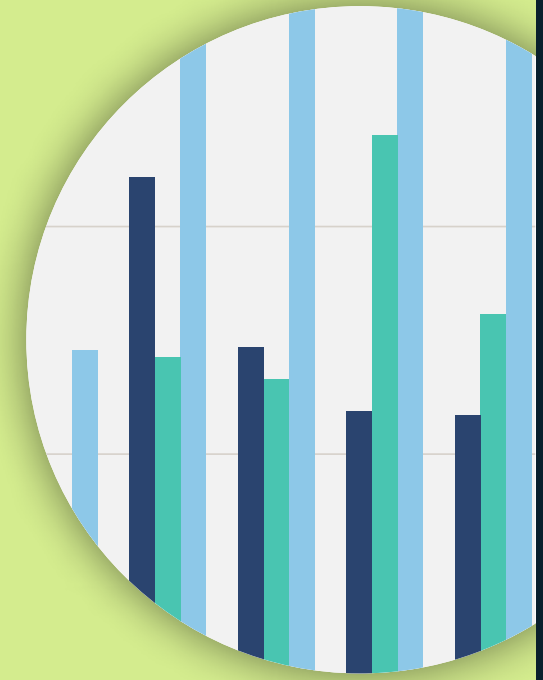


Daha fazla bilgi için bkz. sayfa 90

Temel güvenlik duruşu, ileri düzey çözüm etkinliğinde belirleyici bir faktördür.

Daha fazla bilgi için bkz. sayfa 92

Her ne kadar parola tabanlı saldırılar, kimlik güvenliğini tehlikeye atan temel kaynak olmaya devam etse de, başka tür saldırılar da ortaya çıkmaktadır.



Daha fazla bilgi için bkz. sayfa 93

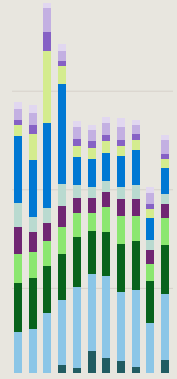
Siber etki operasyonlarına karşı dayanıklılığın insan boyutu, ortak çalışma ve iş birliği yapma yeteneğimizle ilgilidir.

Daha fazla bilgi için bkz. sayfa 102

Başarılı siber saldırıların büyük çoğunluğu temel güvenlik hijyeni kullanılarak önlenebilir.

Daha fazla bilgi için bkz. sayfa 108

Geçen yıl dünyada hacim, karmaşıklık ve sıklık bakımından benzeri görülmemiş bir DDoS hareketliliği yaşandı.



Daha fazla bilgi için bkz. sayfa 98

Giriş

Pandemi, bizi güvenlik uygulamalarımızı ve teknolojilerimizi, Microsoft çalışanlarının işlerini yaptığı her yerde onları koruyacak şekilde yönlendirmeye zorladı. Geçen yıl tehdit aktörleri, pandemi sırasında ortaya çıkan güvenlik açıklarından ve hibrit çalışma ortamına geçiş durumundan yararlanmaya devam etti. O zamandan beri başlıca sorunumuz, çeşitli saldırı yöntemlerinin yaygınlığını ve karmaşıklığını ve artan ulus devlet faaliyetini yönetmek oldu.

Dijital tehdit etkinliği ve siber saldırı karmaşıklık düzeyi her geçen gün artmaktadır. Bugünün karmaşık saldırılarının birçoğu, farklı güvenlik kontrol seviyelerine sahip kimlik mimarilerinde, tedarik zincirlerinde ve üçüncü taraflarda güvenlik açıklarına odaklanmaktadır. Özellikle kimlik avı saldırılarının belirgin ve gerçek bir tehdit olduğunu gördük. Ancak bu tür saldırılar doğru kimlik yönetimi, kimlik avı kontrolü ve uç nokta yönetimi uygulamaları sayesinde genellikle başarıya ulaşmaz. Sonuç olarak, temel hususları hatırlamamız gerekir: Saldırıların yüzde doksan sekizi, temel hijyen önlemleri uygulanarak durdurulabilir. Microsoft'ta kimlikleri ve cihazları, tehdit aktörlerini etkili bir şekilde durdurmak ve verilerimizi korumak için en az ayrıcalıklı erişim ve kimlik avına dayanıklı kimlik bilgileri içeren Sıfır Güven yaklaşımımızın bir parçası olarak yönetiyoruz.

Günümüzde, ileri düzey taktiklere, tekniklere ve prosedürlere erişim siber suç ekonomisinde geniş ölçüde kullanılabilir hâle geldiğinden, gelişmiş teknik becerilere sahip olmayan tehdit aktörleri bile inanılmaz derecede yıkıcı saldırılar başlatabilir. Ukrayna'daki savaş, ulus devlet aktörlerinin fidye yazılımlarını daha sık kullanmasıyla beraber saldırı amaçlı siber operasyonlarını nasıl artırdığını gösterdi. Fidye yazılımı, tehdit aktörlerinin bir ödeme alabilmek için ikili veya üçlü şantaj taktikleri kullandığı ve geliştiricilerin hizmet olarak fidye yazılımı (RaaS) sunduğu karmaşık bir sektördür. Tehdit aktörleri, RaaS ile saldırıları gerçekleştirmek için bir ortak ağ kullanır; böylece daha az yetenekli siber suçluların giriş engeli kaldırılmış ve nihayetinde saldırgan havuzu genişletilmiş olur.

Sonuç olarak Microsoft bir fidye yazılımı eleme programı geliştirdi. Programın amacı, denetimler ve kapsamdaki boşlukları düzeltmek, hizmetlerle ilgili özellik geliştirmelerine katkıda bulunmak ve fidye yazılımı saldırısı olması halinde güvenlik operasyon merkezimiz ve mühendislik ekiplerimiz için kurtarma kılavuzları geliştirmektir.

Son dönemde yaşanan tedarik zinciri ve üçüncü taraf tedarikçi saldırıları, sektörde önemli bir cazibe noktasına işaret ediyor. Bu saldırıların müşterilerimiz, iş ortaklarımız, kamu kuruluşları ve Microsoft için neden olduğu aksaklıklar artmaya devam ederken güvenlik paydaşları arasında siber dayanıklılığa ve iş birliğine verilen özel önem de dikkat çekiyor. Düşmanlar aynı zamanda kurum içi sistemleri hedef alıyor ve altyapıyı modernleşip güvenliğin daha güçlü olduğu bulut ortamına taşıyarak kurumların eski sistemlerde yaşanan güvenlik açıklarını yönetme ihtiyacını destekliyor.

Güvenliğin, teknolojik başarıyı getirdiği bir dönemde yaşıyoruz. Yenilik ve artırılmış verimlilik, sadece kurumları modern saldırılara karşı mümkün olduğunca dayanıklı hâle getiren güvenlik önlemlerinin uygulanmasıyla gerçeğe dönüşebilir. Dijital tehditler arttıkça ve geliştikçe, her kurumun işleyişine siber dayanıklılığı kazandırmak çok önemlidir.

Bret Arsenault
Bilgi Güvenliği Şefi

Siber dayanıklılık: Bağlı durumdaki bir topluma ait son derece önemli temel

Dijital teknolojide yaşanan devrim, kurumların hem çalışma biçiminde hem de sundukları hizmetlerde giderek daha bağlı hâle geldiğini ortaya koymaktadır. Siber ortamdaki tehditlerin arttığı koşullarda, kurumun yapısına siber dayanıklılık kazandırmak finansal ve operasyonel dayanıklılık kadar önem taşımaktadır.

Dijital dönüşüm; kurumların müşteriler, ortaklar, çalışanlar ve diğer paydaşlarla etkileşim kurma biçiminde köklü değişiklere yol açtı. Yeni teknolojiler insanlarla etkileşim kurmak, ürünleri dönüştürmek ve operasyonları optimize etmek için büyük fırsatlar sunmaktadır. Pandemi, insanların yeni biçimlerde ve istedikleri yerden çalışmalarına olanak tanıyan yenilikçi teknolojileri destekleyerek dijital dönüşüm sürecini hızlandırdı.

Siber tehditler daha sık hâle geldikçe, bir kurumun güvenliğini aşmalarını engellemek "her zaman birbirine bağlı" dünyamızda daha da zor bir hâl almaktadır. Siber dayanıklılık, bir kurumun saldırı yağmuruna rağmen operasyonlarına devam etme ve büyümeyi sürdürme yeteneğini temsil eder. Önleme; ayakta kalma ve kurtarma becerileri ile dengelenmelidir; kamu kuruluşları ve kurumlar, siber dayanıklılığın bir parçası olarak varlıkların, verilerin ve diğer kaynakların korunması için güvenlik ve gizliliğin ötesine geçen kapsamlı modeller geliştiriyor.

Siber dayanıklılığa yönelik bütünsel bir yaklaşım geliştirme

Siber dayanıklılık; aşağıdakiler dahil olmak üzere hizmetler ve altyapıya yönelik değişen tehditlere karşı koyabilen bütüncül, uyarlanabilir ve küresel bir yaklaşım gerektirir:

- Siber esneklik çan eğrimizde açıklanan temel siber hijyen.
- Dijital dönüşümün risk/ödül fırsat maliyetini anlama ve yönetme.
- Tehditlerin ve güvenlik açıklarının proaktif bir şekilde algılanmasını sağlayan gerçek zamanlı müdahale becerileri.
- Bilinen saldırılara karşı koruma sağlama ve otomatik sorun giderme yeteneği gibi yeni ve beklenen saldırı vektörlerine karşı önleyici hareketler.
- Arıza yalıtımı ve segmentasyonu ile saldırıların ve felaketlerin etkisini düşürme.
- Kesinti durumunda otomatik kurtarma ve yedekli çalışma.
- Açıkları belirlemeye yönelik operasyonel testleri önceliklendirme ve bulut tabanlı güvenlik çözümleri gibi dış kaynaklarda paylaşılan sorumlulukları ve bağımlılıkları anlama.

Etkili bir siber dayanıklılık programı, mevcut hizmetleri anlama ve bir kesinti durumunda çağrılabilecek güvenilir bir kaynak kataloğuna sahip olma gibi kaynakla ilgili temel konularla başlar. Bu temelden hareketle, program kendi etkinliğini değerlendirebilmeli, kritik hizmetlerin ve bağımlılıklarının performansını ölçebilmeli, kurum içi ve bulut hizmetlerindeki yetenekleri test edip doğrulayabilmeli ve kurumun dijital yaşam döngüsü boyunca sürekli iyileştirmeyi destekleyebilmelidir..

Bütünsel bir yaklaşım sunmak için kurumlarla en kritik kurum içi hizmetlerini ve çevrimiçi hizmetlerini, iş süreçlerini, bağımlılıkları, personeli, satıcıları ve tedarikçileri belirlemek üzere birlikte çalışıyoruz. Ayrıca müşteri ve pazar beklentileri, mevzuat ve sözleşme ile ilgili yükümlülükler ve iç operasyonlarla ilgili varlıkları ve kaynakları belirlemeyi de hedefliyoruz. Bu kritik kaynaklar tanımlandıkça, paralel çabalar tehditleri, kesintileri, potansiyel saldırı vektörlerini, sistem ve işlem güvenlik açıklarını tespit etmeli ve izlemelidir. Bu süreci mevcut beceri eksikliğiyle yapabilmek için kurumun maruz kaldığı genel riske göre önceliklendirmede titiz bir çalışma gerekir.

Bu tür bütüncül bir yaklaşımın; ölçülebilir performans artışı, daha kısa tespit, yanıt ve kurtarma süresi ve kesinti durumunda daha küçük etki alanını desteklemek amacıyla sürekli bir biçimde gelişen tehdit ortamına karşı uyarlanabilir olması gerekir. Bu yaklaşımda, tehditlerin birbirlerine olan bağlantılarının arttığı da dikkate alınmalıdır. Örneğin, bir güvenlik olayı, veri ihlaline ve gizlilik etkilerine neden olabilir; bu durum, birçok dahili ve harici ekibin hızlı bir şekilde yanıt vermek ve etkiyi en aza indirmek için birlikte çalışmasını gerektirir.

> Siber dayanıklılık, bir kurumun siber saldırılar gibi kesintilere rağmen operasyonları sürdürme ve büyüme ivmesini sürdürme becerisidir.

Eyleme dönüştürülebilir içgörüler

1. Bir ihlalin etkisini sınırlayan ve ihlal başarılı olsa bile sistemlerin güvenli ve etkili bir şekilde çalışmaya devam etmesini sağlayan teknoloji sistemleri oluşturun ve yönetin. Ortak kritik varlıklara, çeviklik desteğine ve uyarlanabilirlik mimarisine odaklanın (örneğin; hibrit ve çoklu bulut, çoklu platform), saldırı yüzeylerini azaltın (örneğin, kullanılmayan uygulamaları ve gereğinden fazla verilen erişim haklarını kaldırma), güvenliği ihlal edilmiş kaynakları üstlenin ve düşmanların kendilerini geliştireceğini varsayın.
2. Dijital projeleri planlarken, potansiyel tehditleri fırsatlarla birlikte değerlendirin ve bulut tabanlı güvenlik çözümleri gibi dijital teknoloji tedarik zincirinde dayanıklılığa yönelik paylaşılan sorumlulukları değerlendirin.
3. Tasarım gereği içerisinde güvenliğin yer alacağı sistemler oluşturun ve gelecekte gelişen tehditleri öngörmek, algılamak, bunlara karşı dayanım göstermek, uyum sağlamak ve yanıt vermek için adımlar atın.
4. Yeni gelişmelere ilişkin riskleri anlamak için kurum liderlerinin güvenlik ekiplerinden görüş almasını sağlayın. Benzer şekilde, güvenlik ekipleri iş hedeflerini göz önünde bulundurmalı ve liderlere bu hedeflerin güvenli bir şekilde nasıl uygulanacağı konusunda tavsiyelerde bulunmalıdır.
5. Siber olaylarla ilgili olarak, kurumsal dayanıklılığa yönelik açık operasyonel uygulamaların ve prosedürlerin mevcut olduğundan emin olun.

Sistemleri ve mimariyi modernleştirmenin önemi

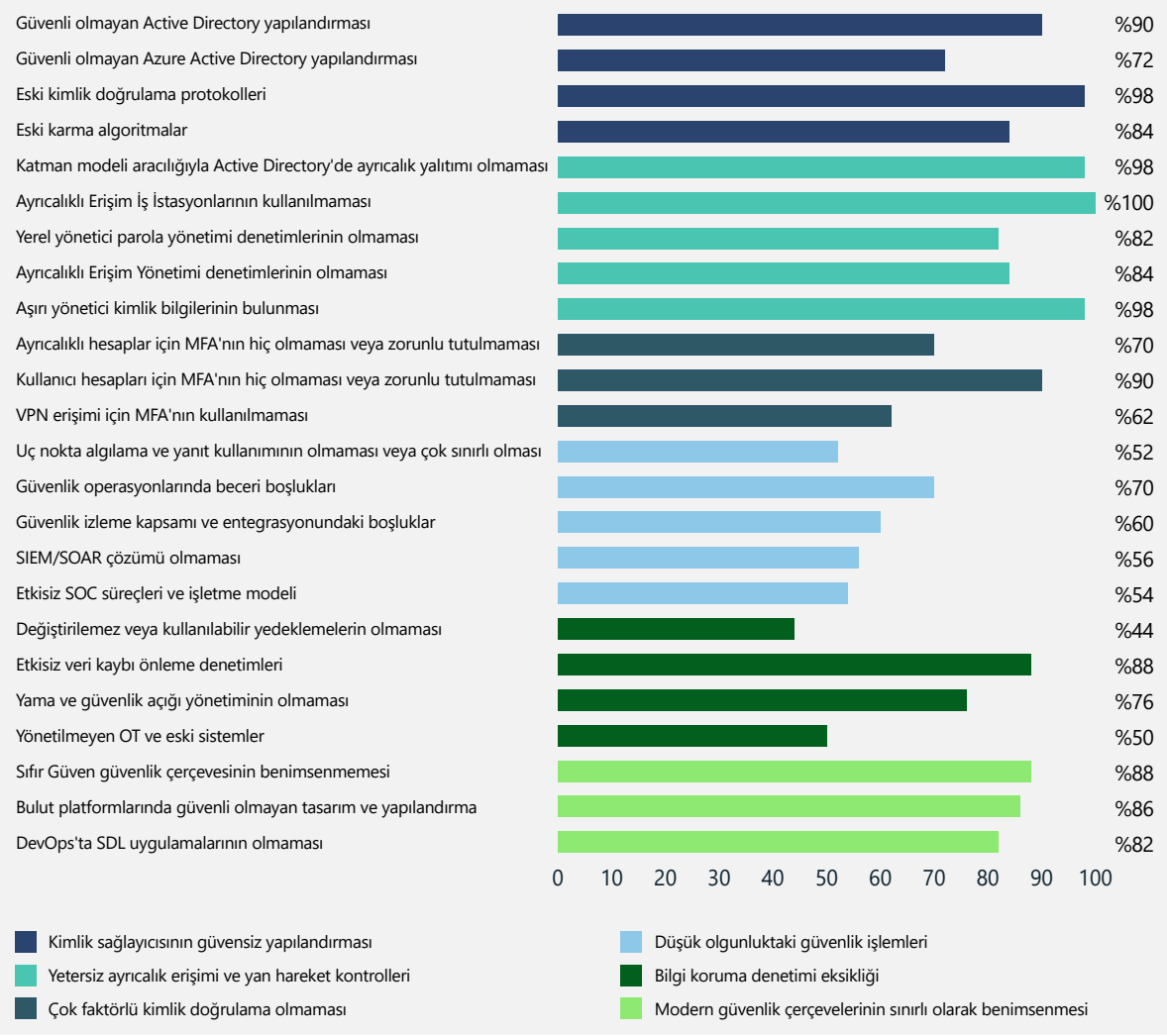
Birbirine fazlasıyla bağlantılı bir dünya için yeni özellikler geliştirirken eski sistemlerin ve yazılımların oluşturduğu tehditleri de yönetmeliyiz.

Eski sistemler: Akıllı telefonlar, tabletler ve bulut hizmetleri gibi modern bağlantı araçlarından önce geliştirilmiş olan sistemler, bunları kullanan her kurum için risk teşkil eder. Bu risk, müşterilerin saldırılara yanıt vermesine ve bunlardan kurtulmasına yardımcı olan bir güvenlik uzmanları grubu olan Microsoft Olay Müdahalesi Güvenlik Hizmetleri ekibinin bulgularıyla da destekleniyor.

Geçen yıl saldırılardan kurtulan müşteriler arasında yaşanan sorunlar, bu sayfadaki grafikte gösterildiği gibi altı kategoride incelenebilir. Bir sonraki sayfada, gelişmiş dayanıklılık için atılabilecek adımlar özetlenmiştir.

Güvenlik olaylarının yüzde 80'inden fazlası, modern güvenlik yaklaşımlarıyla ele alınabilen birkaç eksik unsura kadar izlenebilir.

Siber dayanıklılığı etkileyen temel sorunlar



Bu grafik, kurumsal siber dayanıklılık artışı için için kritik derecede önemli olan, temel güvenlik denetimleri bulunmayan etkilenen müşterilerin yüzdesini göstermektedir. Bulgular, geçen yıla ait Microsoft etkileşimlerine dayanmaktadır.

"Liderler siber dayanıklılığı iş dayanıklılığının kritik bir unsuru olarak düşünmelidir. Liderler, siber aksaklıkları doğal afetler veya diğer öngörülemeyen olaylarla aynı şekilde planlamalı ve stratejiler oluşturmak için operasyonlar, iletişim, hukuk ve benzeri kurum içi paydaşları bir araya getirmelidir. Böyle davranmak, kurumların normal işleyişlerini sürdürmek için kritik iş sistemlerini mümkün olan en kısa sürede yeniden online hâle getirmesine yardımcı olur.

Ama iş bununla sınırlı değildir. Birçok kurum üçüncü taraf tedarikçilere ve hizmet sağlayıcılara bağlı olduğundan, liderler siber dayanıklılık planlamasını iş sürekliliği ve dayanıklılığını daha da artırmak için uçtan uca değer zincirlerine yaymalıdır."

Ann Johnson,
Güvenlik, Uyum, Kimlik ve Yönetim İş Geliştirme Kurumsal Başkan Yardımcısı

Sistemleri ve mimariyi modernleştirmenin önemi

Devamı

Kurumların yaklaşımlarını modernize etmek ve tehditlerden korumak için başvurabilecekleri bazı belirgin alanlar vardır:

Sorun	Eyleme geçirilebilir adımlar
Kimlik sağlayıcısının güvensiz yapılandırması Kimlik platformlarının ve bileşenlerinin yanlış yapılandırılması ve kullanıma sunulması, izinsiz yüksek ayrıcalıklı erişim elde etmek için kullanılan yaygın bir vektördür.	AD ve Azure AD altyapısı gibi kimlik sistemlerini kurarken ve bakımını yaparken güvenlik yapılandırması temellerine ve en iyi uygulamalarına göre hareket edin. Ayrıcalıkların birbirinden ayrılmasını uygulamaya koyup en az ayrıcalık erişimini ve kimlik sistemlerini yönetmek için ayrıcalıklı erişim iş istasyonlarını (PAW) kullanarak erişim kısıtlamalarını hayata geçirin.
Yetersiz ayrıcalık erişimi ve yan hareket kontrolleri Yöneticiler, dijital ortamda gereğinden fazla izne sahiptir; genellikle internet ve üretkenlik risklerine maruz kalarak iş istasyonlarında yönetici kimlik bilgilerini ifşa eder.	Ortamı daha da dayanıklı hâle getirmek ve bir saldırının kapsamını sınırlandırmak için yönetim erişiminin güvenliğini sağlayın ve erişimi sınırlayın. Tam zamanında erişim ve yeterli yönetim gibi Ayrıcalıklı Erişim Yönetimi denetimlerini kullanın.
Çok faktörlü kimlik doğrulama (MFA) olmaması Günümüzün saldırganları içeri sızmıyor, oturum açıyorlar.	MFA, tüm kurumların kullanması gereken kritik ve temel bir kullanıcı erişim denetimidir. MFA, koşullu erişimle birleştiğinde siber tehditlerle mücadelede çok değerli olabilir.
Düşük olgunluktaki güvenlik işlemleri Etkilenen kurumların çoğu, hem geleneksel tehdit algılama araçlarını kullanıyor hem de zamanında müdahale ve düzeltmeyle ilgili geçerli verilere sahip değildi.	Kapsamlı bir tehdit algılama stratejisi için genişletilmiş algılama ve müdahale (XDR) yatırımları ve gürültüyü sinyallerden ayırmak için makine öğrenimini kullanan modern bulut yerel araçları gereklidir. Dijital ortamda derin güvenlik verileri sağlayabilen XDR'yi kullanarak güvenlik operasyon araçlarını modernleştirin.
Bilgi koruma denetimi eksikliği Kurumlar, veri konumlarında tam kapsama sahip olan ve bilgi yaşam döngüsü boyunca etkili kalan ve verilerin iş kritikliğiyle uyumlu olan bütünsel bilgi koruma kontrollerini bir araya getirmek için mücadele etmeye devam ediyor.	Kritik iş verilerinizi ve bulundukları yerleri belirleyin. Bilgi yaşam döngüsü süreçlerini gözden geçirin ve iş sürekliliğini sağlarken veri korumasını zorunlu kılın.
Modern güvenlik çerçevelerinin sınırlı olarak benimsenmesi Kimlik, farklı dijital hizmetlere ve bilişim ortamlarına erişim sunan yeni güvenlik alanıdır. Sıfır güven ilkeleri, uygulama güvenliği ve diğer modern siber çerçeveleri entegre etmek; kurumların, aksi durumda öngörmekte zorlanabilecekleri riskleri proaktif olarak yönetmesini sağlar.	Sıfır Güven çerçeveleri; en az ayrıcalık ve tüm erişimin açık bir şekilde doğrulanması kavramlarını zorunlu kılar ve her zaman tehlikenin var olduğunu varsayar. Kurumlar, iş sistemlerinde daha yüksek güvence seviyeleri için DevOps ve uygulama yaşam döngüsü süreçlerinde güvenlik denetimleri ve uygulamalarını da kullanmalıdır.

Temel güvenlik duruşu, ileri düzey çözüm etkinliğinde belirleyici bir faktördür

Analizimiz sırasında kurumsal savunma sistemlerinde kör noktaların yaygın olduğunu keşfettik; bu noktalar, saldırganların, gelişmiş güvenlik çözümleri kullanılırken bile ilk erişimi elde etmesini, bir başlangıç noktası oluşturmasını ve bir saldırı gerçekleştirmesini sağlıyor.

Çoğu durumda, bir siber saldırının sonucu, daha saldırı başlamadan uzun zaman önce belirlenir. Saldırganlar, ilk erişim elde etmek, izleme yapmak, yanal hareket ve şifreleme veya sızma yoluyla ortalığı birbirine katmak için savunmasız ortamları kullanır. Bir saldırganı erkenden durdurmak, toplam etkiyi azaltma ihtimalini büyük ölçüde artırır.

Microsoft, bu ortamlardaki fiili uygulamada en yaygın eksiklikleri belirlemek için güvenlik duruşlarındaki belirli yapılandırmaları inceledi. Bu sayede, tehdit aktörlerinin ağlara erişim kazanmasına ve fark edilmeden ağ içinde dolaşmasına izin veren, insanlar tarafından işletilen fidye yazılımı saldırılarında en yaygın güvenlik açıklarını görebildik.

Temel güvenlik yapılandırmaları devrede olmalıdır

Bir kurumdaki yerleşik olmayan veya güncelliğini yitirmiş (hem güvenlik açıkları hem de güvenlik aracı durumu ile ilgili olarak) cihazlar, saldırganlar için potansiyel giriş noktaları ve erişim sağlama yollarıdır. Kurumsal cihazların güncellenmiş bir uç nokta algılama ve yanıtı[1] (EDR) ve uç nokta koruma platformu[2] (EPP) çözümü ile entegre edilmesini sağlamak önemli bir adım olsa da, fidye yazılımını durdurmanın garanti olmadığını fark ettik.

EDR ve EPP gibi ileri düzey çözümler, bir saldırganın saldırı akışında erkenden tespit edilmesi ve otomatik iyileştirme ve koruma sağlanması açısından kritik öneme sahiptir. Ancak bu ileri düzey çözümler, bir saldırıyı tespit etme temel yeteneğine bağlı olduğundan temel güvenlik yapılandırmalarının devre olması gerekir. Aslında, temel güvenlik yapılandırmalarının bulunmaması nedeniyle zarara uğrayan ileri düzey çözümlere sahip senaryoların yaygın olduğunu gördük.

Güvenlik yapılandırmalarındaki en iyi uygulamalar, güvenlik operasyonları merkezi (SOC) analistinin yanıt süresine göre daha büyük bir dayanıklılık göstergesidir.

Bir SOC analistinin, müşteri ve iş ortağı grubumuzda altı aydan uzun bir sürede ilgili uyarıyı görmesi ve buna göre hareket etmesi için gereken sürede yüzde 70'lik bir azalma gözlemledik. Bu durum farkındalığın arttığına dair iyi bir işarettir. Bununla birlikte, güvenlik yapılandırması görünürlüğü SOC analist performansını iyileştirirken, kuruluştaki cihazların entegrasyonu ve güncellenmesi ile ürün görünürlüğünü sağlamak, önlemenin daha iyi bir şekilde yapılacağının habercisiydi.

Bilinmeyen cihazların oluşturduğu risk

Müşterilerin hangi varlıkların hangi işletim sistemlerinde çalıştığını bildiği bulut ağlarının aksine kurum içi ağlarda, kurum tarafından izlenmeyen veya yönetilmeyen IoT, masaüstü bilgisayar, sunucu ve ağ cihazları gibi çok çeşitli cihazlar bulunabilir.

Ortalama bir kurumsal ağda, bir EDR aracısı tarafından korunmayan ve kurumsal kaynaklara ve hatta yüksek değerli varlıklara erişebilecek 3.500'den fazla bağlı cihaz bulunur. Uç Nokta için Microsoft Defender (MDE), cihazları tespit etmek ve ağa bağlı olanlar için cihaz adı, işletim sistemi dağıtımı ve cihaz türü gibi cihaz sınıflandırmaları hakkında bilgi sağlamak amacıyla ağ incelemesini kullanır.

3.500

bir kuruluştaki uç nokta algılama ve yanıt aracısı tarafından korunmayan ortalama bağlı cihaz sayısı.

Bir EDR aracısının desteklemediği cihazlarda, en azından bunların varlığından haberdar olun ve güvenlik açıklarını değerlendirip ağ erişimini kısıtlayarak bu cihazları korumak üzere harekete geçin.

Eyleme dönüştürülebilir içgörüler

1. İleri düzey çözümler bile, temel güvenlik yapılandırmalarının eksikliği nedeniyle zayıflayabilir.
2. Gelecekteki saldırılara karşı korunmak amacıyla güvenlik duruşu yapılandırmalarında en iyi uygulamalara yatırım yapın. Bu temel ayarlar, bir kuruluşun saldırılara karşı savunma yeteneği açısından büyük bir yatırım getirisi sağlar.
3. Tüm uygulanabilir cihazları bir EDR çözümüne entegre edin.
4. Ürünlerde daha fazla görünürlük ve daha kapsamlı koruma avantajları sağlamak için güvenlik aracılarını güncellediğinizden ve kurcalamaya karşı koruma sağladığınızdan emin olun.

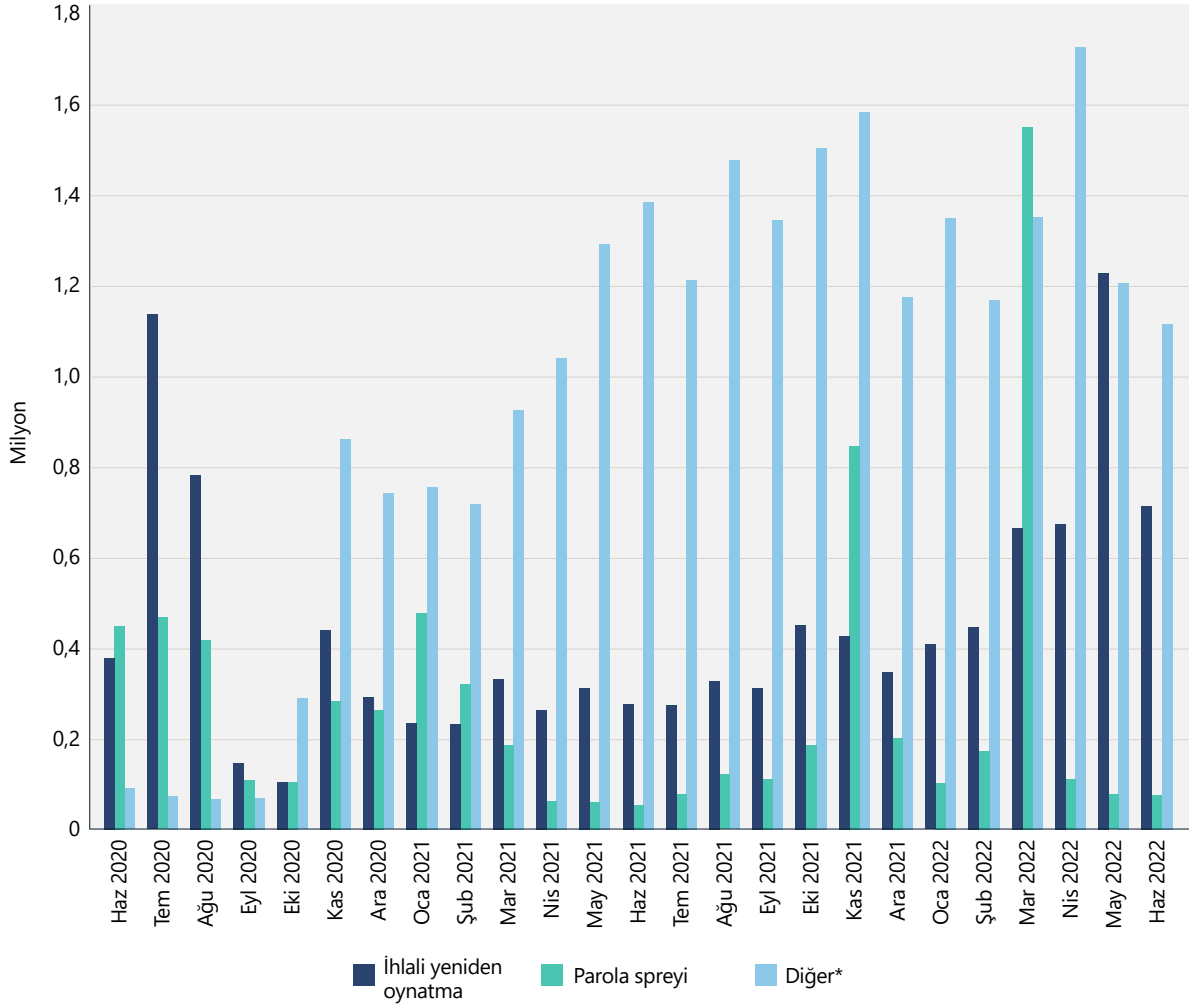
Kimlik sağlığını korumak, kurumsal refah için temel unsurdur

Kimliği korumak her zamankinden daha önemli. Her ne kadar parola tabanlı saldırılar, kimlik güvenliğini tehlikeye atan temel kaynak olmaya devam etse de, başka tür saldırılar da ortaya çıkmaktadır. Karmaşık saldırıların yoğunluğu, önceki parola püskürtme ve ihlal tekrarı normuna bağlı olarak artmaya devam ediyor.

Parola tabanlı saldırılar hâlâ yaygındır; bu yöntemlerle güvenliği ihlal edilen hesapların yüzde 90'ından fazlası güçlü kimlik doğrulamasıyla korunmuyor. Güçlü kimlik doğrulamada, parola + SMS ve FIDO2 güvenlik anahtarları gibi birden fazla kimlik doğrulama faktörü kullanır.

Hedefli parola püskürtme saldırılarında ve binlerce IP adresine yönelik saldırgan trafiği hacminde çok büyük artışlar gördük.

Saldırı kategorisine göre güvenliği ihlal edilen kullanıcılar



Saldırı kategorisine göre aylık olarak güvenliği ihlal edilen kullanıcılar. Kasım 2021 ve Mart 2022'deki ani artışlarda görüldüğü gibi, parola püskürtme saldırılarının hacmi oldukça değişkendi. Bu ani artışlar, binlerce kullanıcıya ve binlerce IP adresine erişildiğini gösteriyor. *"Diğer" kategorisi; kimlik avı, malware, izinsiz bağlantı izleme, kurum içi belirteç düzenleyen kuruluşun güvenliği vd. gibi parola püskürtme ve ihlal tekrarından farklı olan saldırıları ifade eder. Kaynak: Azure AD Kimlik Koruması.

4.500

Bu açıklamayı okumak için gereken sürede biz 4.500 parola saldırısını engelledik.

Kimlik sağlığını korumak, kurumsal refah için temel unsurdur

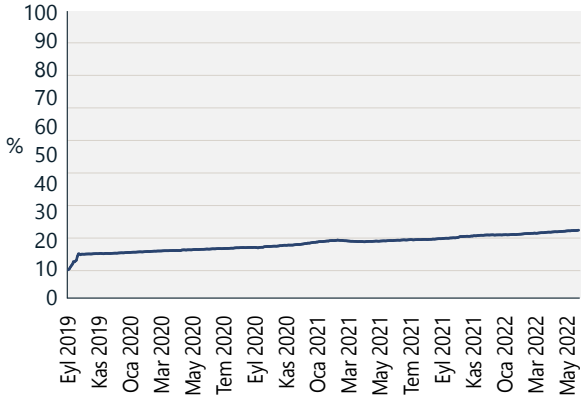
Devamı

Güçlü kimlik doğrulaması benimseme

Olumlu taraftan bakıldığında Azure Active Directory (Azure AD) kurumsal müşteri tabanında güçlü kimlik doğrulaması benimsemesinde istikrarlı bir büyüme görüyoruz. Azure AD için aylık etkin güçlü kimlik doğrulama kullanıcıları (MAU) geçen yıl yüzde 19'dan yüzde 26'ya yükselirken, yönetim hesapları için güçlü kimlik doğrulama MAU'su yüzde 30'dan yaklaşık yüzde 33'e yükseldi.

Bu trend olumlu olsa da, güçlü kimlik doğrulama kapsamının çoğunluğuna ulaşmak için hâlâ önemli bir büyümeye gerek duyulmaktadır. Ortamlarında halihazırda güçlü kimlik doğrulaması kullanmayan müşteriler, kullanıcılarını korumak için güçlü kimlik doğrulama planlaması ve uygulamasına başlamalıdır.[3] Güçlü kimlik doğrulama kurulumu tasarlanırken, parola saldırıları riskini ortadan kaldırarak uygulanabilir en güvenli deneyimi sunması nedeniyle parolasız kimlik doğrulama dikkate alınmalıdır.

Güçlü kimlik doğrulama kullanımı
(Eylül 2019–Mayıs 2022)

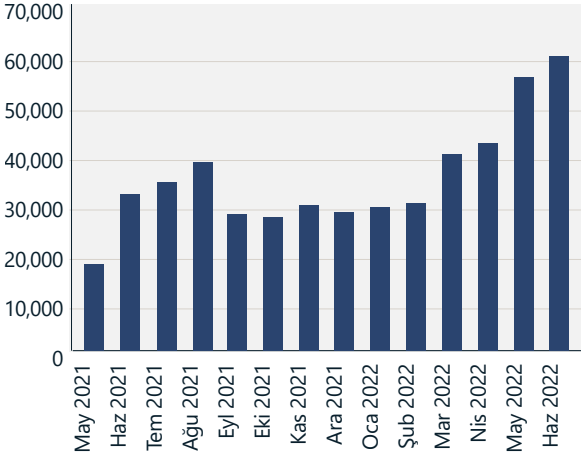


Güçlü kimlik doğrulama kullanımı 2019 yılından bu yana iki katına çıkarken, kullanıcıların yalnızca yüzde 26'sı ve yöneticilerin yüzde 33'ü güçlü kimlik doğrulaması kullanıyor. Kaynak: Azure Active Directory.

Belirteç tekrar saldırılarında istikrarlı artış

2022 yılında diğer saldırı türlerinin payı arttı. Tespit olasılığını azaltmak için özellikle parola tabanlı kimlik doğrulamasından kaçınan hedefli saldırılarda bir artış gördük. Bu saldırılarda; malware, kimlik avı ve diğer yöntemlerle elde edilen tarayıcıda çoklu oturum açma (SSO) tanımlama bilgileri veya yenileme belirteçleri kullanılır. Bazı durumlarda saldırganlar, tespit olasılığını daha da azaltmak için hedeflenen kullanıcının coğrafi konumuna yakın konumlardaki altyapıyı seçer. Azure AD Kimlik Korumasında ayda 40.000'den fazla tespite ulaşan belirteç tekrar saldırılarında istikrarlı bir artış gördük. Belirteç tekrarı, söz konusu belirteçlere sahip bir saldırgan tarafından meşru bir kullanıcı için düzenlenen belirteçlerin kullanılmasını ifade eder. Belirteçler genellikle malware ile, örneğin çerezlerin kullanıcının tarayıcısından sızdırılmasıyla veya gelişmiş kimlik avı yöntemleriyle elde edilir.

Tespit edilen belirteç tekrar saldırılarının hacmi



Aylık olarak tespit edilen belirteç tekrar saldırıları. Kaynak: Azure AD Kimlik Koruması, anormal belirteç algılamasıyla işaretlenen benzersiz oturumlar.

Kimlik sağlığını korumak, kurumsal refah için temel unsurdur

Devamı

Belirteçleri ayıklama

Saldırganların hedeflerine ulaşmak için malware'den çok kimlik bilgilerine ihtiyaçları vardır. Aslında, insanlar tarafından işletilen tüm fidye yazılım saldırılarının yüzde 100'ünde çalıntı kimlik bilgileri yer alıyor. Birçok gelişmiş izinsiz girişte, başlangıçta karmaşık olmayan ve yaygın olarak dağıtılmış kimlik bilgisi hırsızlığı malware'lerinden çalınan ve karanlık web'den satın alınan kimlik bilgileri yer almaktadır. Bu malware sınıfı, oturum bilgileri ve MFA talepleri gibi belirteçleri çalmak için geliştirilmiştir. Buradan, kullanıcıların kurumsal varlıklara giriş yaptığı ev sistemlerinde bulunan enfeksiyonların, kurumsal ağlarda ciddi olaylara yol açabileceği anlamı çıkarılabilir.

Saldırganlar ayrıca bağlantıyı izinsiz izleme saldırılarıyla mağdurların cihazlarından belirteçleri ayıklayabilir. Bu tip saldırılarda mağdur, bir kimlik avı e-postasındaki veya anlık iletideki kötü amaçlı bir bağlantıya tıklar ve kimlik sağlayıcının meşru oturum açma sayfasına benzeyen bir web sitesine yönlendirilir. Gerçekte ise bu, kullanıcı ve kimlik sağlayıcısı arasındaki tüm trafiği aktaran ve ele geçiren saldırgan tarafından programlanmış bir web hizmetidir. Saldırgan, kullanıcı adını ve parolayı ele geçirebilir ve ayrıca MFA sorgulamalarını iletebilir. Kimlik sağlayıcı tarafından verilen ve saldırgan tarafından ele geçirilen belirteçlerde, saldırgan tarafından MFA gereksinimlerini karşılamak için kullanılabilecek MFA talepleri bulunabilir.

Bulut için Microsoft Defender Uygulamaları, 2022 yılı başından bu yana ayda ortalama 895 saldırı tespit etti. Bu saldırı biçimi, Sertifika Tabanlı Kimlik Doğrulama, Windows Hello for Business veya FIDO2 güvenlik anahtarları gibi MFA'nın kimlik avına karşı dayanıklı faktörleri kullanılarak engellenebilir.

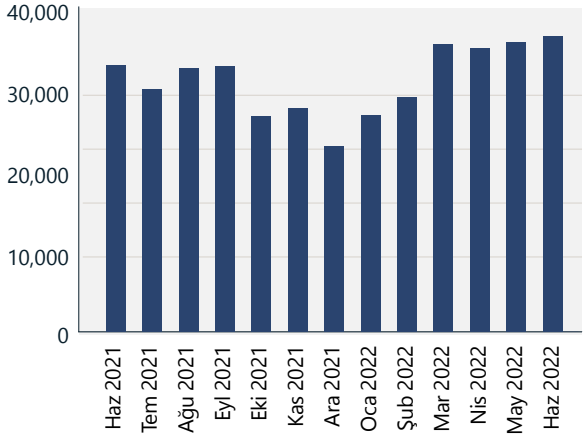
> Parola tabanlı saldırılar, hesap gizliliğinin ihlal edildiği başlıca yöntemdir.

MFA karmaşası

Saldırganlar "MFA karmaşası" kavramını kullanıp kurbanın isteği yanlışlıkla veya karmaşanın bir sonucu olarak kabul edeceğini umarak, kurbanın cihazına yönelik birden fazla MFA isteği oluşturur. Bu saldırı, Microsoft Authenticator gibi modern kimlik doğrulama uygulamalarının sayı eşleştirme[4] ve ek bağlam etkinleştirme[5] gibi özelliklerle birleştirilmesiyle önlenebilir. Azure AD Kimlik Koruması, ayda 30.000 MFA karmaşa saldırısı olduğunu tahmin ediyor.

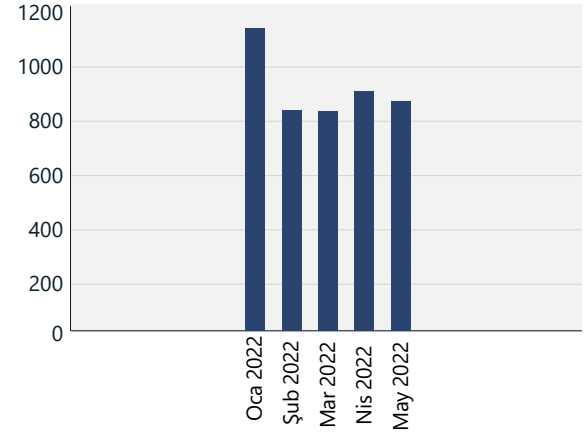
> Karmaşık saldırıların payı artmaya devam ettiğinden, çok faktörlü kimlik doğrulamadaki kimlik avına dayanıklı faktörlere olan ihtiyaç dikkat çekici bir hâl alıyor.

Tahmini MFA karmaşası saldırılarına ilişkin örnekler



Kaynak: Azure AD Kimlik Koruması.

Tespit edilen kimlik avı olayları ve ardından gelen bağlantıyı izinsiz izleme saldırıları



Kaynak: Bulut için Microsoft Defender Uygulamaları.

Eyleme dönüştürülebilir içgörüler

1. Kurumunuzdaki tüm hesapların güçlü kimlik doğrulama önlemleriyle korunduğundan emin olun.
2. Parolasız kimlik doğrulama, parola saldırı riskini ortadan kaldırarak en güvenli ve kullanıcı dostu deneyim sunar.
3. Kurumunuzun tamamında eski kimlik doğrulamasını devre dışı bırakın.
4. Kimlik avına karşı dayanıklı güçlü kimlik doğrulama yöntemleriyle yüksek değerli hesapları ve yönetici hesaplarını koruyun.
5. Kurum içi kimlik sağlayıcısından bulut kimlik sağlayıcısına kadar olan yapıyı modernleştirin ve tutarlı kullanıcı deneyimi ve güvenlik için tüm uygulamalarınızı bulut tabanlı kimlik sağlayıcısına bağlayın.

Daha ayrıntılı bilgi için bağlantılar

- Bu Dünya Parola Gününde, parolaları tamamen kaldırmayı düşünün | Microsoft Güvenlik

İşletim sistemi için varsayılan güvenlik ayarları

Sürekli gelişen güvenlik tehdidi ortamında, siber dayanıklılığı iyileştirmenin varsayılan ayar olarak yapılandırıldığı bilgisayar güvenliğine duyulan ihtiyacın arttığını görüyoruz. İşletim sistemi güvenliği hiç olmadığı kadar acil, karmaşık ve kurum açısından kritik olsa da, doğru bir şekilde davranmak ve yönetmek zor olabilir.

Eskiden bilgisayar ve cihaz güvenliğinde, müşterinin veya BT uzmanının kendi istekleri seviyede yapılandırması beklenen yerleşik güvenlik özellikleri bulunuyordu. Saldırganlar, amaçlarına ulaşmak için otomasyon, bulut altyapısı ve uzaktan erişim teknolojilerinde daha ileri düzey araçlar kullandığından bu yaklaşım artık yeterli olmamaktadır. Yongadan buluta kadar tüm güvenlik katmanlarının varsayılan olarak yapılandırılması kritik hâle geldi. Microsoft, Windows işletim sistemi güvenliğini varsayılan olarak yapılandıracak şekilde değişimden geçirdi.[6]

Savunmayı derinlemesine benimseyen müşteriler (katmanlı güvenlik duruşu, yeni güvenlik özellikleri, düzenli ve tutarlı patch uygulama ve güncellemelerin yanı sıra güvenlik eğitimi ve kimlik avı ve diğer dolandırıcılıkları bildirme farkındalığı gibi) daha az malware'e maruz kalabilir.

Derinlemesine savunmayı basitleştirmek isteyen Windows 11'de; bellek bütünlüğü, Güvenli Önyükleme ve Güvenilir Platform Modülü 2.0 gibi varsayılan olarak açık durumda olan, sıkı bir şekilde entegre edilmiş donanım ve yazılım korumaları bulunmaktadır. Yeterli donanıma sahip olan Windows 10 kullanıcıları, bu ayarları Windows Ayarları uygulamasından veya BIOS menüsünden de açabilir.

Genelde eski cihazların donanım güvenliği ile yazılım güvenliği teknikleri arasında güçlü bir uyum bulunmamaktadır. Güvenliğin varsayılan olarak etkinleştirilmediği cihazlarda, mümkün olduğu takdirde ayarları manuel olarak yapılandırın.[7]

Microsoft, güvenliğin varsayılan olarak etkinleştirilmediği cihazlarda, mümkün olduğu takdirde ayarların manuel olarak yapılandırılmasını öneriyor.

Donanım ve yazılım yaşam döngüsü boyunca koruma sağlamaya yardımcı olan sürekli işletim sistemi güncellemeleri ve güvenlik yamalarının uygulanması konusunda proaktif olun.

Eyleme dönüştürülebilir içgörüler

1. Güvenilir Platform Modülünde oturum açma kimlik bilgilerini bağlayan parolasız bir çözüm kullanın ve özellikle Faster Identity Online (FIDO) Alliance[8] endüstri standardını karşılayan parolasız bir çözüm arayın.
2. Kurumların cihazlarında bulunan kullanılmayan ve eski yürütülebilir tüm dosyaları zamanında temizleyin.
3. Varsayılan olarak etkinleştirilmediği durumda, modern CPU'larda yerleşik olan yetenekleri kullanarak önyüklemeyi güçlendiren, Bellek bütünlüğü, Güvenli Önyükleme ve Güvenilir Platform Modülü 2.0'ı etkinleştirerek ileri düzey üretici yazılımı saldırılarına karşı koruma sağlayın.
4. Veri şifrelemeyi ve kimlik bilgileri korumasını açın.
5. Güvenilmeyen uygulamalara karşı gelişmiş koruma ve diğer yerleşik kötüye kullanım korumalarına ilişkin uygulama ve tarayıcı denetimlerini etkinleştirin.
6. Kötü amaçlı bir aygıtı harici olarak erişilebilen bağlantı noktalarına takmak gibi sıradan fiziksel saldırılara karşı korumaya destek olmak amacıyla bellek erişim korumasını etkinleştirin.

Daha ayrıntılı bilgi için bağlantılar

- Windows Güvenlik Kitabı | Ticari
- Windows 11'deki yeni güvenlik özellikleri hibrit çalışmanın korunmasına yardımcı olacak | Microsoft Güvenlik Blogu

Yazılım tedarik zincirini merkezileştirme

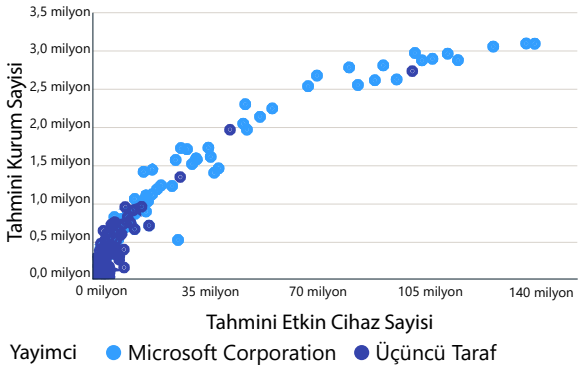
Üçüncü taraf uygulamalara, eklentilere ve uzantılara yönelik saldırılar, müşterinin tedarik ekosisteminde kritik rol oynayan tedarikçilere olan güvenini azaltabilir. Yazılım merkeziliğine bakmak üzere ağ teorisini kullanmak, özellikle merkezi uygulamalar için patch uygulamalarının önemini göstermeye yardımcı olur.

18 milyon yürütülebilir uygulama içeren Windows Uygulama Ağı, beş milyon kurumda kullanılarak yazılım ekosistemimize ilişkin üst düzey bir görünüm sunuyor. En çok kullanılan 100.000 uygulamanın yüzde 97'si üçüncü taraf kurumlar tarafından üretiliyor; bunların güncellemeleri ve güvenlik yamaları bu kurumlar tarafından sağlanıyor. Bu durum, ticari uygulama ekosistemimizin iki önemli özelliğine dikkat çekiyor.

Birincisi, Windows ticari uygulama ekosisteminde bir merkezilik söz konusudur. 1.000 veya daha fazla cihazda yalnızca en iyi 100.000 (18 milyon içinde) uygulama kullanılmaktadır. Başka bir deyişle, bu uygulamaların yüzde 1'inin yarısından biraz fazlası cihaz ekosistemi içinde bu kadar geniş kapsamlı bir etkiye sahiptir.

İkincisi, bu uygulamaların yönetilebilirliği açısından çeşitlilik söz konusudur; ilk 10.000 uygulama tedarikçisi, bu en çok kullanılan ticari uygulamaların güncelleme ve güvenlik yamalarını yönetmektedir. Bu da bir kurumun farklı yazılım tedarikçilerinin güvenlik, uyumluluk ve yönetim kontrolleri üzerinde ne denli karşılıklı bağımlı olduğunu gösteriyor.

En çok kullanılan uygulamalara ilişkin ticari sızma



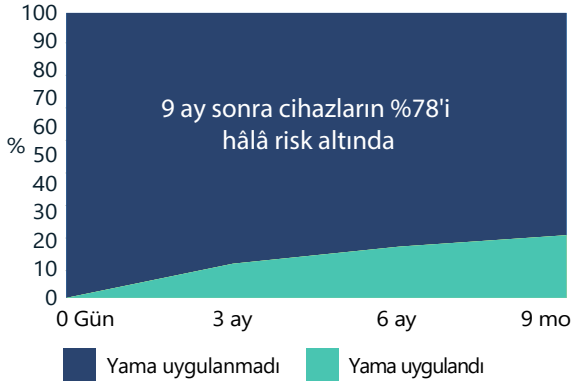
En popüler uygulamalar, milyonlarca kurumda ve on milyonlarca cihazda kullanılmaktadır. Düşmanlar neredeyse her yerde bulunduğu için sürekli olarak bu en iyi uygulamalardaki güvenlik açıklarını arıyor; bu durum kullanıcı tabanındaki milyonlarca cihazı etkileyebilir.

Yamanın yayınlanmasından aylar sonra, hatta ürün desteğinin sona ermesinden yıllar sonra bile milyonlarca ticari cihazda savunmasız uygulama sürümlerinin kullanıldığını gözlemliyoruz. Örneğin, 2017 yılından beri destek sağlanmayan bir PDF okuyucu sürümünü çalıştıran bir milyondan fazla etkin Windows ticari cihazı bulunmaktadır.

Desteklenmeyen uygulamaların eski sürümleri, milyonlarca ticari cihazda halen etkin bir şekilde kullanılmaktadır. Sonuç olarak, kurumlar uygulanmayan yamalar bakımından güvenlik açıkları riski altındadır.

Desteklenen uygulama sürümlerinde kritik yama benimseme hızında bir yatay seyir oluştuğunu görüyoruz; bu durum dayanıklılığı yönlendirecek trendin tam tersini ifade ediyor. Bunun yerine bu eğri, gerekli dayanıklılığa ulaşmak amacıyla her ay yamaların benimsenmesi yönünde üstel bir artış trendi göstermelidir.

Kritik yama kurulum oranı



Farklı tarayıcılara ilişkin 134 sürümü etkileyen kritik bir güvenlik açığını inceledikten sonra, yüzde 78'inde ya da milyonlarca cihazda, yamanın yayınlanmasından dokuz ay sonra bile etkilenen sürümlerden birinin kullanıldığını tespit ettik.

Cihazlarında daha eski uygulama sürümlerinin bulunma olasılığı yüksek olan kurumlarla ilişkili olan özellikleri belirlemek için InterpretML[9] aracını kullandık. Bu göstergelerin en önemlileri arasında şunlar bulunuyor: cihazlarda düşük saat etkileşimi; Asya Pasifik ve Latin Amerika gibi coğrafi alanlar; otomotiv, kimya, telekomünikasyon, nakliye ve lojistik, sağlık ödeyenleri (talep işleyicileri) ve sigortacılık gibi sektörler.

Yazılım dayanıklılık bakım işleminde, kullanılmayan uygulamalar düzenli olarak devre dışı bırakılmalı veya kaldırılmalıdır.

Bir kurumun güvenliği ve uyumluluğu, kendi çabasına ve yazılım tedarikçilerinin çabalarına bağlıdır.

Eyleme dönüştürülebilir içgörüler

1. Kurumunuz aracılığıyla tüm uygulamalar ve uç noktalar için güncellemeleri zamanında uygulayın.
2. Kurumların cihazlarında bulunan kullanılmayan ve eski yürütülebilir tüm dosyaları zamanında temizleyin.

Daha ayrıntılı bilgi için bağlantılar

- Microsoft Intune belgeleri | Microsoft Docs
- Uygulamaları yönetin | Microsoft Docs
- Uç Nokta için Microsoft Defender | Microsoft Güvenlik
- OSS Güvenli Tedarik Zinciri Çerçevesi | Microsoft Güvenlik Mühendisliği
- Microsoft Açık Kaynak Yazılım Güvenli Tedarik Zinciri Çerçevesi | GitHub

Yeni ortaya çıkan DDoS, web uygulaması ve ağ saldırılarına karşı dayanıklılık oluşturma

Hızlandırılmış dijital dönüşüm, geleneksel ağ ve güvenlik çevresi modeline son verdi. Buluta geçiş, işletmelerin dijital varlıkları korumak üzere bulutta yerel ağ güvenliğini benimsemesi gerektiğini ifade eder.

Saldırıların karmaşıklığı, sıklığı ve hacmi artmaya devam ediyor ve artık bu, tatil dönemleriyle de sınırlı değil. Bu da saldırıların yıl boyunca yaşandığını gösteriyor. Bu durum trafiğin yoğun olduğu geleneksel dönemlerin dışında da korumanın önemine dikkat çekiyor.

Dağıtılmış hizmet engelleme (DDoS) saldırıları

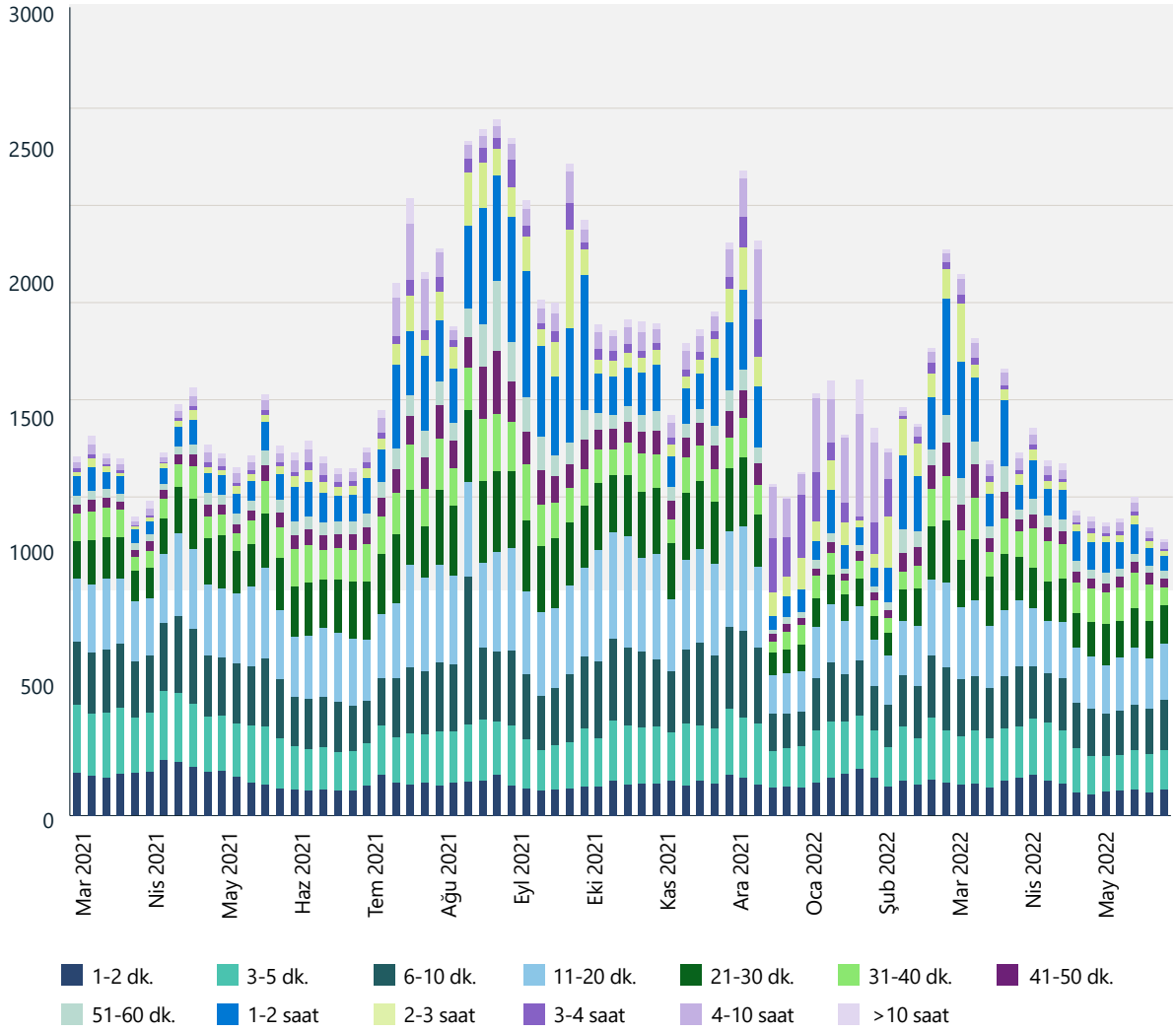
Geçen yıl dünyada hacim, karmaşıklık ve sıklık bakımından benzeri görülmemiş bir DDoS hareketliliği yaşandı. Bu DDoS patlamasının sebebi ulus devletlerin saldırılarında önemli artış ve düşük maliyetli kiralık DDoS hizmetlerinin yaygınlaşmasıydı. Microsoft, bir önceki yıla göre yüzde 40 artışla günde ortalama 1.955 saldırıyı engelledi. Daha önce, en yüksek saldırı sayısı normalde yıl sonunda tatil döneminde görülüyordu. Ancak bu yıl, bir günde kaydedilen en fazla saldırı 10 Ağustos 2021'de yaşandı. Bu da yıl boyunca saldırılara doğru bir kaymanın olduğunu gösterebilir ve geleneksel yoğun trafik dönemlerinin dışında da korumanın önemine dikkat çekiyor.

Kasım 2021'de Microsoft, birden fazla ülkeye yayılan ve yaklaşık 10.000 kaynaktan saniyede 3,4 terabit (Tbps) yoğunlukta bir DDoS saldırısını engelledi. 2022'de, 2+Terabit'in üzerindeki benzer yüksek hacimli saldırılar engellendi. Bu da yalnızca saldırıların karmaşıklığı ve sıklığının değil, aynı zamanda saldırı hacminin (bant genişliği) de arttığını gösteriyor.

Saldırı süresi

Geçen yıl gözlemlenen saldırıların çoğu kısa süreliydi. Saldırıların yaklaşık yüzde 28'i 10 dakikadan az, yüzde 26'sı 10-30 dakika arasında ve yüzde 14'ü 31-60 dakika arasında sürdü. Saldırıların yüzde otuz ikisi ise bir saatten uzun sürdü.

DDoS saldırılarının sayısı ve süre dağılımı
(Mart 2021–Mayıs 2022)



Geçen yılki saldırıların çoğu kısa süreliydi. Saldırıların yaklaşık yüzde 28'i 10 dakikadan kısa sürdü.

Yeni ortaya çıkan DDoS, web uygulaması ve ağ saldırılarına karşı dayanıklılık oluşturma

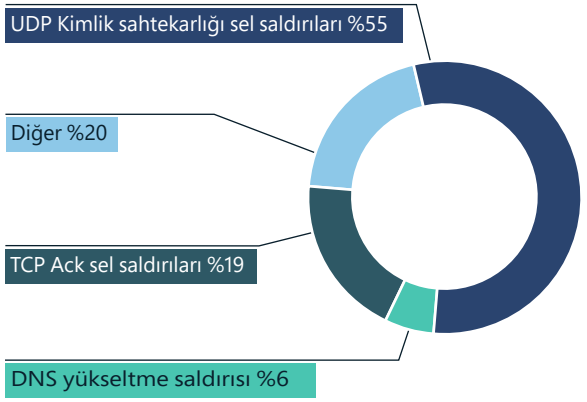
Devamı

DDoS saldırı vektörleri

Geçtiğimiz yıl, yaygın olarak kullanılan saldırı vektörleri, basit hizmet algılama protokolü (SSDP), bağlantısız hafif dizin erişim protokolü (CLDAP), etki alanı adı sistemi (DNS) ve tek bir tepe noktasından oluşan ağ zaman protokolü (NTP) kullanılarak 80 numaralı bağlantı noktasına Kullanıcı Veri Birimi Protokolü (UDP) yansımasından oluşuyordu. Ayrıca, 16.3 milyon tepe RPS (saniye başına istek) ve 9,89 Tbps tepe trafik ile web sitelerini hedefleyen uygulama katmanı DDoS saldırılarında bir artış gördük.

Microsoft, 2022 yılında günde yaklaşık 2.000 DDoS saldırı engellemesiyle tarihte bilinen en büyük DDoS saldırısını engelledi.

DDoS saldırı vektörleri



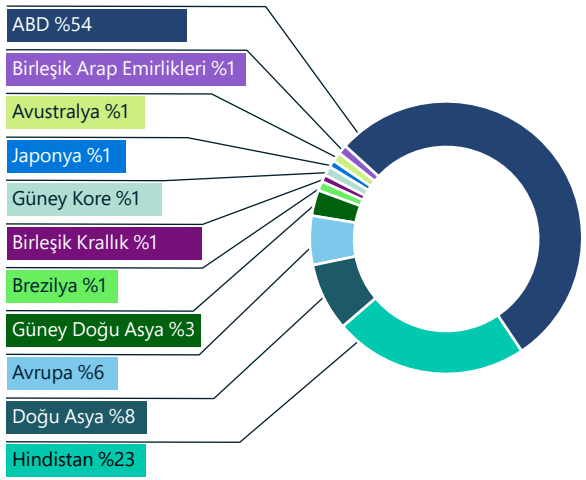
UDP Kimlik sahtekarlığı sel saldırılarının sayısı 2022'nin ilk yarısında yüzde 16'dan yüzde 55'e yükseldi. TCP Ack sel saldırısı yüzde 54'ten yüzde 19'a geriledi.

Oyun endüstrisi, çoğunlukla Mirai botnet mutasyonlarından ve düşük hacimli UDP protokolü saldırılarından kaynaklanan DDoS saldırılarının en büyük hedefi olmaya devam ediyor. UDP, oyun ve canlı yayın uygulamalarında sıklıkla kullanıldığından, saldırı vektörlerinin ezici bir çoğunluğu UDP kimlik sahtekarlığı saldırılarıyken küçük bir kısmı ise UDP yansıtma ve yükseltme saldırılarından oluşuyordu.

Coğrafi hedef bölgeleri

Geçen yıl tespit edilen DDoS saldırılarının yüzde 54'ü Amerika Birleşik Devletleri'ndeki hedeflere yapıldı. Bu eğilimin nedeni, çoğu Azure ve Microsoft müşterisinin Amerika Birleşik Devletleri'nde bulunması olabilir. Ayrıca, Hindistan'a yönelik saldırılar 2021'in ikinci yarısında sadece yüzde 2 oranındayken, 2022'nin ilk yarısında yüzde 23'e çıkarak keskin bir şekilde artmış oldu. Doğu Asya ve özellikle Hong Kong yüzde 8 ile saldırganların popüler hedefi olmaya devam ediyor. Avrupa'da da Amsterdam, Viyana, Paris ve Frankfurt bölgelerine yönelik yoğun saldırıların yapıldığını gördük.

DDoS saldırı hedefi

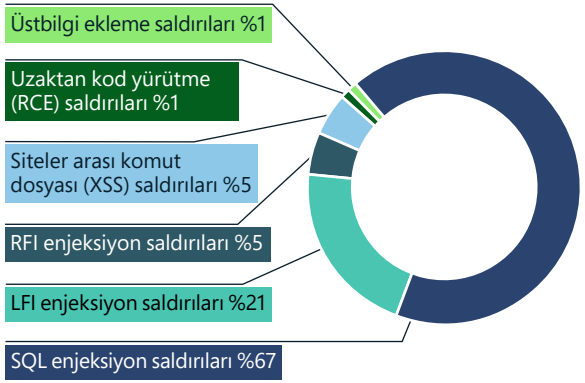


Asya'daki saldırı yoğunluğunun bu kadar fazla olmasını, özellikle Çin, Japonya, Güney Kore ve Hindistan'da oyun ayak izinin büyüklüğüne bağlıyoruz. Akıllı telefon kullanım sıklığı mobil oyunların popülaritesini artırırken bu yaygınlık genişlemeye devam edecek. Bu da bu coğrafi hedefin sürekli genişlemeye devam edeceğini düşündürtüyor.

Web uygulaması kötüye kullanımları

DDoS korumasıyla birlikte web uygulaması güvenlik duvarı (WAF), web ve uygulama programlama arabirimi (API) varlıklarını korumak için derinlemesine savunma stratejisinin ayrılmaz bir parçasını oluşturur. Microsoft, Azure WAF'ler aracılığıyla her ay 300 milyardan fazla WAF kuralının devreye alındığını gözlemledi.

En yaygın saldırı türlerinin dağılımı



Azure WAF'nin her gün milyarlarca Açık Web Uygulaması Güvenlik Projesini (OWASP) tespit ediyor (ilk 10[10]). Bulgularımıza göre, saldırganlar en çok SQL yerleştirme saldırılarını denedi ve bunun arkasından yerel dosya yerleştirme ve uzaktan dosya yerleştirme saldırıları geldi. Bu, yerleştirme saldırılarını üçüncü en yaygın web saldırısı türü olarak gösteren OWASP İlk On listesiyle uyumludur.

Azure web uygulamalarına yönelik bot saldırılarında da bir artış yaşandı ve aylık ortalama 1,7 milyar bot isteği ve bu trafiğin yüzde 4,6'sı kötü botlardan oluşuyor.

Yeni ortaya çıkan DDoS, web uygulaması ve ağ saldırılarına karşı dayanıklılık oluşturma

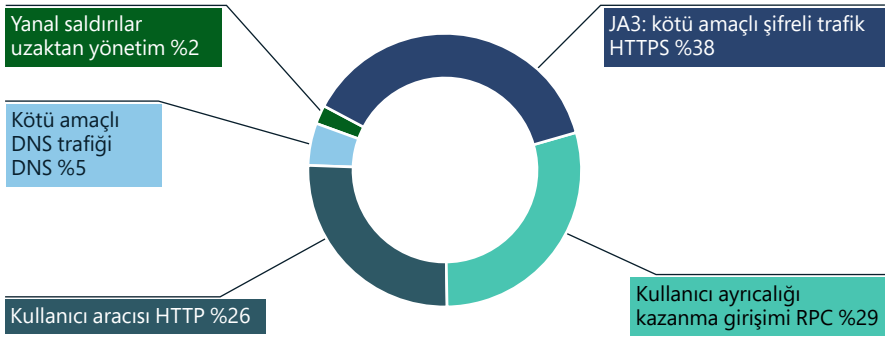
Devamı

Kimlik bilgisi doldurma saldırıları, kredi kartı dolandırıcılığı, siber etki kampanyaları ve tedarik zinciri saldırıları gerçekleştiren bot sayısındaki artış nedeniyle, web uygulamalarına yönelik bot saldırılarında da istikrarlı bir artış bekliyoruz.

Ağa izinsiz girişler: Algılama ve önleme

2022'de ağ katmanı kötüye kullanımlarında, özellikle malware'lerde ciddi bir artış gözlemledik. Azure Güvenlik Duvarı izinsiz giriş algılama ve önleme sistemi (IDPS), sadece Haziran ayında 150 milyondan fazla bağlantıyı engelledi.

IDPS Trafik engelleme nedeni



IDPS trafik uyarısı nedenleri

IDPS trafik uyarısı ve reddetme analizi, saldırganların aşağıdaki yaklaşımları kullandığını gösteriyor. Trafik reddetmede, saldırganların faaliyetlerini gizlemek için SSL kullandıklarını görüyoruz ve uzaktan kod çalıştırma saldırıları daha yaygın hâle geliyor. Uyarı trafiğinde, uzaktan kod çalıştırma saldırılarını gerçekleştirmek için SMB/SMB2 protokollerinin kullanıldığını görüyoruz.

Eyleme dönüştürülebilir içgörüler

1. Bir veri merkezi veya bulut hizmeti içindeki sistemler arasındaki tüm trafiği ve bunlara erişmeye amaçlayan trafiği inceleyin.
2. Tüm yıl boyunca kullanılabilen güçlü bir ağ güvenliği müdahale stratejisi geliştirin.
3. Güçlü bir "sıfır güven" ağ güvenliği uygulamak için buluta özgü güvenlik hizmetlerini kullanın.

Daha ayrıntılı bilgi için bağlantılar

- Azure Güvenlik Duvarı ile fidye yazılımı saldırılarına karşı güvenlik savunmanızı iyileştirin | Azure Blog ve Güncelleştirmeleri | Microsoft Azure
- Bir DDoS yükseltme saldırısının anatomisi | Microsoft Güvenlik Blogu
- Azure Web Uygulaması Güvenlik Duvarı ile uçtan buluta akıllı uygulama koruması | Azure Blog ve Güncelleştirmeleri | Microsoft Azure

Veri güvenliği ve siber dayanıklılığa yönelik dengeli bir yaklaşım geliştirme

Dijital dönüşüm, veri varlıklarının büyük ölçüde genişlemesine ve güvenlik, uyumluluk ve gizlilik risklerinde bir artışa neden oldu. Siber açıdan dayanıklı kurumlar, veri koruma, uyumluluk ve kurtarma yeteneklerine yapılan yatırımları dengelemeli ve farklı türdeki ihlalleri yönetmek için bunları özel düzenleyici müdahale süreçleriyle entegre etmelidir.

Asıl mesele veri ihlallerinin olup olmaması değil, ne zaman olacağıdır. IBM ve Ponemon Institute'un "Veri İhlalinin Maliyeti, 2021" başlıklı araştırması, dünyadaki ortalama veri ihlali maliyetinin 4,24 milyon USD (önceki yıla göre yüzde 10 artış) ve ABD'de 9,05 milyon USD olduğunu gösteriyor. Uyumsuzlukların maliyeti artıran en önemli faktör olduğu görüldü. Buna karşılık, ihlal maliyetinin düşürülmesi, olay müdahalesi (IR) planlaması, Sıfır Güven dağıtım olgunluğu, güvenlik yapay zekası ve otomasyonu ve şifreleme kullanımı gibi en iyi uygulamalarla ilişkilendirildi.

Veri ihlalleri kaçınılmazdır. Dengeli bir esneklik yaklaşımını benimseyen kurumlar, ihlallerin sıklığını, etkisini ve maliyetini azaltacaktır.

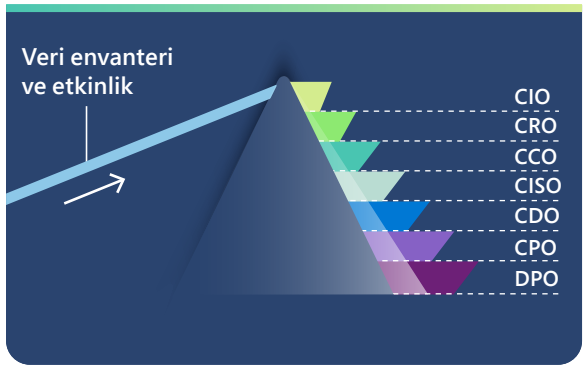
Veri yönetişimi, güvenlik, uyumluluk ve gizlilik birbirine bağlıdır

Verilerin son yıllarda kurumlar için çok önemli bir değer yaratan itici güç olarak öne çıktığını gördük. Aynı zamanda, hem veri yönetişimi hem de güvenliği gerektiren gizlilik düzenlemelerinin yükselişi, risk rolleri arasındaki sınırları ortadan kaldırıyor. Veri Direktörü (CDO) veya Gizlilik Direktörleri (CPO) gibi daha yeni üst düzey pozisyonlar, güvenlik ve uyumluluk konusunda kanuni bir hakka sahipken, veri korumasının uygulanması ve operasyonel hâle getirilmesi genellikle Bilişim Direktörleri (CIO) ve/veya Bilgi Güvenliği Direktörleri (CISO) tarafından yönetilen ekiplere bağlıdır. CDO'lar tarafından yönetilen veri yönetişim girişimlerinin de güvenlik faydaları olduğu için tek yönlü bir durum söz konusu değil. Bu birbirine bağlılığın bir sonucu olarak, BT, veri yönetişimi, güvenlik, uyumluluk ve gizlilik ekiplerinin verimliliği sağlamak ve riski yönetmek için çok daha yakın iş birliği içinde çalışması gerekiyor.

Gelecek, bütün kurumun veri varlığı için birleşik veri riski yönetimi platformlarında saklı

BT, veri yönetişimi, güvenlik, uyumluluk ve gizlilik yönetimi süreçlerini uyumlu hâle getirmek, tipik bir kurumun hibrit, çoklu bulut veri ortamında her disiplin ve tutarsızlık için özel olarak uyarlanmış uygulamalardan oluşan bir ortamda zordur. Kurumların verilerini bulmak ve bilmek, verilerini korumak, verilerin erişimini, kullanımını ve yaşam döngüsünü yönetmek ve veri varlıklarında veri kaybını önlemek için tek bir noktaya ihtiyaç duyduğuna inanıyoruz.

Aynı veri envanteri ve hareket bilgisinden çalışmak, ekipler arasındaki süreçleri kolaylaştırır, daha kapsamlı bir risk görünümü sağlar ve kurumların ihlallere karşı yanıtlarını daha iyi hazırlamalarına ve düzenlemelerine imkan tanır.



"Tek nokta" bir prizma gibi görülmelidir. Veri güvenliği, uyumluluk ve gizlilik konusunda pay sahibi olan ekipler, uyum sağlamak ve ortak çalışmak için aynı veri envanteri ve etkinliğinin farklı ancak tutarlı görünümlerine ihtiyaç duyar. Veri etkinliği; veri güvenliği denkleminin değerli bir parçası olan veri erişimi, değiştirme ve hareket olaylarını içerir.

Etkili veri idaresi, güvenlik, uyumluluk ve gizlilik birbirine bağlı olup ekiplerin ortak çalışmasını gerektirir.

Eyleme dönüştürülebilir içgörüler

1. Savunmayı, kurtarma ile dengeleyin ve uyumluluk, veri koruma ve müdahale yeteneklerine yatırım yaparak veri ihlali etkisini en aza indirin.
2. Veri riski silolarının üzerine çıkan ve tüm veri varlığını kapsayan süreçler ve araçlar geliştirin ve bunları benimseyin.

Daha ayrıntılı bilgi için bağlantılar

- Microsoft Purview—Veri Koruma Çözümleri | Microsoft Güvenlik
- Uyumluluğun ve veri yönetiminin geleceği burada: Microsoft Purview ile tanışın | Microsoft Güvenlik Blogu

Siber etki operasyonlarına karşı dayanıklılık: İnsan boyutu

Son beş yılda, grafiklerdeki ve makine öğrenimindeki gelişmelerle birlikte, internet geneline saniyeler içinde yayılabilen yüksek kaliteli, gerçekçi içeriği hızla oluşturabilen kullanımı kolay araçların yaygınlığı arttı.

Yazılı, işitsel ve görsel içeriklerle bildirilen olaylarda, ne insanların ne de algoritmaların gerçeği kurgudan güvenilir bir şekilde ayırt edemediği bir noktaya geldik. Bu araçların ve ürettiği çıktıların yaygınlaşması, dijital medyanın güvenilirliğini şüpheye düşürüyor ve bölgesel ve küresel olaylar hakkındaki anlayışımızı bozuyor. Teknolojideki ilerlemelerin getirdiği yeni etki operasyonları, demokratik süreçleri ciddi biçimde etkiliyor.[11]

Bu siber etki operasyonlarına karşı geleceğe daha güçlü bir şekilde hazırlanmak için neler yapabileceğimizi düşünmemiz gerekiyor. Teknoloji, bu yapbozun sadece bir parçasıdır. Medya okuryazarlığı, farkındalık ve dikkatle ilgili eğitimler, kaliteli gazeteciliğe yatırımlar (olay yerinde, yerel, ulusal ve uluslararası güvenilir muhabirlerle) etki operasyonları hakkında paylaşım ve uyarı ağları dahil olmak üzere çok sayıda çalışmanın yanı sıra aldatma maksadıyla dijital medya üreten veya manipüle eden kötü niyetli aktörleri cezalandıran yeni düzenlemeler gerekli olacaktır.

Dijital içeriğe olan güveni yeniden sağlamanın, farklı bakış açılarını ve katılımı gerektiren iddialı bir hedef olduğunun da farkındayız. Bu tehditleri tek başına çözebilecek bir şirket, kurum veya hükümet yoktur. İnsanlar olarak ortak çalışma ve iş birliği yapma yeteneğimiz bizim süper gücümüzdür. Bu, herkesin (dünyadaki hükümetler, sanayiler, akademi ve özellikle haber, sosyal ve medya kuruluşları) toplumumuzun sağlığı ve gelişimi için birlikte çalışmasını gerektireceği için özellikle önemlidir.

Daha ayrıntılı bilgi için bağlantılar

- Savunma Bakanlığı siber görevlerinde yapay zeka uygulamaları | Microsoft On the Issues
- Yapay Zeka ve Siber Güvenlik: Artan Zorluklar ve Umut Veren Yönlendirmeler. Senato Silahlı Hizmetler Komitesi, Siber Güvenlik Alt Komitesi nezdinde Siber Alandaki Operasyonlara Yapay Zeka Uygulamaları Hakkında Oturum, 117. Kongre (3 Mayıs 2022; Eric Horvitz'in İfadesi)

Beceri kazandırarak insan faktörünü güçlendirme

İnsan faktörünü dikkate almak, her siber güvenlik beceri stratejisinin önemli bir bileşenidir. Kaspersky'nin BT Güvenliğinde İnsan Faktörü adlı araştırması,[12] siber güvenlik olaylarının yüzde 46'sında, saldırılara istemeden imkan tanıyan dikkatsiz veya üniformalı personelin bulunduğuna dikkat çekiyor.

Microsoft'un Dijital Güvenlik ve Dayanıklılık organizasyonundaki Eğitim ve Farkındalık ekibi, çalışanlarımıza bizim ve müşterilerimizin sistem ve verilerini güvence altına alma konusunda yetki vererek siber güvenliğin insan faktörünü güçlendirmekten sorumludur. Hedeflerimiz:

- Çalışanlar arasında kurumsal çapta merkezi bir temel güvenlik becerisi oluşturarak Microsoft ve müşterilerimiz için riski azaltmak.
- İstenen davranış sonuçlarını desteklemek için çok aşamalı bir eğitim güçlendirme yaklaşımıyla çalışanların güvenlik bilgilerini güçlendirmek.
- Her yıl gerekli güvenlik eğitimleri ve etkinlikleriyle bir güvenlik anlayışını Microsoft kültürünün ayrılmaz bir parçası hâline getirerek kültürel değişimi teşvik etmek.
- Siber güvenlikle ilgili tüm konularda en iyi uygulamalar, kurum politikası bilgileri ve olay raporlaması için tek noktadan yönetilen merkezi bir web kaynağını desteklemek.

Hedefe yönelik, merkezi bir siber güvenlik beceri programı, her Microsoft çalışanına yılda en az bir kez ulaşır. Eğitim sunumları, mevcut siber güvenlik girişimlerini desteklemek ve ölçülebilir davranış sonuçları elde etmek üzere optimize edilmiştir. Microsoft'un Bilgi Riski Yönetim Konseyi (IRMC), eğitimle yönetilecek önemli siber güvenlik davranış değişikliği sonuçlarının belirlenmesinde kilit bir rol oynar.

Tüm siber güvenlik beceri programlarımızla, çözümün verimliliğini, etkililiğini ve mümkün olan her yerde sonuçlarını ölçüyoruz. Örneğin, içeriden bilgi sızdırma tehdidine ilişkin beceri sunumumuz yüzde 95 eğitim uyumluluğuna, kusursuz öğrenci memnuniyetine ulaştı ve kurumun Report It Now aracıyla olası içeriden bilgi sızdırma tehditlerini bildiren yöneticilerde anlamlı bir artışı getirdi. Program şunları içerir:

Güvenlik Temelleri: Temel güvenlik ve gizlilik uygulamalarını ele alan merkezi ve kurumsal çapta siber güvenlik farkındalığı ve uyumluluk eğitimi. Merakla beklenen bu eğitim serisi, siber güvenlik hakkında yeni bilgiler öğrenmeyi ilgi çekici ve etkili hâle getiren eğitirken eğlendirme modelini kullanır.

STRIKE: Microsoft, iş segmenti çözümlerini geliştiren ve sürdüren mühendislere yönelik teknik bir eğitimdir. Yalnızca davetiyeyle verilen bu eğitimde, siber güvenlik hijyeniyle ilgili en iyi uygulamalara ilişkin güncel ve kritik alanları ele alınır ve hedef kitlenin ihtiyaçlarına göre uyarlanmış canlı bir hibrit dağıtım modeli kullanılır.

Programa özel: Hedefe yönelik eğitim programları, Shadow IT, Insider Threat ve Microsoft Federal gibi belirli siber güvenlik girişimlerini destekler. Bu sunumlar "kontrol listesi" eğitim yaklaşımını önlemek üzere yönetici sponsorluğu ve karne puanlamasıyla ilgili siber güvenlik girişimleri için genel katılım stratejisine harfiyen entegre edilmiştir.

MSProtect: Microsoft'un merkezi web kaynağı, siber güvenlikle ilgili tüm konulardaki en iyi uygulamaları, kurum politikası bilgilerini ve olay raporlamasını sunar. Bu isteğe bağlı kaynak, resmi eğitim tekliflerinin dışında çalışanların başvurabileceği bir kaynaktır.

Güvenlik becerisi, zorunlu bir prosedürel çalışma olarak görülmemelidir. Tam tersine, belirlenen hedef davranışlarda sonuçların takip edilmesi için davranış değişikliğine odaklanın ve sunumların etkisini belirlemek için dinleme sistemleri kurun.

Eyleme dönüştürülebilir içgörüler

1. Çalışanlara ihtiyaç duydukları yerde ve zamanda güvenlik eğitimi ve kaynaklarını sağlayın.
2. Kuruluşta paydaşların bilgi alabileceği merkezi bir beceri stratejisi geliştirin.
3. Eğitimin etkisinin verimlilik (nicelik), etkililik (kalite) ve sonuçlar (iş etkisi) açısından izlenmesini ve analiz edilmesini sağlayın.

Daha ayrıntılı bilgi için bağlantılar

- Microsoft, 30 milyon kişiye yardım ettikten sonra beceri girişiminin bir sonraki aşamasını başlattı

Fidye yazılımını ortadan kaldırma programımıza ilişkin içgörüler

Microsoft kimliklerin ve cihazların sağlam bir şekilde yönetilmesini ve sağlıklı olmasını sağlamak için son beş yılda kendi Sıfır Güven serüvenini[13] devam ettiriyor. Fidye yazılımı riski arttıkça, kendimizi ve müşterilerimizi koruma yaklaşımımızı desteklemek için kapsamlı bir bakış açısı geliştirdik.

Kurum içinde kapsamlı bir değerlendirmeden sonra kontroller ve kapsamdaki boşlukları gidermek, Defender for Endpoint, Azure ve M365 gibi hizmetlere yönelik özellik geliştirmelerine katkıda bulunmak ve bir fidye yazılımı saldırısı durumunda kurtarma konusunda SOC ve mühendislik ekiplerimiz için kılavuzlar geliştirmek üzere bir fidye yazılım ortadan kaldırma programı geliştirdik.

İlk adım, Microsoft'a yönelik bir fidye yazılımı saldırısına karşı korumamızın kapsamını anlamaktı. Defender for Endpoint'i kurma ve tüm cihazların yönetilmesini ve Sıfır Güven politikalarımıza uymasını sağlama çabaları zaten devam ediyordu ancak bir saldırıdan etkin bir şekilde kurtulup kurtulamayacağımıza dair daha büyük sorunun tüm yönlerini anlamanın bir yolunu bulmamız gerekiyordu. Bilgi edinmek için, genel kurumsal politikamızla uyumlu olan NIST 8374: Fidye Yazılımı Risk Yönetimi: Bir Siber Güvenlik Çerçevesi (CSF) Profilini[14] bilinen kontrol listemize göre değerlendirdik. Bu analiz, kapsama alanındaki boşlukları hızla tespit etti.

Ardından, CSF'nin Tanımlama, Algılama, Koruma, Yanıt Verme ve Kurtarma işlevlerindeki boşluklara öncelik verdik. Sıfır Güven ve diğer programlarla stratejik uyumu bulduk ve ayrıca mevcut iş akışı eksiklerini belirledik. Bu boşlukları kapatmak için gereken iş ve eforu değerlendirdikten sonra, bunları iki başlığa ayırdık:

- **Kurumu korumak (PtE):** Saldırının başarılı olması durumunda kendimizi korumak ve kurtulabilmek için kurum olarak yapmamız gereken iş adımlarını tanımlayın.
- **Müşteriyi korumak (PtC):** Müşterilerimizi ve işimizi korumak için sunumlarımıza yetenekler ekleyin.

Bulguları kendi kurumumuza entegre etmek

En önemli riskleri ortadan kaldırmak ve kritik hizmetlerimizi bir fidye yazılımı saldırısına karşı korumak için önümüzdeki 6 ila 12 ay boyunca, özel bir fidye yazılımı programının parçası olarak aşağıdaki beş senaryoyu gerçekleştirmeye yönelik yatırımlara odaklanmayı planlıyoruz. Senaryoların her birinde başarılı olduğumuzda, programın kapsamını kademeli olarak işletmenin tüm bölümlerine ulaşacak şekilde genişleteceğiz.

Senaryo 1: Güvenlik ekibi üyeleri, bir fidye yazılımı saldırısıyla ilişkili genel riski anlar ve yöneticilere kontrol eksiklikleri ve risk durumu hakkında farkındalık sağlamak üzere hazırlanmış bir süreci uygulamaya koyar.

Senaryo 2: Güvenlik ekibi üyeleri, hem kendilerinin hem de Microsoft içindeki diğer ekiplerin bir fidye yazılımı saldırısına yanıt vermesine ve kritik hizmetleri kurtarmasına yardımcı olması için tasarlanmış kılavuzlara erişebilir.

Senaryo 3: Kurumsal Dayanıklılık ekip üyelerinin, kritik sistemlerin yedeklenmesi için uyması gereken bir standardı vardır. Kılavuzlar kullanımdadır ve bir fidye yazılımı saldırısı durumunda verilerin kurtarılabilmesi için düzenli yedekleme ve kurtarma alıştırmaları yapılır.

Senaryo 4: Hizmet sahipleri, Microsoft kritik hizmetleri olarak öncelik verilen hizmetlere özel olarak odaklanarak hizmetlerini, müşteri verilerini, uç noktalarını ve ağ varlıklarını fidye yazılımı saldırılarına karşı korumak için gerekli güvenlik ve operasyon kontrollerini ve politikalarını anlar ve uygular.

Senaryo 5: Tüm çalışanlar, bir fidye yazılımı saldırısının nasıl tanınacağını ve güvenlik ekibine nasıl bildirileceğini ve müdahalenin nasıl başlatılacağını anlatan eğitim ve öğretim kaynaklarına erişebilir.

Eyleme dönüştürülebilir içgörüler

1. Kritik hizmetlere yönelik fidye yazılımı saldırılarıyla ilgili uçtan uca kurtarma ve iyileştirme faaliyetlerini belgeleyin ve doğrulayın.
2. Paydaşları, fidye yazılımına özel faaliyetleri ve fidye yazılımı için ödeme yapılıp yapılmayacağını/ne zaman ödeme yapılacağını belirlemek için bir karar süreci ve kılavuzu içerecek şekilde Kurumsal Kriz Yönetimi çalışma kitaplarınızı güncellemeye dahil edin.
3. Kullanıma alınan güvenlik ürünlerinizdeki yeteneklerden yararlanarak algılama ve koruma kapsamını iyileştirin (örneğin, Defender for Endpoint Attack Surface Reduction kuralları).
4. Bir fidye yazılımı saldırısına karşı korumanın temelini belirlemek üzere güvenlik standartları ekibiyle birlikte çalışın ve fidye yazılımı saldırısına karşı koruma konusunda mühendislik ekiplerine eğitim ve belgeler sağlayın.
5. DevOps ekipleri için güvenlik ve operasyon ilkelerinin dağıtımını kolaylaştırmak üzere otomasyonu kullanın ve bir sistem uyumlu değilse hızla belirlenip düzeltildiğinden emin olun.

Daha ayrıntılı bilgi için bağlantılar

- Microsoft'un fidye yazılımlarına karşı sağladığı korumayı paylaşma | Microsoft Inside Track

Kuantum güvenliği etkileri için şimdi harekete geçin

Kuantum bilişiminin günümüzün kriptografisine ve koruduğu her şeye yönelik tehdidi yönetme baskısı devam ediyor. Ulusal Güvenlik Departmanı Savunma ve İstihbarat Topluluk Sistemlerinin Siber Güvenliğini İyileştirmeye ilişkin yakın zamanda yayınlanan Memorandum,[15] Ülkenin Siber Güvenliğini Geliştirmek için 10428 numaralı ABD Başkanlık Kararına[16] dayanıyor ve yazılım tedarik zinciri güvenliğinin, gelecekteki ulus devlet saldırılarını engellemek anlamında kritik bir öneme sahip olduğunu vurgulamaktadır.

Kuantum bilgisayarları nelerdir?

Kuantum bilgisayarları, verileri depolamak ve hesaplamalar yapmak için kuantum fiziğinin özelliklerini kullanan makinelerdir. Bu, en iyi süper bilgisayarlarımızdan bile daha iyi performans gösterebilecekleri belirli görevler için son derece avantajlı olabilir. Kuantum bilişimi, veri şifreleme ve işleme için şimdiden yeni ufuklar açıyor. Çalışmalar, kuantum bilişiminin 2030 gibi erken bir tarihte milyar dolarlık (USD) bir kuantum endüstrisine dönüşeceğini tahmin ediyor.[17] Nitekim kuantum bilişim ve kuantum iletişimi, sağlık ve enerjiden finans ve güvenliğe kadar çok sayıda sektörde dönüştürücü bir etki bırakabilir.

Kuantum bilişim, günümüzün kriptografisi ve koruduğu her şey için bir tehdit oluşturuyor.

Günümüzün kriptografisine yönelik tehdit

Shor'un 1994 algoritması ve birkaç milyondan fazla fiziksel kübitten oluşan endüstriyel ölçekli bir kuantum bilgisayarıyla, yaygın olarak kullanılan açık anahtarlı kriptografik algoritmalarımızın tümü kırılabilir. Rakip kuantum tabanlı saldırılara karşı verimli, dayanıklı ve güvenli olan "kuantum güvenli" şifreleme sistemlerini dikkate almak, değerlendirmek ve standart hâle getirmek çok önemlidir. "Kuantum sonrası kriptografiye", yani kuantum saldırısına dayanıklı mevcut klasik algoritmalar ve protokollere yazılım geçişi, on yıllar olmasa da yakın gelecekte tamamlanacaktır.[18]

Yani kuantum günümüzün kriptografisine ve koruduğu her şeye yönelik tehdidi yönetme baskısı devam ediyor. Düşmanlar artık şifrelenmiş verileri kaydedebilir ve daha sonra bir kuantum bilgisayar mevcut olduğunda bunu kötüye kullanabilir. Kriptografik sonuçlarını değerlendirmeden önce kuantum bilişiminin gelmesini beklersek çok geç kalmış olacağız.

Siber ekosistemde kriptografi kullanıldığından, kriptografi tabanlı güvenlik hizmetlerimiz tehlikeye atılabilir. Örneğin, bu, iletişim (TLS, IPSec), mesajlaşma (e-posta, web konferansı), kimlik ve erişim yönetimi, web'de gezinme, kod imzalama, ödeme işlemi ve koruma için kriptografiye bağlı diğer hizmetleri kapsar.

Kuantum bilgisayarlar hayat buldukça, kriptografik algoritmaların ve yeteneklerin uygulamalarını içeren üçüncü taraf yazılım bileşenlerinin de incelenmesi gerekecektir. Bunun için değer zincirindeki tüm kuruluşların, zincirin güvende kalmasını sağlamak için üzerlerine düşeni yapması gerekir. Sektör kuruluşları ve kamu kuruluşları, yazılım tedarik zincirinin güvenlik ihtiyaçlarını belirlemek için çaba gösteriyor ve bazı durumlarda zincirin güvenliğini sağlamak için yeni şartları zorunlu kılıyor. Ulusal Güvenlik Memorandumu NSM-8[19] Ulusal Güvenlik Sistemlerinde (NSS) kuantum sonrası kriptografinin uygulanması için gereklilikleri ve zaman çizelgelerini belirler. "Modernizasyon planlaması, desteklenmeyen şifreleme kullanımı, onaylanmış görevler için benzersiz protokolleri, kuantuma dayanıklı protokolleri ve gerektiğinde kuantuma dayanıklı kriptografi kullanımına yönelik planlama" ile ilgili 180 gün içinde zamanlama beklentilerini ortaya koyuyor.

Standardizasyonda kuantum yönünden güvenli kriptografiye geçişte uzun çalışmalar gerekir. Açık anahtar kriptografisi kullanan ve standartlar üzerinde çalışan standardizasyon kurumları, artık kuantum sonrası algoritmaları denemeye ve bunlara uyum sağlamaya başlamalıdır.

Yeni kuantum sonrası kriptografi (PQC) algoritmaları (kuantum saldırısına karşı dayanıklı olduğu düşünülen klasik algoritmalar), NIST'nin Kuantum Sonrası Standardizasyon Projesiyle inceleniyor.[20] Bu çalışma, standardizasyon kurumlarındaki küresel çalışmaları da etkileyecektir. ABD hükümetinin algoritma seçimleriyle bazı örtüşmeler var olsa da, uyumlu algoritmalara yönelik farklı ulusal kurum/mevzuat seçimleri uluslararası zorluklara neden olabilir. Bu parçalanma, ürün ve hizmet mühendisliğini karmaşık hâle getirecektir.

Yeni kuantum sonrası şifreleme algoritmaları, NIST'nin Kuantum Sonrası Kriptografi Standardizasyon programıyla inceleniyor. Bu çalışma, standardizasyon kurumlarının küresel çalışmalarını etkileyecektir.

Eyleme dönüştürülebilir içgörüler

SAFECode ve ortak üyelerin yanı sıra, PQC geçişine hazırlık olarak sektörün acilen kısa vadeli faaliyetlere girişmesi gerekiyor.[21] Bunlar arasında:

1. Kriptografi kullanan ürünlerinizin/kodlarınızın envanterini çıkarın.
2. Kurumunuzda kriptografi değiştiğinde gereken kod karmaşasını en aza indirmeyi içeren bir kripto çeviklik stratejisi uygulayın.
3. Kriptografi kullanan ürünlerinizde veya hizmetlerinizde kuantum için güvenli aday algoritmaların kullanımını pilot olarak uygulayın.
4. Şifreleme, anahtar değişimi ve imzalar için farklı ortak anahtar algoritmalarını kullanmaya hazır olun.
5. Uygulamalarınızı çok büyük anahtar boyutlarının, şifrelerin ve imzaların etkisi yönünden test edin.

Daha ayrıntılı bilgi için bağlantılar

- Microsoft, yeni bir tür kübit geliştirmek için gerekli yetenekleri sağladı | Microsoft Araştırması

Daha fazla dayanıklılık için kurum, güvenlik ve BT'yi entegre etme

Güçlü siber dayanıklılık için işletme liderlerinin güvenliği uygularken güvenlik ekipleriyle birlikte çalışması gerekiyor. Microsoft'un deneyimine dayalı olarak, güvenlik liderliği zorlu bir disiplindir ve kuruluşu en etkin şekilde korumak için kuruluş liderlerinden destek gerektirir.

Güvenlik liderleri, risk, teknoloji, ekonomi, örgütsel süreç, iş modelleri, kültür dönüşümü, jeopolitik çıkarlar, casusluk ve uluslararası yaptırımlara uyum ile ilgili konularda farklı dinamik zorluklar yaşar. Bunların her birinin anlaşılması ve yakından yönetilmesi gerekir.

Güvenlik liderleri ayrıca zeki, iyi finanse edilmiş, yüksek motivasyonlu insan saldırganları ve düşük vasıflı ancak etkili siber suçluları engellemekten de sorumludur. Ekipleri, genellikle güvenliğin düşük bir öncelik olduğu veya hiç öncelik olmadığı 30 yıl veya daha uzun bir süre boyunca aşamalı olarak tasarlanan karmaşık teknik varlıkları savunmak zorundadır. Yıllar önce alınan kararlar, biz teknik sorumluluğu üstlenene ve güvenlik açıklarını giderene kadar bugün bile risk oluşturabilir.

Kurum liderleri ve politika yapıcılar, güvenlik liderlerini aktif olarak destekleyerek ve entegre güvenlik ile kuruluşun geri kalanı arasında bir köprü kurmalarına yardımcı olarak güvenlik üzerinde önemli bir pozitif etkiye sahip olabilir. Microsoft, bu uyumluluğa sahip müşterilerle çalıştığında, bu müşterilerin daha dayanıklı bir kurum oluşturduğunu ve ayrıca uyum sağlama ve yenilik yapma çevikliklerini geliştirdiklerini gözlemliyoruz.

Kurumsal liderlik, güvenlik liderlerini üç temel alana odaklanarak destekleyebilir:

1. Tasarım gereği güvenlik oluşturma

Güvenlik bazen iş süreçlerinde bir engel veya sonradan akla gelen bir düşünce olarak ele alınmakta ve çoğu zaman ancak bir riskten kaçınmak veya ucuz ve kolay bir şekilde düzeltmek için çok geç kalındığında kararlarda dikkate alınmaktadır.

Kurum liderleri ve politika yapıcılar şunları sağlamalıdır:

Yeni girişimlere güvenliği erkenden dahil edin. Yeni dijital girişimler ve bulut kullanımı, her yeni uygulama veya dijital yetenekle kurumsal riski en aza indirmek için güvenliğe öncelik vermelidir. Güvenlik entegre edildiğinde, aynı anda hem güvenlik hem de üretkenlik avantajları elde etmek için bu süreçleri eski sistemleri modernize etmek için kullanabilirsiniz.

Güvenlik için önleyici bakımı normalleştirin. Temel güvenlik bakımının (güvenlik güncellemeleri ve yamaları ve güvenli yapılandırmaların uygulanması gibi) tam kurumsal desteğe (bütçeler, planlanmış kesinti süresi, satıcı ürün desteği için satın alma gereksinimleriyle beraber) sahip olduğundan emin olun.

Ne yazık ki, birçok kurum bu yaygın uygulamaları erteliyor veya kısmen uyguluyor. Bu da saldırganların kötüye kullanımı açısından fırsat yaratıyor. Güvenlik normalleştirme ihtiyacı US NIST 800-40'ta belirtilmiştir.[22]

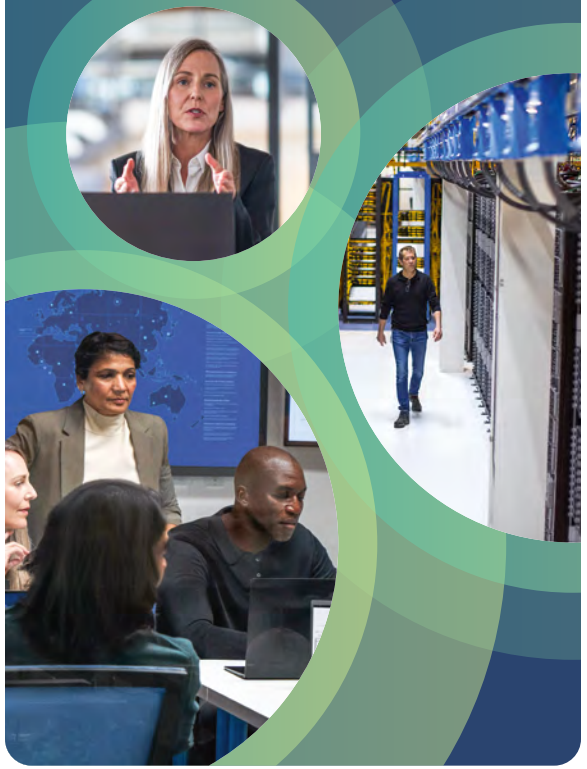
2. Güvenliği devreye alın

Kurum liderleri, kaynakların önceliklendirilmesini ve güvenlik felaketlerine karşı hazırlıklı olmak için kritik güvenlik süreçlerine aktif olarak katılmalı ve bunları desteklemelidir. Bunların arasında aşağıdakilerin uygulanması bulunur:

Kritik iş varlıklarını tanımlamak. Güvenlik liderleri ve ekipleri, güvenlik kaynaklarını en önemli şeylere yönlendirmek için işletme için hangi varlıkların kritik olduğunu bilmelidir. Bu da genellikle daha önce gündeme gelmemiş yeni soruları sormayı ve yanıtlamayı içeren yeni bir uygulamadır.

Siber güvenlik iş devamlılığı ve olağan üstü durum kurtarma uygulamaları. Siber saldırılar, pek çok veya tüm iş operasyonlarını kesintiye uğratan veya durduran büyük olaylara dönüşebilir. Kurumdaki ekipleri bu durumlara hazırlamak, iş operasyonlarını eski hâline getirme süresini kısaltacak, kuruluşa verilen zararı sınırlayacak ve müşterilerin, vatandaşların ve bileşenlerin güvenini sürdürmeye yardımcı olacaktır. Bu da mevcut bir iş devamlılığı ve olağan üstü durum kurtarma sürecine entegre edilmelidir.

Güvenlik riski kararları en iyi şekilde, tüm riskleri ve fırsatları tam olarak bilen iş veya görev sahipleri tarafından verilir.



Daha fazla dayanıklılık için kurum, güvenlik ve BT'yi entegre etme

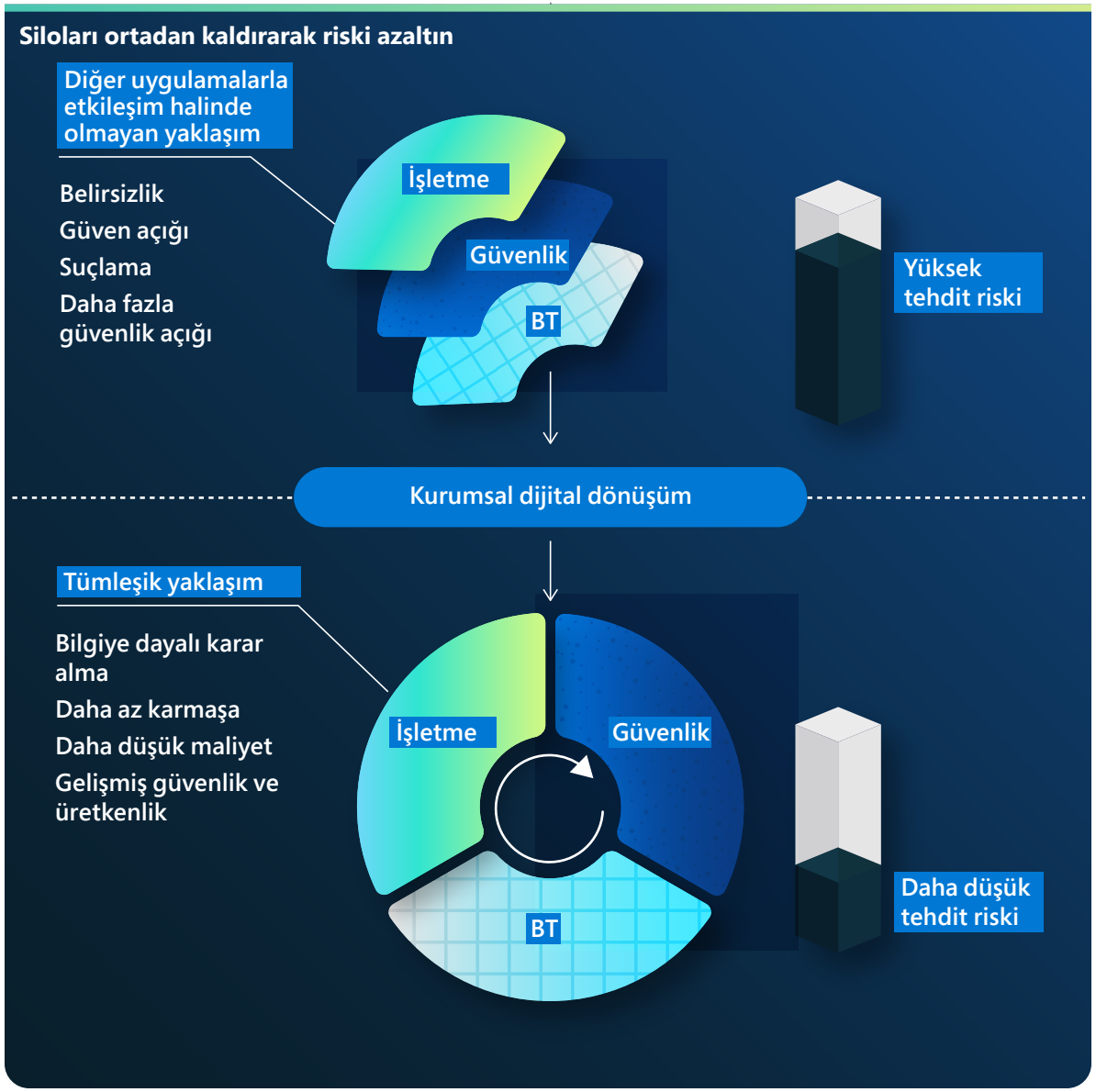
Devamı

3. Güvenliği doğru şekilde konumlandırın

Kurumların güvenlik riski sorumluluğunu yapılandırma biçimleri, genellikle onları yetersiz güvenlik riski kararları alma durumlarına hazırlıklı hâle getirir. Risk kararları en iyi şekilde, tüm riskleri ve fırsatları tam olarak anlayan iş veya görev sahipleri tarafından verilir, ancak kurumlar genellikle (örtülü veya açık şekilde) bunun yerine güvenlik ekibindeki uzmanlara güvenlik riski sorumluluğunu verir. Bu, işletme sahiplerini işleri için önemli bir risk üzerinde anlayış ve kontrolden mahrum bırakırken, güvenlik ekiplerine de aşırı bir yük getirir. Kurumlar bunu şu şekilde düzeltebilir:

İşletme sahiplerinin hazırlanması: İşletme sahiplerini genel olarak güvenlik riski ve bu tehditlerin işlerini nasıl etkileyeceği konusunda eğitin. Güvenlik ekiplerini doğrudan bu sürece dahil etmek, güvenlikle olan ilişkiyi ve genel iş çevikliğini de artırır.

İşletme sahiplerine güvenlik riski atama: İşletme sahipleri güvenlik riskini anlamak ve kabul etmek için yeterli bilgiyi edindikçe, kuruluş güvenlik riskinin sorumluluğunu açıkça onlara devretmeli ve güvenlik ekiplerini de bu riski yönetmekten ve süreç sahibine uzmanlık ve rehberlik sağlamaktan sorumlu tutmaya devam etmelidir.



"Siber dayanıklılık, doğru veri yedeklemesiyle başlayan klasik iş devamlılığı ve olağan üstü durum kurtarma; süreçler, teknoloji ve bunların bağımlılıkları (kişiler ve üçüncü taraflar dahil) için kurtarma yeteneklerine doğru ilerleme ve her zaman açık, kendi kendini iyileştiren hizmetlere, kritik roller için dayanıklılığa ve kritik üçüncü taraflar için yük devretmelere geçişi kapsayan bir skala üzerindedir. En dayanıklı kuruluşlar, BT, işletme yöneticileri ve güvenlik uzmanları arasındaki entegrasyonu destekler. Maksimum dayanıklılık sürecin başından itibaren dayanıklılık tasarımı yapmayı, güvenli değişiklik yönetimini ve detaylı hata izolasyonunu içerir. Siber dayanıklılık, tüm tehlikeleri kapsayan iyi bir planlama programındaki senaryolardan sadece biridir. Siber riskler arttıkça ve siber güvenlik ile dayanıklılık arasındaki bağlantı daha da önemli hâle geldikçe, Bilgi Güvenliği Direktörünün (CISO) kurumsal dayanıklılık programına olan bağlılığı daha da güçlenir. Her yıl daha fazla CISO, kurum genelinde dayanıklılık için sorumluluk alıyor."

Lisa Reshaur
Genel Müdür, Risk Yönetimi, Microsoft

Daha ayrıntılı bilgi için bağlantılar

- Dayanıklılıktan dijital azme: Kurumlar kritik dönemlerde hayatta kalmak için dijital teknolojiyi nasıl kullanıyor? | Resmi Microsoft Blogu
- BT ve güvenlik ekipleri uç nokta güvenliğini geliştirmek için birlikte nasıl çalışabilir | Microsoft Güvenlik

Siber dayanıklılık çan eğrisi

Her kurumun benimsemesi gereken dayanıklılık başarı faktörleri

Gördüğümüz gibi, birçok siber saldırı, temel güvenlik hijyenine uygun hareket edilmediği için başarılı oluyor. Her kurumun benimsemesi gereken asgari standartlar şunlardır:

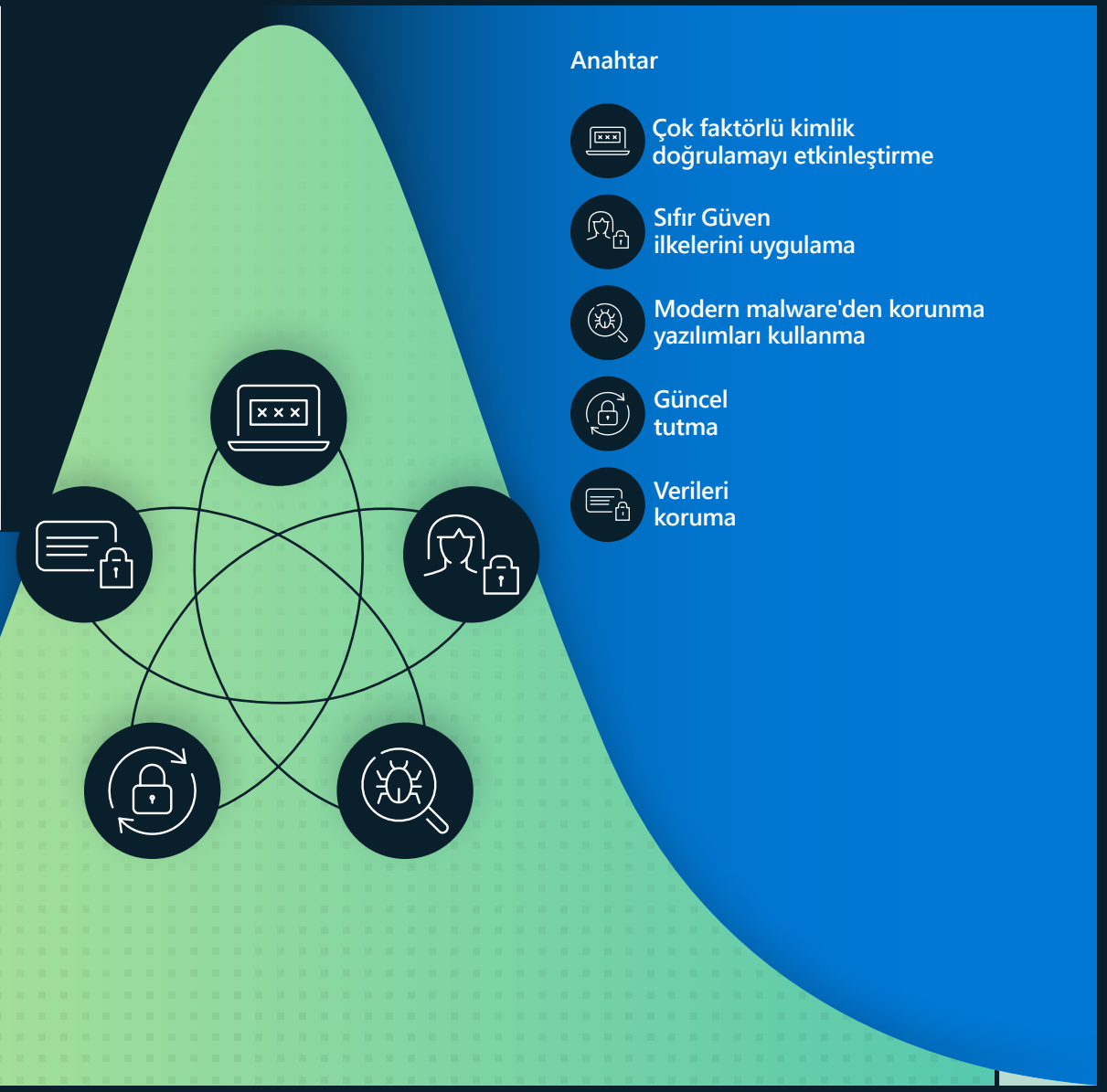
- **Çok faktörlü kimlik doğrulamayı (MFA)** etkinleştirme: Kullanıcı parolalarının güvenliğinin tehlikeye girmemesini sağlamak ve kimliklerle ilgili ekstra dayanıklılık sunmaya yardımcı olmak için.
- **Sıfır Güven ilkelerini uygulama:** Bir kurum üzerindeki etkiyi sınırlayan tüm dayanıklılık planlarının olmazsa olmazı. Bu ilkeler aşağıdaki gibidir:

1. – Açıkça doğrulama: kaynaklara erişime izin vermeden önce kullanıcıların ve cihazların iyi durumda olduğundan emin olun.
2. – En düşük ayrıcalık erişimini kullanın—sadece bir kaynağa erişim için gereken ayrıcalığa izin verin, daha fazlasını değil.
3. – İhlalin olduğunu varsayın—sistem savunmalarının ihlal edildiğini ve sistemlerin güvenliğinin tehlikede olabileceğini varsayın. Yani olası saldırılar için ortamı sürekli olarak takip edin.

- **Genişletilmiş algılama ve yanıt anti-malware'i kullanma:** Saldırıları tespit etmek, otomatik olarak engellemek ve güvenlik operasyonlarına ilişkin bilgi edinmek için yazılımı uygulayın. Tehdit algılama sistemlerinden gelen bilgileri izlemek, tehditlere zamanında yanıt verebilmek için çok önemlidir.
- **Güncel tutma:** Yama uygulanmamış ve güncel olmayan sistemler, birçok kurumun saldırıların hedefinde olmasının temel nedenidir. Ürün yazılımı, işletim sistemi ve uygulamalar dahil tüm sistemlerin güncel olduğundan emin olun.
- **Verileri koruma:** Önemli verilerinizin nerede bulunduğunu ve doğru sistemlerin uygulanıp uygulanmadığını bilmek, uygun korumayı uygulamak için çok önemlidir.

%98

Temel güvenlik hijyeni, hâlâ saldırıların %98'ine karşı koruma sağlar.



Son Notlar

1. Uç Noktada Algılama ve Yanıtlama (EDR), kurumsal ağların gelişmiş tehditleri önlemesine, tespit etmesine, araştırmasına ve yanıt vermesine yardımcı olmak üzere tasarlanmış bir kurumsal uç nokta güvenlik platformudur. Uç nokta algılama ve yanıt verme yetenekleri, neredeyse gerçek zamanlı ve eyleme geçirilebilir gelişmiş saldırı algılamaları sağlar. Güvenlik analistleri, uyarıları etkin bir şekilde önceliklendirebilir, bir ihlalin tüm kapsamına ilişkin bilgi elde edebilir ve tehditleri ortadan kaldırmak için müdahale adımları atabilir.
2. Bir Uç Nokta Koruma Platformu (EPP), dosya tabanlı malware'leri önlemek, güvenilir ve güvenilir olmayan uygulamalardan gelen kötü amaçlı etkinlikleri tespit edip engellemek ve güvenlik olayları ve uyarılarına dinamik olarak yanıt vermek için gerekli araştırma ve düzeltme yeteneklerini sunmak üzere uç nokta cihazlarında kullanılan bir çözümdür.
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. Windows Güvenlik kitabı: Ticari
7. Windows 11'deki yeni güvenlik özellikleri hibrit çalışmanın korunmasına yardımcı olacak | Microsoft Güvenlik Blogu
8. FIDO Alliance: Şifrelerden Daha Güvenli Açık Kimlik Doğrulama Standartları
9. https://interpret.ml/
10. OWASP İlk On | OWASP Vakfı
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. Ülkenin Siber Güvenliğinin İyileştirilmesine İlişkin 14028 Sayılı Kararname
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. "The Long Road Ahead to Transition to Post-Quantum Cryptography," https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

Katkıda Bulunan Ekipler

Katkıda Bulunan Ekipler

Bu rapordaki veriler ve içgörüler, birçok farklı Microsoft ekibinde çalışan, güvenlik odaklı çeşitli profesyonellerden oluşan bir gruptan alınmıştır. Toplu olarak, hedefleri Microsoft, Microsoft müşterileri ve genel olarak dünyayı siber saldırılardan korumaktır. Bu analizleri, dünyayı herkes için daha güvenli bir yer hâline getirme gibi ortak bir hedefle, şeffaflık ruhuyla paylaşmaktan gurur duyuyoruz.

İyi Araştırma Laboratuvarı için YZ: Dünyadaki birçok zorluğun üstesinden gelmek için verinin ve yapay zekanın gücünden yararlanma. Laboratuvar, geçim kaynaklarını ve ortamları iyileştirmek için yapay zekayı kullanarak Microsoft dışındaki kurumlarla birlikte çalışıyor. Odak alanları arasında çevrimiçi güvenlik (dezenformasyon, siber güvenlik, çocuk güvenliği), afet müdahalesi, sürdürülebilirlik ve Sağlık için YZ yer alıyor.

Azure Edge & Platform, Kurumsal ve İşletim Sistemi Güvenliği: Windows, Azure ve diğer Microsoft ürünlerinde temel işletim sistemi ve platform güvenliğinden sorumludur. Ekip, çipten buluta kadar güvenlik açığı, kimlik çalınması ve kötü amaçlı yazılım tehditlerini azaltmak için Microsoft platformlarında sektöründe lider güvenlik ve donanım çözümleri geliştirir. PC, Edge ve Sunucu genelinde Microsoft'un Secured-core platformunun, Microsoft Pluton Security Processor'ın ve daha fazlasının geliştiricileri.

Azure Networking, Core: DDoS platformu, ağ edge platformu ve Azure WAF, Azure Güvenlik Duvarı ve Azure DDoS Koruma Standardı gibi ağ güvenliği ürünleri dahil olmak üzere Microsoft WAN, veri merkezi ağları ve Azure'ın yazılım tanımlı ağ altyapısına odaklanan bir bulut ağ ekibi.

Bulut Güvenliği Araştırma ekibi: Bu ekip, Microsoft bulut güvenliğini sağlayarak, yenilikçi güvenlik özellikleri ve ürünleri oluşturarak ve araştırmalar yaparak Microsoft'un müşterilerini kuruluşlarını güvenli bir şekilde dönüştürmeleri için korur ve güçlendirir.

Müşteri Güvenliği ve Güveni (CST): Microsoft ürünlerinde ve çevrimiçi hizmetlerinde müşteri güvenliğinin sürekli iyileştirilmesini sağlayan disiplinler arası bir ekiptir. Kurum genelinde mühendislik ve güvenlik ekipleriyle birlikte çalışan CST, uyumluluğu sağlar, güvenliği artırır ve müşterileri korumak ve Microsoft'a küresel güveni artırmak için daha fazla şeffaflık sağlar.

Müşteri Başarısı: Müşteri Başarısı güvenlik ekipleri, güvenlik dönüşümünü ve modernizasyonunu hızlandırmak için en iyi uygulamaları, çıkarılan dersleri ve rehberliği paylaşmak üzere doğrudan müşterilerle beraber çalışır. Bu ekip, Microsoft'un ve müşterilerimizin yolculuğundan öğrenilen en iyi uygulamaları ve dersleri referans stratejilerine, referans mimarilerine, referans planlarına ve daha fazlasına birleştirir ve organize eder.

Siber Savunma Operasyon Merkezi (CDOC): Microsoft'un siber güvenlik ve savunma tesisi, kurumsal altyapımızı ve müşterilerin erişebildiği bulut altyapısını korumak için kurum genelindeki güvenlik uzmanlarını bir araya getiren bir kaynaştırma merkezidir. Olay müdahale ekipleri, Microsoft'un hizmet, ürün ve cihaz gruplarındaki veri bilimcileri ve güvenlik mühendisleriyle birlikte çalışarak tehditleri 7 gün 24 saat korumaya, tespit etmeye ve bunlara yanıt vermeye yardımcı olur.

İleri Demokrasi Girişimi: Sağlıklı bir bilgi ekosistemini destekleyerek, açık ve güvenli demokratik süreçleri koruyarak ve kurumsal yurttaşlık sorumluluğunu savunarak demokrasinin temellerini korumak, korumak ve ilerletmek için çalışan bir Microsoft ekibi.

Dijital Suçlar Birimi (DCU): Teknoloji, adli tıp, hukuk davaları, suç yönlendirmeleri ile hem kamu hem de özel ortaklıkları kullanarak dünya çapında siber suçla mücadelede uzmanlaşmış avukatlar, müfettişler, veri bilimcileri, mühendisler, analistler ve iş profesyonellerinden oluşan bir ekip.

Dijital Diplomasi: Yükselen ulus devlet çatışması karşısında barışçıl, istikrarlı ve güvenli bir siber alan için çalışan eski diplomatlar, politika yapıcılar ve hukuk uzmanlarından oluşan uluslararası bir ekip.

Dijital Güvenlik ve Esneklik (DSR): Kurumumuzu güvende tutarken ve hem kurumumuzu hem de müşteri verilerini korurken Microsoft'un en güvenilir cihazları ve hizmetleri oluşturmasını sağlama konusunda uzmanlaşmış bir kuruluş.

Dijital Güvenlik Birimi (DSU): Microsoft'u ve müşterilerini korumak için yasal, jeopolitik ve teknik uzmanlık sağlayan siber güvenlik avukatları ve analistlerinden oluşan bir ekip. DSU, Microsoft'un dünya çapındaki gelişmiş siber düşmanlara karşı kurumsal güvenlik savunmalarına güven duyulmasını sağlar.

Dijital Tehdit Analiz Merkezi (DTAC): Siber saldırılar ve operasyonları etkileme gibi ulus devlet tehditlerini analiz eden ve raporlayan uzmanlardan oluşan bir ekip. Ekip, müşterilerimize ve Microsoft'a etkili müdahale ve korumalar konusunda bilgi sağlamak üzere bilgi ve siber tehdit istihbaratını jeopolitik analizle birleştirir.

Kurumsal ve Güvenlik: Akıllı bulut ve akıllı uç için modern, güvenli ve yönetilebilir bir platform sağlamaya odaklanan bir ekip.

Kurumsal Mobilite: Verileri bulutta ve kurum içinde güvende tutmak için modern iş yeri ve modern yönetim sunmaya yardımcı olan bir ekip. Endpoint Manager, Microsoft ve müşterilerin mobil cihazları, masaüstü bilgisayarları, sanal makineleri, gömülü cihazları ve sunucuları yönetmek ve izlemek için kullandığı hizmetleri ve araçları içerir.

Katkıda Bulunan Ekipler

Devamı

Kurumsal Risk Yönetimi: Microsoft'un üst düzey liderliğiyle risk tartışmalarına öncelik vermek üzere iş birimleri arasında çalışan bir ekip. ERM, birden fazla operasyonel risk ekibini birbirine bağlar, Microsoft'un kurumsal risk çerçevesini yönetir ve NIST Siber Güvenlik Çerçevesini kullanarak kurumun iç güvenlik değerlendirmesini kolaylaştırır.

Küresel Siber Güvenlik Politikası: Müşterileri Microsoft teknolojisini benimseme sırasında güvenliklerini ve dayanıklılıklarını güçlendirmeleri için güçlendiren siber güvenlik kamu politikasını teşvik etmek amacıyla hükümetler, STK'lar ve sektör ortaklarıyla birlikte çalışan bir ekiptir.

Kimlik ve Ağ Erişimi (IDNA) Güvenliği: Tüm Microsoft müşterilerini yetkisiz erişim ve dolandırıcılıktan korumak için çalışan bir ekip. IDNA Güvenliği; mühendisler, ürün yöneticileri, veri bilimcileri ve güvenlik araştırmacılarından oluşan disiplinler arası bir ekiptir.

M365 Güvenliği: Kurumsal müşterilerin güvenliğini sağlamak üzere Uç Nokta için Microsoft Defender (MDE), Kimlik için Microsoft Defender (MDI) ve bunun gibi diğer güvenlik çözümlerini geliştiren kurum.

Mühendislik ve Araştırmada Microsoft Yapay Zeka, Etik ve Etkiler (AETHER): Microsoft'ta yeni teknolojilerin geliştirilmesini ve sorumlu bir şekilde sahaya sürülmesini sağlama misyonuna sahip bir danışma kurulu.

Microsoft Bing Arama ve Dağıtım: Birinci sınıf internet arama motoru hizmetleri sağlamada ve dünyanın her yerindeki kullanıcıların kendileri için önemli olan konuları ve gündemdeki hikayeleri takip etme ve kullanıcılara gizliliklerinin kontrolünü verme gibi güvenilir arama sonuçlarını ve bilgileri hızlı bir şekilde bulmalarını sağlama konusunda uzmanlaşmış bir ekip.

Microsoft Müşteri ve İş Ortağı Çözümleri: Microsoft'un güvenlik ve teknik satış uzmanları ve danışmanları gibi alan görevlerinden sorumlu birleşik ticari pazar organizasyonu.

Microsoft Defender Experts: Microsoft'un en büyük küresel ürün odaklı güvenlik araştırmacıları, uygulamalı bilim insanları ve tehdit bilgileri analistleri organizasyonu. Defender Experts, Microsoft 365 güvenlik ürünlerinde ve Microsoft Defender Experts tarafından yönetilen hizmetlerde yenilikçi algılama ve yanıt verme özellikleri sunar.

IoT için Microsoft Defender: IoT/OT malware'leri, protokolleri ve donanım yazılımının tersine mühendislik eylemleri konusunda uzman araştırmacılardan oluşan bir ekip. Ekip, kötü amaçlı eğilimleri ve kampanyaları ortaya çıkarmak için IoT/OT tehditlerini araştırır.

Microsoft Defender Threat Intelligence (RiskIQ): Microsoft'un kapsamlı harici telemetri koleksiyonunun analizi yoluyla taktik istihbarat üreten, daha önce bilinmeyen tehdit altyapısını keşfetmek için gelişen tehdit ortamını gösteren ve tehdit aktörlerine ve kampanyalarına bağlam ekleyen bir ekip. Ekip, savunma görevlilerine önemli taktik istihbarat sağlamak üzere düzenli aralıklar halinde özgün araştırmalar yayınlar.

Microsoft Güvenlik İş Geliştirme Ekibi: Microsoft'un siber güvenlik büyüme stratejisine, ortaklıklarına ve stratejik yatırımlarına liderlik eden ekip.

Microsoft Güvenlik Yanıt Merkezi (MSRC): Microsoft'un müşterilerini ve iş ortağı ekosistemini korumak için çalışan güvenlik araştırmacılarından oluşan bir ekip. Microsoft Siber Savunma Operasyon Merkezi'nin (CDOC) ayrılmaz bir parçası olan MSRC, tehditleri gerçek zamanlı olarak tespit etmek ve müdahale etmek için kurum genelindeki güvenlik müdahale uzmanlarını bir araya getirir.

Microsoft Olay Müdahalesi için Güvenlik Hizmetleri: Soruşturmadan başarılı kontrol altına alma ve kurtarmayla ilgili faaliyetlere kadar tüm siber saldırılarda müşterilere yardımcı olan bir siber güvenlik uzmanları ekibi. Hizmetler, son derece entegre iki ekip vasıtasıyla sunulur: Tespit ve Müdahale Ekibi (DART) kurtarma için araştırma ve altyapıya odaklanırken, Güvenlik Açığı Kurtarma Güvenlik Uygulaması (CRSP) koruma ve kurtarma noktalarına odaklanır.

Microsoft Tehdit İstihbarat Merkezi (MSTIC): Microsoft'un ulus devlet tehditleri, kötü amaçlı yazılım, kimlik avı ve daha fazlası dahil olmak üzere Microsoft müşterilerini etkileyen en gelişmiş ve ileri düzey düşmanlara karşı istihbarat tanımlama, izleme ve toplama konularına odaklanan merkezi ekibidir.

One Engineering System (1ES): Microsoft geliştiricilerinin mümkün olduğunca üretken ve güvenli olmalarına yardımcı olmak üzere birinci sınıf araçlar sağlama misyonuna sahip bir ekip. Ekip, Microsoft'un uçtan uca yazılım tedarik zincirini koruma altına almak üzere merkezi stratejiye öncülük eder.

Operasyonel Tehdit İstihbarat Merkezi (OPTIC): Microsoft Siber Savunma Operasyon Merkezi'nin (CDOC) Microsoft'u ve müşterilerimizi koruma misyonunu destekleyen siber tehdit istihbaratını yönetmekten ve yaymaktan sorumlu ekip.

Microsoft

Tehdit ortamını aydınlatmak ve dijital savunmayı güçlendirmek.

- Daha fazlasını öğrenin: **https://microsoft.com/mddr**
- Derinlemesine inceleme:**https://blogs.microsoft.com/on-the-issues/**
- Bağlı kalın: **@msftissues ve @msftsecurity**