Microsoft

Rapport om Microsofts digitala försvar 2022

Belyser hotbilden och stärker ett digitalt försvar.

Innehåll

Alla data, insikter och händelser i den här rapporten kommer från juli 2021 till juni 2022 (Microsofts räkenskapsår 2022), om inget annat anges.

Det bästa sättet att visa och navigera i den här rapporten är att använda Adobe Reader, som du kan hämta kostnadsfritt från Adobes webbplats.

Rapportintroduktion 02

Cyberbrottslighetens tillstånd 06

En översikt över cyberbrottslighetens tillstånd 07
Introduktion 08
Utpressningstrojaner och utpressning: ett hot på nationell nivå 09
Insikter om utpressningstrojaner från personal i frontlinjen 14
Cyberbrott som tjänst 18
Den föränderliga hotbilden från nätfiske 21
En tidslinje med botnätangrepp från Microsofts tidiga samarbeten 25
Cyberbrottslingars missbruk av infrastruktur 26
Är hacktivismen här för att stanna? 28

Hot från nationalstater 30

En översikt över hot från nationalstater 31
Introduktion 32
Bakgrund till nationalstatsdata 33
Exempel på nationella statsaktörer och deras verksamhet 34
Den föränderliga hotbilden 35
IT-försörjningskedjan som en inkörsport till det digitala ekosystemet 37
Snabbt utnyttjande av sårbarheter 39
Ryska statliga aktörers cybertaktik i krigstid hotar Ukraina och andra 41
Kina utökar de globala angreppen för att få konkurrensfördelar 44
Iran blir alltmer aggressivt efter maktskiftet 46
Nordkoreas cyberkapacitet används för att uppnå regimens tre huvudsakliga mål 49
Cyberlegoknektar hotar stabiliteten i cyberrymden 52
Organisera cybersäkerhetsnormer för fred och säkerhet i cyberrymden 53

Enheter och infrastruktur 56

En översikt över enheter och infrastruktur 57
Introduktion 58
Länder agerar för att förbättra den kritiska infrastrukturens säkerhet och motståndskraft 59
IoT och OT i blickfånget: trender och angrepp 62
Hackning av försörjningskedjan och inbyggd programvara 65
Fokus på sårbarheter i inbyggd programvara 66
Rekognosceringsbaserade OT-angrepp 68

Cyberpåverkan 71

En översikt över cyberpåverkan 72
Introduktion 73
Trender inom cyberpåverkansoperationer 74
Fokus på påverkansoperationer under covid-19 och Rysslands invasion av Ukraina 76
Hålla koll på det ryska propagandaindexet 78
Syntetiska medier 80
En helhetsmetod för att skydda mot cyberpåverkan 83

Cyberåterhämtning 86

En översikt över cyberåterhämtning 87
Introduktion 88
Cyberåterhämtning: En förutsättning i ett uppkopplat samhälle 89
Vikten av att modernisera system och arkitektur 90
Det grundläggande säkerhetsläget är en avgörande faktor för avancerade lösningars effektivitet 92
Att upprätthålla identitetshälsan är avgörande för organisationers välbefinnande 93
Standardsäkerhetsinställningar för operativsystemet 96
Centralitet i försörjningskedjan för programvara 97
Skapa motståndskraft mot nya DDoS-, webbprogram- och nätverksangrepp 98
Utveckla en balanserad strategi för datasäkerhet och cyberåterhämtning 101
Motståndskraft mot cyberpåverkan: den mänskliga dimensionen 102
Stärka den mänskliga faktorn med kompetenshöjning 103
Insikter från vårt program för att undanröja utpressningstrojaner 104
Åtgärda säkerhetskonsekvenserna av kvantdatorer nu 105
Integrera företag, säkerhet och IT för bättre motståndskraft 106
Klockkurvan för cybermotståndskraft 108

Bidragande team 110

Introduktion av Tom Burt

Corporate Vice President, Customer Security & Trust

"De biljoner signaler som vi analyserar från vårt världsomspännande ekosystem av produkter och tjänster avslöjar den aggressivitet, omfattning och skala som digitala hot har i världen."

En ögonblicksbild av läget …

Hotbildens omfattning och skala

Mängden lösenordsangrepp har stigit till uppskattningsvis 921 angrepp varje sekund – en ökning med 74 procent på bara ett år.

Nedmontering av cyberbrottslighet

Hittills har Microsoft undanröjt fler än 10 000 domäner som används av cyberbrottslingar och 600 som används av nationella statsaktörer.

Åtgärda sårbarheter

93 % av våra insatser mot utpressningstrojaner avslöjade otillräckliga kontroller av åtkomst med behörigheter och laterala rörelser.

Den 23 februari 2022 förändrades cybersäkerhetsvärlden – hybridkrigets tidsålder inleddes. Den dagen – timmar innan missiler skickades iväg och stridsvagnar rullade över gränserna – inledde ryska aktörer en massiv, destruktiv cyberattack mot ukrainska myndigheter och mål inom teknik- och finansbranschen. I kapitlet Hot från nationalstater i den här tredje årliga utgåvan av Rapport om Microsofts digitala försvar (MDFR) kan du läsa mer om attackerna och vilka lärdomar vi kan dra av dem. Den viktigaste lärdomen är att molnet ger den bästa fysiska och logiska säkerheten mot cyberattacker och möjliggör hotunderrättelser och slutpunktsskydd som har visat sitt värde i Ukraina.

För att undersöka årets utveckling inom cybersäkerhet måste vi naturligtvis börja där, men årets rapport gör också en djupdykning i mycket annat. I rapportens första kapitel fokuserar vi på cyberbrottslingars verksamhet, och i kapitel två går vi in på hot från nationalstater. Båda gruppernas angreppsteknik har blivit betydligt mer raffinerad, vilket också dramatiskt har ökat effekten av vad de gör. De flesta nyhetsrubriker har handlat om Ryssland, men efter ett presidentskifte har även iranska aktörer eskalerat sina angrepp och riktat destruktiva attacker mot Israel och utpressningstrojaner och hack-and-leak-operationer mot viktig infrastruktur i USA. Kina ökade också sin spionageverksamhet i Sydostasien och på andra håll på södra halvklotet i ett försök att motverka USA:s inflytande och stjäla viktiga data och viktig information.

Utländska aktörer använder också mycket effektiva metoder för att underlätta propagandakampanjer i regioner runtom i världen, vilket avhandlas i kapitel tre. Ryssland har till exempel ansträngt sig mycket för att övertyga både sina medborgare och medborgare i andra länder om att landets invasion av Ukraina var berättigad – samtidigt som de också publicerade propaganda som misskrediterade vaccin mot covid i väst och på samma gång talade varmt om hur bra situationen hanterats i det egna landet. Dessutom riktar aktörerna allt oftare in sig på IoT-enheter (sakernas internet) eller drifttekniksystemenheter (OT) som startpunkter för nätverk och kritisk infrastruktur, vilket avhandlas i kapitel fyra. Avslutningsvis avhandlar vi i det sista kapitlet de insikter och lärdomar vi har dragit under det senaste årets försvar mot angrepp som riktats mot Microsoft och våra kunder och granskar årets utveckling inom cybermotståndskraft.

Varje kapitel innehåller de viktigaste lärdomarna och insikterna utifrån Microsofts unika ställning. De biljoner signaler som vi analyserar från vårt världsomspännande ekosystem av produkter och tjänster avslöjar den aggressivitet, omfattning och skala som digitala hot har i världen. Microsoft vidtar åtgärder för att försvara våra kunder och det digitala ekosystemet mot dessa hot, och du kan läsa om vår teknik som identifierar och blockerar miljardtals nätfiskeförsök, identitetsstölder och andra hot mot våra kunder.

Introduktion av Tom Burt

fortsättning

Vi använder också juridiska och tekniska metoder för att beslagta och montera ned infrastruktur som används av cyberbrottslingar och nationella statsaktörer samt meddela kunderna när de hotas eller angrips av en nationell statsaktör. Vi jobbar för att utveckla alltmer effektiva funktioner och tjänster som använder AI-/ML-teknik för att identifiera och blockera cyberhot och för att säkerhetspersonal ska kunna försvara mot och identifiera cyberintrång snabbare och effektivare.

Men det kanske viktigaste av allt är att vi genom MDFR delar med oss av våra bästa råd om vad enskilda personer, organisationer och företag kan göra för att försvara sig mot de ökande digitala hoten. God cyberhygien är det bästa försvaret och kan avsevärt minska risken för cyberattacker.



Cyberbrottslighetens tillstånd

Cyberbrottslingar fortsätter att agera som avancerade vinstdrivande företag. Angriparna anpassar sig och hittar nya sätt att implementera sina metoder, vilket gör det svårare att veta hur och var de har sin kampanjs infrastruktur. Samtidigt blir cyberbrottslingarna mer sparsamma. För att sänka sina omkostnader och framstå som mer legitima tar de sig in i affärsnätverk och företagsenheter och använder dem för nätfiskekampanjer, för att sprida skadlig kod eller utnyttja deras datorkraft för mining av kryptovaluta.

Läs mer på s. 6

> "Insatsen med cybervapen i hybridkriget i Ukraina är början på en ny era av konflikter."

Hot från nationalstater

Nationella statsaktörer inleder alltmer avancerade cyberattacker som syftar till att undvika upptäckt och främja deras strategiska prioriteringar. Insatsen med cybervapen i hybridkriget i Ukraina är början för en ny era av konflikter. Ryssland har också stöttat sitt krig genom informationspåverkan med hjälp av propaganda för att påverka opinionen i Ryssland, Ukraina och globalt. Utanför Ukraina har nationella statsaktörer ökat sin aktivitet och börjat använda framsteg inom automatisering, molninfrastruktur och fjärråtkomst för att kunna angripa flera olika mål. Företags IT-försörjningskedjor som ger tillgång till slutmålen angreps ofta. Cybersäkerhetshygien har blivit ännu viktigare, eftersom aktörerna snabbt utnyttjar oupptäckta sårbarheter, använder både avancerade metoder och råstyrkemetoder för att stjäla autentiseringsuppgifter och döljer sin verksamhet genom att använda programvara med öppen källkod eller legitim programvara. Iran följer dessutom i Rysslands fotspår när det gäller användning av destruktiva cybervapen, till exempel utpressningstrojaner.

Den här utvecklingen kräver att världen snabbt implementerar ett konsekvent och globalt ramverk som prioriterar mänskliga rättigheter och skyddar människor från staters besinningslösa beteenden på nätet. Alla länder måste samarbeta för att införa normer och regler för ansvarsfullt nationalstatsbeteende.

Läs mer på s. 30



Enheter och infrastruktur

Pandemin och det snabba införandet av internetanslutna enheter av alla de slag som en komponent i den accelererande digitaliseringen, har kraftigt ökat attackytan i vår digitala värld. Cyberbrottslingar och nationalstater är snabba att utnyttja möjligheterna. Säkerheten för maskin- och programvara inom IT har visserligen stärkts på senare år, men säkerheten för IoT- och OT-enheter har inte lyckats hålla jämna steg. Hotaktörer utnyttjar sådana enheter för att ta sig in i nätverk för att sedan röra sig lateralt och få fotfäste i en försörjningskedja eller störa målorganisationens OT-verksamhet.

Läs mer på s. 56

Introduktion av Tom Burt

fortsättning

Cyberpåverkan

Nationalstater använder alltmer avancerade påverkansoperationer för att distribuera propaganda och påverka den allmänna opinionen både nationellt och internationellt. Kampanjerna urholkar förtroendet, ökar polariseringen och hotar demokratiska processer. Skickliga avancerade, beständiga manipulatörer använder traditionella medier och internet samt sociala medier för att kraftigt öka sina kampanjers omfattning, skala och effektivitet och den enorma påverkan de har i det globala informationsekosystemet. Under det senaste året har vi sett detta användas under Rysslands hybridkrig i Ukraina, men vi har också sett Ryssland och andra nationer, däribland Kina och Iran, i allt högre grad använda propagandainsatser i sociala medier för att utöka sitt globala inflytande i en rad frågor.

Läs mer på s. 71





Cyberåterhämtning

Säkerhet är en viktig faktor för teknisk framgång. Innovation och ökad produktivitet går bara att uppnå genom att införa säkerhetsåtgärder som gör organisationer så motståndskraftiga som möjligt mot moderna angrepp. Pandemin utmanade oss på Microsoft att justera våra säkerhetsrutiner och säkerhetstekniker för att skydda våra medarbetare var de än arbetar. Det senaste året har hotaktörer fortsatt att utnyttja de sårbarheter som exponerades under pandemin och övergången till en hybridarbetsmiljö. Sedan dess har vårt främsta problem varit att hantera förekomsten och komplexiteten av olika angreppsmetoder och den ökade nationalstatsaktiviteten. I det här kapitlet beskriver vi de problem vi har ställts inför och de försvar vi har mobiliserat som svar på detta, tillsammans med våra över 15 000 partner.

Läs mer på s. 86

Vår unika utgångspunkt

37 md
blockerade e-posthot

34,7 md
blockerade identitetshot

43 biljoner
signaler syntetiseras dagligen med avancerad dataanalys och AI-algoritmer för att förstå och skydda mot digitala hot och kriminell cyberaktivitet.

>8 500
tekniker, forskare, datavetare, cybersäkerhetsexperter, hotjägare, geopolitiska analytiker, utredare och insatspersonal i 77 länder.

>15 000
partner i vårt säkerhetsekosystem som ökar cybermotståndskraften för våra kunder.

2,5 md
slutpunktssignaler analyseras dagligen

1 juli 2021 till 30 juni 2022

Introduktion av Tom Burt

fortsättning

Vi menar att Microsoft – på egen hand och genom nära samarbeten med andra inom det privata näringslivet, myndigheter och civilsamhället – har ett ansvar att skydda de digitala system som ligger till grund för vårt samhälles sociala väv och främja säkra datormiljöer för alla, var de än befinner sig. Det är på grund av det ansvaret som vi har publicerat MDFR varje år sedan 2020. Rapporten är kulmen på Microsoft enorma datamängder och omfattande forskning. Här delar vi med oss av våra unika insikter om hur den digitala hotbilden utvecklas och beskriver vilka viktiga åtgärder vi kan vidta i dag för att öka ekosystemets säkerhet.

Vi vill förmedla allvaret i situationen och få våra läsare att vidta omedelbara åtgärder utifrån de data och insikter vi presenterar både här och i våra många cybersäkerhetspublikationer under året. När vi överväger allvaret i hotet mot det digitala landskapet – och vad det innebär i den fysiska världen – är det viktigt att komma ihåg att vi alla kan göra något för att skydda oss själva, våra organisationer och företag mot digitala hot.

Tack för att du tar dig tid att gå igenom årets rapport om Microsofts digitala försvar. Vi hoppas att den ger dig värdefulla insikter och rekommendationer så att vi alla tillsammans kan försvara det digitala ekosystemet.

Tom Burt
Corporate Vice President,
Customer Security & Trust

Vi har två mål med den här rapporten:

1. Vi vill belysa den föränderliga digitala hotbilden för våra kunder, partner och intressenter som spänner över hela ekosystemet och särskilt peka på nya cyberattacker och trendutvecklingen för historiskt beständiga hot.
2. Vi vill ge våra kunder och partner möjlighet att förbättra sin cyberåterhämtning och reagera på hoten.



Cyberbrottslighetens tillstånd

I takt med att cyberförsvaret förbättras och alltfler organisationer proaktivt vidtar förebyggande åtgärder anpassar angriparna sina metoder.

En översikt över cyberbrottslighetens tillstånd 07

Introduktion 08

Utpressningstrojaner och utpressning: ett hot på nationell nivå 09

Insikter om utpressningstrojaner från personal i frontlinjen 14

Cyberbrott som tjänst 18

Den föränderliga hotbilden från nätfiske 21

En tidslinje med botnätangrepp från Microsofts tidiga samarbeten 25

Cyberbrottslingars missbruk av infrastruktur 26

Är hacktivismen här för att stanna? 28

En översikt över

cyberbrottslighetens tillstånd

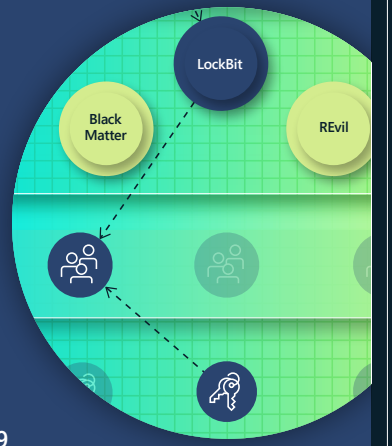
I takt med att cyberförsvaret förbättras och alltfler organisationer proaktivt vidtar förebyggande åtgärder anpassar angriparna sina metoder.

Cyberbrottslingar fortsätter att agera som avancerade vinstdrivande företag. Angriparna anpassar sig och hittar nya sätt att implementera sina metoder, vilket gör det svårare att veta hur och var de har sin kampanjs infrastruktur. Samtidigt blir cyberbrottslingarna mer sparsamma. För att sänka sina omkostnader och framstå som mer legitima tar de sig in i affärsnätverk och företagsenheter och använder dem för nätfiskekampanjer, för att sprida skadlig kod eller utnyttja deras datorkraft för mining av kryptovaluta.

Cyberbrottsligheten fortsätter att öka medan industrialiseringen av cyberbrottsekonomin sänker kompetensbarriären genom att ge ökad tillgång till verktyg och infrastruktur.

Läs mer på s. 18

Hotet från utpressningstrojaner och utpressning blir allt djärvare och attackerna riktas mot myndigheter, företag och kritisk infrastruktur.

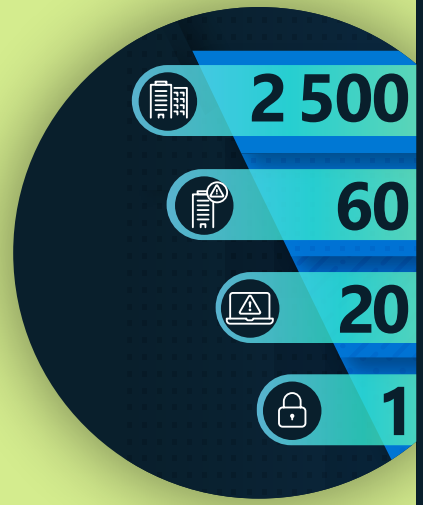


Läs mer på s. 9

Angripare hotar i allt högre grad att avslöja känsliga data för att uppmuntra till lösenbetalningar.

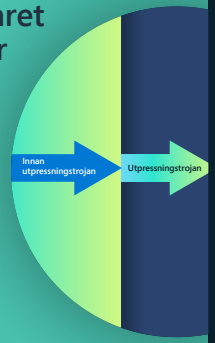
Läs mer på s. 10

Utpressningstrojaner med människor bakom är vanligast, eftersom en tredjedel av de mål som angrips på det sättet går att ta sig in i och 5 % av dem pressas på pengar.



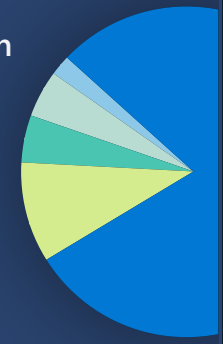
Läs mer på s. 9

Det mest effektiva försvaret mot utpressningstrojaner inkluderar multifaktora-utentisering, frekventa säkerhetskorrigeringar och nolltillitsprinciper i nätverksarkitekturen.



Läs mer på s. 13

Nätfiskemetoder som urskillningslöst riktas mot alla inkorgar blir allt vanligare och intrång i företags e-post, till exempel för fakturabedrägerier, är en allvarlig cyberbrottsrisk för företag.



Läs mer på s. 21

För att störa cyberbrottslingars och nationella statsaktörers skadliga infrastruktur använder Microsoft innovativa rättsliga metoder och våra offentliga och privata partnerskap.



Läs mer på s. 25

Introduktion

Cyberbrottsligheten fortsätter att öka inom både slumpmässiga och riktade angrepp.

I takt med att cyberförsvaret förbättras och alltfler myndigheter och företag proaktivt vidtar förebyggande åtgärder, ser vi att angripare använder två strategier för att få den tillgång som krävs för att underlätta cyberbrott. En metod är en kampanj med breda mål som är volymberoende. Den andra utnyttjar övervakning och mer selektiv inriktning för att öka avkastningen. Även när målet inte är att generera intäkter – till exempel vid nationalstatsaktiviteter för geopolitiska ändamål – används både slumpmässiga och riktade angrepp. Det senaste året har cyberbrottslingar fortsatt att förlita sig på social manipulering och att utnyttja aktuella frågor för maximal framgång. Till exempel minskade nätfiskeförsöken med covid-tema samtidigt som antalet lockbeten som gick ut på att be om donationer för att stödja medborgarna i Ukraina ökade.

Angriparna anpassar sig och hittar nya sätt att implementera sina metoder, vilket gör det svårare att veta hur och var de har sin kampanjs infrastruktur. Vi har sett att cyberbrottslingar blir mer sparsamma och att angriparna inte längre betalar för teknik. För att sänka sina omkostnader och framstå som mer legitima tar de sig in i affärsnätverk och företagsenheter och använder dem för nätfiskekampanjer, för att sprida skadlig kod eller utnyttja deras datorkraft för mining av kryptovaluta.

I det här kapitlet granskar vi även den ökade hacktivismen, något som orsakas av att privatpersoner genomför cyberattacker mot sociala eller politiska mål. Tusentals personer runtom i världen, både experter och nybörjare, har mobiliserats sedan februari 2022 för att genomföra attacker som att stänga ned webbplatser och läcka stulna data som ett led i kriget mellan Ryssland och Ukraina. Det är för tidigt att förutse om den här trenden kommer att fortsätta när de aktiva striderna upphör.

Organisationer måste regelbundet granska och stärka åtkomstkontrollerna och införa säkerhetsstrategier för att försvara sig mot cyberattacker. Men det är inte allt de kan göra. Vi förklarar hur vår enhet för digitala brott (DCU) har använt civila rättsfall för att beslagta skadlig infrastruktur som används av cyberbrottslingar och nationella statsaktörer. Vi måste bekämpa hoten gemensamt genom både offentliga och privata partnerskap. Vi hoppas att vi genom att dela med oss av det vi har lärt oss under de senaste tio åren kan hjälpa andra att förstå och överväga proaktiva åtgärder som de kan vidta för att skydda sig själva och det övriga ekosystemet mot det ständigt växande hotet från cyberbrott.

Amy Hogan-Burney
General Manager, Digital Crimes Unit

Utpressningstrojaner och utpressning: ett hot på nationell nivå

Angrepp med utpressningstrojaner utgör en allt större fara för alla människor eftersom kritisk infrastruktur, företag i alla storlekar och statliga och lokala myndigheter råkar ut för brottslingar som utnyttjar ett växande cyberbrottsligt ekosystem.

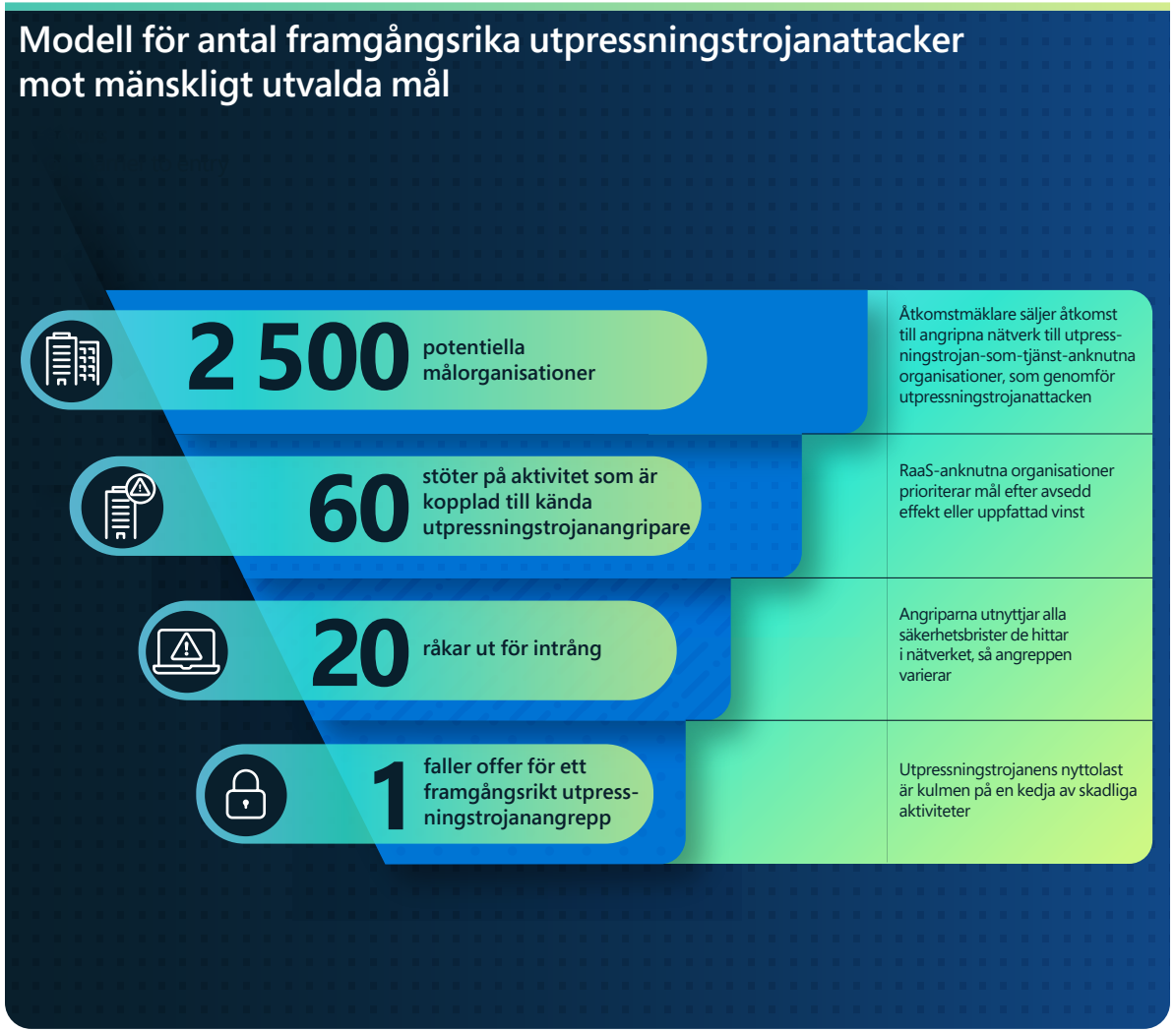
Under de senaste två åren har betydande incidenter med utpressningstrojaner – t.ex. angrepp mot viktig infrastruktur, hälso- och sjukvård och IT-tjänster – fått stor uppmärksamhet från allmänheten. I takt med att attackerna med utpressningstrojaner har blivit allt djärvare i omfattning, har effekterna av dem blivit större. Här följer några exempel på attacker som inträffade 2022:

- I februari påverkades betalningshanteringssystemen för hundratals bensinstationer i norra Tyskland av en attack mot två företag.[1]
- I mars stoppade en attack mot posten i Grekland tillfälligt postleveransen och påverkade hanteringen av finansiella transaktioner.[2]
- I slutet av maj tvingade en utpressningstrojanattack Costa Ricas myndigheter att utlysa ett nationellt nödläge efter att sjukhusen stängdes och tull- och skatteuppbörden störddes.[3]
- En annan attack i maj orsakade försenade och inställda flyg för ett av Indiens största flygbolag och strandsatte hundratals passagerare.[4]

Attackernas framgångar och omfattningen av effekterna beror på industrialiseringen av cyberbrottslighetsekonomin, vilket ger tillgång till verktyg och infrastruktur och utökar cyberbrottslingarnas kapacitet genom att sänka kompetenskraven.

På senare år har utpressningstrojanerna övergått från en modell där ett enda ”gäng” både kunde utveckla och distribuera utpressningstrojanens nyttolast till en utpressningstrojan-som-tjänst-modell (RaaS). RaaS innebär att en grupp hanterar utvecklingen av utpressningstrojanens nyttolast och tillhandahålla tjänster för betalning och utpressning genom dataläckage till andra cyberbrottslingar – de som faktiskt utför utpressningstrojanattackerna. De kallas anknutna organisationer och tar sin del av vinsten. Den här franchiseverksamheten inom cyberbrottsekonomin har breddat angreppspoolen. Industrialiseringen av cyberbrottslingarnas verktygsuppsättning har gjort det enklare för angriparna att utföra intrång, exfiltrera data och distribuera utpressningstrojaner.

Utpressningstrojaner med människor bakom[5] är fortfarande ett allvarligt hot mot organisationer. Begreppet myntades av forskare på Microsoft för att beskriva hot som drivs av människor som fattar beslut i alla skeden av attacken utifrån vad de upptäcker i sitt målnätverk. På så sätt skiljer de sig från utpressningstrojanattacker i industriell skala.



Modell baserad på Microsoft Defender för Endpoint-data (EDR) (januari–juni 2022).

Utpressningstrojaner och utpressning: ett hot på nationsnivå

fortsättning

Attacker med utpressningstrojaner har blivit allt allvarligare eftersom införandet av en dubbel strategi för intäktsgenerering genom utpressning har blivit standard. Det innebär att angripare exfiltrerar data från enheter de har tagit sig in i, krypterar data på enheterna och sedan publicerar eller hotar att publicera de stulna uppgifterna offentligt för att pressa offren att betala en lösensumma.

De flesta som använder utpressningstrojaner testar helt enkelt att lägga upp utpressningstrojaner i alla nätverk de får tillgång till, men en del angripare väljer i stället att köpa åtkomst från andra cyberbrottslingar och utnyttja anslutningar mellan åtkomstmäklare och personer som står bakom utpressningstrojaner.

Våra unikt breda signalunderrättelser kommer från många källor – identitet, e-post, slutpunkter och molnet – och ger insikt i den växande utpressningstrojanekonomin, som har ett komplett system med anknutna organisationer med verktyg som är konstruerade för mindre tekniskt kompetenta angripare.

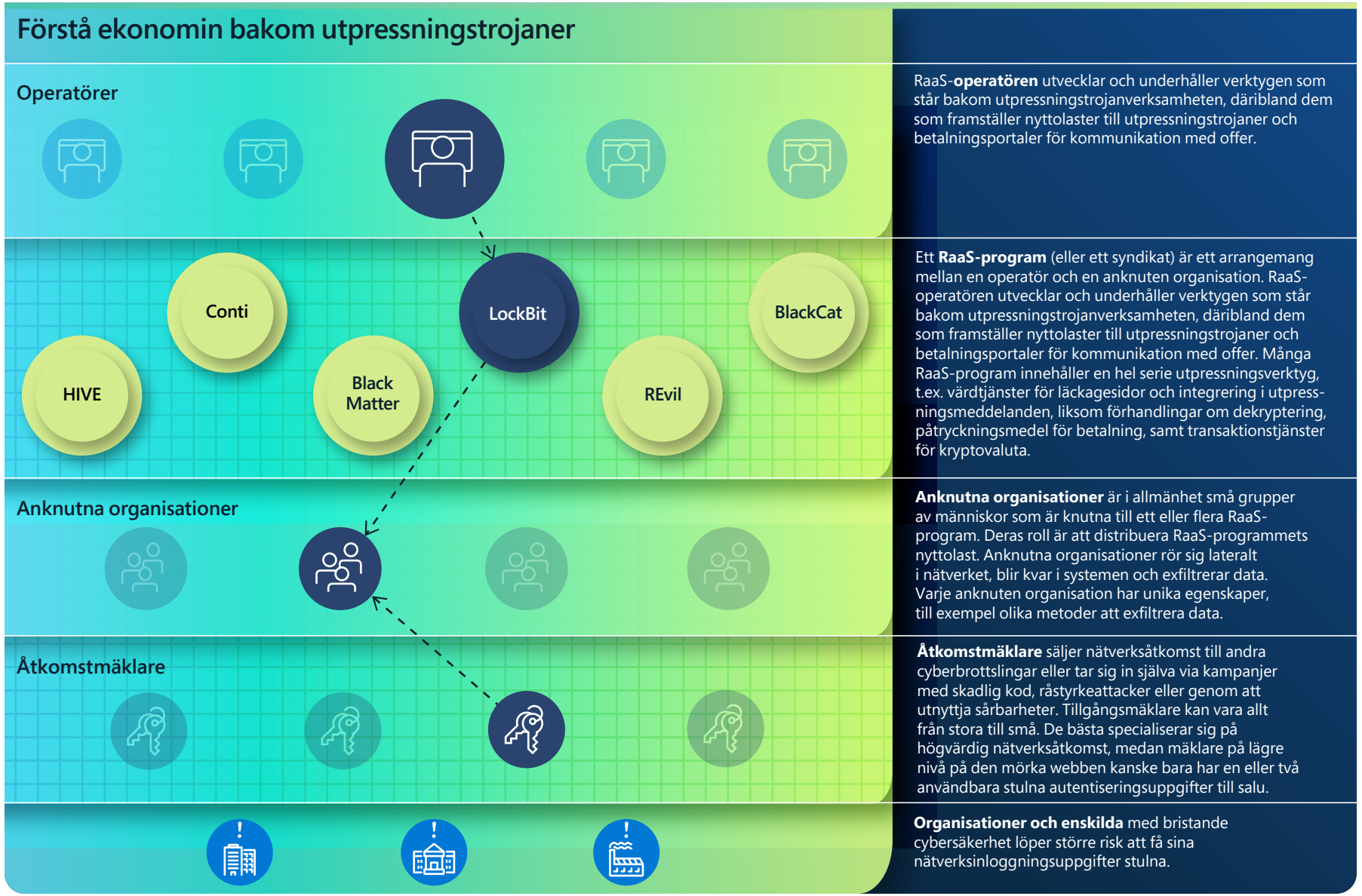
Allt närmare band mellan specialiserade cyberbrottslingar har gjort att attacker med utpressningstrojaner inträffar oftare, är mer avancerade och lyckas bättre. Det har drivit på utvecklingen av ekosystemet för cyberbrott till att involvera aktörer med olika metoder, mål och kompetens som hjälper varandra med den initiala åtkomsten till målen, betalningstjänster och dekrypterings- eller publiceringsverktyg eller webbplatser.

Operatörerna bakom utpressningstrojaner kan nu köpa åtkomst till organisations- eller myndighetsnätverk online eller skaffa autentiseringsuppgifter och åtkomst via personliga relationer med mäklare vars främsta syfte är att tjäna pengar på den åtkomst de har skaffat sig.

Operatörerna använder sedan den köpta åtkomsten för att installera en utpressningstrojannyttolast som har köpts via marknader eller forum på den mörka webben. I många fall är det RaaS-teamet som förhandlar med offren, inte av operatörerna själva. De här kriminella transaktionerna är väldigt enkla och med tanke på anonymiteten på den mörka webben och hur svårt det är att genomdriva lagar över gränserna löper de inblandade inga större risker att bli anhållna och lagförda.

För att komma tillrätta med den här sortens hot på ett hållbart och framgångsrikt sätt måste hela myndighetssfären samarbeta med den privata sektorn för att vidta åtgärder.





Till skillnad från hur utpressningstrojaner ibland skildras i medier är det ovanligt att en enda variant av utpressningstrojan hanteras av ett och samma gäng. I stället är det separata aktörer som skriver skadlig kod, får åtkomst till potentiella offer, distribuerar utpressningstrojaner och hanterar utpressningsförhandlingar. Industrialiseringen av det kriminella ekosystemet har lett till

- åtkomstmäklare som bryter sig in och delar ut åtkomst (åtkomst som tjänst)
- utvecklare av skadlig kod som säljer verktyg
- kriminella och anknutna organisationer som genomför intrång
- krypterings- och utpressningstjänstleverantörer som hanterar intäktsgenereringen åt anknutna organisationer (RaaS).

Alla mänskligt hanterade utpressningstrojankampanjer är beroende av säkerhetsbrister. Det vanligaste är att angriparna utnyttjar organisationens dåliga cyberhygien, vilket till exempel kan handla om att säkerhetskorrigeringar implementeras för sällan eller att multifaktorautentisering (MFA) saknas.

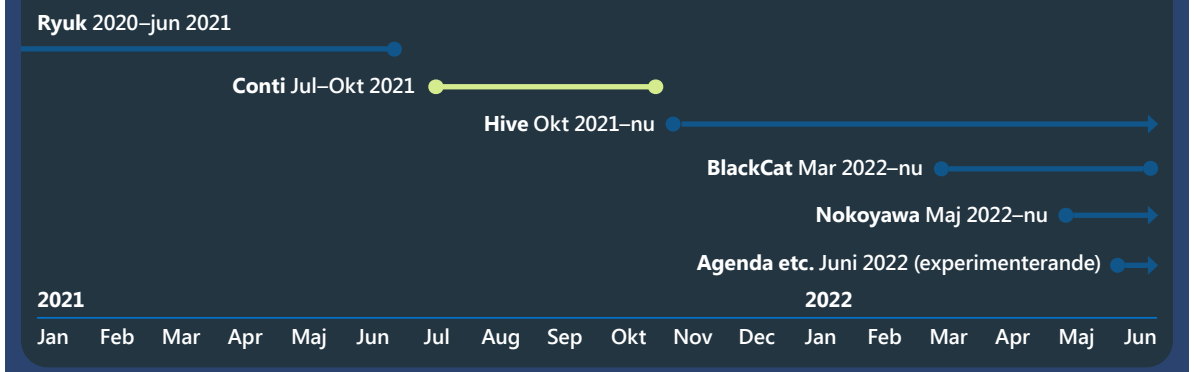
Fallstudie: Upplösningen av Conti

Conti, en av de främsta varianterna av utpressningstrojaner under de senaste två åren, började stänga ned sin verksamhet i mitten av 2022. Microsoft Threat Intelligence Center (MSTIC) observerade en betydande minskning av aktiviteten i slutet av mars och början av april. Vi observerade den senaste insatsen av Conti-utpressningstrojaner i mitten av april. Men på samma sätt som när andra utpressare stängt ned sin verksamhet fick upplösningen av Conti ingen betydande inverkan på det totala antalet utpressningstrojanattacker. MSTIC konstaterade att organisationer anknutna till Conti valde att distribuera andra utpressningstrojannyttolaster, t.ex. BlackBasta, Lockbit 2.0, LockbitBlack och HIVE. Det stämmer väl överens med data från tidigare år och tyder på att utpressare som stänger ned sin verksamhet dyker upp igen några månader senare eller återdistribuerar sin tekniska kapacitet och sina resurser till nya grupper.

Hotunderrättelseteamen på Microsoft håller reda på utpressningstrojanaktörer i form av enskilda grupper (som kallas "DEVs") utifrån deras specifika verktyg i stället för att knyta dem till den skadliga kod de använder. Det innebar att vi, när Contis anknutna organisationer skingrades, kunde fortsätta spåra dessa DEVs genom deras användning av andra verktyg eller RaaS-kit. Några exempel:

- DEV-0230, som är anknutet till Trickbot, hade använt Conti mycket. I slutet av april observerade MSTIC att gruppen använde QuantumLocker.
- DEV-0237 övergick från Contis utpressningstrojankit till HIVE och Nokoyawa. De använde t.ex. HIVE i attacken den 31 maj mot Costa Ricas myndigheter.
- DEV-0506, en annan flitig användare av Contis utpressningstrojankit, observerades nyttja BlackBasta.

Exempel på en anknuten organisation (DEV-0237) som snabbt växlar mellan RaaS-program



Efter att ett RaaS-program som Conti försvinner övergår den anknutna utpressningstrojanorganisationen till ett annat (Hive) nästan direkt.

RaaS utvecklar ekosystemet för utpressningstrojaner och förhindrar att de tillskrivs någon

Eftersom utpressningstrojaner med människor bakom sköts av enskilda operatörer varierar angreppsmönstren beroende på målet och kan förändras under själva angreppet. Tidigare fanns det ofta en nära relation mellan den första intrångsmetoden, verktygen och valet av nyttolast för utpressningstrojan mellan olika kampanjer med en och samma variant av utpressningstrojan. Det underlättade tillskrivningen. Men RaaS-modellen ställer allt på ända. Därför väljer Microsoft att spåra de anknutna organisationer som distribuerar nyttolaster för utpressningstrojaner vid specifika attacker, i stället för att spåra dem som utvecklar nyttolaster för utpressningstrojaner i egenskap av operatörer.

Med andra ord förutsätter vi inte längre att HIVE-utvecklaren står bakom en attack med HIVE-utpressningstrojaner. Snarare rör det sig troligen om en anknuten organisation.

Cybersäkerhetsbranschen har kämpat för att på lämpligt vis snappa upp den här uppdelningen mellan utvecklare och operatörer. Branschen rapporterar fortfarande ofta incidenter med utpressningstrojaner med namnet på nyttolasten, vilket ger det felaktiga intrycket att en enda grupp eller utpressningstrojangäng ligger bakom alla attacker med just den utpressningstrojannyttolasten och att alla incidenter som går att förknippa med den utnyttjar samma tekniker och infrastruktur. För att hjälpa dem som försvarar nätverken är det viktigt att ta reda på mer om de stadier som föregår olika anknutna organisationers angrepp – t.ex. exfiltrering av data och andra beständighetsmekanismer – och de identifierings- och skyddsmöjligheter som kan finnas.

Angrepp med utpressningstrojaner kräver autentiseringsuppgifter för att lyckas, i betydligt högre grad än annan skadlig kod. För att lyckas med mänskligt hanterade infektioner av utpressningstrojaner i en hel organisation behövs tillgång till ett konto med mycket hög behörighet.

Fokus på utpressningstrojan-attacker med människor bakom

Under det senaste året har Microsofts experter på utpressningstrojaner genomfört djupgående undersökningar av över 100 utpressningstrojanincidenter med människor bakom för att spåra angriparnas metoder och förstå hur vi kan skydda våra kunder bättre.

Det är viktigt att observera att den analys vi beskriver här endast är möjlig för idrifttagna, hanterade, enheter. Enheter som inte är idrifttagna och är ohanterade utgör den minst säkra delen av en organisations maskinvarutillgångar.

De vanligaste metoderna i utpressningstrojanens faser:

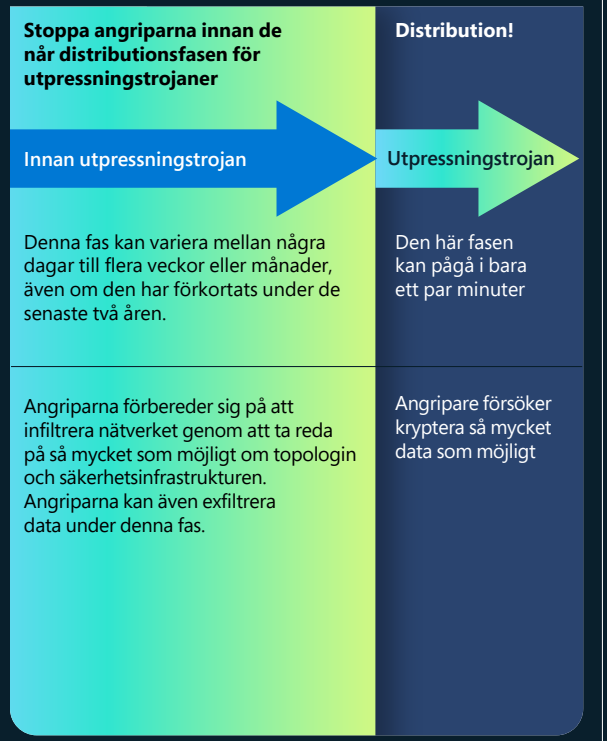
75 %
använder administratörsverktyg.

75 %
använder stulna användarkonton med hög behörighet för att sprida skadliga nyttolaster via SMB-protokollet.

99 %
försöker manipulera identifierade säkerhets- och säkerhetskopieringsprodukter med verktyg som är inbyggda i operativsystemet.

Ett normalt angrepp med människor bakom

Utpressningstrojanattacker med människor bakom kan delas in i fasen innan utpressningstrojanen och fasen då utpressningstrojanen distribueras. Under fasen innan utpressningstrojanen förbereder sig angriparna på att infiltrera nätverket genom att ta reda på organisationens typologi och säkerhetsinfrastruktur.



Våra undersökningar visade att de flesta aktörerna bakom utpressningstrojanattacker med människor bakom utnyttjar liknande säkerhetsbrister och har gemensamma angreppsmönster och tekniker.

En hållbar säkerhetsstrategi

För att bekämpa och förhindra attacker av den här typen måste organisationen tänka om och fokusera på det heltäckande skydd som krävs för att bromsa och hindra angriparna innan de kan gå vidare från fasen innan utpressningstrojanen till den fas då utpressningstrojanen distribueras.

Företag måste tillämpa bästa säkerhetspraxis konsekvent och aggressivt i sina nätverk för att begränsa angreppsklasserna. Eftersom det är människor som fattar besluten kan de här attackerna med utpressningstrojaner leda till flera, till synes olika säkerhetsproduktvarningar som är lätta att missa eller inte åtgärda i tid. När det genereras många varningar kan det vara svårt att urskilja vilka som är viktiga och säkerhetscenter kan förenkla sin tillvaro genom att hålla koll på trender i varningarna eller gruppera dem efter incidenter för att lättare se helheten. Säkerhetscentren kan sedan hantera varningar med hjälp av härdningskapacitet som regler för att minska attackytorna. Härdning mot vanliga hot kan inte bara minska antalet varningar utan även stoppa många angripare innan de får tillgång till nätverket.

Organisationer måste kontinuerligt upprätthålla god försvarsförmåga och nätverkshygien för att skydda sig mot attacker med utpressningstrojaner med människor bakom.

Användbara insikter

Angripare som använder utpressningstrojaner är ute efter enkla vinster, så ett sätt att störa cyberbrottslingarnas ekonomi är att stärka säkerheten för att göra attacken mer kostsam.

1. Hantera autentiseringsuppgifter bättre. Angrepp med utpressningstrojaner kräver autentiseringsuppgifter för att lyckas, i betydligt högre grad än annan skadlig kod. Om angriparna ska lyckas infektera en hel organisation med en utpressningstrojan måste människorna bakom insatsen få tillgång till ett konto med omfattande behörighet, till exempel en domänadministratör eller behörighet att redigera grupprinciper.
2. Granska autentiseringsuppgifters exponering.
3. Prioritera installationen av Active Directory-uppdateringar.
4. Prioritera molnhärdning.
5. Minska attackytan.
6. Härda tillgångar som går att nå från internet och förstå nätverkets periferi.
7. Minska överbelastningen av varningar i säkerhetscentret genom att härda nätverket för att minska antalet varningar så att det finns kapacitet för högprioriterade incidenter.

Länkar till mer information

- RaaS: Understanding the cybercrime gig economy and how to protect yourself | Microsoft Security Blog
- Människodrivna angrepp med utpressningstrojaner: En katastrof som går att förebygga | Microsoft Security-bloggen

Insikter om utpressningstrojaner från personal i frontlinjen

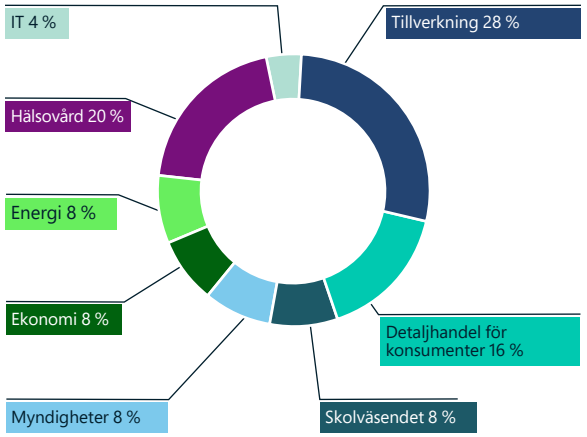
Från och med 2019 har organisationer över hela världen upplevt alltfler attacker med utpressningstrojaner med människor bakom. Men brottsbekämpande insatser och geopolitiska händelser under det senaste året har haft en betydande effekt på cyberbrottsorganisationerna.

Microsoft Security Service Line hjälper kunder under hela cyberattacken, från utredning till framgångsrika inneslutnings- och återställningsaktiviteter. Insats- och återställningstjänster erbjuds via två mycket samordnade team. Det ena fokuserar på utredningen och grundjobbet för återställning och det andra hanterar inneslutning och återhämtning. I det här avsnittet presenterar vi en sammanfattning av vad vi har sett vid arbetet med utpressningstrojaner under det senaste året.

93 %

av Microsofts undersökningar vid återställningsinsatser mot utpressningstrojaner visade att kontrollerna av behörighet och laterala rörelser var otillräckliga.

Incidenter med utpressningstrojaner och återställningsuppdrag per bransch

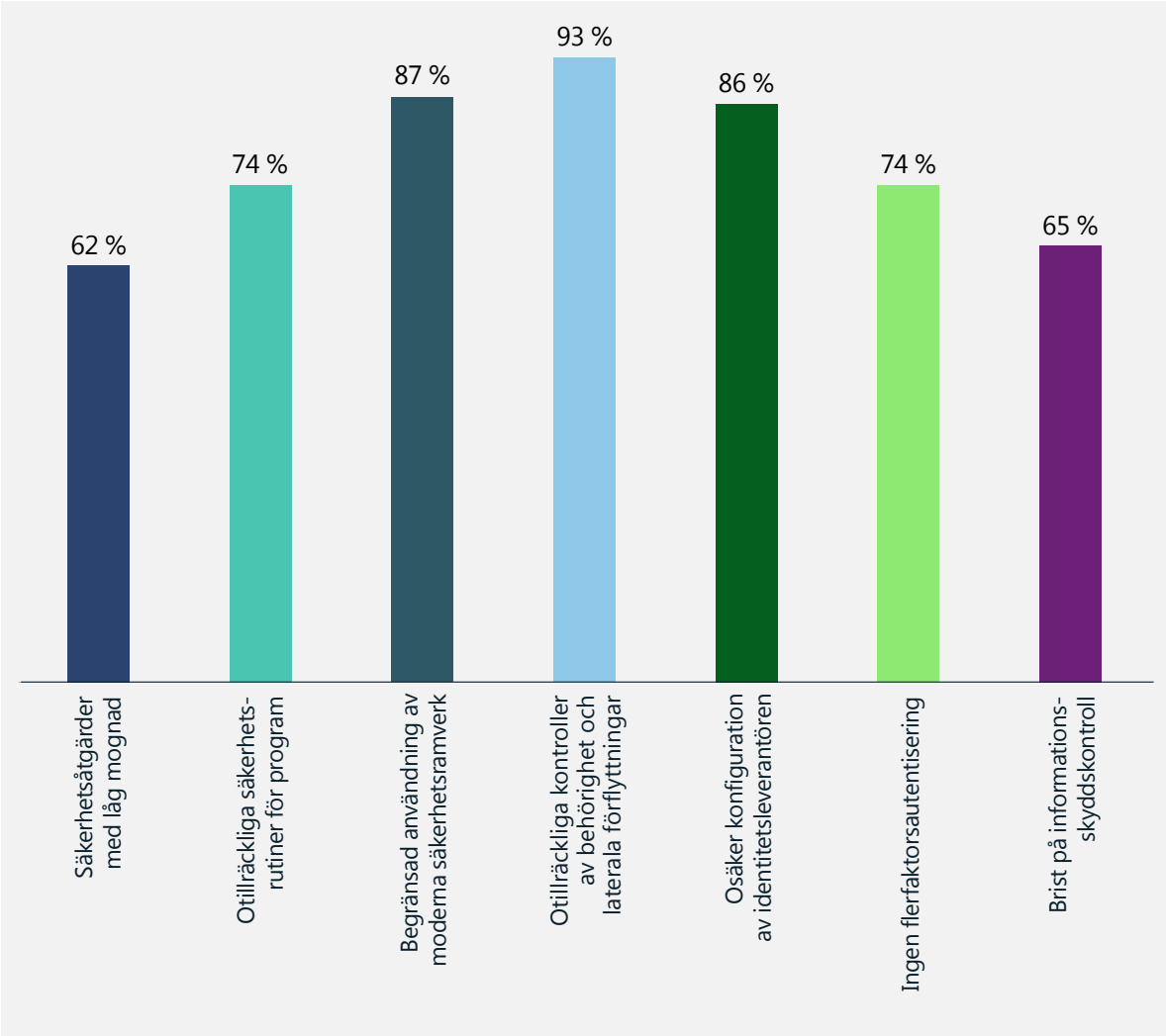


När nya små grupper och hot dyker upp måste försvarsteamen bli medvetna om nya utpressningstrojanhot samtidigt som de skyddar sig mot tidigare okända kategorier av utpressningstrojaner. Strategin med snabb utveckling som de kriminella grupperna använder har lett till att smarta utpressningstrojaner har paketerats i lättanvända kit. Det ger större flexibilitet att göra breda angrepp mot många mål.

På de följande sidorna ska vi titta närmare på de vanligaste bidragande faktorerna till bristande skydd mot utpressningstrojaner. Vi har identifierat tre huvudkategorier:

1. Bristande identitetskontroller
2. Ineffektiva säkerhetsåtgärder
3. Begränsat dataskydd

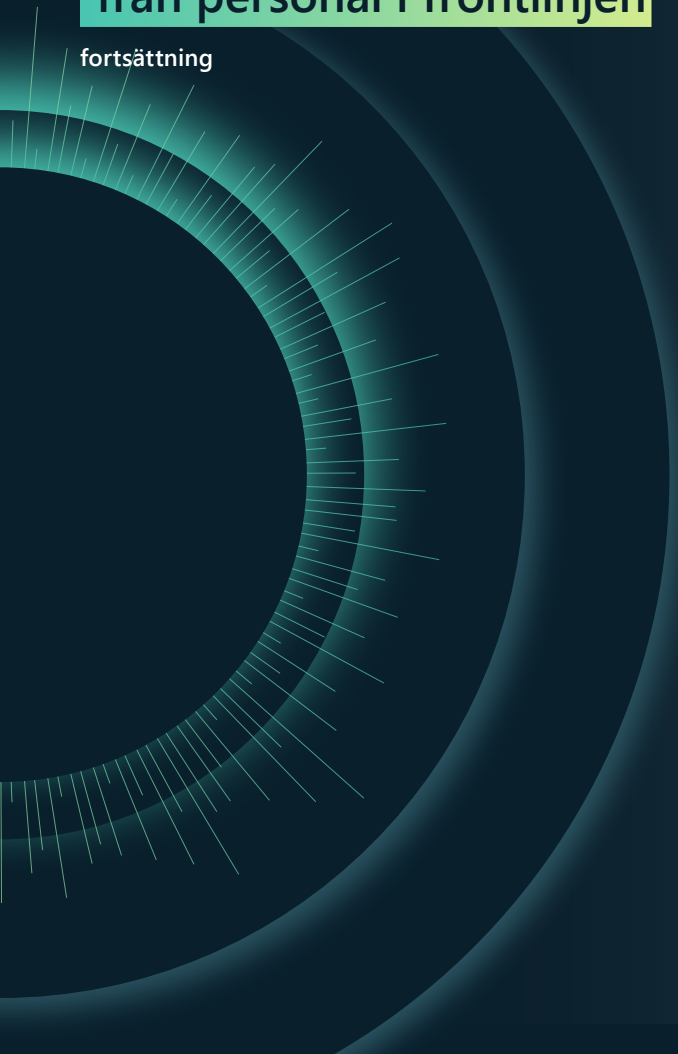
Översikt av de vanligaste upptäckterna vid hantering av utpressningstrojaner



Den vanligaste upptäckten vid hantering av incidenter med utpressningstrojaner är att kontrollerna av behörighet och laterala rörelser är otillräckliga.

Insikter om utpressningstrojaner från personal i frontlinjen

fortsättning



De tre viktigaste bidragande faktorerna vi ser när vi hjälper till på plats:

① **Bristande identitetskontroller:** Angrepp med stöld av autentiseringsuppgifter är fortfarande en av de främsta bidragande faktorerna

② **Ineffektiva säkerhetsrutiner** utgör inte bara möjligheter för angripare utan påverkar även återställningstiden avsevärt

③ I slutänden handlar allt om data – organisationer kämpar för att införa effektiva **dataskyddsstrategier som** överensstämmer med deras affärsbehov

① Bristande identitetskontroller

Utpressningstrojaner som människor står bakom utvecklas löpande och utnyttjar stöld av autentiseringsuppgifter och laterala rörelser som traditionellt förknippas med riktade attacker. Framgångsrika attacker bygger ofta på långvariga kampanjer där angriparen har brutit sig in i identitetssystem som Active Directory (AD), så att de mänskliga operatörerna kan stjäla autentiseringsuppgifter, komma åt system och bli kvar i nätverket.

Active Directory- (AD) och Azure AD-säkerhet

88 %

av alla kunder som har råkat ut för intrång använde inte bästa praxis för AD- och Azure AD-säkerhet. Det här har blivit en vanlig attackvektor som går ut på att angriparna utnyttjar felkonfigurationer och svagare säkerhetsställningar i viktiga identitetssystem för att få ökad åtkomst och kunna påverka verksamheten mer.

Minst privilegierad åtkomst och användning av arbetsstationer med privilegierad åtkomst

Inga av de aktuella organisationerna har skilt administrativa autentiseringsuppgifter och principer för minst privilegierad åtkomst åt korrekt via särskilda arbetsstationer vid hanteringen av sina viktiga identitetstillgångar och mest värdefulla tillgångar, t.ex. egna system och affärskritiska program.

Säkerhet för privilegierade konton

88 %

av alla engagemang har inte använt MFA för känsliga konton och konton med höga behörigheter, vilket skapar ett säkerhetshål som angriparna kan använda för att komma åt autentiseringsuppgifter och dra igång ytterligare attacker med legitima autentiseringsuppgifter.

84 %

av alla organisationer har administratörer som inte använder kontroller för behörighetsidentitet, till exempel just-in-time-åtkomst, för att förhindra ytterligare obehörig användning av privilegierade autentiseringsuppgifter.

Insikter om utpressningstrojaner från personal i frontlinjen

fortsättning

② Ineffektiva säkerhetsåtgärder

Våra data visar att organisationer som har utsatts för attacker med utpressningstrojaner har betydande luckor i hanteringen av sin säkerhetsverksamhet, sina verktyg och sin informationstekniks livscykel. Enligt tillgängliga data är följande brister vanligast:

Korrigeringar:

68 %

av alla påverkade organisationer saknade en effektiv sårbarhets- och korrigeringshanteringsprocess, och den stora andelen manuella rutiner i stället för automatiska korrigeringar medförde allvarliga säkerhetsluckor. Tillverkningsindustrin och den kritiska infrastrukturen kämpar fortfarande med underhåll och korrigeringar av äldre driftsystem.

Brist på verktyg för säkerhetsåtgärder:

De flesta organisationer uppgav att de inte hade komplett insyn i säkerheten på grund av brist på eller felkonfigurerade säkerhetsverktyg, vilket ledde till sämre identifierings- och svarseffektivitet.

60 %

av organisationerna uppgav att de inte använde något EDR-verktyg[6], vilket är en grundläggande teknik för detektering och respons.

60 %

investerade inte i SIEM-teknik (Security Information and Event Management), vilket ledde till avgränsad övervakning, begränsad förmåga att upptäcka heltäckande hot och ineffektiva säkerhetsåtgärder. Automatiseringen är fortfarande bristande i SOC-verktyg och SOC-processer, vilket innebär att SOC-personalen måste ägna otaliga timmar åt att förstå säkerhetstelemetrin.

84 %

av alla organisationer som påverkades hade inte möjliggjort integrering av sina multimolnmiljöer i verktygen för säkerhetsåtgärder.

Svars- och återställningsprocesser:

76 %

av de aktuella organisationerna saknade en effektiv insatsplan, vilket förhindrade lämplig beredskap för kriser i organisationen och påverkade både reaktionstiden och återhämtningstiden negativt.

③ Begränsat dataskydd

Många organisationer som har råkat ut för intrång saknade lämpliga dataskyddsprocesser, vilket ledde till avsevärt förlängda återställningstider och sämre förmåga att återgå till verksamheten. Bland de vanligaste bristerna finns följande:

Oföränderliga säkerhetskopior:

44 %

av alla organisationer hade inte oföränderliga säkerhetskopior för de påverkade systemen. Data visar även att administratörer inte hade säkerhetskopior och återställningsplaner för viktiga tillgångar som AD.

Skydd mot dataförluster:

Angriparna hittar vanligtvis ett sätt att ta sig in i systemen genom att utnyttja sårbarheter i organisationen, exfiltrera viktiga data för utpressning, stöld av immateriella tillgångar eller intäktsgenerering.

92 %

av alla påverkade organisationer införde inte effektiva kontroller för att förebygga dataförluster för att minska riskerna, vilket ledde till allvarliga dataförluster.

Utpressningstrojaner minskade i vissa regioner och ökade i andra

I år observerade vi färre rapporterade fall av utpressningstrojaner till våra insatsteam i Nordamerika och Europa jämfört med föregående år. Samtidigt ökade fallen som rapporterades i Latinamerika.

En tolkning av det här är att cyberbrottslingarna vänder sig bort från områden som upplevs ha högre risk att intressera polisen till förmån för mjukare mål. Eftersom Microsoft inte har observerat någon betydande förbättring av säkerheten i världens företagsnätverk som skulle förklara minskningen av antalet supportsamtal om utpressningstrojaner, tror vi att den mest sannolika orsaken är en kombination av olika geopolitiska händelser 2022 och den brottsbekämpande verksamheten under 2021 och 2022 som ökade kostnaderna för brottslig verksamhet.

En av de vanligaste RaaS-operationerna förknippas med en rysktalande kriminell grupp som heter REvil (eller Sodinokibi) och har varit aktiv sedan 2019. I oktober 2021 togs REvils servrar ned som ett led i den internationella brottsbekämpande GoldDust-kampanjen.[7] I januari 2022 grep Ryssland 14 påstådda REvil-medlemmar och gjorde räder på 25 platser som förknippades med dem.[8] Det här var den första gången som Ryssland agerade mot utpressningstrojanangripare i landet.

De polisiära insatserna bromsade troligen in förekomsten av angrepp under 2022, men hotaktörerna kan mycket väl utveckla nya strategier för att undvika att bli fångade i framtiden. Dessutom verkar spänningarna mellan Ryssland och USA på grund av Rysslands invasion av Ukraina ha satt stopp för Rysslands begynnande samarbete i den globala kampen mot utpressningstrojaner. Efter en kort tid av osäkerhet efter REvil-gripandena upphörde USA och Ryssland att samarbeta för att lagföra utpressningstrojanangripare, vilket innebär att cyberbrottslingarna än en gång kan se Ryssland som en fristad.

I framtiden tror vi att takten för utpressningstrojanaktiviteter beror på svaren på några viktiga frågor:

1. Kommer länder att vidta åtgärder för att hindra utpressningstrojanangripare från att verka inom sina gränser eller försöka störa aktörer som verkar i utlandet?
2. Kommer utpressningstrojangrupper att byta taktik för att undanröja behovet av utpressningstrojaner och tillgripa utpressningsliknande angrepp?
3. Kommer organisationer att kunna modernisera och utveckla sin IT-verksamhet snabbare än brottslingarna hinner utnyttja sårbarheterna?
4. Kommer framsteg med att spåra och söka roten till betalningar av lösensummor att tvinga mottagarna av pengarna att byta taktik och förhandlingsmetoder?

De polisiära insatserna bromsade troligen in förekomsten av angrepp under 2022, men hotaktörerna kan mycket väl utveckla nya strategier för att undvika att bli fångade i framtiden.

2×

Attackerna med utpressningstrojaner minskade i vissa regioner, men lösenkraven mer än fördubblades.

Användbara insikter

1. Fokusera på holistiska säkerhetsstrategier eftersom alla kategorier av utpressningstrojaner utnyttjar samma säkerhetsbrister för att ta sig in i nätverk.
2. Uppdatera och underhålla säkerhetsgrunderna för att öka grundnivån på det djupgående skyddet och modernisera säkerhetsverksamheten. Genom att flytta till molnet går det snabbare att upptäcka hot och snabbare att reagera.

Länkar till mer information

- Skydda din organisation mot utpressningstrojaner | Microsoft Security
- 7 ways to harden your environment against compromise | Microsoft Securitys blogg
- Improving AI-based defenses to disrupt human-operated ransomware | Microsoft 365 Defender Research-teamet
- Security Insider: Explore the latest cybersecurity insights and updates | Microsoft Security

Cyberbrott som tjänst

Cyberbrott som tjänst (CaaS) är ett växande och föränderligt hot mot kunder i hela världen. Microsoft Digital Crimes Unit (DCU) observerade fortsatt tillväxt av CaaS-ekosystemet med alltfler onlinetjänster som underlättar olika cyberbrott, till exempel angrepp mot affärskorrespondens och utpressningstrojaner som sköts av människor. Nätfiske är fortfarande en populär angreppsmetod, eftersom cyberbrottslingarna kan tjäna mycket på att stjäla och sälja åtkomst till stulna konton.

Som reaktion på den växande CaaS-marknaden byggde DCU ut sina lyssnande system för att upptäcka och identifiera CaaS-produkter på internet, den djupa webben, vissa utvalda forum[9], särskilda webbplatser, nätdiskussionsforum och meddelandeplattformar.

Cyberbrottslingarna samarbetar nu i olika tidszoner och på olika språk för att leverera specifika resultat. Till exempel har en CaaS-webbplats som administreras av en person i Asien verksamhet i Europa och skapar skadliga konton i Afrika. Eftersom verksamheten bedrivs i många länder innebär det komplexa juridiska och polisiära utmaningar. Därför fokuserar DCU sina insatser på att slå undan benen för den skadliga kriminella infrastruktur som används för att underlätta CaaS-angrepp och samarbetar med polisen runtom i världen för att lagföra brottslingar.

Cyberbrottslingarna använder alltmer analys för att maximera sin räckvidd, omfattning och vinst. Precis som vanliga företag måste CaaS-webbplatser säkerställa att deras produkter och tjänster fungerar för att upprätthålla ett gott rykte. Till exempel automatiserar CaaS-webbplatser rutinmässigt åtkomsten till knäckta konton för att säkerställa att autentiseringsuppgifterna är giltiga. Cyberbrottslingarna slutar sälja specifika konton när lösenorden återställs eller sårbarheter korrigeras. Vi har i allt högre grad sett att CaaS-webbplatser erbjuder köparna on-demand-verifiering som en del av sin kvalitetskontrollprocess. På så sätt kan köparna vara säkra på att CaaS-webbplatsen säljer aktiva konton och lösenord samtidigt som de potentiella kostnaderna för CaaS-handlaren minskar om de stulna autentiseringsuppgifterna åtgärdas före försäljningen.

DCU har även sett CaaS-webbplatser som erbjuder köparna möjlighet att handla knäckta konton från specifika geografiska platser, utvalda onlinetjänsteleverantörer och specifika individer, yrken och branscher. Ofta efterfrågas konton med fokus på yrkesmänniskor eller avdelningar som hanterar fakturor, t.ex. ekonomichefer eller kundreskontran. På samma sätt råkar branscher som deltar i offentliga upphandlingar ofta illa ut på grund av all den information som görs tillgänglig genom det offentliga anbudsförfarandet.

DCU:s CaaS-undersökningar har avslöjat ett antal viktiga trender:

Antalet tjänster och sofistikeringsgraden ökar.

Ett exempel är utvecklingen av webbskal som vanligtvis består av knäckta webbservrar som används för att automatisera nätfiskeangrepp. DCU har sett att CaaS-återförsäljare gör det enklare att ladda upp nätfiskekit eller skadlig kod via särskilda webbinstrumentpaneler. CaaS-säljarna försöker sedan ofta sälja ytterligare tjänster till hotaktören via instrumentpanelen, till exempel spammeddelandetjänster och särskilda spammottagarlistor baserat på angivna attribut, däribland geografisk plats eller yrke. I vissa fall har vi sett ett och samma webbskal användas i flera angreppskampanjer, vilket tyder på att hotaktörerna kan ha ständig åtkomst till den knäckta servern. Vi har också sett en ökning av de anonymiseringstjänster som är tillgängliga i CaaS-ekosystemet, samt erbjudanden om VPN- och VPS-konton (virtuella privata nätverks- och serverkonton). I de flesta fall anskaffades de VPN/VPS som erbjöds inledningsvis via stulna kreditkort. CaaS-webbplatser erbjöd också ett större antal RDP- (Remote Desktop Protocol), Secure Shell- (SSH) och cPanel-anslutningar som kan användas som plattform för att iscensätta cyberbrott. CaaS-handlarna konfigurerar RDP, SSH och cPanels med lämpliga verktyg och skript för att underlätta olika typer av cyberattacker.

Tjänster för att skapa homoglyfdomäner kräver allt oftare betalning i kryptovaluta.

Homoglyfdomäner imiterar legitima domännamn genom att använda tecken som är identiska eller nästan identiska till utseendet med ett annat tecken. Syftet är att lura betraktaren att tro att homoglyfdomänen är den äkta domänen. Dessa domäner är ett vanligt förekommande hot och en inkörsport för en betydande mängd cyberbrott. CaaS-webbplatser säljer nu anpassade homoglyfdomännamn, vilket gör det möjligt för köparen att begära specifika företags- och domännamn att imitera. När betalningen har erlagts använder CaaS-handlarna ett verktyg som genererar homoglyfer för att välja domännamnet och sedan registrera den skadliga homoglyfen. Betalningen för den här typen av tjänst sker nästan alltid med kryptovaluta.

2 750 000

webbplatsregistreringar blockerades av DCU i år för att få ett försprång gentemot kriminella som planerade att använda dem för global cyberbrottslighet.

Cyberbrott som tjänst

fortsättning

CaaS-säljare erbjuder i allt högre grad stulna autentiseringsuppgifter.

Stulna autentiseringsuppgifter möjliggör obehörig åtkomst till användarkonton, däribland e-postmeddelandetjänster, företags fildelningsresurser och OneDrive för företag. Om en administratörs autentiseringsuppgifter stjäls kan obehöriga användare få tillgång till konfidentiella filer, Azure-resurser och företagsanvändarkonton. I många fall identifierade DCU:s undersökningar obehörig användning av samma autentiseringsuppgifter på flera servrar som ett sätt att automatisera verifieringen av inloggningsuppgifter. Det här mönstret tyder på att den drabbade användaren kan ha utsatts för flera nätfiskeangrepp eller ha skadlig kod på sin enhet så att botnäts tangentloggare kan samla in autentiseringsuppgifter.

Det har börjat dyka upp CaaS-tjänster och CaaS-produkter med utökade funktioner för att undvika upptäckt.

En CaaS-säljare erbjuder nätfiskepaket med högre komplexitet och fler anonymiseringsfunktioner som har utformats för att kringgå identifieringssystem och förebyggande system för bara sex dollar per dag. Tjänsten erbjuder en rad omdirigeringar som utför kontroller innan trafik tillåts till nästa lager eller plats. En av tjänsterna genomför över 90 kontroller och skapar en sorts enhetsfingeravtryck, till exempel kontrollerar den om det är en virtuell maskin, vilken webbläsare och maskinvara som används och mycket annat. Om alla kontroller ger grönt ljus skickas trafiken till en målsida som används för nätfiske.

Kompletta cyberbrottstjänster säljer prenumerationer på hanterade tjänster.

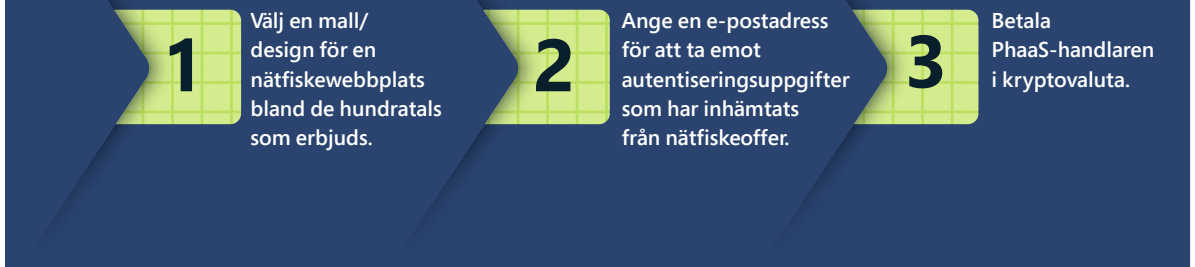
Normalt kan varje steg av genomförandet av ett brott på nätet exponera hotaktören om den operativa säkerheten är dålig. Risken för exponering och identifiering ökar om tjänster köps från flera CaaS-platser. DCU observerade en oroande trend på den mörka webben: antalet tjänster som erbjuds för att anonymisera programvarukod och generalisera webbplatstext för att minska exponeringen ökar. Leverantörer av kompletta prenumerationstjänster för cyberbrottslighet hanterar alla tjänster och garanterar resultat, vilket ytterligare minskar exponeringsriskerna för den OCN som prenumererar. Den minskade risken har ökat de här kompletta tjänsternas popularitet.

Nätfiske som tjänst (PhaaS) är ett exempel på en heltäckande cyberbrottstjänst. PhaaS är en utveckling av tidigare tjänster som kallas FUD (Fully Undetectable Services, fullständigt oidentifierbara tjänster) och erbjuds på prenumerationsbasis. Normalt hålls en nätfiskewebbplats aktiv i en månad enligt PhaaS-villkoren.

DCU har också hittat en CaaS-handlare som erbjuder DDoS (distribuerad denial of service) enligt en prenumerationsmodell. Modellen innebär att CaaS-handlaren skapar och underhåller det botnät som krävs för att utföra angrepp. Varje DDoS-prenumerationskund får en krypterad tjänst för att förbättra driftsäkerheten och ett års support dygnet runt. DDoS-prenumerationstjänsten erbjuder olika arkitekturer och angreppsmetoder, så köparen väljer helt enkelt en resurs att angripa och säljaren ger tillgång till en rad knäckta enheter i dess botnät för att utföra angreppet. Kostnaden för DDoS-prenumerationen är endast 500 USD.

DCU:s arbete med att utveckla verktyg och metoder som identifierar och stör CaaS-cyberbrottslingar sker löpande. Utvecklingen av CaaS-tjänster innebär stora utmaningar, särskilt när det gäller att störa betalning i kryptovaluta.

PhaaS, cyberbrottslingar som erbjuder flera tjänster i samma prenumeration. I allmänhet behöver köparen bara vidta tre åtgärder:



När dessa steg har slutförts skapar PhaaS-handlaren tjänster med tre eller fyra lager med omdirigerings- och värdlagringsresurser för att rikta in sig på specifika användare. Kampanjen lanseras därefter och offrens användaruppgifter inhämtas, verifieras och skickas till den e-postadress som tillhandahålls av köparen. Mot extra betalt erbjuder sig många PhaaS-handlare att vara värd för nätfiskewebbplatser i den offentliga blockkedjan så att de kan nås av en valfri webbläsare, och omdirigeringar kan skicka användare vidare till en resurs i den distribuerade liggaren.

Kriminellt bruk av kryptovalutor

I takt med att kryptovaluta blir allt vanligare utökar även brottslingar sin användning av den för att kringgå polisiära åtgärder och åtgärder mot penningtvätt (ÅMP). Det gör det svårare för polisen att spåra och hålla reda på betalningar av kryptovaluta till cyberbrottslingar.

Penninginsatserna i blockkedjelösningar globalt ökade med cirka 340 procent under de senaste fyra åren, och nya kryptovalutaplånböcker ökade med cirka 270 procent. Det finns över 83 miljoner unika plånböcker globalt och den totala marknadsvärderingen för alla kryptovalutor var cirka 1,1 biljoner USD 28 juli 2022.[10]



Källa: Twitter.com – @PeckShieldAlert (PeckShield är ett blockkedjesäkerhetsföretag med säte i Kina).

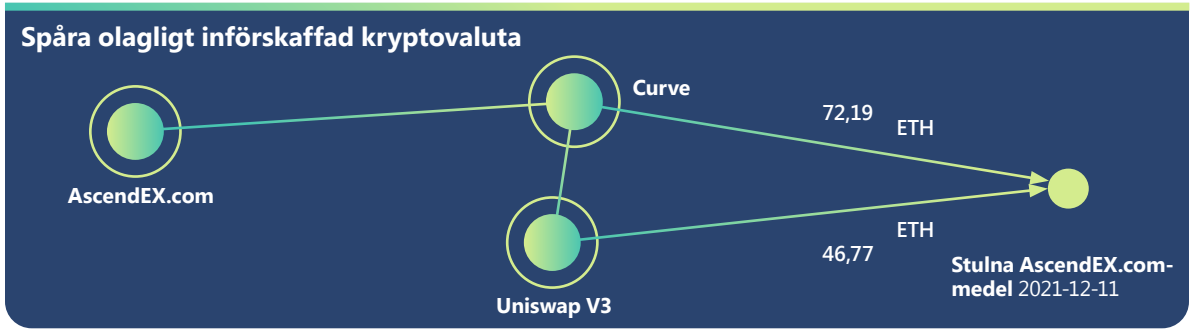
Spåra betalningar för utpressningstrojaner

Utpressningstrojaner är en av de största källorna till olagligt införskaffad kryptovaluta. I ett försök att störa den skadliga tekniska infrastruktur som används vid angrepp med utpressningstrojaner – till exempel attacken mot Zloader i april 2022[11] – spårar Microsofts DCU kriminellas plånböcker för att göra det möjligt att spåra och återställa kryptovaluta.

DCU-utredarna har observerat utpressningstrojanangripare som utvecklar sin kommunikationstaktik med offren för att dölja vart pengarna tar vägen. Ursprungligen lade cyberbrottslingarna in Bitcoin-adresser i sina utpressningsmeddelanden. Men då var det enkelt att följa betalningstransaktionerna i blockkedjan. Därför slutade utpressningstrojanangriparna att ange plånboksadresser och lade i stället till e-postadresser eller länkar till chattwebbplatser för att meddela betalningsadressen till offren. En del aktörer skapade till och med unika webbsidor och inloggningsuppgifter för varje offer för att förhindra säkerhetsutredare och polisen från att få tillgång till brottslingarnas plånboksadresser genom att låtsas vara offer. Trots de kriminellas försök att dölja sina spår kan vissa lösenbetalningar ändå återvinnas genom att offren samarbetar med polisen och kryptoanalysföretag som kan spåra förflyttningar i blockkedjan.

Trend: DEX-penningtvätt av olagliga intäkter

Ett stort problem för cyberbrottslingarna är hur de ska omvandla sin kryptovaluta till reda pengar. Cyberbrottslingarna har flera potentiella växlingsmöjligheter, men alla medför vissa risker. En metod för att minska risken är att tvätta intäkterna genom en decentraliserad börs (DEX)



Med hjälp av kryptovalutaverktyget Chainalysis upptäckte Microsofts digitalbrottsenhet att AcendEX-hackarna bytte sina stulna medel på en mindre DEX, Curve, utöver Uniswap. Bilden illustrerar penningtvättvägarna som teamet har upptäckt. Varje cirkel representerar ett kluster med plånböcker, och siffrorna på varje rad representerar den totala mängden Ethereum som överfördes för penningtvätt.

innan pengarna tas ut via något tillgängligt utbetalningsalternativ, t.ex. centrala börser (CEX), peer-to-peer (P2P) och kassaväxling (OTC). DEX:er är lockande alternativ för penningtvätt, eftersom de ofta inte följer ÅMP-regler.

I december 2021 angrep hackare den globala handelsplattformen för kryptovaluta AscendEx och stal cirka 77,7 miljoner USD i kryptovaluta som tillhörde dess kunder.[12] AscendEx anlitade blockkedjeanalysföretag och kontaktade andra CEX-företag så att plånböckerna som tog emot stulna medel kunde svartlistas. Dessutom etiketterades adresser dit kryptovalutan skickades som sådana i Ethereum-blockkedjeutforskaren Etherscan.[13] För att kringgå varningarna och svartlistningen skickade hackarna 1,5 miljoner USD i Ethereum till Uniswap, en av världens största DEX:ar, 18 februari 2022.[14]

Om DEX:ar skulle använda mer kraftfulla ÅMP-insatser skulle det hämma penningtvätten på deras plattformar och tvinga cyberbrottslingarna att använda andra metoder som kryptovalutatumling eller olicensierade börser. Uniswap meddelade t.ex. nyligen att de kommer att börja använda svartlistning för att hindra plånböcker som det är känt är inblandade i olagliga aktiviteter från att handla på börsen.[15]

Användbara insikter

1. Om du har blivit utsatt för ett cyberbrott och har betalat brottslingen i kryptovaluta bör du kontakta polisen lokalt. De kan kanske hjälpa till att spåra och återvinna förlorade medel.
2. Bekanta dig med penningtvättåtgärderna när du väljer en DEX.

Länkar till mer information

- Hardware-based threat defense against increasingly complex cryptojackers | Microsoft 365 Defender Research-teamet

Den föränderliga hotbilden från nätfiske

Metoder för att nätfiske av autentiseringsuppgifter är på uppgång och är fortfarande ett betydande hot mot användare överallt, eftersom de urskillningslöst riktas mot alla som har e-post. Bland de hot som våra forskare spårar och skyddar mot är mängden nätfiskeangrepp flera storleksordningar större än alla andra hot.

Med hjälp av data från Defender för Office ser vi skadlig aktivitet med e-post och knäckta identiteter. Azure Active Directory Identity Protection ger ännu mer information genom varningar om knäckta identiteter. Med hjälp av Defender for Cloud Apps ser vi dataåtkomsthändelser med knäckta identiteter och Microsoft 365 Defender (M365D) ger korrelation mellan produkter. Det laterala rörelsemåttet kommer från Defender for Endpoint (attackbeteendevarningar och -händelser), Defender for Office (skadlig e-post) och än en gång M365D för korrelation mellan produkter.

710 miljoner
nätfiskemeddelanden blockeras varje vecka.

1 h 12 m
är mediantiden som det tar för en angripare att komma åt dina privata data om du faller offer för ett nätfiskemeddelande.[16]

1 h 42 m
är mediantiden som det tar för en angripare att börja röra sig lateralt i företagets nätverk när en enhet har knäckts.[17]

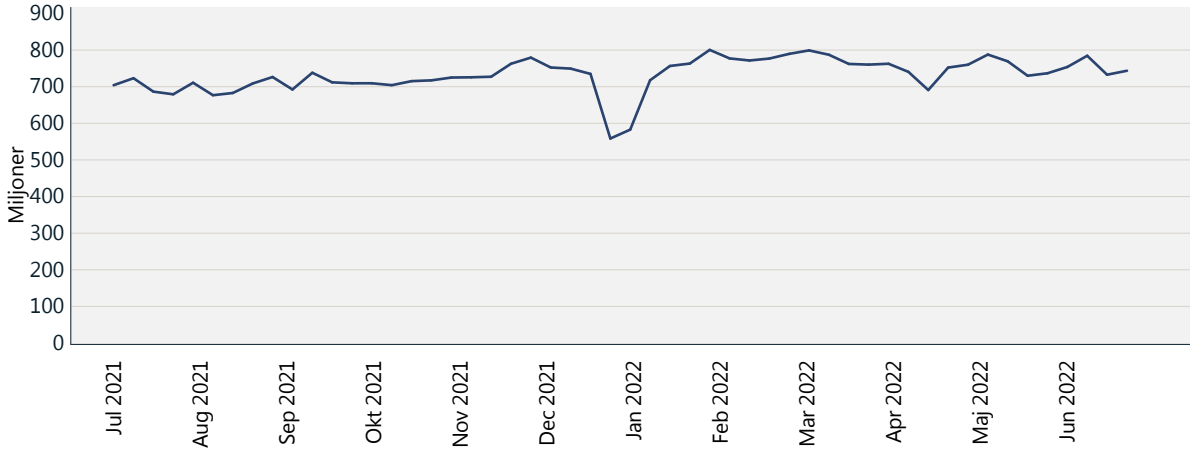
Autentiseringsuppgifter för Microsoft 365 är fortfarande en av de mest eftertraktade kontotyperna för angripare. Så fort inloggningsuppgifter knäcks kan angriparen logga in på företagets datorsystem och infektera det med skadlig kod och utpressningstrojaner, stjäla konfidentiella företagsdata och information genom att öppna SharePoint-filer och fortsätta med nätfisket genom att skicka ytterligare skadliga e-postmeddelanden via Outlook, bland andra åtgärder.

Utöver kampanjer med bredare mål, nätfiske efter autentiseringsuppgifter, donationer och personlig information riktar sig angriparna mot särskilda företag för att tjäna mer. Nätfiskeangrepp via e-post mot företag för ekonomisk vinning kallas BEC-angrepp (business email compromise) med ett gemensamt namn. Microsoft identifierar miljontals BEC-meddelanden varje månad, vilket motsvarar 0,6 procent av alla nätfiskemeddelanden som observeras. En rapport från IC3[18] som publicerades i maj 2022 visar på en uppåtgående trend för kända förluster på grund av BEC-angrepp.

Metoderna som används vid nätfiskeangrepp fortsätter att bli allt mer avancerade. Som reaktion på motåtgärder tar angriparna fram nya sätt att genomföra sina metoder och gör det svårare att veta hur och var de har sin kampanjs infrastruktur. Det innebär att organisationer regelbundet måste ompröva sin strategi för att implementera säkerhetslösningar i syfte att blockera skadliga e-postmeddelanden och stärka åtkomstkontrollen för enskilda användarkonton.

531 000
Utöver webbadresserna som Defender for Office blockerade stod vår digitalbrottsenhet bakom stängningen av 531 000 unika nätfiskewebbadresser utanför Microsoft.

Upptäckta nätfiskemeddelanden



Antalet upptäckta nätfiskeförsök per vecka fortsätter att öka. Minskningen i december–januari är en väntad säsongsvariation, som rapporterades även förra året. Källa: Exchange Online Protection-signaler.

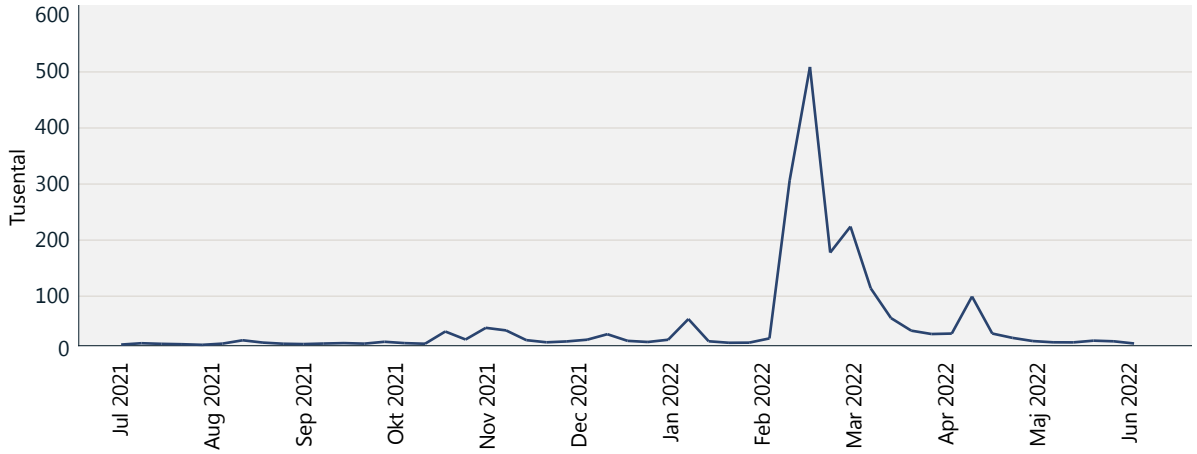
Den föränderliga hotbilden från nätfiske

fortsättning

År efter år fortsätter vi att se en stadig ökning av nätfiskemeddelanden. Övergången till distansarbete 2020 och 2021 medförde betydligt fler nätfiskeangrepp som syftade till att dra nytta av den förändrade arbetsmiljön. Nätfiskarna är snabba att använda nya e-postmallar med beten som anpassas efter stora världshändelser som covid-19-pandemin och teman som är kopplade till samarbets- och produktivitetsverktyg som Google Drive eller fildelning i OneDrive. Covid-19-teman har börjat minska men i början av mars 2022 blev kriget i Ukraina ett nytt lockbete. Våra forskare observerade en häpnadsväckande ökning av antalet e-postmeddelanden som försöker efterlikna legitima organisationer och be om donationer av kryptovaluta i Bitcoin och Ethereum som ett påstått sätt att stödja ukrainska medborgare.

Bara några dagar efter krigets inledning i Ukraina i slutet av februari 2022 ökade antalet identifierade nätfiskemeddelanden med Ethereum-adresser som påträffades hos företagskunder dramatiskt. Den totala mängden nådde sin höjdpunkt den första veckan i mars, då en halv miljon nätfiskemeddelanden innehöll Ethereum-plånboksadresser. Före kriget var antalet Ethereum-plånboksadresser i andra e-postmeddelanden som upptäcktes vara nätfiskeförsök betydligt färre, i genomsnitt några tusen per dag.

Nätfiskemeddelanden med Ethereum-plånboksadresser



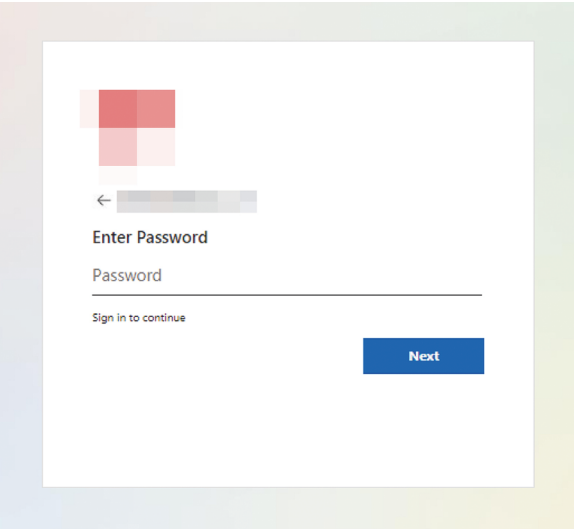
Det totala antalet e-postmeddelanden som upptäcktes vara nätfiskeförsök med Ethereum-plånboksadresser ökade kraftigt i början av konflikten mellan Ukraina och Ryssland och har sedan minskat en del.

Nätfiskarna förlitar sig mer än någonsin på legitim infrastruktur för sin verksamhet. Det leder till en ökning av antalet nätfiskekampanjer som syftar till att utnyttja olika aspekter av en verksamhet, så att angriparna inte själva behöver köpa, vara värd för eller driva egna. Skadliga e-postmeddelanden kan till exempel komma från knäckta avsändarkonton. Angriparen drar fördel av att sådana e-postadresser har bättre rykte och betraktas som mer tillförlitliga än nyskapade konton och domäner. I en del avancerade nätfiskekampanjer har vi observerat angripare som i stället väljer att skicka och förfalska från domäner med DMARC[19] felaktigt konfigurerat med en ”ingen åtgärd”-policy, vilket skapar stora möjligheter till e-postförfalskning.

Stora nätfiskeorganisationer använder oftast molntjänster och virtuella molnmaskiner för att organisera storskaliga angrepp. Angriparna kan automatisera processen helt och distribuera och leverera e-post från virtuella datorer med SMTP-e-postvidarebefordran eller e-postinfrastruktur i molnet för att dra nytta av de höga leveranshastigheterna och det goda ryktet hos sådana legitima tjänster. Om skadlig e-post tillåts skickas via de här molntjänsterna måste försvararna förlita sig på kraftfulla e-postfiltreringsfunktioner för att hindra e-post från att ta sig in i deras miljö.

Microsoft-konton är fortfarande högprioriterade mål för nätfiskeoperatörer, vilket framgår av alla de nätfiskemålsidor som utger sig för att vara inloggningssidan till Microsoft 365. Nätfiskarna försöker till exempel matcha Microsofts inloggningsfunktion i sina nätfiskekit genom att generera en unik webbadress som är anpassad efter mottagaren. Adressen pekar mot en skadlig webbsida som har utvecklats för att samla in autentiseringsuppgifter, men en parameter i webbadressen innehåller den specifika mottagarens e-postadress. När det tilltänkta offret kommer till sidan fyller nätfiskekitet i användarens inloggningsdata och infogar en företagslogotyp som är anpassad efter e-postmottagaren, vilket speglar utseendet på det utsatta företagets anpassade inloggningssida i Microsoft 365.

En nätfiskesida som utger sig för att vara en inloggningssida till Microsoft med dynamiskt innehåll

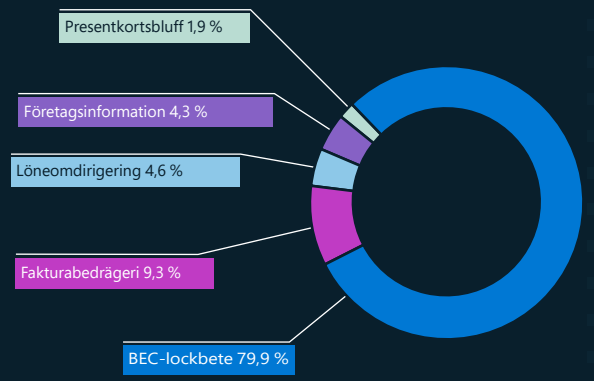


Fokus på intrång i företags e-post

Cyberbrottslingarna utvecklar alltmer komplexa system och tekniker för att komma runt säkerhetsinställningar och rikta in sig mot individer, företag och organisationer. Därför investerar vi betydande resurser för att ytterligare stärka vårt BEC-efterlevnadsprogram.

BEC är den mest kostsamma ekonomiska cyberbrottsligheten. Den stod för uppskattningsvis 2,4 miljarder USD i justerade förluster 2021, vilket motsvarar mer än 59 % av de fem största förlusterna på grund av internetbrott globalt.[20] För att förstå problemets omfattning och hur användarna bäst kan skyddas mot BEC har Microsofts säkerhetsforskare tagit reda på vilka teman som är vanligast förekommande vid angreppen.

BEC-teman (januari–juni 2022)



BEC-teman som procent av förekomsterna

BEC-trender

BEC-angriparna försöker normalt först börja prata med potentiella offer för att få god kontakt. Angriparen utger sig för att vara en kollega eller affärsbekant och leder gradvis in samtalet på en penningöverföring. Introduktionsmeddelandet, som vi ser är ett BEC-lockbete, representerar nästan 80 procent av de identifierade BEC-e-postmeddelandena. Andra trender som Microsofts säkerhetsforskare har identifierat under det senaste året är till exempel:

- De vanligaste metoderna som observerades vid BEC-angrepp 2022 var förfalskning[21] och personifiering.[22]
- Den BEC-undertyp som orsakade störst ekonomisk skada för offren var fakturabedrägerier (baserat på volym och de begärda belopp som vi såg i våra BEC-kampanjundersökningar).
- Stöld av affärsinformation som leverantörsreskontrarapporter och kundkontakter möjliggör för angriparen att begå övertygande fakturabedrägerier.
- De flesta förfrågningar om att löner ska skickas någon annanstans kom från kostnadsfria e-posttjänster och sällan från knäckta konton. E-postvolymen från de källorna hade toppar runt den första och femtonde i varje månad, de vanligaste lönedatumen.
- Trots att de är välkända sätt att begå bedrägeri utgjorde presentkortsbedrägerier endast 1,9 % av de BEC-angrepp som upptäcktes.

Användbara insikter

Försvar mot nätfiske

För att minska organisationens nätfiskeexponering bör IT-administratören införa följande policyer och funktioner:

1. Kräv användning av MFA för alla konton för att begränsa obehörig åtkomst.
2. Aktivera funktioner för villkorsstyrd åtkomst till konton med mycket hög behörighet för att blockera åtkomst från länder, regioner och IP-adresser som vanligtvis inte genererar trafik i organisationen.
3. Överväg att låta chefer, anställda som deltar i betalnings- eller inköpsaktiviteter och andra konton med hög behörighet använda fysiska säkerhetsnycklar.
4. Använd webbläsare som stöder tjänster som Microsoft SmartScreen för att analysera om webbadresser är suspekta och blockera åtkomst till kända skadliga webbplatser.[23]
5. Använd en maskininlärningsbaserad säkerhetslösning som karantänsätter sannolika nätfiskeförsök och öppnar webbadresser och bilagor i en isolerad miljö innan e-posten når inkorgen, t.ex. Microsoft Defender för Office 365.[24]
6. Använd skyddsfunktioner mot personifiering och förfalskning i hela organisationen.
7. Konfigurera policyer för DomainKeys Identified Mail (DKIM) och Domain-based Message Authentication Reporting & Conformance (DMARC) för att förhindra leverans av icke autentiserade e-postmeddelanden som kan försöka förfalska riktiga avsändare.
8. Granska klienters och användares skapade tillåt-regler och ta bort breda domän- och IP-baserade undantag. De här reglerna har ofta företräde och kan släppa in kända skadliga e-postmeddelanden via e-postfiltrering.
9. Kör nätfiskesimulatorer regelbundet för att mäta den potentiella risken i hela organisationen och för att identifiera och utbilda sårbara användare.

Länkar till mer information

- From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud | Microsoft 365 Defender Research-teamet, Microsoft Threat Intelligence Center (MSTIC)

Homoglyfbedrägeri

BEC och nätfiske är vanliga tekniker för social manipulering. Social manipulering är viktigt för brottslingar och övertygar offer om att interagera med brottslingar genom att vinna dennas förtroende.

I fysisk handel används varumärken för att säkra förtroendet för en produkts eller tjänsts ursprung, och förfalskade produkter är ett missbruk av varumärket. På samma vis låtsas cyberbrottslingar vara en kontakt som offret är bekant med vid ett nätfiskeangrepp och använder homoglyfer för att lura potentiella offer.

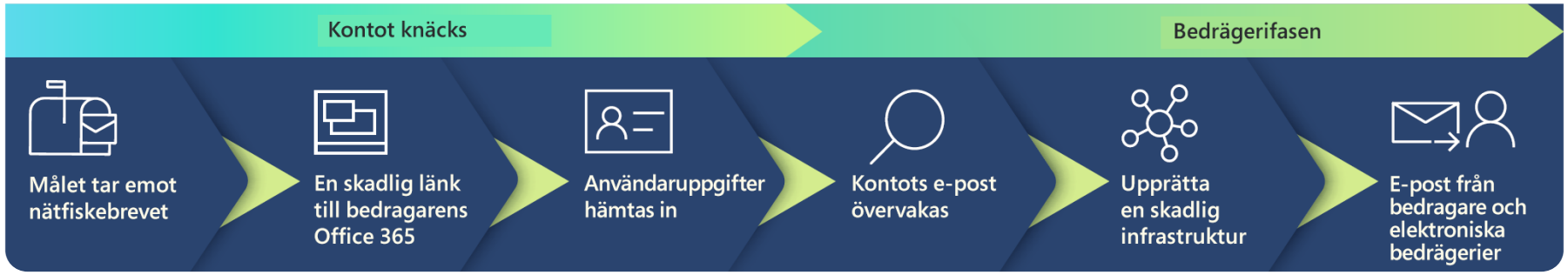
En homoglyf är ett domännamn som används för e-postkommunikation i BEC, där ett tecken ersätts med ett som är identiskt eller nästan identiskt till utseendet för att lura målet.

Homoglyfmetoder som används vid BEC-försök

BEC består i allmänhet av två faser, varav den första innebär att autentiseringsuppgifter knäcks. Dessa typer av läckage av autentiseringsuppgifter kan vara ett resultat av nätfiskeangrepp eller stora dataintrång. Autentiseringsuppgifterna säljs eller handlas sedan på den mörka webben.

Den andra fasen är bedrägerifasen, då angriparen använder knäckta autentiseringsuppgifter för att ägna sig åt avancerad social manipulering med hjälp av e-postdomäner som innehåller homoglyfer.

Ett BEC-angrepps förlopp



Metod	Andel domäner som nyttjar homoglyfmetoden
Byt I mot l	25 %
Byt l mot i	12 %
Byt g mot q	7 %
Byt m mot rn	6 %
Byt .com mot .cam	6 %
Byt o mot 0	5 %
Byt l mot ll	3 %
Byt i mot ii	2 %
Byt w mot vv	2 %
Byt ll mot l	2 %
Byt a mot e	2 %
Byt m mot nn	1 %
Byt I mot ll, byt i mot l	1 %
Byt u mot o	1 %

En analys av över 1 700 homoglyfdomäner mellan januari och juli 2022. 170 homoglyfmetoder användes, men 75 % av domänerna nyttjade bara 14 metoder.

En homoglyf i aktion

En homoglyfdomän som ser likadan ut som en e-postdomän som offret känner igen registreras hos en e-postleverantör med ett identiskt användarnamn. Ett kapat e-postmeddelande skickas sedan från den kapade domänen med nya betalningsanvisningar.

Genom att utnyttja öppna underrättelsekällor och tillgång till e-posttrådar söker brottslingen upp personer med ansvar för fakturering och betalningar. Sedan skapar de en personifiering av en e-postadress för den person som skickar fakturor. Personifieringen består av ett identiskt användarnamn och en e-postdomän som är en homoglyf för den äkta avsändaren.

Angriparen kopierar en e-postkedja med en legitim faktura och ändrar sedan fakturan så att den innehåller angriparens egna bankuppgifter. Den nya, ändrade fakturan skickas sedan igen från homoglyfpersonifieringen till offret. Eftersom sammanhanget är rimligt och e-postmeddelandet ser äkta ut följer offret många gånger instruktionerna i bedrägerimeddelandet.

Användbara insikter

1. Använd webbläsare som stöder tjänster för att analysera om webbadresser är suspekta och blockera åtkomsten till kända skadliga webbplatser, t.ex. Säkra länkar och SmartScreen.[25]
2. Använd en maskininlärningsbaserad säkerhetslösning som karantänsätter sannolika nätfiskeförsök och öppnar webbadresser och bilagor i en isolerad miljö innan e-posten når inkorgen.

Länkar till mer information

- Internet Crime Complaint Center (IC3) | Intrång i företags e-post: En bluff värd 43 miljarder dollar
- Spoof intelligence insight – Office 365 | Microsoft Docs
- Impersonation insight – Office 365 | Microsoft Docs

En tidslinje med botnätangrepp från Microsofts tidiga samarbeten

I mer än ett decennium har DCU arbetat proaktivt med att stoppa cyberbrottslighet, vilket har resulterat i att 26 skadliga program och nationalstater har stoppats. I takt med att DCU-teamet använder alltmer avancerade taktiker och verktyg för att stänga ner olagliga verksamheter, märker vi att cyberbrottslingarna också utvecklar sina metoder för att försöka ligga steget före. Här är en tidslinje som visar ett urval av de botnät som DCU har satt stopp för och de strategier som Microsoft använde för att stänga ner dem.

2008

Conficker-botnätet

Beskrivning: En mask spred sig snabbt och var inriktad på Windows. Den infekterade miljontals datorer och enheter i samma nätverk och orsakade nätverksavbrott över hela världen.

Samarbete: Bildandet av Conficker Working Group, det första konsortiet i sitt slag. Microsoft samarbetade med 16 organisationer över hela världen för att besegra boten.

Microsofts insats: Gruppen samarbetade i många länder och lyckades stänga ner Conficker.

2009

Waledac-botnätet

Beskrivning: Ett komplext spambotnät med amerikanska domäner som samlade in e-postadresser och distribuerade spam som smittade upp till 90 000 datorer över hela världen.[26]

Samarbete: Ett annat konsortium, Microsoft Malware Protection Center (MMPC), skapades med fokus på nära samarbete med akademiker.[27]

Microsofts insats: Microsoft använde en nivåindelad störningsstrategi för C2 och överraskade aktörerna genom att ta domäner i USA i beslag utan föregående meddelande.[28] Microsoft tilldelades tillfälligt ägarskapet av nästan 280 domäner som används av Waledacs servrar.

2011

Microsoft Digital Crimes Unit bildas

Samarbete: Utformat av ett samspelt team av utredare, jurister och tekniker för att förhindra cyberbrott som påverkar Microsofts ekosystem.

Microsofts metod: Målet är att förstå de tekniska aspekterna av olika varianter av skadlig kod bättre och förmedla insikterna till Microsofts jurister för att utveckla en effektiv avbrottsstrategi.

2013

Rustock-botnätet

Beskrivning: En bakdörrstrojan som skickade skräppost via e-post med internetleverantörer som primära C2:or; utformad för att sälja läkemedel.

Samarbete: Microsoft samarbetade med Pfizer Pharmaceuticals för att förstå de läkemedel som Rustock sålde och samarbetade nära med nederländska myndigheter.[29]

Microsofts insats: Microsoft samarbetade med amerikansk och nederländsk polis för att stänga ner C2-servrarna i landet. Registrerade och blockerade alla framtida domängeneratoralgoritmer.

Sirefef/Zero Access-botnätet

Beskrivning: Ett reklambotnät som var utformat för att dirigera människor till farliga webbplatser och installera skadlig kod eller stjäla personlig information, infekterade mer än två miljoner datorer och kostade annonsörer mer än 2,7 miljoner USD per månad, främst i USA och Västeuropa.

Samarbete: Nära samarbete med FBI och Europols Cybercrime Center för att få omkull peer-to-peer-infrastrukturen.

Microsofts insats: Gick med i Zero Access-nätverket, ersatte de kriminellas C2-servrar och lyckades ta över serverdomäner för nedladdning.

2019

Trickbot-botnätet

Beskrivning: Ett avancerat botnät med fragmenterad infrastruktur över hela världen som riktade in sig på branschen för finansiella tjänster och bröt sig in i IoT-enheter.

Samarbete: Microsoft samarbetade med Financial Services Information Sharing and Analysis Center (FS-ISAC) för att stänga ner Trickbot.[30]

Microsofts insats: DCU byggde ett system för att identifiera och spåra botinfrastruktur och genererade aviseringar till aktiva internetleverantörer. Hänsyn togs till specifika lagar i olika länder.

2022

Fortsatt fokus på störningar

Beskrivning: Microsoft störde infrastrukturen för sju hotaktörer under det senaste året, vilket hindrade dem från att distribuera ytterligare skadlig kod, styra offrens datorer och rikta in sig på ytterligare offer.

Samarbete: I samarbete med internetleverantörer, nationella myndigheter, polis och den privata industrin delade Microsoft information för att hjälpa över 17 miljoner offer för skadlig kod i hela världen.

I framtiden

DCU fortsätter att utvecklas och arbetar för att använda sin erfarenhet av att störa botnät till att utföra samordnade åtgärder som sträcker sig längre än till bara skadlig kod. Våra fortsatta framgångar kräver kreativ teknik, utbyte av information, innovativa juridiska teorier och offentliga och privata partnerskap.

Cyberbrottslingars missbruk av infrastruktur

Internetgatewayer som kriminella kommando- och kontrollinfrastrukturer

IoT-enheter har blivit ett allt mer populärt mål för cyberbrottslingar som använder utbredda botnät. Om routrarna inte har korrigerats och lämnas exponerade direkt mot internet kan hotaktörer missbruka dem för att få tillgång till nätverk, utföra skadliga angrepp och till och med stödja sin egen verksamhet.

Microsoft Defender for IoT-teamet forskar på utrustning som varierar från äldre industriella styrsystem till toppmoderna IoT-sensorer. Teamet undersöker IoT- och OT-specifik skadlig kod för att bidra till listan med intrångsindikatorer.

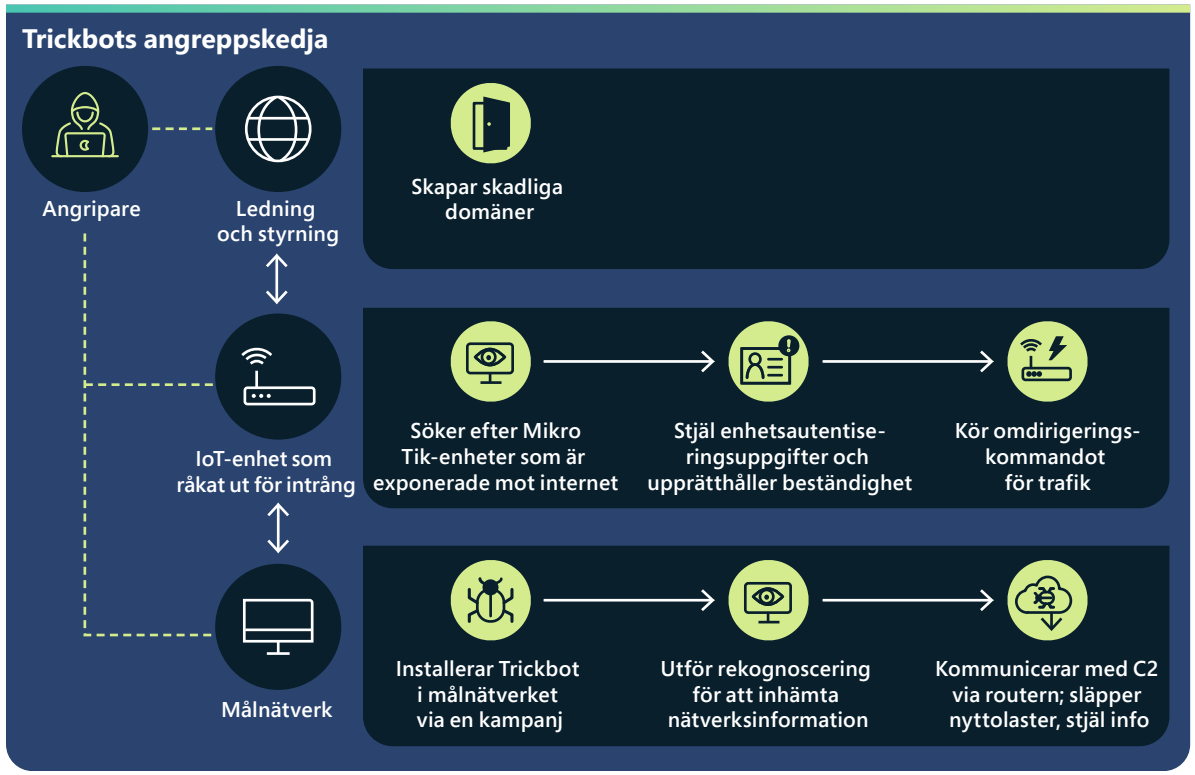
Routrar är särskilt sårbara attackvektorer eftersom de finns överallt i internetanslutna hem och organisationer. Vi har spårat aktiviteten på MikroTik-routrar, en populär router runt om i världen i hem och på företag. Vi har identifierat hur de används för styrning och kontroll (C2), DNS-angrepp och kapning av mining av kryptovaluta.

Mer specifikt identifierade vi hur Trickbot-operatörer använder knäckta MikroTik-routrar och konfigurerar om dem så att de införlivas i deras C2-infrastruktur. Trickbots missbruk av de här enheterna förvärras av att de är så populära och deras unika maskin- och programvara gör att hotaktörerna kan kringgå traditionella säkerhetsåtgärder, utöka sin infrastruktur och bryta sig in i fler enheter och nätverk.



Exponerade routrars potentiella sårbarheter kan utnyttjas.

Genom att spåra och analysera trafik med SSH-kommandon (Secure Shell) observerade vi angripare som använde MikroTik-routrar för att kommunicera med Trickbots infrastruktur efter att ha fått tag på legitima autentiseringsuppgifter till enheter. Autentiseringsuppgifterna kan erhållas genom råstyrkeattacker, utnyttjande av kända sårbarheter med lättillgängliga korrigeringsfiler samt standardlösenord. När en enhet används utfärdar angriparen



Trickbots angreppskedja som visar användningen av MikroTik IoT-enheter som proxyservrar för C2.

ett unikt kommando som dirigerar om trafiken mellan två portar i routern och inrättar kommunikationslinjen mellan Trickbot-påverkade enheter och C2.

Vi har sammanställt vår kunskap om de olika metoderna för att angripa MikroTik-enheter utöver enbart Trickbot samt kända vanliga sårbarheter och exponeringar i ett verktyg med öppen källkod för MikroTik-enheter, som kan extrahera de kriminaltekniska artefakter som rör angrepp på dessa enheter.[31]

Enheter som agerar omvänd proxy för skadlig C2-kod är inte bara unika för Trickbot- och MikroTik-routrar. I samarbete med Microsoft RiskIQ-teamet hittade vi tillbaka till den inblandade C2-enheten och genom att identifiera SSL-certifikat identifierade vi Ubiquiti- och LigoWave-enheter som även de är utsatta.[32] Det här är en tydlig indikation på att IoT-enheter håller på att bli aktiva komponenter i nationalstaters samordnade angrepp och ett populärt mål för cyberbrottslingar som använder utbredda botnät.

Kryptobrottslingar missbrukar IoT-enheter

Gatewayenheter är ett allt mer värdefullt mål för hotaktörer, eftersom antalet kända sårbarheter kontinuerligt har ökat från år till år. De används för mining av kryptovaluta och andra typer av skadlig aktivitet.

I takt med att kryptovalutorna har blivit alltmer populära har många personer och organisationer investerat beräkningskraft och nätverksresurser från enheter som routrar till mining av kryptovalutor i blockkedjan. Men mining av kryptovaluta är en tids- och resursintensiv process med låg sannolikhet att lyckas. För att öka sannolikheten att lyckas med miningen samlas program för brytning av kryptovaluta i distribuerade samarbetsnätverk och tar emot hashvärden i förhållande till den andel av kryptovalutan som de har lyckats bryta med sina anslutna resurser.

Under det senaste året har Microsoft observerat ett växande antal angrepp som missbrukar routrar för att dirigera om mining av kryptovaluta. Cyberbrottslingar bryter sig in i routrar som är anslutna till miningpooler och dirigerar om miningtrafiken till deras IP-adresser med DNS-förgiftningsangrepp, vilket ändrar DNS-inställningarna för de angripna enheterna. De berörda routrarna registrerar fel IP-adress för ett visst domännamn och skickar sina miningresurser – eller hashar – till pooler som används av hotaktörer. De poolerna kan sedan användas för anonym mining av kryptovaluta till kriminella aktiviteter eller använda legitima hashvärden som genereras av programmen för mining av kryptovaluta för att förvärva en andel av den brutna kryptovalutan och på så sätt skörda frukterna av arbetet.

Eftersom fler än hälften av alla kända sårbarheter som hittades 2021 inte har korrigerats är det väldigt svårt att uppdatera och säkra routrar i företagsnätverk och privata nätverk för enhetsägare och administratörer.

Enhetsintrång för olaglig mining av kryptovaluta.



En del av hasharna från den ursprungliga poolen stjäls av hotaktörer, eller så överförs resurser till deras pool, eller så har routrar skadlig kod som stjäl resurser för mining.

DNS-förgiftning av gatewayenheter stör legitim mining och omdirigerar resurser till kriminell mining av kryptovaluta.

Virtuella maskiner som kriminell infrastruktur

Alla flyttar till molnet. Det gäller även cyberbrottslingar, som utnyttjar ovetande offers privata tillgångar genom nätfiske eller distribution av skadlig kod som stjäl autentiseringsuppgifter. Många cyberbrottslingar väljer att konfigurera sin skadliga infrastruktur på molnbaserade virtuella maskiner, i programbehållare och mikrotjänster.

När cyberbrottslingen har fått åtkomst kan en rad händelser inträffa för att skapa infrastrukturen – till exempel ett antal virtuella maskiner genom skript och automatiserade processer. De skriptade, automatiserade processerna används för att inleda skadlig aktivitet, däribland storskaliga skräppostangrepp, nätfiskeangrepp och illasinnade webbsidor. Det kan till och med omfatta konfiguration av en uppskalad virtuell miljö för mining av kryptovaluta och då kan offret få en räkning på hundratusentals dollar mot slutet av månaden.

Cyberbrottslingarna inser att de inte har all tid i världen innan de upptäcks och kastas ut. Därför har de skalat upp och arbetar nu proaktivt med oförutsedda händelser i åtanke. De har observerats förbereda knäckta konton i förväg och övervaka sina miljöer. Så snart ett konto (som har upprättats med hundratusentals virtuella maskiner) upptäcks går de till nästa konto – som redan har förberetts för omedelbar aktivering av skript – och deras skadliga aktivitet löper vidare med bara ett kort eller inget avbrott.

Precis som molninfrastrukturen kan lokal infrastruktur användas vid angrepp med virtuella lokala miljöer som är okända för den lokala användaren. Det kräver att den första åtkomstpunkten förblir öppen och tillgänglig. Lokala privata tillgångar har också missbrukats av cyberbrottslingar för att starta en framåtriktad molninfrastrukturkedja, som inrättas för att dölja deras ursprung för att undvika att suspekt infrastruktur upptäcks.

Användbara insikter

1. Inför god cyberhygien och utbilda medarbetarna om cybersäkerhet med råd så att de undviker social manipulering.
2. Genomför regelbundna automatiska kontroller av avvikande användaraktivitet genom storskaliga identifieringar för att minska de här typerna av angrepp.
3. Uppdatera och säkra routrar i företagsnätverk och privata nätverk.

Är hacktivismen här för att stanna?

Hacktivism är visserligen inte ett helt nytt fenomen, men på grund av kriget i Ukraina tillkom en hel mängd frivilliga. En del av dem tar order från länders myndigheter för att distribuera cyberverktyg och skada politiska motståndares, organisationers och till och med hela länders rykte eller tillgångar.

I februari 2022 uppmanade den ukrainska regeringen privatpersoner över hela världen att genomföra cyberattacker mot Ryssland som del av landets 300 000 man starka "IT-armé".[33] Samtidigt började etablerade hacktivistgrupper som Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans och RaidForum2 utföra attacker till stöd för Ukraina. Andra grupper, däribland en del av utpressningstrojangänget Conti, ställde sig på Rysslands sida.[34]

Under de följande månaderna var Anonymous aktiviteter mycket synliga. Hackare som agerade i gruppens namn – eller i något av dess anknutna organisationers namn – slog tillfälligt ut tusentals ryska och belarusiska webbplatser, läckte hundratals gigabyte stulna data, hackade ryska TV-kanaler så att de sände ut proukrainskt material och erbjöd sig till och med att betala Bitcoin för ryska stridsvagnar som överlämnades.

Uppkomsten av medborgarhackare

Sociala medier gjorde det möjligt för tusentals tilltänkta medborgarhackare att organisera och mobilisera sig snabbt och de fick också anvisningar om hur de skulle kunna genomföra angrepp enkelt, till exempel DDoS-angrepp. Organisatörerna använde Twitter, Telegram och privata forum för att samla hackare, organisera verksamheten och sprida hackinginstruktionsböcker.

Men de flesta av de här hackarna har sannolikt begränsade kunskaper, även om de får instruktioner. Det tyder på två potentiella framtidsscenarier: ett där hundratals eller tusentals individer med endast grundläggande teknisk kunskap använder angreppsmallar för att genomföra framtida samordnade eller enskilda hacktivistangrepp mot mål, och ett annat där slutet på striderna i Ukraina får dem att lämna hacktivismen bakom sig, åtminstone tills nästa politiska eller sociala fråga inspirerar dem att handla.

Politisering av hackare

Den stora risken med den politiska mobiliseringen är användningen av tekniskt kunniga hackare som kan fortsätta att genomföra cyberattacker mot myndighetsmål i utlandet för att stödja sina egna nationella prioriteringar, antingen på eget initiativ eller på uppmaning av den egna staten.

Iran, Kina och Ryssland använder redan hacktivism som utgångspunkt för rekrytering till landets hackningsgrupper. I april 2022 lanserade den proryska hackningsgruppen Killnet DDoS-angrepp mot tjeckiska järnvägar, regionala flygplatser och Tjeckiens civilförsvarsserver, trots att Tjeckien inte är direkt inblandat i kriget.[35] Samtidigt kan vissa länder nyttja hacktivism som täckmantel för traditionellt cyberspionage eller sabotageverksamhet – till exempel iransk verksamhet mot Israel.

I en miljö med alltfler DDoS-angrepp som går att koppla till hacktivism utmanas teknikindustrin att snabbt dechiffrera skillnaden mellan normalt och onormalt trafikflöde till en webbplats. Microsoft och dess partner har utvecklat ett antal verktyg som särskiljer skadlig DDoS-trafik och spårar den tillbaka till sitt ursprung. Dessutom kan Microsoft Azure-plattformen identifiera maskiner på plattformen som producerar osedvanligt höga nivåer av utgående trafik och stänga ned dem.

Framväxten av protestprogram

Protestprogram har uppkommit som ett direkt resultat av känslomässiga reaktioner på kriget mellan Ryssland och Ukraina. Vissa utvecklare av program med öppen källkod använde sin programvaras popularitet som ett sätt att förmedla sitt budskap eller vidta åtgärder mot en pågående geopolitisk situation. Det här omfattade ofarliga textfiler som öppnades på en dator eller i en webbläsare för att sprida fredsmeddelanden, men även riktade angrepp baserade på IP-adressgeolokalisering och destruktiva åtgärder som att tömma en hårddisk. När andra globala händelser inträffar kan vi vänta oss att protestprogrammen kommer att dyka upp igen. Eftersom det i allmänhet handlar om fall där välrenommerade personer som sköter om öppen källkod bestämmer sig för att göra personliga uttalanden med hjälp av sina egna komponenter med öppen källkod, finns det för närvarande inget skydd som hindrar de här typerna av ändringar från att ske i källfilspaketen och därför bör användarna vara medvetna om potentiella effekter.

Sociala medier gjorde det möjligt för tusentals tilltänkta medborgarhackare att organisera och mobilisera sig snabbt och de fick också anvisningar om hur de skulle kunna genomföra angrepp enkelt, till exempel DDoS-angrepp.

Användbara insikter

1. Teknikindustrin måste samarbeta för att utforma ett heltäckande svar på det här nya hotet.
2. Ledande teknikföretag, däribland Microsoft, har verktyg för att identifiera skadlig trafik som förknippas med DDoS-angrepp och inaktivera de ansvariga maskinerna.
3. De som använder öppen källkod bör hålla extra koll när det råder geopolitiska stridigheter.

Slutnoter

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. Identifiering och reaktion på slutpunkter. 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. Ett forum med urval är ett diskussionsforum på nätet som kräver att en befintlig medlem går i god för en ny medlem som läggs till.
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. Datakälla: Defender för Office (skadlig e-post/aktivitet med knäckta identiteter), Azure Active Directory Identity Protection (händelser som rör/varningar om knäckta identiteter), Defender for Cloud Apps (dataåtkomsthändelser med knäckta identiteter) och M365D (korrelation mellan olika produkter).
17. Datakälla: Defender for Endpoint (varningar/händelser som rör attackbeteenden), Defender for Office (skadlig e-post) och M365D (relationer mellan produkter).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Domänbaserad meddelandeautentisering, rapportering och överensstämmelse: ett protokoll för e-postautentisering, policyer och rapporter som har utformats för att ge ägare till e-postdomäner möjlighet att skydda sin domän från obehörig användning.
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 mot John Doe 1–27, m.fl., nr 1:10CV156, (E.D.Va. 22 feb 2010).
27. Se Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27 sep 2011.
28. Närmare bestämt tillåter artikel 65 i de federala reglerna för civilprocesser en part att söka en sådan åtgärd om 1) parten kommer att lida omedelbar och irreparabel skada om hjälp inte ges och 2) parten försöker meddela den andra parten i god tid. Dessutom kräver lagen att ett avvägningstest tillämpas, ett som väger av svarandens rätt till förhandsbesked och vilken skada allmänheten kan lida.
29. Microsoft Corporation mot John Doe 1–11, m.fl., nr 2:11cv222, (W.D. Wa. 9 feb 2011).
30. Microsoft Corp. mot Doe, nr 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, den *1 (E.D. Va. 12 aug 2021).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
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

Hot från nationalstater

Nationella statsaktörer inleder alltmer avancerade cyberattacker för att undvika upptäckt och främja sina strategiska prioriteringar.

En översikt över hot från nationalstater 31
Introduktion 32
Bakgrund till nationalstatsdata 33
Exempel på nationella statsaktörer och deras verksamhet 34
Den föränderliga hotbilden 35
IT-försörjningskedjan som en inkörsport till det digitala ekosystemet 37
Snabbt utnyttjande av sårbarheter 39
Ryska statliga aktörers cybertaktik i krigstid hotar Ukraina och andra 41
Kina utökar de globala angreppen för att få konkurrensfördelar 44
Iran blir alltmer aggressivt efter maktskiftet 46
Nordkoreas cyberkapacitet används för att uppnå regimens tre huvudsakliga mål 49
Cyberlegoknektar hotar stabiliteten i cyberrymden 52
Organisera cybersäkerhetsnormer för fred och säkerhet i cyberrymden 53

En översikt över

hot från nationalstater

Nationella statsaktörer inleder alltmer avancerade cyberattacker för att undvika upptäckt och främja sina strategiska prioriteringar. Insatsen med cybervapen i hybridkriget i Ukraina är början för en ny era av konflikter.

Ryssland har också stöttat sitt krig genom informationspåverkan med hjälp av propaganda för att påverka opinionen i Ryssland, Ukraina och globalt. Den här första fullskaliga hybridkonflikten har också gett oss andra viktiga lärdomar. För det första är det bästa sättet att skydda digital drift och data – både i cyberrymden och i verkligheten – att flytta ut i molnet. De första ryska angreppen riktades mot lokala tjänster med skadlig kod som rensade lagring och en av de första missilerna som skickades iväg riktades mot fysiska datacenter.

Ukraina reagerade genom att snabbt flytta arbetsbelastningar och data till moln i hyperskala i datacenter utanför Ukraina. För det andra har framsteg inom cyberhotsunderrättelseverksamheten och slutpunktsskydd med understöd av data och avancerade AI- och ML-tjänster i molnet hjälpt Ukraina att försvara sig mot ryska cyberattacker.

På annat håll har nationella statsaktörer ökat sin aktivitet och använder framsteg inom automatisering, molninfrastruktur och fjärråtkomst för att angripa en bredare uppsättning mål. Företags IT-försörjningskedjor som ger tillgång till slutmålen angreps ofta. Cybersäkerhetshygien har blivit ännu viktigare, eftersom aktörerna snabbt utnyttjar oupptäckta sårbarheter, använder både avancerade metoder och råstyrkemetoder för att stjäla autentiseringsuppgifter och döljer sin verksamhet genom att använda programvara med öppen källkod eller legitim programvara. Och Iran gör som Ryssland och använder destruktiva cybervapen, däribland utpressningstrojaner, som stapelvara i sina attacker.

Den här utvecklingen kräver att världen snabbt implementerar ett konsekvent och globalt ramverk som prioriterar mänskliga rättigheter och skyddar människor från staters besinningslösa beteenden på nätet. Alla länder måste samarbeta för att införa överenskomna normer och regler för ansvarsfullt nationalstatsbeteende.

Defending Ukraine: Early Lessons from the Cyber War – Microsoft On the Issues

Ökad inriktning på kritisk infrastruktur, särskilt IT-sektorn, finansiella tjänster, transportsystem och kommunikationsinfrastruktur.

Läs mer på s. 35

IT-försörjningskedjan används som en port för att komma åt mål.

NOBELIUM

Läs mer på s. 36

Kina utökar sin globala inriktning särskilt på mindre nationer i Sydostasien för att få underrättelser och konkurrensfördelar.

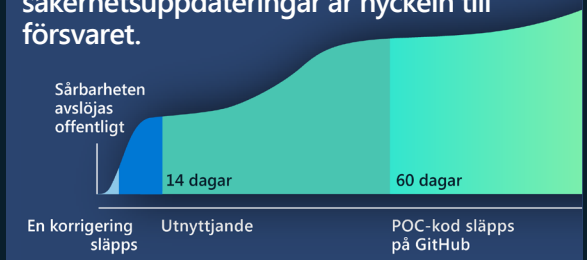


Läs mer på s. 44

Iran blev alltmer aggressivt efter maktskiftet, utökade angreppen med utpressningstrojaner bortom sina regionala motståndare till offer i USA och EU, samt riktade in sig på högprofilerad amerikansk, kritisk infrastruktur.

Läs mer på s. 46

Identifiering och snabbt utnyttjande av okorrigerade sårbarheter har blivit en viktig taktik. Snabb installation av säkerhetsuppdateringar är nyckeln till försvaret.



Läs mer på s. 39

Nordkorea riktade in sig på försvars- och rymdföretag, kryptovaluta, nyhetskanaler, avhoppare och hjälporganisationer för att uppnå regimens mål: att bygga upp sitt försvar, stärka ekonomin och säkerställa stabiliteten i landet.

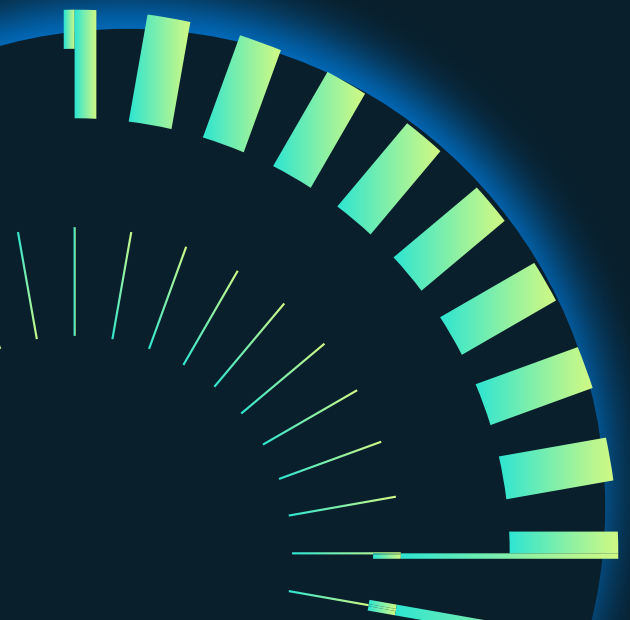
Läs mer på s. 49

Cyberlegoknektar hotar stabiliteten i cyberrymden eftersom den här växande industrin av privata företag utvecklar och säljer avancerade verktyg, tekniker och tjänster så att kunderna (ofta länder) ska kunna bryta sig in i nätverk och enheter.

Läs mer på s. 52

Introduktion

Efter uppmärksammade angrepp 2020 och 2021 lade nationella statsaktörer ned betydande resurser på att anpassa sig till nya säkerhetsskydd som hade införts av organisationer för att försvara sig mot avancerade hot.



Precis som storföretag började brottslingarna använda nya framsteg inom automatisering, molninfrastruktur och fjärråtkomstteknik för att utöka sina angrepp mot en bredare uppsättning mål. De här taktiska justeringarna ledde till nya metoder och storskaliga angrepp mot företagens försörjningskedjor. IT-säkerhetshygienen fick ännu större betydelse, eftersom aktörer utvecklade nya sätt att snabbt utnyttja oupptäckta sårbarheter, utöka sina metoder för att ta sig in i företagsnätverk och dölja sin verksamhet med hjälp av öppen källkod eller legitim programvara. Nya angreppsmetoder gav nya och mer svårupptäckta sätt att få tillgång till ett måls nätverk. Och när de fysiska angreppen under kriget eskalerade fick cyberattacker en framträdande roll för den militära aktiviteten.

Konflikten i Ukraina visar med all önskvärd tydlighet hur cyberattacker utvecklas för att påverka världen parallellt med fysiska militära konflikter. Elsystem, telekomsystem, medier och annan kritisk infrastruktur utsattes alla för både fysiska angrepp och cyberattacker. Försök till nätverksintrång som ofta observerats som ett led i spionage och kampanjer för att exfiltrera information fokuserades under hybridkriget på destruktiva angrepp med skadlig kod mot kritiska infrastruktursystem. Genom att koppla systemens säkerhet till molnet kunde potentiellt förödande angrepp upptäckas och avbrytas tidigt.[1]

För första gången under en större cyberhändelse använde beteendedetekteringar som utnyttjar maskininlärning kända angreppsmönster för att lyckas identifiera och stoppa ytterligare angrepp utan förkunskap om den bakomliggande skadliga koden – redan innan någon människa var medveten om hoten. Vi bekräftade även värdet av att dela med oss av hotunderrättelser i realtid med dem som skyddar systemen och gav dem viktig information för att förutse och försvara sig mot aktiva angrepp.

Nationella statsaktörer runtom i världen fortsätter att utöka sin verksamhet på nya och gamla sätt. Kina, Nordkorea, Iran och Ryssland utförde alla angrepp mot Microsoft kunder. IT-tjänsternas försörjningskedja blev ett vanligt mål när aktörerna bytte fokus mot uppströmstjänster som kan vara åtkomstpunkter för flera organisationer. Det är troligt att aktörer kommer att fortsätta utnyttja betrodda relationer i företagens försörjningskedjor. Därför betonar vi vikten av omfattande efterlevnad av autentiseringsregler, noggranna korrigeringar och kontokonfiguration för fjärråtkomstinfrastruktur samt regelbundna granskningar av partnerrelationer för att verifiera deras autenticitet.

Nationella statsaktörer har, ungefär som utpressningstrojanangripare och andra kriminella, reagerat på ökad exponering genom att i större utsträckning rikta in sig på illa konfigurerade eller icke-korrigerade storföretagssystem (VPN-/VPS-infrastruktur, lokala servrar, extern programvara) och genomföra attacker så att säga ur hand i mun. Många använder skadlig kod som går att köpa och red team-verktyg med öppen källkod för att dölja sin illasinnade aktivitet.

För att proaktivt försvara sig mot alla avancerade aktörer har det därför blivit absolut nödvändigt att upprätthålla god IT-säkerhetshygien i grunden genom till exempel prioriterade korrigeringar, funktioner mot manipulering, verktyg för hantering av attackytor som RiskIQ som ger överblick över attackytan och multifaktorautentisering i hela företaget.

Nationella statsaktörer har också börjat använda utpressningstrojaner som taktik vid sina attacker. De återanvänder ofta skadlig kod som har skapats av kriminella när de angriper. Vi har sett aktörer från både Iran och Nordkorea utnyttja köpta utpressningstrojanverktyg för att skada utvalda system, ofta med kritisk infrastruktur, hos rivaler i regionen. Slutligen har vi också sett ett växande hot från cyberlegoknektar som utvecklar och säljer verktyg, metoder och tjänster för att göra det möjligt att utnyttja sårbara externa lösningar. De sofistikerade och smidiga angreppen från nationella statsaktörer kommer att fortsätta att utvecklas från år till år. Organisationer måste därför hålla sig underrättade om aktörernas förändringar och utveckla sitt försvar parallellt.

John Lambert
Corporate Vice President och Distinguished Engineer, Microsoft Threat Intelligence Center

Bakgrund till nationalstatsdata

Nationalstatshot är cyberhotaktiviteter som har sitt ursprung i ett visst land med den uppenbara avsikten att främja nationella intressen. Nationella statsaktörer utgör några av de mest avancerade och beständiga hot som våra kunder ställs inför, bland annat stöld av immateriella rättigheter, spionage, övervakning, stöld av autentiseringsuppgifter och destruktiva angrepp.

Vi investerar betydande resurser för att upptäcka, förstå och motverka dessa hot. När en organisation eller enskild kontoinnehavare är måltavla eller råkar ut för intrång genom observerade nationalstatsaktiviteter, levererar Microsoft en varning i form av en nationalstatsavisering (NSA) direkt till kunden, inklusive den information de behöver för att undersöka aktiviteten. I juni 2022 hade vi levererat över 67 000 NSA:er sedan vi började göra det 2018.

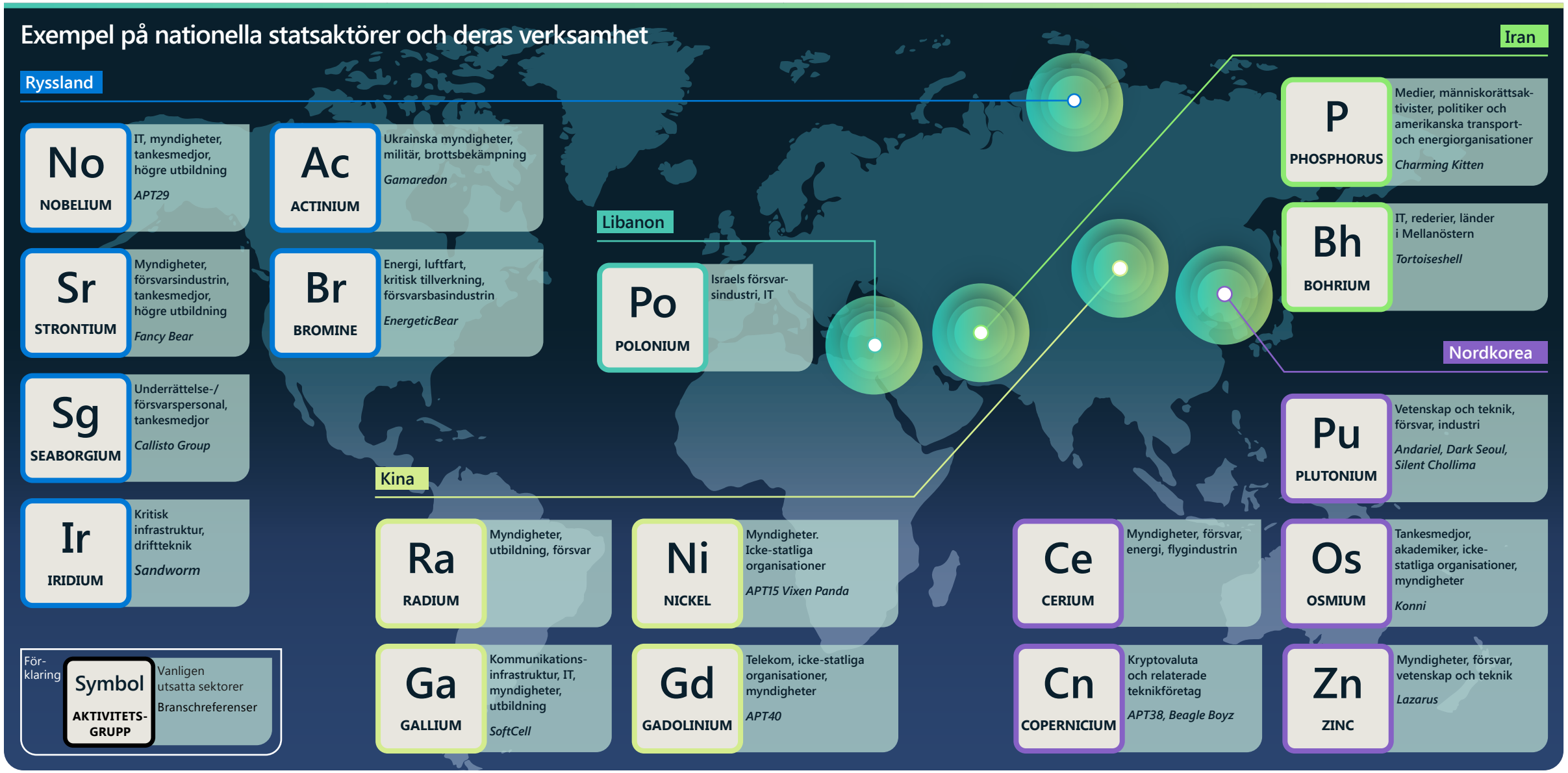
Microsofts NSA-data presenteras i det här kapitlet för att ge en bild av mätbar aktivitet. Den nivå på nationalstatsaktivitet som visas i diagrammen bygger på antalet NSA:er som Microsoft har utfärdat till kunder som svar på upptäckt av nationella statsaktörer som riktar in sig på eller bryter sig in i minst ett konto i kundorganisationen.



De fyra främsta nationalstaterna vars hotgrupper vi tar med i den här rapporten är Ryssland, Kina, Iran och Nordkorea. Från de ursprungsländerna kommer de mest uppmärksammade aktörer som har riktat in sig på Microsofts kunder under det senaste året. Rapporten innehåller också våra observationer om hotgrupper från Libanon och från cyberlegoknektar eller offensiva aktörer i den privata sektorn som hyr ut sina tjänster.

Microsoft identifierar nationalstatsgrupper med namn på grundämnen (t.ex. NOBELIUM), av vilka bara några visas på följande sida. Vi använder beteckningen DEV-##### som ett tillfälligt namn på ett okänt, framväxande eller föränderligt kluster med hotaktivitet, så att vi kan spåra det som en unik uppsättning information tills vi blir mycket säkra på ursprunget eller identiteten hos aktören bakom aktiviteten.

När det uppfyller kriterierna konverteras en DEV till en namngiven aktör eller slås samman med befintliga aktörer. I hela det här kapitlet nämner vi exempel på nationalstats- och DEV-grupper för att ge en djupare bild av angreppsmål, angreppsmetoder och analys av motiv. Även om många av grupperna använder samma verktyg som cyberbrottslingar, utgör de unika hot i form av skräddarsydd skadlig kod, förmågan att upptäcka och dra nytta av helt nya sårbarheter samt total straffrihet.


Exempel på nationella statsaktörer och deras verksamhet
Ryssland
No
NOBELIUM
IT, myndigheter, tankesmedjor, högre utbildning
APT29
Ac
ACTINIUM
Ukrainska myndigheter, militär, brottsbekämpning
Gamaredon
Sr
STRONTIUM
Myndigheter, försvarsindustrin, tankesmedjor, högre utbildning
Fancy Bear
Br
BROMINE
Energi, luftfart, kritisk tillverkning, försvarsbasindustrin
EnergeticBear
Sg
SEABORGIUM
Underrättelse-/försvarspersonal, tankesmedjor
Callisto Group
Ir
IRIDIUM
Kritisk infrastruktur, driftteknik
Sandworm
Libanon
Po
POLONIUM
Israels försvarsindustri, IT
Iran
P
PHOSPHORUS
Medier, människorättsaktivister, politiker och amerikanska transport- och energiorganisationer
Charming Kitten
Bh
BOHRIUM
IT, rederier, länder i Mellanöstern
Tortoiseshell
Nordkorea
Pu
PLUTONIUM
Vetenskap och teknik, försvar, industri
Andariel, Dark Seoul, Silent Chollima
Kina
Ra
RADIUM
Myndigheter, utbildning, försvar
Ni
NICKEL
Myndigheter. Icke-statliga organisationer
APT15 Vixen Panda
Ce
CERIUM
Myndigheter, försvar, energi, flygindustrin
Os
OSMIUM
Tankesmedjor, akademiker, icke-statliga organisationer, myndigheter
Konni
Ga
GALLIUM
Kommunikations-infrastruktur, IT, myndigheter, utbildning
SoftCell
Gd
GADOLINIUM
Telekom, icke-statliga organisationer, myndigheter
APT40
Cn
COPERNICIUM
Kryptovaluta och relaterade teknikföretag
APT38, Beagle Boyz
Zn
ZINC
Myndigheter, försvar, vetenskap och teknik
Lazarus
Förklaring
Symbol
AKTIVITETS-GRUPP
Vanligen utsatta sektorer
Branschreferenser

Den föränderliga hotbilden

Microsoft uppdrag att hålla reda på nationalstatsaktiviteter och meddela kunder när vi ser att de drabbas eller har råkat ut för intrång är rotat i vårt uppdrag att skydda våra kunder från angrepp.

Aviseringar är en viktig del av vårt arbete för att meddela kunderna om de observerade angreppen har förhindrats av våra säkerhetsprodukter eller om angreppen har genomförts på grund av okända säkerhetsbrister. Spårningsaviseringar hjälper Microsoft med tiden att hitta ändrade hottrender per aktör och fokusera produktskyddet på att proaktivt mildra hot mot kunder i våra molntjänster.

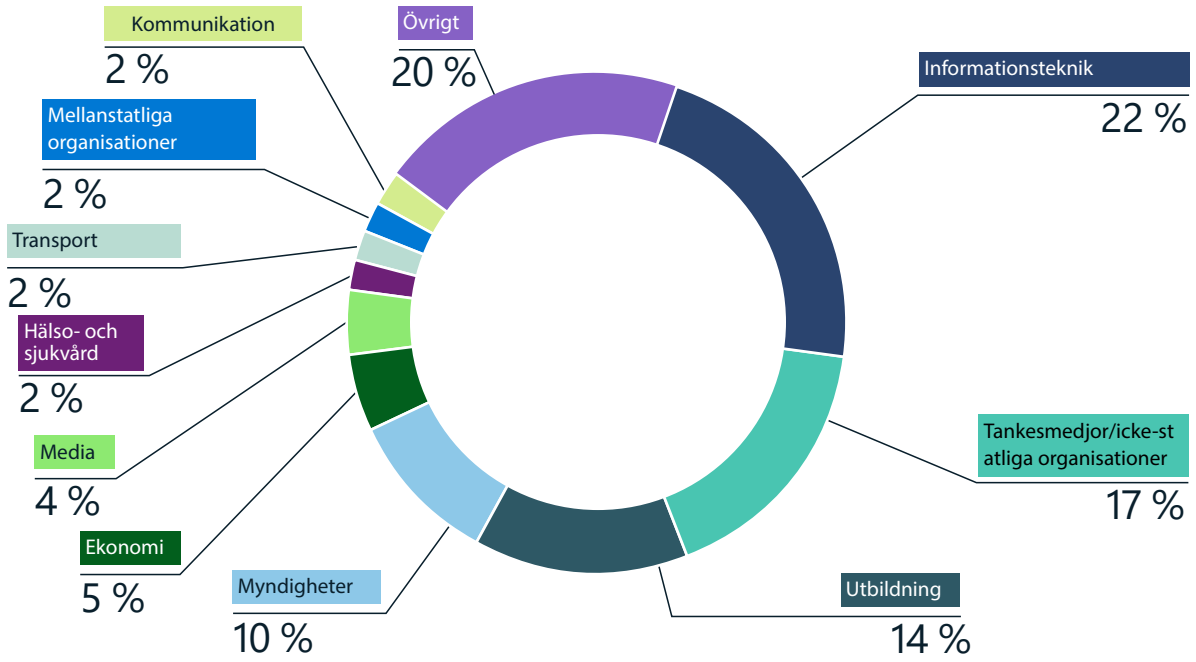
Spårningen hjälper oss också att dela med oss av data och insikter om det vi ser. Analytikerna som spårar aktörerna och följer deras angrepp förlitar sig på en kombination av tekniska indikatorer och geopolitisk expertis för att kunna förstå vad som motiverar aktörerna och kombinera tekniska och globala sammanhang till nya insikter. Den här datahanteringen ger en unik bild av nationalstataktörernas prioriteringar och hur deras motiv kan spegla de politiska, militära och ekonomiska prioriteringarna för de nationalstater som använder dem.

Den politiska utvecklingen under det senaste året har format prioriteringarna och risktoleransen hos statligt sponsrade hotgrupper i hela världen. I takt med att geopolitiska relationer har brutits ned och vissa länder blivit mer toppstyrda, har cyberaktörerna blivit mer orädda och aggressiva. Exempel:

- Ryssland kompletterade sina militära insatser på marken med obevekliga cyberattacker mot Ukrainas myndigheter och landets kritiska infrastruktur.[2]
- Iran sökte aggressivt vinna insteg i USA:s kritiska infrastruktur, t.ex. hamnmyndigheter.
- Nordkorea fortsatte sina ansträngningar för att stjäla kryptovaluta från finans- och teknikföretag.
- Kina utökade sin globala cyberspionageverksamhet.

Även om nationella statsaktörer kan vara tekniskt avancerade och använda en mängd olika taktiker, kan deras angrepp ofta dämpas genom god cyberhygien. Många av aktörerna förlitar sig på relativt lågteknologiska metoder, till exempel harpunfiskemeddelanden, för att leverera avancerad skadlig kod i stället för att investera i att utveckla anpassade intrångsmetoder eller använda riktad social manipulering för att uppnå sina mål.

Branschsektorer som nationella statsaktörer riktar in sig på



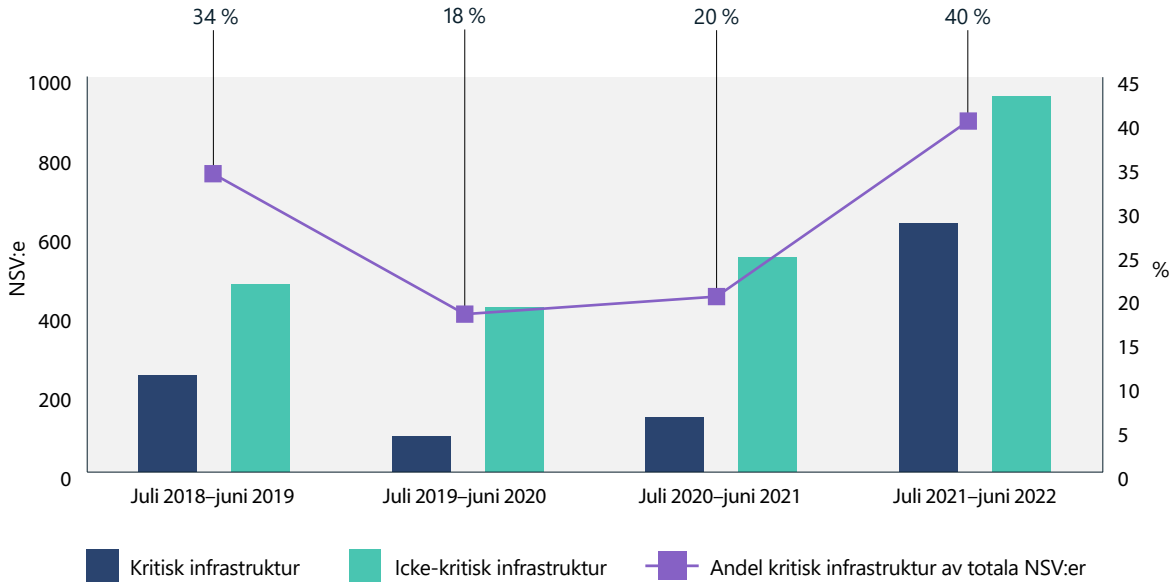
Nationalstatsgrupper riktade in sig på en rad sektorer. Ryska och iranska statliga aktörer riktade in sig på IT-branschen som ett sätt att få tillgång till IT-företagens kunder. Tankesmedjor, icke-statliga organisationer, universitet och myndigheter förblev andra vanliga mål för nationella statsaktörer.

Nationella statsaktörer har en mängd olika mål vilket kan resultera i att de riktar in sig på en specifik grupp av organisationer eller individer i taget. Under det senaste året har angreppen i försörjningskedjan ökat, med särskilt fokus på IT-företag. Genom att bryta sig in hos IT-tjänsteleverantörer kan hotaktörer ofta nå sitt ursprungliga mål genom en betrodd relation med företaget som hanterar uppkopplade system, eller kanske utföra angrepp i mycket större skala genom att bryta sig in hos hundratals kunder nedströms under ett angrepp. Efter IT-sektorn var det tankesmedjor, akademiker anknutna till universitet och myndighetspersoner som oftast råkade illa ut. De är önskvärda ”mjuka spionagemål” för att samla in information om geopolitiska frågor.

Den föränderliga hotbilden

fortsättning

Trender för kritisk infrastruktur

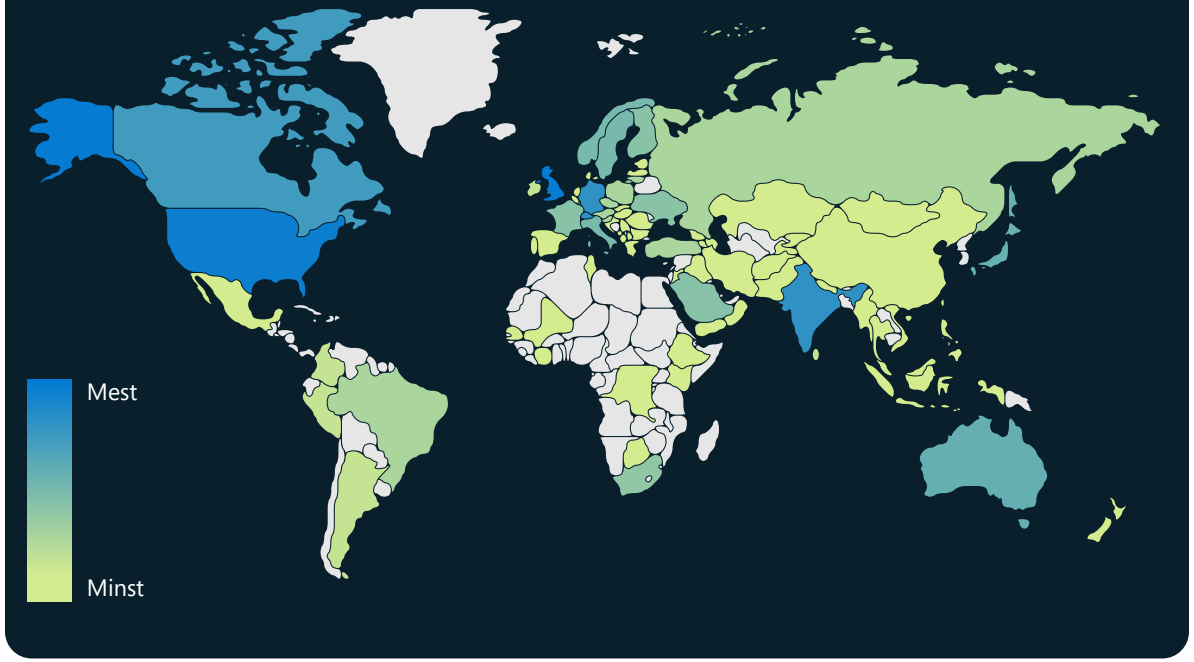


Nationalstatsgruppers inriktning på den kritiska infrastrukturen[3] ökade under det senaste året. Aktörerna fokuserade på företag inom IT-sektorn, finansiella tjänster, transportsystem och kommunikationsinfrastruktur.

"Före invasionen av Ukraina trodde många länder att data behövde bli kvar i landet för att vara trygga. Efter invasionen ses migrering av data till molnet och flyttar utanför landets gränser som god styrning och en del av återhämtningsplaneringen."

Cristin Flynn Goodwin,
Associate General Counsel, Customer Security & Trust

Nationella statsaktörers geografiska inriktning



Nationalstatsgruppers cyberinriktning sträckte sig över hela världen under förra året, med särskilt fokus på amerikanska och brittiska företag. Organisationer i Israel, Förenade Arabemiraten, Kanada, Tyskland, Indien, Schweiz och Japan var också några av de mest utsatta, enligt våra NSA-data.

Användbara insikter

1. Identifiera och skydda dina potentiella högvärdiga datamål, tekniker som är utsatta för risk, information och affärsverksamhet som kan vara anpassade till de strategiska prioriteringarna för nationalstatsgrupper.
2. Gör det möjligt för molnskydd att storskaligt identifiera och begränsa kända och nya hot mot nätverket.

IT-försörjningskedjan som en inkörsport till det digitala ekosystemet

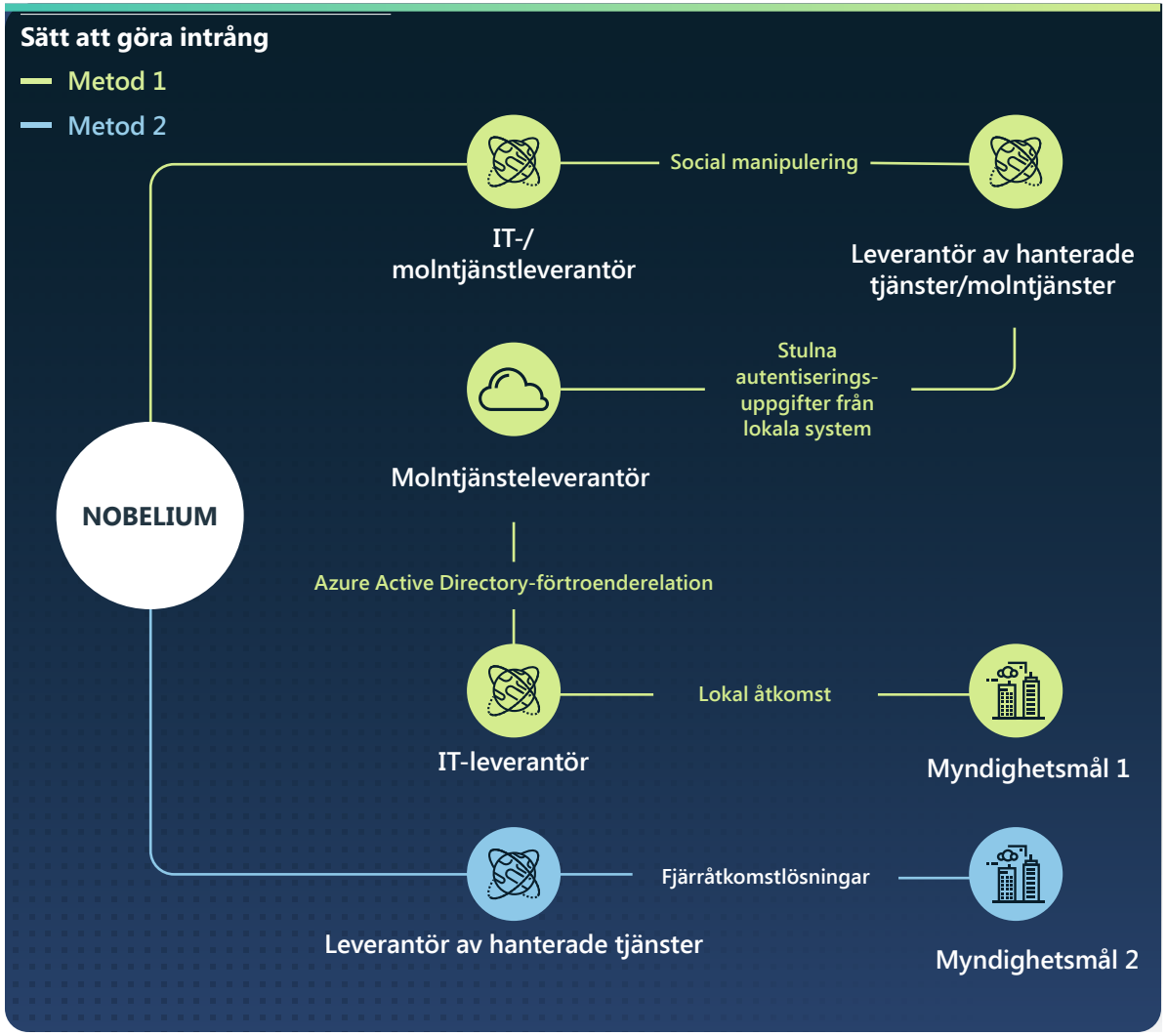
Nationalstaternas inriktning på IT-tjänsteleverantörer kan möjliggöra för hotaktörerna att ta sig in i andra intressanta organisationer genom att utnyttja det förtroende och den åtkomst som leverantörerna i försörjningskedjan har. Under det senaste året riktade nationalstaters cyberhotgrupper in sig mot IT-tjänsteleverantörer för att angripa tredje man och få tillgång till klienter nedströms, till exempel myndigheter, policysektorn och sektorn för kritisk infrastruktur.

IT-tjänsteleverantörer är lockande mellanhandsmål eftersom de tillhandahåller tjänster till hundratals direkta och tusentals indirekta kunder som kan vara av intresse för utländska underrättelsetjänster. Om de utnyttjas kan företagens vanliga affärsrutiner och delegerade administrativa behörigheter ge skadliga aktörer tillgång till och möjlighet att manipulera IT-tjänsteleverantörens klientnätverk utan att omedelbart upptäckas.

Under det senaste året försökte NOBELIUM tränga sig in i och utnyttja privilegierade konton i molnlösningar och andra leverantörer av hanterade tjänster för att försöka komma åt mål nedströms, främst amerikanska och europeiska myndighets- och policykunder.

NOBELIUM visade tydligt hur metoden att göra intrång på en plats för att få tillgång till flera kan användas mot upplevda geopolitisk motståndare. Det senaste året har hotaktören gett sig på både tredje man och gjort direkta intrång hos känsliga organisationer i NATO-stater, som Ryssland uppfattar som ett existentiellt hot. Mellan juli 2021 och början av juni 2022 gick 48 procent av Microsofts aviseringar till kunder om rysk hotverksamhet mot onlinetjänster till företag i IT-sektorn i NATO-medlemsländer, sannolikt som mellanliggande åtkomstpunkter. Sammantaget gick 90 procent av alla aviseringar om rysk hotaktivitet under samma period till kunder i NATO-medlemsstater, främst inom IT-sektorn, tankesmedjor och icke-statliga organisationer samt myndigheter, vilket tyder på en strategi om att försöka komma åt dessa mål med olika metoder.

Det har skett en övergång från att utnyttja programvaruförsörjningskedjan till att utnyttja försörjningskedjan för IT-tjänster, och man riktar in sig på molnlösningar och leverantörer av hanterade tjänster för att nå kunder nedströms.



Det här diagrammet visar NOBELIUM:s mångfacetterade strategi för att göra intrång hos sina slutmål och de oavsiktliga skadorna på andra offer längs vägen. Utöver de åtgärder som visas ovan inledde NOBELIUM lösenordsattacker och nätfiskeangrepp mot de inblandade och riktade till och med in sig på personliga konton för minst en myndighetsanställd för att skapa ytterligare en potentiell intrångsväg.

IT-försörjningskedjan som en inkörsport till det digitala ekosystemet

fortsättning

Under året upptäckte Microsoft Threat Intelligence Center (MSTIC) ett ökande antal iranska statliga och Iran-anslutna aktörer som bröt sig in hos IT-företag. I många fall upptäcktes aktörerna stjäla inloggningsuppgifter för att få tillgång till klienter nedströms för en rad syften, från underrättelseinsamling till destruktiva hämndangrepp.

- I juli och augusti 2021 tog sig DEV-0228 in hos en israelisk leverantör av affärsprogramvara och senare hos kunder nedströms i den israeliska försvars-, energi- och rättssektorn.[4]
- Från augusti till september 2021 märkte Microsoft av en stark ökning av iranska statliga aktörer som riktade in sig på IT-företag baserade i Indien. Frånvaron av större geopolitiska händelser som skulle kunna orsaka en sådan ökning tyder på att målet är indirekt tillgång till dotterbolag och kunder utanför Indien.
- I januari 2022 trängde sig DEV-0198, en grupp som vi bedömer är knuten till Iran, in hos en israelisk molnlösningsleverantör. Microsoft bedömer att aktören förmodligen använde knäckta autentiseringsuppgifter från leverantören för att autentisera sig inför ett israeliskt logistikföretag. MSTIC observerade att samma aktör försökte utföra en destruktiv cyberattack mot logistikföretaget senare samma månad.
- I april 2022 trängde sig POLONIUM, en grupp i Libanon som vi bedömer samarbetade med iranska statliga grupper om IT-försörjningskedjemetoder, in hos ett annat israeliskt IT-företag för att få tillgång till israeliska försvars- och rättsorganisationer.[5]

Aktiviteten under förra året visar att hotaktörer som NOBELIUM och DEV-0228 börjar få bättre inblick i hur en organisations betrodda relationer ser ut än organisationerna har själva. Det ökade hotet betonar vikten av att organisationer förstår och förstärker sina gränser och ingångspunkterna till sina digitala egendomar. Det understryker också betydelsen av att IT-tjänsteleverantörer noggrant övervakar sin egen cybersäkerhetshälsa. Organisationerna bör till exempel tillämpa multifaktorautentisering och policyer för villkorsstyrd åtkomst som gör det svårare för skadliga aktörer att få tillgång till privilegierade konton eller sprida sig i ett nätverk.

Att genomföra en grundlig genomgång och granskning av partnerrelationer är ett sätt att minimera onödiga behörigheter mellan din organisation och leverantörer uppströms och omedelbart ta bort åtkomsten för alla relationer som verkar obekanta. Ökad förtrogenhet med aktivitetsloggar och granskning av tillgänglig aktivitet gör det lättare att upptäcka avvikelser att undersöka vidare.

Nationalstater som riktar in sig på tredje man kan utnyttja känsliga organisationer genom att dra nytta av förtroende och åtkomst i en försörjningskedja.

Användbara insikter

1. Gå igenom och granska tjänsteleverantörsrelationer och delegerade behörighetsåtkomster uppströms och nedströms för att minimera onödiga behörigheter. Ta bort åtkomsten från alla partnerrelationer som ser obekanta ut eller som ännu inte har granskats.[6]
2. Aktivera loggning och granska all autentiseringsaktivitet till fjärråtkomstinfrastruktur och virtuella privata nätverk (VPN). Fokusera på konton som har konfigurerats med autentisering med enbart en faktor för att bekräfta äktheten och undersöka avvikande aktiviteter.
3. Aktivera MFA för alla konton (även tjänstkonton) och se till att MFA tillämpas för alla fjärranslutningar.
4. Använd lösningar utan lösenord för att skydda konton.[7]

Länkar till mer information

- NOBELIUM targeting delegated administrative privileges to facilitate broader attacks | Microsoft Threat Intelligence Center (MSTIC)
- Iranian targeting of IT sector on the rise | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Threat Intelligence Center (MSTIC)

Snabbt utnyttjande av sårbarheter

När organisationerna stärker sin cybersäkerhetsställning reagerar nationella statsaktörer genom att använda nya och unika taktiker för att gå till angrepp och undvika upptäckt. Identifiering och utnyttjande av tidigare okända sårbarheter – dag noll-sårbarheter – är en viktig metod.

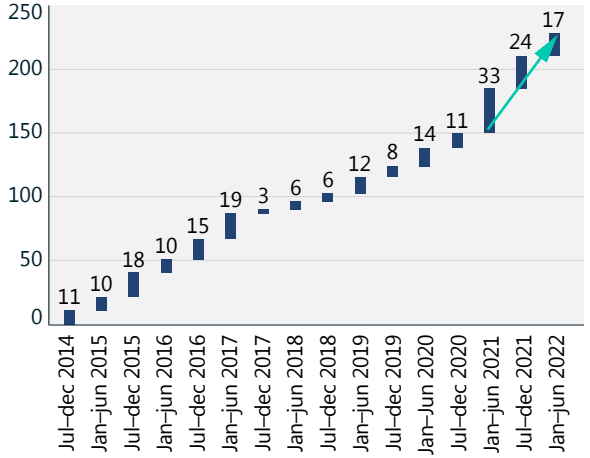
Dag noll-sårbarheter är ett särskilt effektivt sätt att bryta sig in, och när de väl har offentliggjorts kan sårbarheterna snabbt återanvändas av andra nationalstater och kriminella. Antalet offentliggjorda dag noll-sårbarheter under det gångna året är i nivå med det föregående året, som var det högsta hittills.

Eftersom cyberhotsaktörer – både nationalstater och kriminella – blir allt skickligare på att utnyttja sårbarheter av den här typen har vi observerat att det tar kortare tid mellan publiceringen av en sårbarhet och att den blir tillgänglig för köp. Därför är det viktigt att organisationer korrigerar intrångsmöjligheter omedelbart. På samma sätt är det viktigt att organisationer och enskilda som upptäcker nya sårbarheter tar sitt ansvar och meddelar eller rapporterar dem till de aktuella leverantörerna så snart som möjligt, i enlighet med samordnade förfaranden för offentliggörande av sårbarheter.

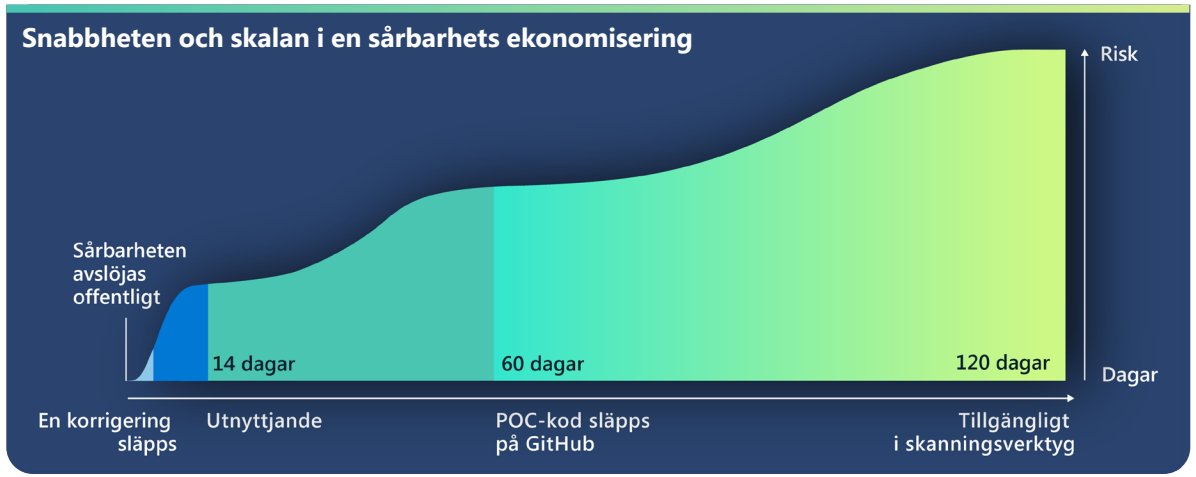
Det säkerställer att sårbarheter identifieras och korrigeringar utvecklas i tid för att skydda kunderna från tidigare okända hot.

Många organisationer förutsätter att det är mindre troligt att de utsätts för dag noll-sårbarhetsangrepp om sårbarhetshantering är en integrerad del av deras nätverkssäkerhet. Men eftersom intrångsmetoder har blivit en handelsvara blir de nu tillgängliga betydligt fortare. Dag noll-sårbarheter upptäcks i många fall av andra aktörer och återanvänds väldigt ofta inom kort tid, vilket innebär att okorrigerade system utsätts för risk. Även om det kan vara svårt att upptäcka dag noll-intrång är aktörernas åtgärder efter intrånget ofta lättare att identifiera och om de kommer från helt korrigerad programvara kan det vara ett tecken på intrång.

Korrigeringar som släpps för dag noll-sårbarheter



Antalet offentligt avslöjade dag noll-sårbarheter från List of Common Vulnerabilities and Disclosures (CVE).



I snitt tar det bara två veckor innan en intrångsmöjlighet blir tillgänglig för alla efter att en sårbarhet har avslöjats offentligt. Diagrammet visar en analys av utvecklingen av en intrångsmöjlighet från dag noll-sårbarheter jämte antalet system som är sårbara för det givna intrånget och aktiva på internet från offentliggörandet.

Även om angrepp med dag noll-sårbarheter initialt brukar ske mot en begränsad mängd organisationer, används de snart av hela ekosystemet med hotaktörer. Det är startskottet till en kapplöpning bland hotaktörerna att utnyttja sårbarheten så mycket som möjligt innan de potentiella målen installerar korrigeringar.

Vi observerar många nationella statsaktörer som utvecklar intrångsmöjligheter från okända sårbarheter, men nationella statsaktörer i Kina är särskilt skickliga på att upptäcka och utveckla dag noll-intrång. Kinas lag om rapportering av sårbarheter trädde i kraft i september 2021. Kina är det första landet i världen som kräver att sårbarheter rapporteras till en myndighet för granskning innan de avslöjas för produktens eller tjänstens ägare. Den här nya lagen kan möjliggöra för delar av det kinesiska styret att samla på sig rapporterade sårbarheter för att använda dem som vapen. Kinesiska aktörers ökade bruk av dag noll-sårbarheter under det senaste året återspeglar sannolikt det första helåret med Kinas krav på att kinesiska säkerhetsexperter ska rapportera sårbarheter och är ett stort steg mot ökad användning av dag noll-sårbarheter i statens tjänst. De sårbarheter som beskrivs nedan utvecklades och distribuerades först av nationella statsaktörer baserade i Kina för angrepp, innan de upptäcktes och spreds bland andra aktörer i det övriga hotekosystemet.

Snabbt utnyttjande av sårbarheter

fortsättning

Även organisationer som inte är mål för nationalstatsangrepp har begränsad tid på sig att åtgärda dag noll-sårbarheter på de aktuella systemen innan de utnyttjas av alla andra hotaktörer i ekosystemet.

De här exemplen på nyligen identifierade sårbarheter visar att organisationer i snitt har 60 dagar på sig från det att en sårbarhet korrigeras till att konceptkod görs tillgänglig på nätet och ofta återanvänds av andra aktörer. På samma vis har organisationerna i snitt 120 dagar på sig innan en sårbarhet är tillgänglig i automatiserade verktyg för sökning efter och nyttjande av sårbarheter som Metasploit – vilket ofta leder till att intrångsmöjligheten används i mycket stor skala. Det här visar att även organisationer som inte är mål för nationella statsaktörer har begränsad tid på sig att åtgärda dag noll-sårbarheter på de aktuella systemen innan sårbarheterna utnyttjas av alla andra hotaktörer i ekosystemet.

CVE-2021-35211 SolarWinds Serv-U

I juli 2021 släppte SolarWinds ett säkerhetsråd om CVE-2021-35211 och tackade Microsoft för aviseringen.[8] Då upptäckte vi att den nationalstatsförknippade hotaktören DEV-0322 aktivt utnyttjade sårbarheten SolarWinds Serv-U. Vårt RiskIQ-team observerade att 12 646 IP-adresser stod värd för internetanslutna versioner av de aktuella enheterna mellan 15 juni och 9 juli.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

I september 2021 observerade våra forskare aktörer knutna till Kina som utnyttjade Zoho ManageEngine hos flera företag i USA. Sårbarheten rapporterades offentligt den 6 september som CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, vilken många organisationer brukar använda för att hantera lösenordsåterställningar.[9] DEV-0322 utnyttjade sårbarheten senare i september och använde den som ett sätt för att få fotfäste i nätverk och utföra ytterligare åtgärder, däribland dumpning av autentiseringsuppgifter, installation av särskilda binärfiler och av skadlig kod för att undvika att bli utkastade. När problemet tillkännagavs observerade RiskIQ 4 011 instanser av de här systemen som var aktiva och på internet.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

I slutet av oktober 2021 observerade vi DEV-0322 utnyttja en sårbarhet (CVE-2021-44077) i en andra Zoho ManageEngine-produkt, ServiceDesk Plus – ett program för IT-support med tillgångshantering. DEV-0322 utnyttjade sårbarheten för att rikta in sig på och göra intrång hos företag inom hälso- och sjukvård, informationsteknik, högre utbildning och kritiska tillverkningssektorer. Den 2 december utfärdade FBI och Cybersecurity and Infrastructure Security Agency (CISA) en gemensam varning till allmänheten om nationella statsaktörer som utnyttjar sårbarheten. När problemet tillkännagavs observerade RiskIQ 7 956 instanser av de här systemen som var aktiva och på internet.

CVE-2021-42321 Microsoft Exchange

Ett dag noll-intrång för en sårbarhet i Exchange, CVE-2021-42321, avslöjades under Tianfu Cup, ett internationellt cybersäkerhetstoppmöte och en hackningstävling som pågick den 16 och 17 oktober 2021 i Chengdu i Kina. Säkerhetsforskare på Microsoft observerade att utnyttjandet av sårbarheten i Exchange fanns för allmänt bruk den 21 oktober, bara tre dagar efter att sårbarheten avslöjades. När problemet tillkännagavs observerade RiskIQ 61 559 instanser av de här systemen som var aktiva och på internet. Vi fortsatte att observera exploateringsaktiviteten till i november 2021.

CVE-2022-26134 Confluence

En till Kina anknuten aktör hade sannolikt kod för dag noll-utnyttjande av sårbarheten Confluence (CVE-2022-26134) fyra dagar innan sårbarheten avslöjades offentligt den 2 juni och utnyttjade den förmodligen mot ett företag i USA. När problemet tillkännagavs observerade RiskIQ 53 621 instanser av sårbara Confluencesystem på internet.

Sårbarheter tas upp och utnyttjas i mycket stor skala och efter allt kortare tid.

Användbara insikter

1. Prioritera korrigering av dag noll-sårbarheter så snart de släpps. Vänta inte in cykeln för hantering av korrigeringar.
2. Dokumentera och inventera alla företagets tillgångar i form av maskinvara och programvara för att fastställa risker och snabbt avgöra när ni ska korrigera.

Ryska statliga aktörers cybertaktik i krigstid hotar Ukraina och andra

I år har ryska statliga aktörer använt cyberoperationer som komplement till militära insatser under Rysslands invasion av Ukraina, ofta med samma taktik och tekniker som används mot mål utanför Ukraina. Det är viktigt att organisationer över hela världen vidtar åtgärder för att stärka sin cybersäkerhet mot digitala hot från hotaktörer i Ryssland.

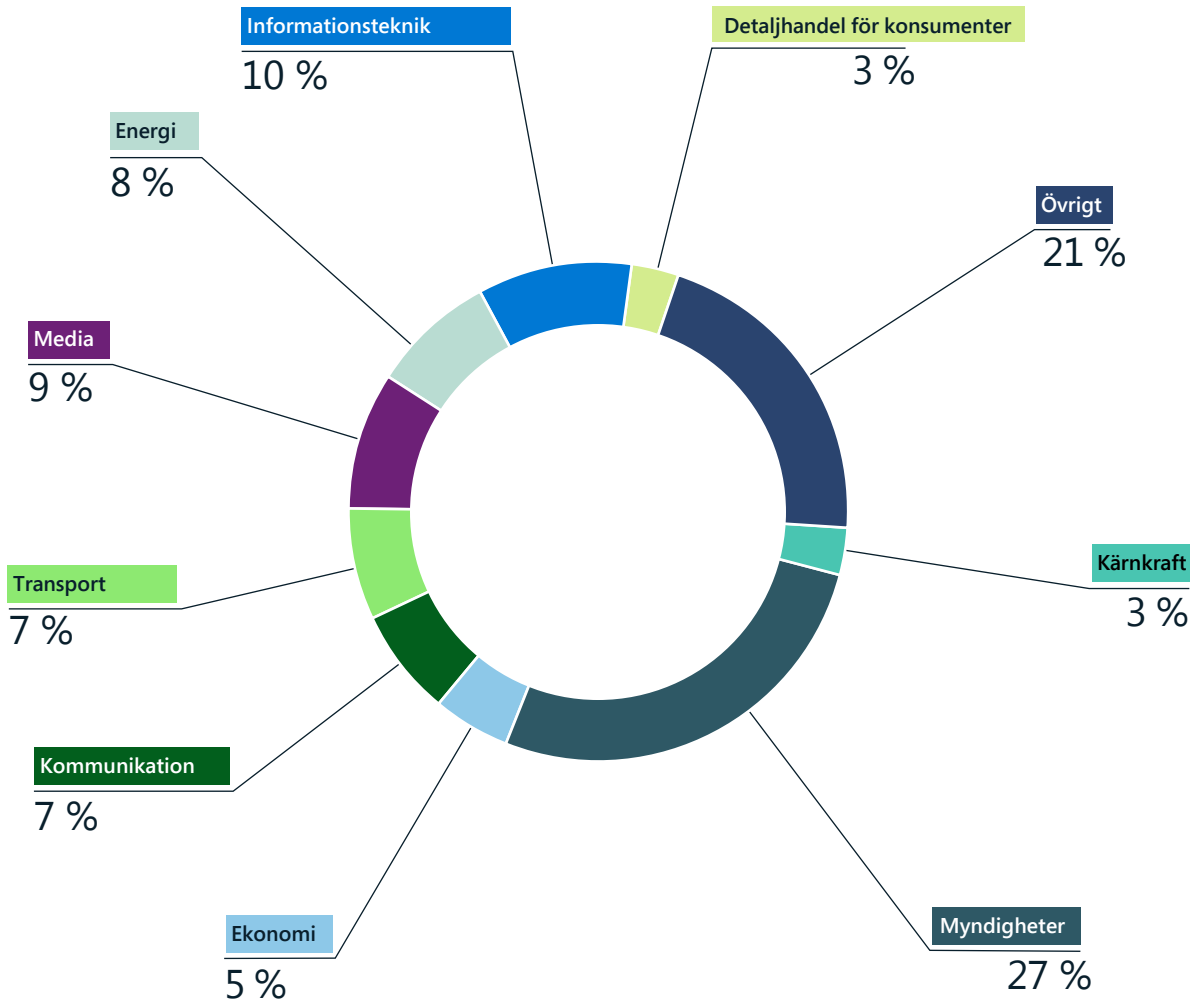
Situationen på fältet fortsätter att fluktuera eftersom den militära konflikten består, och Ukraina och dess allierade bör vara beredda på att försvara sig om ryska statliga cyberoperatörer gör fler eller mer intensiva intrång i enlighet med militära mål. Under krigets första fyra månader observerade Microsoft hotaktörer som var knutna till den ryska militären inleda flera vågor av destruktiva cyberattacker mot nästan 50 olika ukrainska myndigheter och företag och spionagefokuserade intrång mot många andra. Med undantag av insatser mot onlinetjänstkunder riktades 64 procent av den ryska hotaktiviteten mot kända mål mot organisationer i Ukraina mellan slutet av februari och juni.

Vid varje insats använde de ryska hotaktörerna många av de metoder, tekniker och rutiner som vi såg användas före invasionen mot mål både i och utanför Ukraina. Aktörerna hade för avsikt att förstöra data och rubba jämvikten för ukrainska myndigheter under den inledande perioden av konflikten. Sedan dess har de försökt sabotera transporter av militärt och humanitärt bistånd till Ukraina, störa allmänhetens tillgång till tjänster och medier och stjäla information med mer långsiktigt underrättelsevärde eller ekonomiskt värde för Ryssland.

Inriktningen på transporter hotar ett oerhört viktigt område för ukrainska medborgare som försöker överleva konflikten. Enligt en UNICEF-sponsrad undersökning i maj var de svarande i konfliktdrabbade stadsområden mest oroliga för transport och bränsle, störningar av försörjningen, säkerhet och begränsad tillgång på mat, sjukvård och finansiella tjänster.[10] I juni sade FN:s krissamordnare för Ukraina att minst 15,7 miljoner människor i Ukraina var i akut behov av humanitärt bistånd, och att antalet skulle öka allt eftersom kriget fortsatte.[11]

Utanför Ukraina upptäckte Microsoft ryska nätverksintrångsförsök mot 128 organisationer i 42 länder mellan slutet av februari och juni. USA var Rysslands främsta mål. Polen som är transitland för mycket av det internationella militära och humanitära biståndet till Ukraina, var också ett betydande mål under perioden. Hotaktörer som var knutna till den ryska staten gav sig på organisationer i Baltikum och datornätverk i Danmark, Norge, Finland och Sverige i april och maj.

De mest drabbade sektorerna i Ukraina sedan invasionen



Federala, statliga och lokala myndigheter i Ukraina har fortsatt vara prioriterade mål för ryska statliga och statsanknutna hotgrupper under hela konflikten. Aktörernas fokus på transport-, energi-, finans- och mediesektorns organisationer belyser den risk som dessa cyberoperationer utgör för tjänster som ukrainska medborgare förlitar sig på.

Ryska statliga aktörers cybertaktik i krigstid hotar Ukraina och andra

fortsättning

Vi har sett en ökning av liknande aktiviteter som är inriktade på NATO-ländernas utrikesministerier.

Ryska hotgrupper har fortsatt arbetet för att bryta sig in i kritisk infrastruktur både inom och utanför Ukraina under det senaste året. IRIDIUM distribuerade den skadliga koden Industroyer2 i ett misslyckat försök att göra miljontals människor i Ukraina strömlösa. Utanför Ukraina gjorde BROMINE intrång mot organisationer inom tillverkning och industriella styrsystem i början av 2022.

Ryska statliga och statligt anknutna aktörer riktade cyberverksamhet mot Ukraina, dess allierade och andra värdefulla underrättelsemål i år med hjälp av många av följande tekniker, metoder och rutiner:

Harpunfiske med skadliga bilagor eller länkar

Ryska statliga och Rysslandsanknutna grupper som ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM och IRIDIUM använde nätfiskekampanjer för att komma åt önskade konton och nätverk i organisationer i och utanför Ukraina. I många kampanjer använde man knäckta eller förfalskade konton på de aktuella organisationerna eller inom samma bransch och övertygande teman för att locka offer.

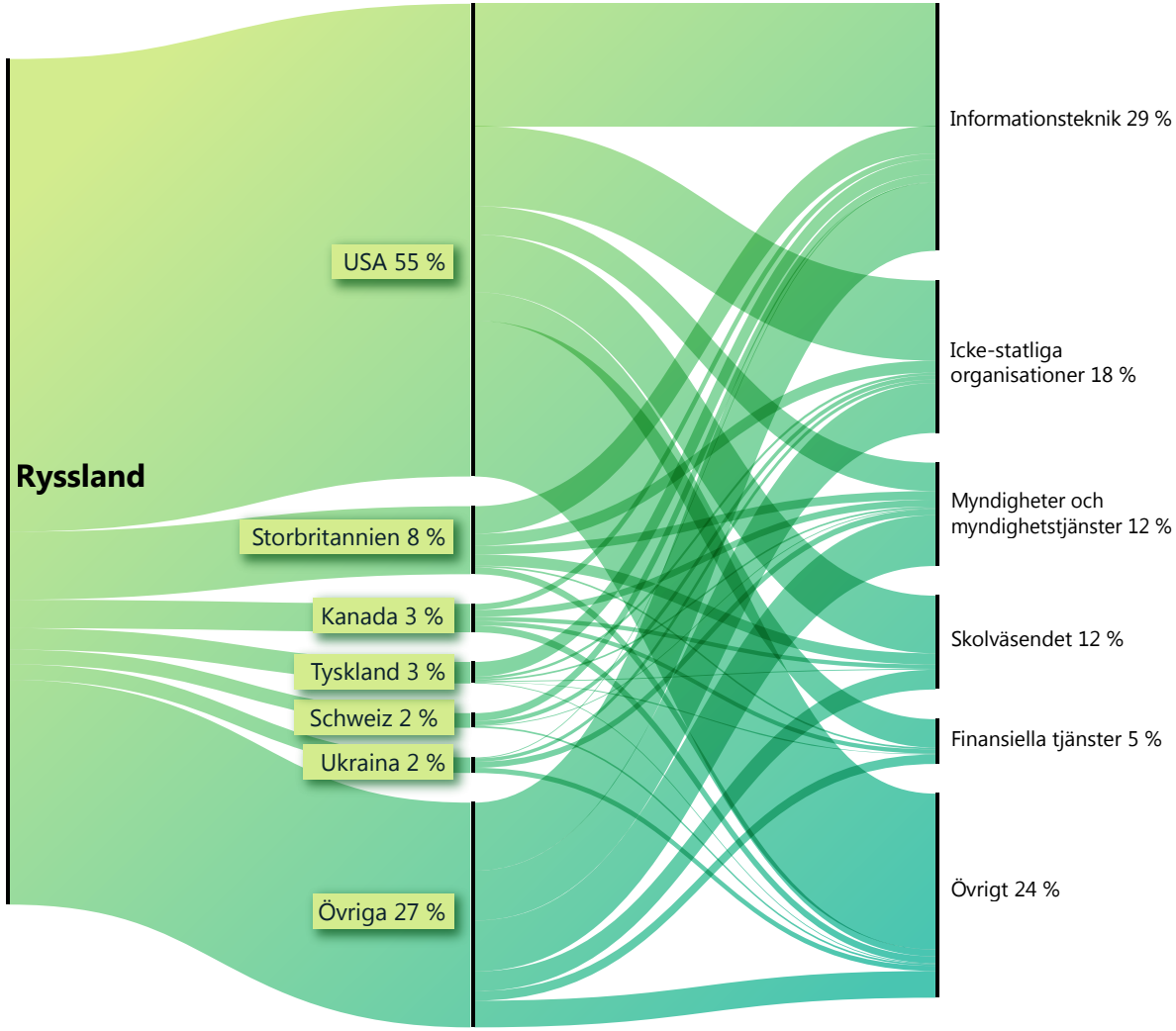
NOBELIUM använde knäckta diplomatkonton för att skicka nätfiskemeddelanden förklädda till diplomatisk kommunikation till anställda på många utrikesdepartement över hela världen. STRONTIUM skapade förfalskade konton utifrån offentligt tillgängliga namn på kontoinnehavare på tankesmedjor i USA och skickade nätfiskemeddelanden för att få tillgång till konton på dessa tankesmedjor. SEABORGIUM nätfiskade med beten som rörde rapporteringen om Ukraina-konflikten för att få tillgång till konton på tankesmedjor som hanterar internationella frågor i de nordiska länderna.

Utnyttjande av försörjningskedjan för IT-tjänster för att påverka kunder nedströms

I slutet av 2021 gjorde ryska statliga aktörer intrång hos IT-tjänsteleverantörer och använde den åtkomsten för att ändra utseendet på webbplatser och i januari distribuerade de genom DEV-0586 den destruktiva skadliga koden Whispergate.[12] DEV-0586 tog sig även in i ett IT-företags nätverk. Det företaget tog fram resurshanteringssystem åt Ukrainas försvarsministerium och andra organisationer inom kommunikations- och transportsektorn, vilket tyder på att gruppen även utforskade alternativ för angrepp mot tredje man inom de sektorerna.

I hela världen, men särskilt i USA och Västeuropa, riktade NOBELIUM in sig på IT-tjänsteleverantörer för att få tillgång till myndigheter och andra känsliga nätverk under 2021–2022 (se diskussionen om sårbarheter i försörjningskedjan tidigare i det här kapitlet).

Ryssland: De mest drabbade länderna och branscherna



Trots ökat fokus på Ukraina-baserade organisationer sedan början av 2022 var företag i Nordamerika och Västeuropa fortfarande de nättjänstkunder som de ryska aktörerna var mest inriktade på. NOBELIUM:s kampanj mot IT-sektorn gjorde den till den mest utsatta sektorn under det senaste året.

Ryska statliga aktörers cybertaktik i krigstid hotar Ukraina och andra

fortsättning

Utnyttjande av offentligt tillgängliga appar för att initialt bryta sig in i nätverk

Sedan åtminstone slutet av 2021 har STRONTIUM jobbat med att utveckla och förfina sina möjligheter att utnyttja offentligt tillgängliga tjänster för att stjäla information, till exempel Microsoft Exchange-servrar. STRONTIUM utnyttjade okorrigerade Exchange-servrar för att komma åt ukrainska myndighetskonton och militära och försvarsindustrirelaterade organisationer i USA, Libanon, Peru och Rumänien, samt andra myndigheter i Armenien, Bosnien, Kosovo och Malaysia. DEV-0586, som också är knutet till den ryska militären, utnyttjade sårbarheter i Confluence-servern för att få åtkomst till myndigheter och organisationer i IT-sektorn i Ukraina och andra östeuropeiska länder.

Ryska statliga och till staten anknutna hotaktörer använder samma tekniker, metoder och rutiner för att ta sig in hos intressanta organisationer både i krigstid och i fredstid.

Användning av administrativa konton och protokoll samt inbyggda verktyg för nätverksidentifiering och lateral förflyttning

När ryska aktörer först hade brutit sig in i ett nätverk observerade Microsoft att de utnyttjade legitima konton och program för att utföra grundläggande underhållsuppgifter och på så vis undvika upptäckt så länge som möjligt. De förlitade sig på knäckta identiteter med administrativ kapacitet och giltiga administrationsprotokoll, verktyg och metoder för att förflytta sig lateralt i olika nätverk utan att omedelbart dra till sig uppmärksamhet från automatiserade övervakare och nätverksförsvarare.

Grundläggande cyberhygien och användning av verktyg för slutpunktsdetektering och svarsinsatser kan mildra de negativa effekterna av sådana insatser både i fredstid och i krigstid.

Den pågående konfliktens oförutsägbarhet kräver att organisationer i hela världen vidtar åtgärder för att stärka cybersäkerheten mot digitala hot från ryska staten och hotaktörer som är knutna till Ryssland.

Användbara insikter

1. Minimera stölden av autentiseringsuppgifter och kontomissbruk genom att skydda användarnas identiteter med MFA-identitetsskyddsverktyg och genom att upprätthålla minst privilegierad åtkomst för att säkra de känsligaste och mest privilegierade kontona och systemen.
2. Installera uppdateringar för att säkerställa att alla system har bästa möjliga skydd så snart som möjligt och hålls uppdaterade.
3. Använd lösningar mot skadlig kod, slutpunktsidentifiering och identitetsskydd i hela organisationen. En kombination av säkerhetslösningar som prioriterar försvar på djupet och utbildad och kompetent personal kan ge organisationen möjlighet att identifiera, upptäcka och förhindra intrång som påverkar verksamheten.
4. Utför utredningar och återställningar om ni upptäcker eller blir aviserade om ett hot mot er miljö genom att säkerhetskopiera kritiska system och aktivera loggning. Vi rekommenderar alla att ha en konkret åtgärdsplan för incidenthantering.

Länkar till mer information

- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- The hybrid war in Ukraine | Microsoft On the Issues
- Cyber threat activity in Ukraine: analysis and resources | Microsoft Security Response Center (MSRC)
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues
- Malware attacks targeting Ukraine government | Microsoft On the Issues
- MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

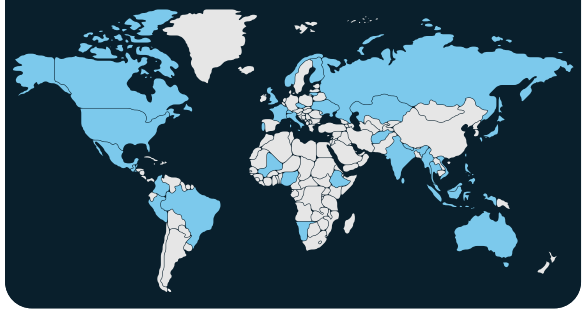
Kina utökar de globala angreppen för att få konkurrensfördelar

I dagens komplexa geopolitiska klimat försöker kinesiska statliga och statsanknutna hotaktörer som bedriver cyberverksamhet ofta främja landets strategiska militära mål, ekonomiska mål och mål med relationerna till utlandet som ett led i Kinas mål att uppnå konkurrensfördelar. Under det senaste året har Microsoft observerat omfattande kinesisk hotaktivitet som riktar sig mot länder i hela världen.

Sedan mitten av 2021 har Kina försökt säkerställa ekonomisk och finansiell stabilitet mitt under den värsta covid-19-ökningen på två år.[13] Kina fortsatte att byta position vid geopolitiska händelser, t.ex. kampen för att balansera sitt ”gränslösa” partnerskap med Ryssland[14] och behålla sin position i världen.[15] Kinas hållning gentemot USA och dess allierade i fråga om Taiwan[16] och Sydkinesiska havet har dessutom fortsatt att försvåra förbindelserna med många länder.[17]

Kinesiska statliga och statsanknutna hotgrupper ökade sin inriktning på mindre länder över hela världen, med fokus på Sydostasien, för att få konkurrensfördelar på alla fronter.

Länder som kinesiska statliga och statligt anslutna grupper angriper

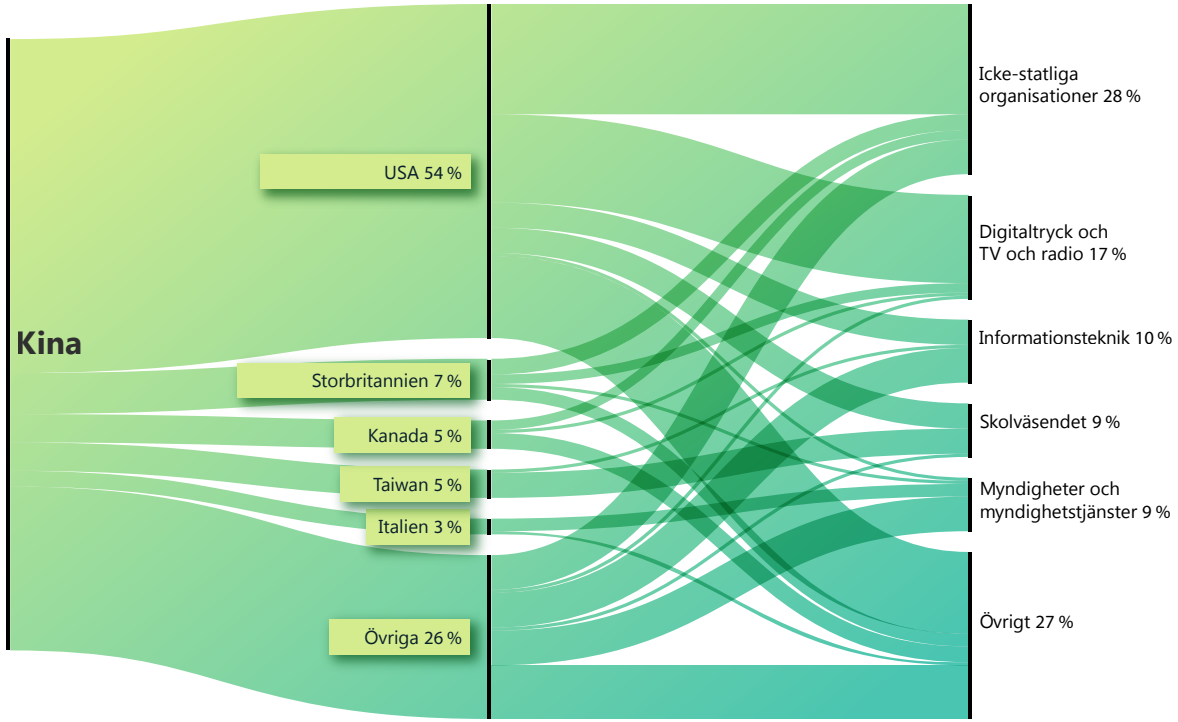


Kina har också fortsatt att utöka sitt ekonomiska inflytande globalt genom det tidigare etablerade Ett bälte, en väg-initiativet och försökte återuppliva en omfattande investeringsram med EU[18] och förhandla fram ett nytt regionalt handelsavtal med 15 länder i Asien och Stillahavsområdet som kallas det regionala övergripande ekonomiska partnerskapet.[19] Microsoft bedömer att Kina kommer att fortsätta att använda insamling av information på cyberväg som ett verktyg för att främja sina strategiska politiska, militära och ekonomiska mål på grund av de observerade cyberverksamheterna och den stora bredd av de företag som angrips.

Cyberattacker främjar förmodligen ekonomiska och militära intressen.

Microsoft observerade ett stort fokus på mindre länder i världen från kinesiska statliga och statsanknutna hotgrupper, vilket tyder på att Kina sannolikt använder cyberspionage som en komponent i sitt globala ekonomiska och militära inflytande.

Kina: De mest drabbade länderna och branscherna



Tankesmedjor/icke-statliga organisationer, medier, IT-, myndighets- och utbildningssektorn var bland de mest drabbade sektorerna av kinesiska hotgrupper, förmodligen för löpande insamling av underrättelser och rekognoscering.

Målen omfattade bland annat länder i Afrika, Västindien, Mellanöstern, Oceanien och södra Asien, med särskilt fokus på länderna i Sydostasien och Stillahavsöarna.

I enlighet med Kinas Ett bälte, en väg-strategi angrep kinesiska hotgrupper företag och myndigheter i Afghanistan, Kazakstan, Mauritius, Namibia och Trinidad och Tobago.[20] Trinidad och Tobago var till exempel det första karibiska landet som 2018 stödde Kinas Ett bälte, en väg-strategi och Kina ser landet som en viktig partner i regionen. NICKEL har angripit nätverk i Trinidad och Tobago sedan 2021. Till exempel genomförde NICKEL i mars 2022 rekognoscering mot en myndighet, sannolikt för att samla in underrättelser.

Kina utökar de globala angreppen för att få konkurrensfördelar

fortsättning

Samtidigt observerade Microsoft att kinesiska statliga och statsanknutna hotgrupper fokuserade sin nätverksverksamhet mot företag i Sydostasien och expanderade till Stilla havsländer när Kina bytte sitt militära och ekonomiska fokus för att hantera utmaningarna med USA:s förnyade intresse för regionen. I januari 2022 observerade Microsoft att RADIUM angrep ett energiföretag och en energianknuten myndighet i Vietnam och en indonesisk myndighet. RADIUM:s verksamhet harmonierar förmodligen väl med Kinas strategiska mål i Sydkinesiska sjön.[21] I slutet av februari och början av mars knäckte GALLIUM fler än hundra konton som hörde till en framstående mellanstatlig organisation i Sydostasien. Tidpunkten för GALLIUM:s angrepp på organisationen i regionen sammanföll med tillkännagivandet av ett planerat möte mellan USA och regionala ledare. GALLIUM-aktörerna fick troligen i uppdrag att övervaka kommunikationen och samla in information före evenemanget.

När Kina utökade sitt inflytande i Stilla havet följde kinesiska hotgrupper efter. I april undertecknade Kina och Salomonöarna ett säkerhetsavtal som skulle "främja fred och säkerhet". Avtalet gör att Kina kan få sätta in beväpnad polis och militär på Salomonöarna.[22] I maj var Kina värd för det andra mötet mellan Kinas och Stillahavsöarnas utrikesministrar på Fiji och föreslog att man skulle gå vidare med ett "omfattande strategiskt partnerskap" för att främja politiska, kulturella, sociala, säkerhetsmässiga och klimatförändringsmässiga intressen samt även bekämpa pandemin.[23] Samtidigt i maj identifierade Microsoft GADOLINIUM:s skadliga kod i myndighetssystem på Salomonöarna. RADIUM körde även skadlig kod på system hos ett telekommunikationsföretag i Papua Nya Guinea. Vi bedömer att aktiviteterna sannolikt gällde underrättelseinsamling för att stödja Kinas övergripande regionala strategi.

Microsoft stör NICKEL:s verksamhet, men hotgruppen ger inte upp.

I december 2021 lämnade Microsoft Digital Crimes Unit (DCU) in inlagor till den amerikanska domstolen för östra distriktet i Virginia och ville få rätt att beslagta 42 kommando- och kontrolldomäner (C2-domäner) som NICKEL kontrollerade. C2-domänerna har använts vid insatser mot länder, diplomatiska organ och icke-statliga organisationer i Central- och Sydamerika, Västindien, Europa och Nordamerika sedan september 2019.[24] Genom verksamheten har NICKEL fått långsiktig åtkomst till många organisationer och konsekvent exfiltrerat data från vissa offer sedan slutet av 2019.

I takt med att Kina fortsätter att upprätta bilaterala ekonomiska förbindelser med alltfler länder – ofta i avtal som förknippas med Ett bälte, en väg – ökar Kinas globala inflytande. Vi bedömer att kinesiska statliga och statsanknutna hotaktörer kommer att rikta in sig på myndigheter, diplomater och icke-statliga organisationer för att få nya insikter, förmodligen för ekonomiskt spionage eller på jakt efter traditionella underrättelser. Sedan Microsofts insatser har NICKEL riktat in sig på flera myndigheter, förmodligen för att försöka återfå sin förlorade åtkomst. Mellan slutet av mars och maj 2022 gav sig NICKEL på minst fem myndigheter över hela världen. Det tyder på att gruppen hade ytterligare ingångsställen till entiteterna eller att de återfick åtkomsten via nya C2-domäner. NICKEL:s förmåga att upprepade gånger göra intrång hos samma myndigheter globalt visar hur viktigt arbetet är på hög nivå.

Kina är mer bestämda i sin utrikespolitiska inställning. Vi bedömer att ekonomiskt spionage via cyberattacker och insamling av underrättelser sannolikt kommer att fortsätta.

Användbara insikter

1. Stärk cyberförsvaret och motverka cyberhot proaktivt. Svårigheterna att kasta ut kinesiska hotaktörer visar att organisationerna måste identifiera, skydda, upptäcka och reagera på eventuella intrång direkt.
2. Hotaktörer missbrukar vanligen planerade uppgifter[25] för att hålla sig kvar och undvika försvarsåtgärder. Se därför till att ytterligare säkerhetsriktlinjer används i er miljö för att skydda mot den här vanliga metoden.[26]
3. Vi observerar fortfarande att webbskal används som ett sätt att bryta sig in i nätverk.[27] Organisationer bör stärka sina system mot webbskalsangrepp, som kan ge angriparna möjlighet att köra kommandon på distans.[28]

Länkar till mer information

- NICKEL riktar in sig på statliga organisationer i hela Latinamerika och Europa | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Skydda människor från nya cyberattacker | Microsoft On the Issues

Iran blir alltmer aggressivt efter maktskiftet

Microsoft har observerat att iranska statliga grupper och anknutna aktörer ökar omfattningen och takten i sina cyberattacker mot Israel, ökar angreppen med utpressningstrojaner bortom regionala fiender till offer i USA och EU, samt riktar in sig mot viktig infrastruktur i USA för att åtminstone vara förberedda på potentiellt destruktiva cyberattacker.

Iranska statliga aktörers växande cyberaggression följer på att landet har fått en ny president. Sommaren 2021 ersatte den hårdföra presidenten Ibrahim Raisi den mer diplomatiska presidenten Hassan Rouhani. Till skillnad från Raisi, som är skyddsling till den högste ledaren och nära allierad med Islamiska revolutionsgardet, gjorde den tidigare presidenten Rouhanis förkärlek till diplomati att han ofta motsatte sig den högsta ledaren och revolutionsgardets ledning.[29] Raisi-administrationens toppstyrning tycks ha ökat de iranska aktörernas benägenhet att bli djärvare i åtgärderna mot Israel och västvärlden, särskilt USA, trots diplomatiska insatser för att återuppta kärnteknikavtalet med Iran.

Iranska cyberattacker mot Israel har ökat i takt och omfattning

Några veckor efter att det att Raisi hade bildat sitt utrikespolitiska team[30] återupptog statliga iranska aktörer destruktiva cyberattacker mot Israel i snabbare takt än tidigare år. Utpressningstrojanattacker och hack-and-leak-operationer genomfördes med några veckors mellanrum i början av september och involverade minst tre aktörer med koppling till Iran. Det tyder på att angreppen kan ha varit en del av en landsomfattande vedergällningskampanj mot Israel. I minst ett fall bedömde Microsoft att en utpressningstrojanattack mot en israelisk organisation i slutet av 2021 var tänkt att dölja ett underliggande dataraderingsangrepp. Microsofts analys av den skadliga koden visade att den utpressningstrojan som levererades till offret var programmerad att köra kod som raderade hårddiskar efter kryptering.

År 2022 eskalerade iranska cyberattacker sina attacker och val av mål. I februari försökte DEV-0198 genomföra en destruktivt attack mot israelisk kritisk infrastruktur. Microsoft bedömer även att det sannolikt var en aktör med koppling till Iran som låg bakom en avancerad cyberattack som satte i gång varningssirener om raketanfall i Israel i juni, antagligen genom att använda programvara som justerar ljud via IP-nätverk.

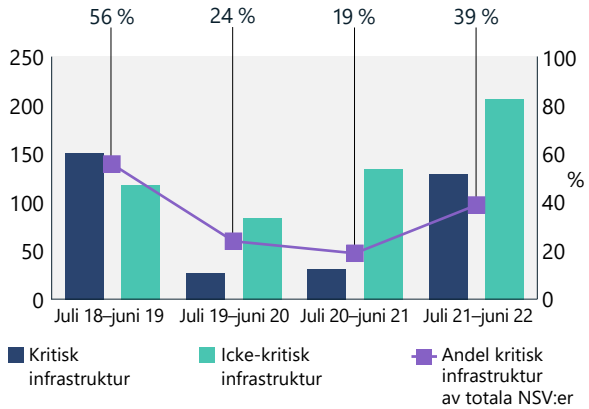
Iranska hot mot USA och Israels kritiska infrastruktur som har inträffat under året

Iranska statliga aktörer som Microsoft bedömer är anknutna till IRGC (PHOSPHORUS och DEV-0198) gav sig på känd amerikansk och israelisk kritisk infrastruktur från slutet av 2021 till mitten av 2022. Syftet var troligen att ge Teheran möjlighet att hämnas mot samma sektorer som högre IRGC-tjänstemän beskyllde USA och Israel för att ha stört i Iran.[31] Vi bedömer att verksamheten är knuten till uttalanden i slutet av oktober 2021 från IRGC-generalen Gholamreza Jalali, chef för Irans passiva försvarsorganisation, som upprepade anklagelser från andra inflytelserika personer inom regimen om att USA och Israel ska ha genomfört cyberattacker mot Irans hamnar, järnvägar och bränslepåfyllningsstationer.[32] Jalali formulerade anklagelsen igen i förberedda kommentarer i ett tal under en fredagsbön på ett podium med bilden av en missil som träffade ordet USA, vilket tyder på att hans överordnade var av samma uppfattning.[33]

PHOSPHORUS började söka av amerikanska organisationer i stor omfattning i oktober 2021 efter okorrigerade Fortinet- och ProxyShell -sårbarheter. När de knäckts användes de okorrigerade systemen för att utföra attacker med utpressningstrojaner, i flera fall mot kritisk infrastruktur i USA och andra västländer. Det här var de första bekräftade fallen av utpressningstrojanattacker med koppling till den iranska staten utanför Mellanöstern. Efter cyberattackerna mot Irans bränslepåfyllningsstationer i slutet av oktober upptäckte Microsoft en ökning av iranska utpressningstrojanattacker mot amerikanska företag, vilket tyder på en möjlig korrelation.

Samtidigt övergick PHOSPHORUS – många gånger genom harpunfiske – till att rikta in sig särskilt mot amerikanska kritiska infrastrukturföretag, däribland större hamnar och internationella flygplatser, transitsystem, allmännyttiga företag och olje- och gasföretag. Den här spjutspetsverksamheten, som ofta utfördes via harpunfiske, varade fram till mitten av 2022. Offren stämmer helt överens med de sektorer som Teheran har anklagat USA och Israel för att ha angripit i Iran och var sannolikt avsedda som hämndaktioner. Intrången i nästan identiska mål skulle kunna ge möjlighet att försvåra framtida angrepp av den typen, samtidigt som man undviker att eskalera konflikten genom att bara signalera orsaken till angreppen, utan att erkänna någon skuld.

Pånyttfött iranskt intresse för infrastruktur



Irans satsning på den kritiska infrastrukturen ökade till de högsta nivåer som har observerats sedan slutet av 2018 och början av 2019. Vi använde det amerikanska Presidential Policy Directive 21 (PPD-21) för att avgöra om ett företag uppfyller kriterierna för kritisk infrastruktur. (Juli 2021–juni 2022).

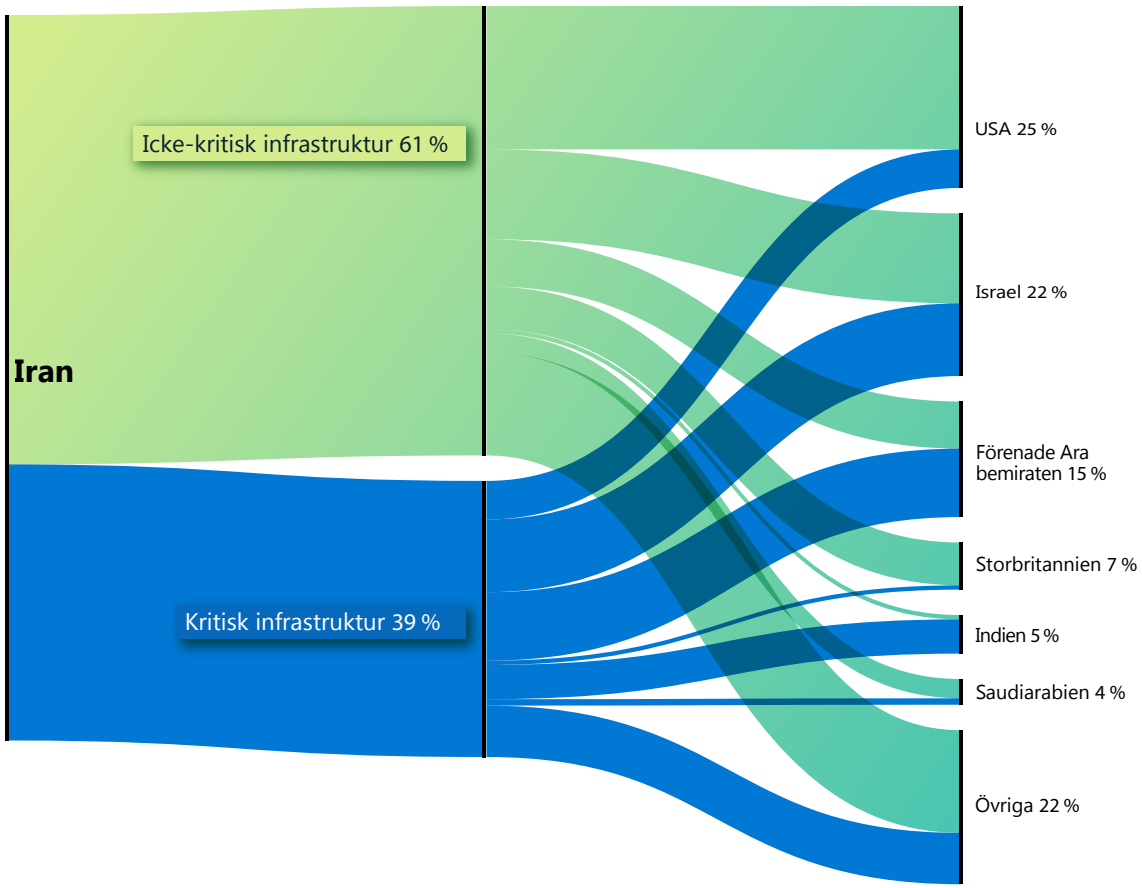
Iran blir alltmer aggressivt efter maktskiftet

fortsättning

I Israel gav sig DEV-0198 på israeliska järnvägar, logistikföretag, programvaruleverantörer till logistikföretag och bränsleföretag med fokus på bensinstationer. I början av 2022 genomförde gruppen ett störande angrepp mot ett stort israeliskt logistikföretags nätverk, vilket tvingade företaget att stänga av sina datorer och stänga en del av sin verksamhet för att begränsa angreppet. I ett annat fall observerade vi att gruppen försökte komma åt en större israelisk transportleverantörs nätverk via stulna eller återanvända autentiseringsuppgifter. Samtidigt knäckte en annan iransk aktör, DEV-0343 – vars inriktning på försvars-, sjötransport- och satellitbildföretag antyder kopplingar till IRGC – konton hos israeliska transport- och hamnrelaterade organisationer i början av 2021.

Iranska hotgrupper förblir sannolikt ett hot mot amerikanska och israeliska transport- och energiföretag, i synnerhet med tanke på att de diplomatiska insatserna för att återuppliva det iranska kärnkraftsavtalet avtar och Washington, Tel Aviv och Teheran försöker hitta alternativa tvångsmedel för att få fram eftergifter.

Irans inriktning på kritisk infrastruktur per land



Irans angrepp mot kritisk infrastruktur skedde huvudsakligen mot israeliska, arabemiratiska och amerikanska organisationer.

Iranska aktörer förblir sannolikt ett hot mot amerikanska och israeliska transport- och energiföretag under det kommande året.

Iranska grupper har utökat utpressningstrojanattackerna bortom sina regionala motståndare och riktar in sig på högprofilerade, viktiga infrastrukturmål i USA och Israel.

Användbara insikter

1. Förbättra organisationens övergripande cyberhygien genom att införa lösningar utan lösenord, till exempel MFA, och använda dem för alla fjärranslutningar för att komma till rätta med eventuellt knäckta autentiseringsuppgifter.
2. Utvärdera äktheten av all inkommande e-posttrafik för att se till att avsändaradressen är legitim.
3. Korrigera tidigt och ofta.[34]
4. Gå igenom och granska samtliga partnerrelationer med tjänsteleverantörer för att minimera onödiga behörigheter mellan din organisation och leverantörer uppströms. Microsoft rekommenderar att ni omedelbart tar bort åtkomsten från alla partnerrelationer som ser obekanta ut eller som ännu inte har granskats.[35]

Länkar till mer information

- Iranian targeting of IT sector on the rise | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Iran-linked DEV-0343 targeting defense, GIS, and maritime sectors | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Libanonbaserad grupp med kopplingar till Iran riktar sig mot Israel

Microsoft övervakar cyberhotsaktiviteter oavsett plattform, avsett offer eller geografisk region. Vi har insyn och jagar aktiva hot i hela världen för att skriva bättre identifieringsmekanismer åt våra kunder.

Även om hot från Ryssland, Kina, Iran och Nordkorea utgör majoriteten av de nationalstatsaktiviteter vi observerar, spårar och meddelar vi också om hot från Natos medlemsländer och demokratiska nationer. Förra året presenterade vi aktivitet av en aktör i Turkiet (SILICON) och en i Vietnam (BISMUTH). I år fyller vi i detaljerna om en Libanonbaserad grupp som vi tidigare har avslöjat offentligt.[36]

Microsoft avslöjade en tidigare odokumenterad Libanonbaserad grupp som vi med relativ tillförlitlighet bedömer drivs i samband med aktörer som är anknutna till Irans underrättelse- och säkerhetsdepartement (MOIS). Ett sådant samarbete eller order från Teheran stämmer väl överens med avslöjanden sedan slutet av 2020 om att Irans regering anlitar tredje man för att utföra cyberverksamhet, vilket underlättar för Iran att förneka inblandning.

POLONIUM gav sig på eller bröt sig in hos ett tjugotal organisationer i Israel och en mellanstatlig organisation med verksamhet i Libanon mellan februari och maj 2022 innan Microsoft gick emellan och offentligt avslöjade verksamheten. Nästan hälften av de israeliska organisationerna ingick i Israels försvarsindustri eller hade kopplingar till israeliska försvarsföretag, vilket tyder på att gruppen har liknande intressen som Iran när det gäller att samla in underrättelser om och/eller direkt motverka Israel.[37]

POLONIUM:s bedömda länkar till MOIS-grupper bygger på observerade överlapp mellan offer och gemensamma verktyg och tekniker.

- Offren överlappar varandra: En iransk statlig grupp som är kopplad till Irans MOIS, som Microsoft spårar som MERCURY, har tidigare brutit sig in hos flera POLONIUM-offer, vilket tyder på konvergerande uppdragskrav eller en möjlig överlämning av offer mellan grupper.
- Gemensamma verktyg och tekniker: I likhet med POLONIUM observerade MSTIC att DEV-0588 (som även kallas CopyKittens) ofta använder AirVPN för sina insatser och att DEV-0133 (som även kallas Lyceum[38]) använder OneDrive för C2 och exfiltrering. I likhet med iranska statliga aktörer använde POLONIUM en molntjänstleverantör för att bryta sig in hos ett israeliskt luftfartsföretag och en advokatbyrå.[39]

POLONIUM installerade ett antal specialimplantat med hjälp av molntjänster för C2 och dataexfiltrering – särskilt OneDrive och DropBox. POLONIUM skapade ofta unika OneDrive-program för sina offer, sannolikt för att undvika upptäckt.

I juni 2022 stängde Microsoft av fler än tjugo OneDrive-appar som POLONIUM hade skapat, aviserade de berörda organisationerna och satte in en rad uppdateringar av säkerhetsunderrättelser för att sätta POLONIUM-utvecklade verktyg i karantän.

Microsoft upptäckte och inaktiverade POLONIUM:s missbruk av OneDrive för C2.

Användbara insikter

1. Uppdatera antivirusverktyg[40] och se till att molnskydden[41] är aktiverade för att identifiera relaterade indikatorer.
2. Kunder med tjänsteleverantörsrelationer måste gå igenom och granska alla partnerrelationer för att minimera onödiga behörigheter mellan organisationen och leverantörer uppströms.[42] Ta omedelbart bort åtkomsten för alla partnerrelationer som verkar obekanta eller som inte har granskats.

Länkar till mer information

- Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

Nordkoreas cyberkapacitet används för att uppnå regimens tre huvudsakliga mål

Nordkoreas cyberprioriteringar under det senaste året har återspeglat statens angivna globala prioriteringar. Kim Jong Un framhävde de tre prioriteringarna om att bygga upp försvarskapacitet, stärka landets dåliga ekonomi och säkerställa inhemsk stabilitet i flera viktiga tal.[43] De åtgärder som har vidtagits av nordkoreanska statliga aktörer visar tydligt att cybersfären används för att uppnå de tre målen.

Nordkoreanska statliga aktörer använde en rad metoder för att försöka tränga sig in hos luftfartsföretag runtom i världen.

Nordkoreanska statliga hotgrupper, främst CERIUM och ZINC, använde en mängd metoder för att försöka tränga sig in i nätverk på försvars- och luftfartsföretag runtom i världen. När Nordkorea inledde sin mest aggressiva period med missiltester någonsin under första halvåret 2022, använde landet cyberspionage för att hjälpa nordkoreanska forskare att få ett försprång vid utvecklingen av inhemska försvarssystem och motåtgärder mot de framsteg som dess fiender gjorde.

Vi har observerat COPERNICIUM rikta in sig på en mängd olika kryptovalutarelaterade företag runtom i världen, ofta framgångsrikt, för att stödja Nordkoreas dåliga ekonomi. Även om vi inte kan bekräfta om gruppen lyckats få loss pengar efter intrången, observerade vi att COPERNICIUM infekterade dussintals maskiner genom att skicka skadliga dokument som maskerades som förslag från andra kryptovalutaföretag.

Slutligen arbetade en grupp som Microsoft spårar under namnet DEV-0215 för att upprätthålla stabilitet och lojalitet i Nordkorea genom att rikta in sig på nyhetsorganisationer som rapporterar om nordkoreanska frågor. Nyhetsorganisationerna har källor både i Nordkorea och i avhoppargrupper, som Pyongyang ser som ett hot mot sin existens. Dessutom arbetade gruppen för att få tillgång till nätverk av koreansktalande kristna grupper, som brukar vara uttalat mot Nordkorea och arbeta aktivt med nordkoreanska avhoppare.

Inriktning på försvars- och luftfartsföretag

Nordkoreanska statliga aktörer ledda av CERIUM och ZINC lägger mycket arbete på att utveckla taktik som syftar till att göra intrång i försvars- och luftfartsföretag. CERIUM satte upprepade gånger in nålstick mot sydkoreanska virtuella privata nätverk (VPN) genom att hämta klienter och leta efter brister. Gruppen hämtade också vanliga program som används av sydkoreanska militär- och myndighetskunder, förmodligen för att leta efter sårbarheter. Gruppen följde aktuella händelser noga och skrev nya lockbeten med omtalade ämnen för att uppmuntra offren att klicka på deras skadliga kod och länkar.

Både ZINK och CERIUM använde sociala medier och social manipulering i kampanjer. ZINK inriktade sig särskilt på att skapa falska profiler på LinkedIn och andra professionella sociala medier, där operatörerna låtsades rekrytera till stora försvars- och luftfartsföretag. Med hjälp av de här profilerna skickade de länkar eller skadliga filbilagor till potentiella offer med hjälp av direktmeddelanden i sociala medier eller per e-post.

Utöver anställda i företag gav sig CERIUM också i stor omfattning på sydkoreanska militärer och visade särskilt intresse för både sydkoreanska militära akademier och militärer som arbetar i den akademiska världen.

Inriktning på kryptovaluta för att väga upp för förluster

Sedan FN-ledda sanktioner inleddes 2016 har Nordkoreas ekonomi fortsatt att krympa och läget har förvärrats av naturkatastrofer som översvämningar[44] och torka[45] samt en nästan total stängning av gränsen för import sedan covid-19-pandemin kom igång i början av 2020.[46] Även om Nordkorea öppnade sina gränser för handel med Kina ett kort tag i början av 2022 stängdes de snart igen.[47] I mitten av maj rapporterade Nordkorea sitt första inhemska fall av covid-19.[48] Landet har sedan dess tillämpat en liknande covid-strategi som Kina, med gigantiska nedstängningar för att bekämpa viruset, vilket har påverkat Nordkoreas redan bräckliga ekonomi negativt.

Den nordkoreanska statliga gruppen COPERNICIUM försökte kompensera för en del av de förlorade intäkterna genom att stjäla pengar – vanligtvis i form av kryptovaluta – från alla företag vars nätverk de lyckades ta sig in i. Vi observerade intrång i tiotals maskiner som tillhörde kryptovalutarelaterade företag i USA, Kanada, Europa och i hela Asien. COPERNICIUM bröt sig även in i maskiner som tillhör kryptovalutarelaterade företag hos Nordkoreas främsta allierade, Kina, både på fastlandet och i Hongkong. Gruppen utnyttjade sociala medier i hög grad för sin inledande rekognoscering och kontaktförsök med målen. Aktörerna skapade profiler och låtsades vara utvecklare eller höga tjänstemän i företag som jobbar med kryptovaluta. Sedan upprättade de relationer med andra i branschen och skickade skadliga länkar eller filer när de fått kontakt.

Nordkoreas cyberkapacitet används för att uppnå regimens tre huvudsakliga mål

fortsättning

En grupp som är relaterad till PLUTONIUM utvecklar och distribuerar utpressningstrojaner

En grupp aktörer med ursprung i Nordkorea som Microsoft spårar under namnet DEV-0530 började utveckla och använda utpressningstrojaner under angrepp i juni 2021. Gruppen som kallade sig H0lyGh0st använde en utpressningstrojannyttolast med samma namn i sina kampanjer och lyckades ta sig in hos småföretag i flera länder redan i september 2021.

Microsoft bedömde att DEV-0530 hade kopplingar till en annan nordkoreansk grupp som spåras under namnet PLUTONIUM (eller DarkSeoul eller Andariel). Även om det bara är DEV-0530 som använder utpressningstrojanen H0lyGh0st i sina kampanjer, observerade MSTIC kommunikation mellan de två grupperna, liksom att DEV-0530 använder verktyg som skapats uteslutande av PLUTONIUM.

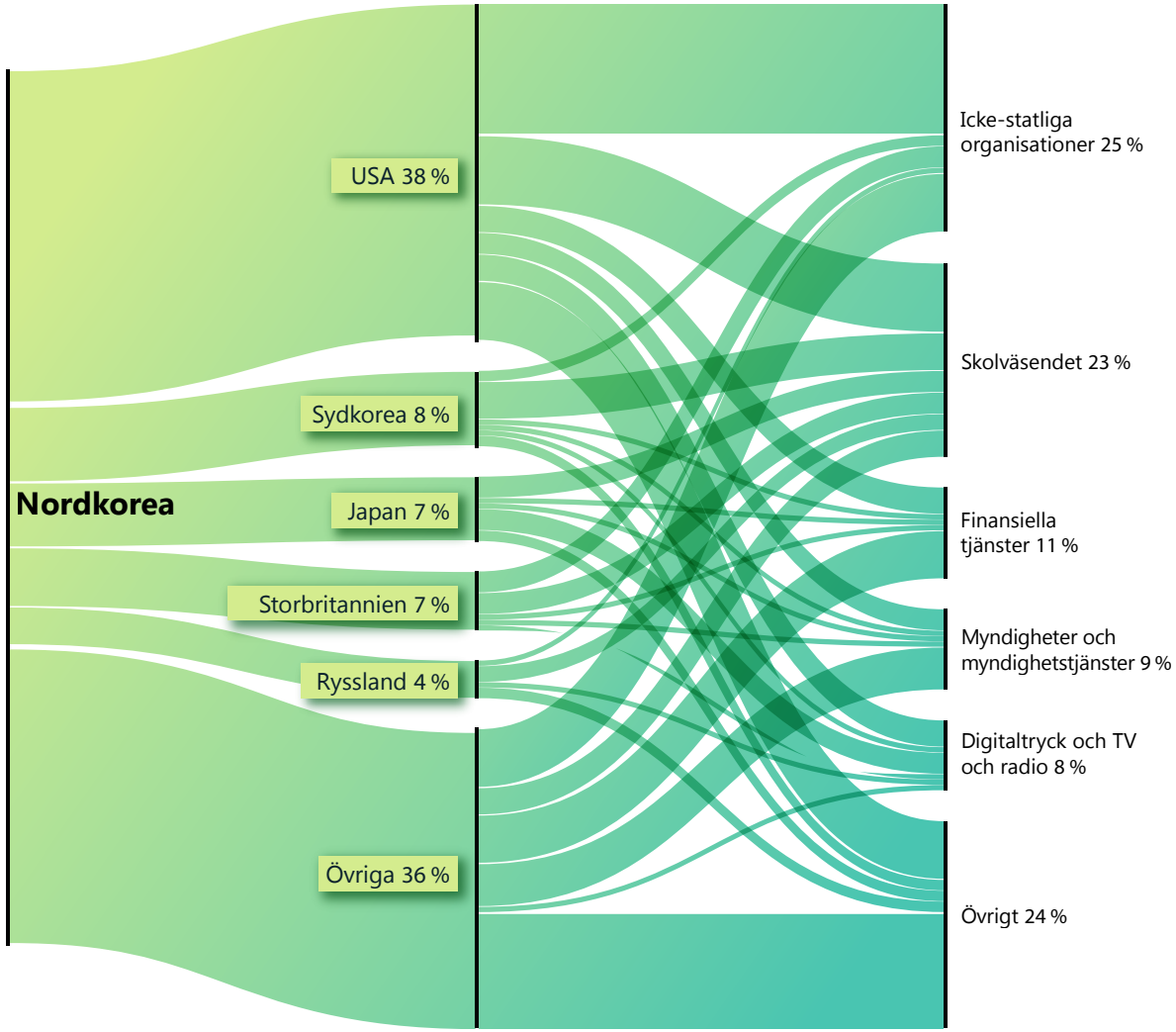
Det är inte säkert att DEV-0530:s verksamhet sponsrades av staten. Även om angrepp med utpressningstrojaner kunde ha beställts av staten av samma anledning som den står bakom stöld från kryptovalutaföretag, är det också möjligt att aktörerna bakom DEV-0530 agerade självständigt för att själva tjäna pengar. Om det var nordkoreanska hackare som agerade självständigt skulle det förklara varför aktiviteten inte var så utbredd jämfört med de statligt sponsrade stöldåtgärderna mot kryptovalutaföretag.

Inriktning på nordkoreanska nyhetskanaler, avhoppare, religiösa grupper och hjälporganisationer

Under det senaste året var Den store efterträdaren Kim Jong Un offentligt mer fokuserad på inre säkerhet och lojalitet än missiler och kärnvapen. Minst två nordkoreanska statsgrupper fokuserade på aspekter som regimen skulle se som inhemska hot, vilket återspeglar intresset för interna frågor.

Den första var en grupp som Microsoft spårar under namnet DEV-0215, som riktar in sig på medieorganisationer som noga följer nordkoreanska nyheter. En trolig anledning till intresset för de här medierna är att de får sina nyheter från nordkoreanska avhoppare, kinesiska medborgare som samarbetar nära med Nordkorea, och till och med några nordkoreanska medborgare inne i landet, som använder en rad metoder för att kommunicera med omvärlden. De nordkoreanska myndigheterna betraktar de här grupperna som ett hot mot sin överlevnad. Särskilt gäller det medborgare i Nordkorea, som skulle ses som förrädare och spioner. DEV-0215 försökte förmodligen identifiera mediernas källor så att de skulle kunna neutralisera potentiella informationsläckor.

Nordkorea: De mest utsatta länderna och branscherna



Nordkorea betraktar USA, Sydkorea och Japan som sina främsta fiender. Även om Ryssland är allierat sedan länge, riktar sig nordkoreanska hotaktörer mot ryska tankesmedjor, akademiker och diplomater för att få information om Rysslands åsikter i globala frågor.

Nordkoreas cyberkapacitet används för att uppnå regimens tre huvudsakliga mål

fortsättning

Microsoft såg också tecken på att DEV-0215 riktade in sig mot koreansktalande kristna samfund. Evangeliska kristna koreanska kyrkor brukar vara kritiska mot både Nordkorea och sydkoreanska regeringar som gynnar engagemang med Nordkorea. Många av de här kyrkorna bedriver uppsökande verksamhet hos avhoppare och en del ägnar sig åt humanitärt arbete med Nordkorea. Nordkorea betraktar dem som ett hot – även om antalet avhoppare från Nordkorea mer eller mindre avstannat helt under pandemin[49] – eftersom de här kristna grupperna ofta spelar en avgörande roll för att hjälpa avhoppare att fly. DEV-0215 har genererat falska dokument om kristna konferenser för koreansktalande som lockbeten för att rikta in sig på gruppen och ta reda på vilka som hjälper till att organisera avhopp.

Slutligen visade den statliga gruppen OSMIUM ett stadigt intresse för internationella hjälporganisationer under hela året, däribland organisationer som tidigare har hjälpt Nordkorea. Även om Nordkorea i allmänhet har tackat blankt nej till erbjudanden om hjälp utifrån, särskilt sedan utbrottet av covid-19[50], är det möjligt att Nordkorea överväger att tacka ja till erbjudanden om hjälp men att man är försiktig med följderna vad säkerhet beträffar av att tillåta utländska biståndsarbetare i landet. Nordkorea kanske gör intrång i nätverken hos hjälporganisationer över hela världen för att avgöra om de ska tillåta sådant stöd i sitt eget land.

Användbara insikter

1. Nordkoreanska statliga aktörer är skickliga, obevekliga och kreativa, men alla organisationer kan försvara sig mot dem.
2. De flesta framgångsrika angrepp går att stoppa med grundläggande cyberhygien, till exempel tvåfaktorsautentisering eller att inte öppna bilagor från okända personer i en virtuell miljö.

Länkar till mer information

- Nordkoreanska hotaktörer ger sig på små och medelstora företag med utpressningstrojanen H0lyGh0st | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)



Bland experter på Nordkorea har det länge debatterats om den nordkoreanska regeringen menar allvar med sina offentliga uttalanden eller om det mest handlar om effektsökeri. Likheten mellan cyberattackerna och de prioriteringar som Nordkorea har pratat om bekräftar dock tron på att Nordkorea menar vad man säger när landet offentligt talar om sina mål.

Cyberlegoknektar hotar stabiliteten i cyberrymden

Det finns ett växande antal privata företag som utvecklar och säljer verktyg, tekniker och tjänster som gör att deras kunder – ofta länder – kan bryta sig in i nätverk, datorer, telefoner och internetanslutna enheter. Företagen är en tillgång för nationella statsaktörer och utsätter i många fall dissidenter, människorättsivrare, journalister, förespråkare för civilsamhället och andra privata medborgare för risker. Vi kallas dem cyberlegoknektar eller offensiva aktörer inom den privata sektorn.

En värld där företag inom den privata sektorn skapar och säljer cybervapen är farligare för konsumenter, företag i alla storlekar och för länder. De här offensiva verktygen går att använda på sätt som är oförenliga med normer och värderingar för god styrning och demokrati. Microsoft anser att skyddet av mänskliga rättigheter är en grundläggande skyldighet och vi tar det på stort allvar genom att begränsa ”övervakning som tjänst” över hela världen.

Microsoft har bedömt vissa statliga aktörer i demokratiska och auktoritära regimer som lägger ut utvecklingen eller användningen av övervakning som tjänst-teknik på entreprenad. På så sätt undviker de ansvar och tillsyn och skaffar sig kapacitet som annars skulle vara svår att utveckla på egen hand.

> Cybervapnen förser nationalstaterna med övervakningskapacitet som de inte skulle ha kunnat utveckla på egen hand.

Marknaden där cyberlegoknektarna verkar saknar insyn. Trots det fortsätter vi att observera de här grupperna som använder dag noll-intrång och till och med nollklicksintrång som inte kräver att offren gör något alls och därmed ger tillgång till övervakning som tjänst.

Microsoft offentliggjorde nyligen en offensiv aktör i den europeiska privata sektorn som vi kallar KNOTWEED, ett företag i Österrike som heter DSIRF. Flera nyhetsrapporter har kopplat företaget till utvecklingen och försöket att sälja en skadlig koduppsättning som heter Subzero.[51] Offren omfattar advokatbyråer, banker och strategiska konsultföretag i länder som Österrike, Storbritannien och Panama.[52]

Eftersom de här offensiva övervakningsfunktionerna inte längre är högt säkerhetsklassade funktioner som har tagits fram av försvars- och underrättelseorgan utan kommersiella produkter som nu säljs till företag och enskilda, måste alla regelverk för cybervapen se bortom exportkontroll. Effekten av de här cybervapnen kan vara förödande.

När en cyberlegoknekt utnyttjar en sårbarhet i en produkt eller tjänst utsätts hela datorekosystemet för risk. När sårbarheter identifieras offentligt har företagen kort tid på sig att släppa skydd innan breda angrepp följer (se den tidigare diskussionen om utnyttjande av sårbarheter). Det här är en farlig och svår cykel för både programvaruleverantörer (som snabbt måste utveckla korrigeringar) och för konsumenter av produkter (som måste installera korrigeringarna omedelbart).

Som en av grundarna till Cybersecurity Tech Accord[53] – en ledande allians där fler än 150 teknikföretag samlas – har Microsoft åtagit sig att inte delta i offensiv verksamhet på nätet. Vi står fast vid det engagemanget och vårt ansvar för mänskliga rättigheter inom det här området. Vi har ägnat oss åt tekniska störningar och rättsliga insatser för att belysa de negativa effekterna av de tjänster som tillhandahålls av cyberlegoknektar och kommer att fortsätta skydda våra kunder när vi ser missbruk.

> Cyberlegoknektar skapar och tillhandahåller funktioner för övervakning som tjänst som är tekniskt avancerade och allmänt tillgängliga, däribland avancerad skadlig kod samt en rad metoder.

Användbara insikter för myndigheter

1. Inför krav på insyn och tillsyn för övervakning som tjänst, särskilt vid upphandling, inklusive förbud mot offensiva aktörer, vilket USA har gjort med handelsdepartementets lista över företag som befinner sig på svarta listan.
2. Inför begränsningar efter anställning för tidigare medarbetare inom den här sektorn.
3. Sträva efter att införa kundkännedomsansvar och uppmuntra företag att upprätthålla sina åtaganden om mänskliga rättigheter.

Länkar till mer information

- Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Fortsätt kampen mot den privata sektorns cybervapen | Microsoft On the Issues

Organisera cybersäkerhetsnormer för fred och säkerhet i cyberrymden

Vi behöver snabbt införa ett konsekvent och globalt ramverk som prioriterar mänskliga rättigheter och skyddar människor från staters besinningslösa beteende på nätet. Ingenstans syns detta tydligare än i det pågående kriget i Ukraina. Utöver en global strategisk insats kan länder agera nu för att få en omedelbar positiv effekt.

För fem år sedan propagerade Microsoft för en digital Genève-konvention för att främja ansvar och skyldigheter inom olika sektorer för att försvara freden och säkerheten på nätet. Cyberrymden började framträda som ett separat och föränderligt område fyllt av konflikter och konkurrens mellan länder där angrepp blir allt vanligare, även i fredstid.

I dag finns det fortfarande ett tydligt behov av ett sådant ramverk, vilket framgår tydligt av ryska cyberattacker mot Ukraina som ett led i Rysslands invasion. Det här kriget har skapat en ny frontlinje som skiljer sig dramatiskt från vad vi har sett tidigare.

För att bringa stabilitet till cyberrymden krävs det att de globala styrningsinstitutionerna stärks och förnyas så att de passar för ändamålet. Cyberrymden skiljer sig i grunden från andra områden – den är gränslös, syntetisk och underhålls till stor del av det privata näringslivet. Det betyder att teknikindustrin måste ta mer ansvar både för produkters och tjänsters säkerhet och det övriga digitala ekosystemet. Även om det har skett betydande framsteg på alla fronter har utmaningarna vuxit dramatiskt.

Vi måste kavla upp ärmarna ännu mer för att tillsammans försvara säkerheten i cyberrymden. Vi kan inte ta de rättigheter och friheter som vi har kommit att förvänta oss på nätet för givna. Samtidigt som vi kämpar för att ta itu med utmaningarna planerar illasinnade aktörer hur och var de ska slå till härnäst med hjälp av AI. De utnyttjar desinformation och hittar sätt att undergräva det spirande metaversumet. Människorättsförsvarare, teknikindustrin och länder som respekterar rättigheter måste samarbeta för att uppnå en positiv vision om en säker och trygg onlinevärld. Vägen dit är lång, men det finns saker som länder kan göra nu för att omedelbart förbättra cybersäkerhetens ekosystem:

- Nämn normer, lagar och konsekvenser i tillskrivningar. En viktig förbättring under de senaste fem åren har varit hur snabbt och samordnat länder tillskrivs cyberattacker. För att stärka medvetandet om de internationella förväntningarna är det viktigt att uttalandena inte bara namnger och pekar ut de ansvariga utan också betonar vilka internationella lagar eller normer som har kränkts och vilka påföljder det kommer att medföra.
- Förtydliga tolkningen av internationell rätt på nätet. Även om länderna är överens om att internationell rätt gäller på nätet kvarstår frågor om hur den ska tillämpas i specifika fall. Det märks tydligt i efterdyningarna av invasionen av Ukraina. Länder kan göra mycket för att sätta upp förväntningar, undvika missförstånd och skapa förtroende genom att tala om hur de ser på sina skyldigheter enligt internationell rätt.
- Rådgör med andra intressenter. När internationella forum fortsätter att komma fram till de bästa sätten att underlätta robust inkludering av många intressenter, kan länder ställa sig bakom välgrundade dialoger genom att rådgöra med alla intressenter, i synnerhet teknikindustrin, för att säkerställa att dialogen underlättas av personer med oumbärlig expertis.
- Bilda ett stående organ för att stödja ansvarsfullt beteende från länder i cyberrymden. Arbetet med internationella diplomatiska forum för att främja ansvarsfullt beteende från länder online har aldrig varit viktigare. Det finns ett tydligt behov av en permanent FN-mekanism för att handskas med cyberrymden som konfliktområde.
- Definiera nya normer för föränderliga hot. Cyberrymdshot utvecklas ständigt i takt med de tekniska innovationerna. Även om internationella normer bör vara teknikneutrala måste de uppdateras och justeras när hotbilden och vårt sätt att använda tekniken förändras. Än i dag ser vi att brister i det befintliga internationella ramverket missbrukas. Stater bör åta sig att uttryckligen skydda viktiga processer som ligger till grund för det digitala ekosystemet och som inte skyddas nu, t.ex. programuppdateringsprocessen. Dessutom behöver en del specifika områden ytterligare skydd. Som pandemin har visat är det viktigt med normer för att skydda hälso- och sjukvården.

Nationella statsaktörer och deras angrepp ökar i volym och blir alltmer avancerade, vilket skapar en ohållbar situation.

Omedelbara åtgärder är absolut nödvändiga. Det finns åtgärder som stater kan vidta nu för att genast förbättra cybersäkerhetsekosystemet, bland annat att införa överenskomna normer och regler för länders beteende i cyberrymden och samarbeta med alla andra intressenter för att åtgärda nya luckor.

Multilaterala institutioner måste konstrueras om för att ta itu med det akuta problemet med cyberattacker från nationalstater.

Länkar till mer information

- A moment of reckoning: the need for a strong and global cybersecurity response | Microsoft On the Issues
- Cyberattacks targeting health care must stop | Microsoft On the Issues
- The next chapter of cyber diplomacy at the United Nations beckons | Microsoft On the Issues

Slutnoter

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. Den kritiska infrastrukturen i det här kapitlet definieras av Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience (februari 2013).
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

Slutnoter, fortsättning

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. Korrigera i synnerhet Exchange-servrar mot ProxyShell-sårbarheter (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065, CVE-2021-34473). Korrigera även Fortinets FortiOS SSL VPN-enheter mot sårbarheter.
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. Som vi har nämnt i vår teknikblogg innebär identifieringen av mål i ett land inte nödvändigtvis att en DSIRF-kund finns i samma land, eftersom internationella insatser är vanliga.
53. Hem | Cybersecurity Tech Accord (cybertechaccord.org)

Enheter och infrastruktur

På grund av den allt snabbare digitaliseringen är säkerheten i den digitala infrastrukturen viktigare än någonsin.

En översikt över Enheter och infrastruktur 57

Introduktion 58

Länder agerar för att förbättra den kritiska infrastrukturens säkerhet och motståndskraft 59

IoT och OT i blickfånget: trender och angrepp 62

Hackning av försörjningskedjan och inbyggd programvara 65

Fokus på sårbarheter i inbyggd programvara 66

Rekognosceringsbaserade OT-angrepp 68

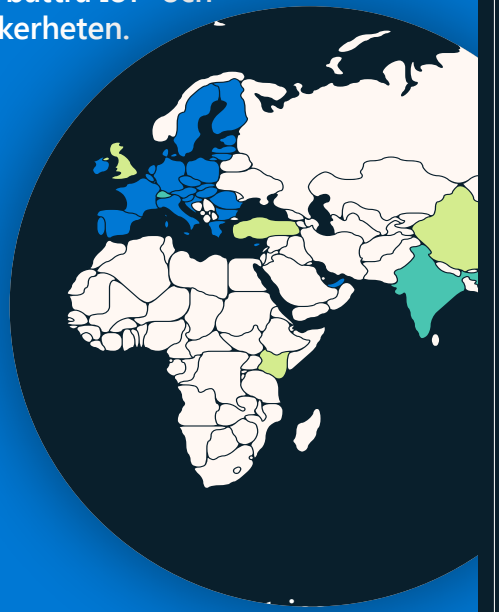
En översikt över

enheter och infrastruktur

Pandemin och det snabba införandet av internetanslutna enheter av alla de slag som en komponent i den accelererande digitaliseringen, har kraftigt ökat attackytan i vår digitala värld.

Cyberbrottslingar och nationalstater är snabba att utnyttja möjligheterna. Även om säkerheten för IT-maskinvara och programvara har stärkts på senare år har säkerheten för IoT- (sakernas internet) och OT-enheter (driftteknik) inte hållit jämna steg. Hotaktörer utnyttjar sådana enheter för att ta sig in i nätverk för att sedan röra sig lateralt och få fotfäste i en försörjningskedja eller störa målorganisationens OT-verksamhet.

Myndigheter över hela världen anstränger sig för att skydda den kritiska infrastrukturen genom att förbättra IoT- och OT-säkerheten.

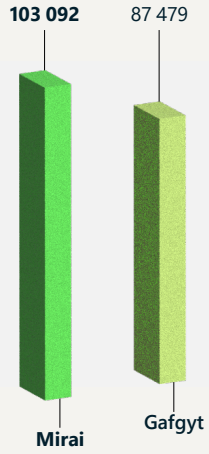


Läs mer på s. 59

Globalt konsekventa och driftkompatibla säkerhetspolicyer behövs för att säkerställa ett brett införande.

Läs mer på s. 59

Skadlig kod som tjänst har blivit en storskalig verksamhet mot exponerad IoT och OT i infrastruktur och allmännyttan samt företagsnätverk.



Läs mer på s. 63

Angreppen mot fjärrhanteringsenheter ökar. Över 100 miljoner angrepp observerades i maj 2022, en femfaldig ökning på ett år.

Läs mer på s. 62



Angriparna utnyttjar i allt högre grad sårbarheter i IoT-enheters inbyggda programvara för att infiltrera företagsnätverk och inleda förödande angrepp.

Läs mer på s. 65

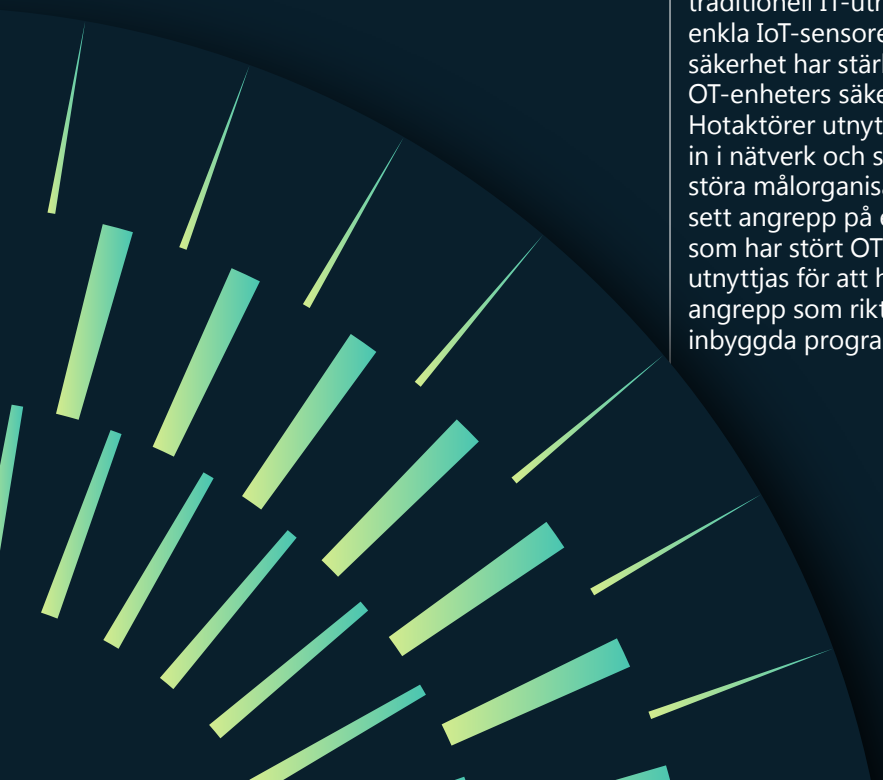
32 % av den analyserade inbyggda programvaran innehöll minst tio kända kritiska sårbarheter.



Läs mer på s. 66

Introduktion

Den accelererande digitaliseringen har ökat cybersäkerhetsrisken för den kritiska infrastrukturen och cyber-fysiska system.



De senaste åren har vi sett en aldrig tidigare skådad förändring i den digitala världen. Organisationer utvecklas för att utnyttja framsteg inom databehandlingskapacitet från både det intelligenta molnet och den intelligenta nätverksgränsen. Till följd av att pandemin tvingat organisationer att digitalisera för att överleva och att branscher över hela världen i snabb takt börjat använda enheter som är öppna mot internet ökar attackytan i den digitala världen exponentiellt.

Den snabba migreringen har lämnat säkerhetsexperterna i bakvattnet. Under det senaste året har vi observerat hot där enheter utnyttjas i alla delar av organisationen, från traditionell IT-utrustning till OT-styrenheter eller enkla IoT-sensorer. Även om IT-utrustningens säkerhet har stärkts på senare år har IoT- och OT-enheters säkerhet inte hållit jämna steg. Hotaktörer utnyttjar sådana enheter för att ta sig in i nätverk och sedan röra sig lateralt eller för att störa målorganisationens OT-verksamhet. Vi har sett angrepp på elnät, utpressningstrojanattacker som har stört OT-drift, IoT-routrar som utnyttjas för att hålla sig kvar i nätverk och angrepp som riktas mot sårbarheter i den inbyggda programvaran.

Även om förekomsten av IoT- och OT-sårbarheter är ett problem för alla organisationer, löper kritisk infrastruktur ökad risk, eftersom hotaktörerna har lärt sig att kritiska tjänster som stängs av är ett kraftfullt argument. Utpressningstrojanattacken mot Colonial Pipeline Company 2021 visade hur brottslingar kan störa en viktig tjänst för att öka sannolikheten att få en lösensumma. Och Rysslands cyberattacker mot Ukraina demonstrerar att vissa nationalstater ser cyberattacker mot kritisk infrastruktur som acceptabelt sabotage för att uppnå sina militära mål.

Men det ljusnar vid horisonten. Beslutsfattare och nätverksförsvarare agerar för att förbättra den kritiska infrastrukturens cybersäkerhet, däribland de IoT- och OT-enheter de förlitar sig på. Beslutsfattare påskyndar utvecklingen av lagar och förordningar för att bygga upp allmänhetens förtroende för cybersäkerheten i kritisk infrastruktur och enheter.

Microsoft samarbetar med länder runtom i världen för att ta detta tillfälle i akt att förbättra cybersäkerheten och vi välkomnar fler till bordet. Vi är dock oroade över att inkonsekventa, skräddarsydda eller komplexa krav kan få oavsiktliga effekter och kanske minska säkerheten i vissa fall genom att avleda knappa säkerhetsresurser mot efterlevnad av flera certifieringar med samma slutmål.

Ur säkerhetsåtgärdssynpunkt använder alla som försvarar nätverk flera metoder för att förbättra organisationens IoT-/OT-säkerhetsläge. En metod är att införa kontinuerlig övervakning av IoT- och OT-enheter. En annan är att ”vänsterskifta”, vilket innebär att man kräver och inför bättre cybersäkerhetsmetoder för själva IoT- och OT-enheterna. En tredje metod är att införa en säkerhetsövervakningslösning som omfattar både IT- och OT-nätverk. Den här helhetssynen har dessutom den betydande fördelen av att bidra till viktiga organisatoriska rutiner, till exempel att ”riva barriärerna” mellan OT och IT, vilket i sin tur gör det möjligt för organisationen skaffa sig ett bättre säkerhetsläge och uppnå affärsmålen.

Michal Braverman-Blumenstyk
Corporate Vice President, Chief Technology Officer, Cloud and AI Security

Länder agerar för att förbättra den kritiska infrastrukturens säkerhet och motståndskraft

Länder i hela världen tar fram och utvecklar policyer för att hantera cybersäkerhetsrisker i den kritiska infrastrukturen. Många inför även policyer för att förbättra IoT- och OT-enheters säkerhet. Den växande globala vågen av policyinitiativ skapar enorma möjligheter att förbättra cybersäkerheten, men innebär också utmaningar för intressenter i hela ekosystemet.

Det är viktigt men komplicerat att skapa en helhetsvision för hantering av cyberrisker i den kritiska infrastrukturen, särskilt med tanke på alla samband mellan tekniker och globala leverantörer, alla olika sätt att använda tekniken och motsvarande risker, samt behovet av att investera i strategier på både kort och lång sikt. Effektivt avgränsade policyer som ligger bakom iterativt lärande och förbättringar och stöder global, sektoröverskridande interoperabilitet, kan underlätta hanteringen av komplexitet och möjliggöra en mer säkerhetsmedveten digitalisering. Men en fragmenterad strategi för lagstiftning skulle kunna leda till överlappande och inkonsekventa lagkrav. Det skulle kunna påverka resurser och i slutänden undergräva säkerhetsmålen.

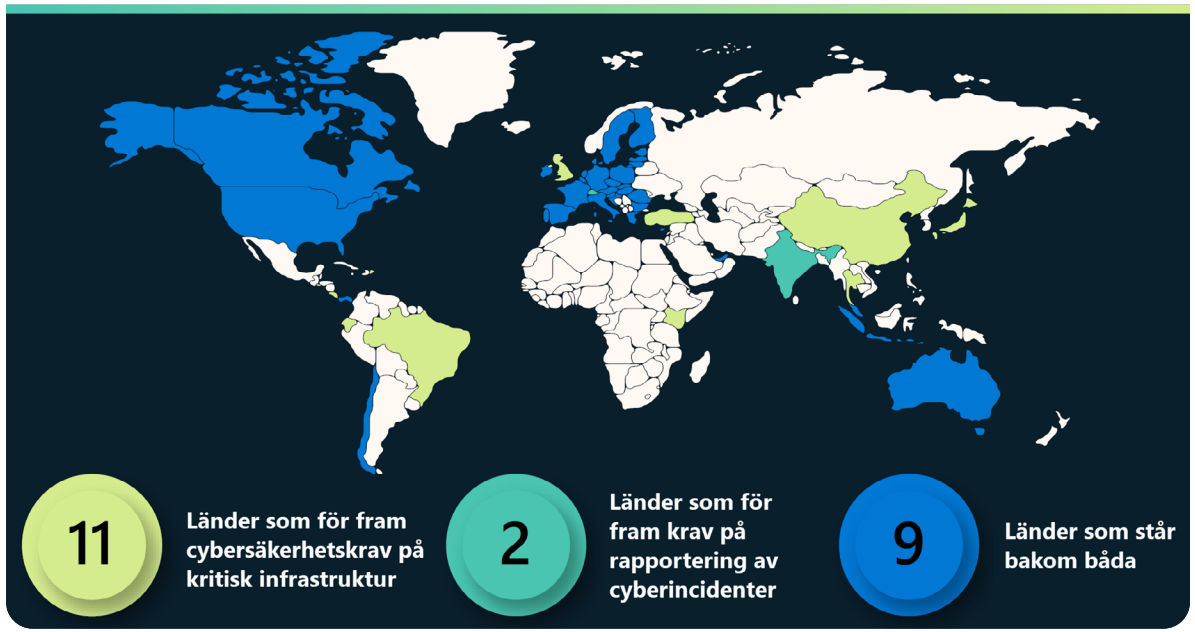
Organisationer skulle till exempel kunna avleda resurser från innovation och säkerhet till byråkratiska efterlevnadsövningar.

Microsoft vill samarbeta med länder över hela världen för att nå fram till effektiva strategier för cybersäkerhet i den kritiska infrastrukturen, öka inblicken i svårigheterna och möjligheterna samt stödja insatser för att förbättra det samfällda riskläget.

Policyutveckling inom hanteringen av cybersäkerhet i den kritiska infrastrukturen

Under det senaste året har flera länder och områden, däribland Australien, Chile, Europeiska unionen (EU), Japan, Singapore, Storbritannien och USA, utvecklat, uppdaterat eller genomfört sektoröverskridande eller sektorspecifika cybersäkerhetskrav.[1] Många av dem – och andra som Indien[2] och Schweiz[3] – har redan utfärdat eller håller på att utveckla krav på rapportering av cybersäkerhetsincidenter för den kritiska infrastrukturen och viktiga tjänsteleverantörer.[4]

En del anmärkningsvärda politiska utvecklingar skedde i Australien, EU, Indonesien och USA under det senaste året. Australien införde två lagar för att bli bättre på att hantera sektoröverskridande cybersäkerhetsrisker för den kritiska infrastrukturen. Lagarna pekar bland annat ut nya kritiska infrastruktursektorer, kräver att riskhanteringsplaner tas fram, föreskriver rapporter om cybersäkerhetsincidenter och ger staten möjlighet att ingripa om den bedömer att en organisation som sköter om kritisk infrastruktur inte vill eller kan reagera lämpligt på en incident.



EU gjorde framsteg mot att uppdatera sitt NIS-direktiv från 2016, som utgör en ram för EU:s medlemsstater att reglera tekniska tjänster och produkter som bedöms vara viktiga för unionens ekonomi och samhällsfunktionen. NIS 2-förslaget omfattar revideringar som skulle införa en ny kritisk digital infrastrukturskategori, öka kraven på rapportering av cyberincidenter och införa ytterligare krav på riskhantering av cybersäkerheten. EU tog även fram ett förslag till uppdatering av sin rättsakt om digital operativ motståndskraft för finanssektorn (DORA), vilket gav nya krav på den informationskommunikationsteknik som används inom sektorn för finansiella tjänster.

I maj utfärdade Indonesien en presidentförordning om skydd av viktig informationsinfrastruktur (IIV) som kommer att börja gälla i maj 2024 och bland annat omfattar sektorer som energi, transport, finans och hälsa. Indonesiens mål med förordningen är att skydda kontinuiteten vid genomförandet av förordningen, förhindra cyberattacker och öka beredskapen att hantera cyberincidenter. IIV-leverantörer kommer att ansvara för att ha ett säkert och tillförlitligt skydd, implementera effektiv hantering av cyberrisker och rapportera cyberriskresultat till motsvarande myndigheter. Förordningen innehåller ett krav på att rapportera cyberincidenter inom 24 timmar.

Länder agerar för att förbättra den kritiska infrastrukturens säkerhet och motståndskraft

fortsättning

Den amerikanska kongressen stiftade en lag som bemyndigade Cybersecurity and Infrastructure Security Agency (CISA) att utfärda förordningar som kräver rapportering av cyberincidenter av dem som sköter den kritiska infrastrukturen och US Transportation Security Administration (TSA) utfärdade nya sektorspecifika cybersäkerhetskrav inom transportsektorn. År 2021 utfärdade TSA två säkerhetsdirektiv till dem som hanterar pipelines för farliga vätskor och naturgas som reaktion på angreppet med en utpressningstrojan mot Colonial Pipeline Company:

- Det första direktivet kräver att operatörerna utser en cybersäkerhetssamordnare, rapporterar cyberincidenter inom tolv timmar och genomför en sårbarhetsbedömning av sina system.
- Det andra direktivet, som TSA reviderade 2022, kräver att de inför specifika begränsningsåtgärder för att skydda mot angrepp med utpressningstrojaner och andra kända hot mot IT- och OT-system, utvecklar och genomför en beredskaps- och reaktionsplan för cybersäkerhet inom 30 dagar samt genomgår en årlig granskning av utformningen av cybersäkerhetsarkitekturen.

TSA byggde vidare på sina förordningar för pipelines genom att utfärda två ytterligare säkerhetsdirektiv senare under 2021. De fastställde cybersäkerhetskrav som gällde godståg, passagerarjärnvägsbolag och transportsystem per järnväg. Direktiven kräver att operatörerna utser en cybersäkerhetssamordnare, rapporterar cybersäkerhetsincidenter inom 24 timmar, utvecklar och inför en incidentresponsplan för cybersäkerhet och genomför en sårbarhetsbedömning av cybersäkerheten. TSA meddelade samtidigt att man även uppdaterade sina flygsäkerhetsprogram och krävde att flygplats- och flygbolag genomförde de två första bestämmelserna, utsåg en samordnare och rapporterade incidenter inom 24 timmar.

Policyutveckling inom IoT- och OT-enhetssäkerhet

I tiotals länder arbetar myndigheterna aktivt med att utveckla krav för att främja cybersäkerheten för IKT-produkter och IKT-tjänster, däribland IoT- och OT-enheter. När det gäller IKT-produkter och IKT-tjänster är de största problemen säkerheten i programvaruförsörjningskedjan och IoT-säkerheten.

- Europeiska kommissionen föreslog cyberåterhämtningsakten, som skulle inrätta cybersäkerhetskrav för fristående programvara och uppkopplade enheter och kompletterande tjänster.[5] Relevanta metoder för programvaruleverantörer är att utnyttja en säker livscykel för programvaruutveckling[6] och tillhandahålla en programvaruförteckning.[7] Nya säkerhetskrav skulle gälla för uppkopplade enheter, och alla tillverkare skulle få i uppgift att hantera samordnade processer för att avslöja sårbarheter[8] för lanserade produkter.

Beslutsfattarna har även fokuserat på den fortsatta spridningen av IoT-enheter och OT-enheter i nätverk.

- I Storbritannien kommer förslaget till en produktsäkerhets- och telekommunikationsinfrastrukturlag att kräva att tillverkare av produkter som konsumenter kan ansluta, t.ex. smarta TV-apparater, slutar att använda standardlösenord som är ett enkelt mål för cyberbrottslingar, upprättar en policy för att avslöja sårbarheter (t.ex. ett sätt att ta emot meddelanden om säkerhetsbrister) och ger insyn i den kortaste tid inom vilken de kommer att tillhandahålla säkerhetsuppdateringar.[9]
- I EU införs nya säkerhetsnormer eller säkerhetskrav via flera lagstiftningsinstrument, däribland en delegerad akt till radioutrustningsdirektivet som gäller trådlösa enheter och syftar till att förbättra nätverksåterhämtningen, skydda konsumenternas integritet och minska risken för penningbedrägerier.[10] Dessutom kan det kräva användning av ett molncertifieringssystem[11] som för närvarande håller på att utvecklas på grund av 2019 års cybersäkerhetsakt i EU[12].

Behovet av konsekvens

I många fall bedrivs all verksamhet i alla regioner, sektorer och med alla tekniker och operativa riskhanteringsområden samtidigt, vilket leder till potentiellt överlapp eller inkonsekvenser i fråga om omfattning, krav och komplexitet för organisationer som vill ta till sig råd eller uppvisa efterlevnad. Utan en allmänt accepterad IoT-definition är omfattningen särskilt besvärlig för bestämmelser som gäller IoT och OT. Exemplen ovan kan gälla för ”uppkopplade produkter och kringtjänster”, ”produkter som konsumenter kan ansluta” och ”trådlösa enheter”. Samtidigt strävar många länder efter att införa mer robusta bedömningssystem för att få bättre koll på om och hur organisationer och produkter uppfyller nuvarande, kommande och föränderliga krav. När de här trenderna sammanstrålar ökar komplexiteten. Uppmuntrande nog tog man upp en del frågor under samrådet om EU:s cyberåterhämtningsakt om hur nya regleringar skulle kunna samverka med befintliga cybersäkerhetsregleringar, vilket tyder på att avsikten är att undvika motstridiga cybersäkerhetskrav.

Iterativa metoder som är riskbaserade och resultat- eller processorienterade (i stället för implementeringsspecifika) kan främja förbättrad cybersäkerhet och kontinuerliga förbättringar. På samma sätt skulle ett fokus på att möjliggöra interoperabilitet mellan sektorer, regioner och politikområden konsekvent kunna öka cybersäkerheten i samverkande globala försörjningskedjor.

Länder agerar för att förbättra den kritiska infrastrukturens säkerhet och motståndskraft

fortsättning

Det finns alltmer komplexa strategier för cybersäkerheten inom den kritiska infrastruktur som håller på att utvecklas i regioner och sektorer och för ämnesområden. Den här aktiviteten medför stora möjligheter och betydande svårigheter. Hur myndigheterna väljer att gå vidare kommer att bli avgörande för digitaliseringens och hela ekosystemets säkerhet framöver.

Påskynda ekosystemomfattande investeringar i programvaruförsörjningskedjans säkerhet och nolltillitsarkitektur

Den amerikanska presidentordern 14028, som handlar om att förbättra cybersäkerheten, har varit en katalysator för att påskynda Microsofts löpande initiativ om att investera i vår egen och den ekosystemomfattande försörjningskedjans säkerhet och för att ge våra kunder möjlighet att uppfylla nolltillitsmål.

Vi menar sedan lång tid tillbaka att en förbättring av programvaruförsörjningskedjan kräver att man delar med sig av lärdomar och bästa praxis, vilket vi började med genom vår offentliga version av Microsofts Security Development Lifecycle för cirka 15 år sedan.

Dessutom samarbetar vi nära med National Cybersecurity Center of Excellence för att visa metoder för en nolltillitsarkitektur som tillämpas på både lokal teknik och molnteknik och som inför nya produktfunktioner, däribland möjligheten att framtvinga nätfiskeresistent autentisering för hybrid- och multimolnmiljöer.

I dag går vi bortom EO:s krav på att visa överensstämmelse med säkerhetskraven för programvaruförsörjningskedjan och tillhandahålla information om programvarors materialsedlar på två sätt:

1. För det första delar vi ut en version med öppen källkod av vårt verktyg för generering av sådana materialsedlar, som vi har tagit fram för att det ska vara enkelt att integrera med CI/CD-kanaler som stöder kompilering på Windows, Linux, Mac, iOS och Android.[13]
2. För det andra bidrar vi till utvecklingen av branschstandarder för integritet, insyn i och förtroende för försörjningskedjan. Det gör det möjligt att byta ut verifierbar information om försörjningskedjan automatiskt, inklusive artefakter som visar överensstämmelse med krav som de som följer av EO:s råd om programvaruförsörjningskedjan.

Användbara insikter

1. Multilaterala institutioner måste konstrueras om för att ta itu med det akuta problemet med cyberattacker från nationalstater.
2. Utveckla strategier för cybersäkerhet som är konsekventa och driftkompatibla i regioner och sektorer och för ämnesområden.

Länkar till mer information

- Continued investments in supply chain security in support of the cybersecurity Executive Order | Microsoft Tech Community
- US Government sets forth Zero Trust architecture strategy and requirements | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Supply Chain Integrity, Transparency, and Trust | github.com
- Implementing a Zero Trust Architecture | NCCoE (nist.gov)

IoT och OT i blickfånget: trender och angrepp

Den alltmer sammankopplade digitala världen innebär att enheter snabbt tas ut på nätet, kommunicerar med större system, samlar in data och ger insyn i tidigare dolda utrymmen. Det ger både organisationer och hotaktörer nya möjlighet och cyberbrottsligheten blir både en bransch värd miljarder dollar och en risk.

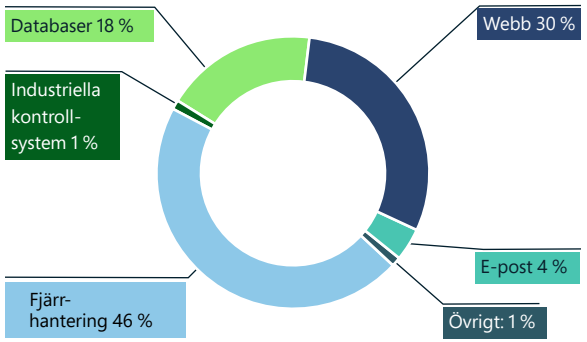
IoT-enheter – allt från skrivare till webbkameror, klimatstyrningsenheter och teknik för tillträde till byggnader – utgör unika säkerhetsrisker för individer, organisationer och nätverk. Även om de är viktiga för många organisationers verksamhet kan de snabbt bli en ansvars- och säkerhetsrisk. Det snabba införandet av IoT-lösningar i nästan alla branscher har ökat antalet attackvektorer och exponeringsrisken för organisationer.

Skadlig kod som tjänst blivit en storskalig verksamhet mot den civila infrastrukturen och allmännyttiga företag (t.ex. sjukhus, olja och gas, elnät, transporttjänster och annan kritisk infrastruktur) samt företagsnätverk. Betydande forskningsinsatser krävs av hotaktörerna för att upptäcka och utnyttja konfigurationen för driftmiljöer och inbäddade IoT- och OT-enheter.

IoT-enheter utgör unika säkerhetsrisker som ingångs- och vändpunkter i nätverket. Miljontals IoT-enheter är okorrigerade eller exponerade.

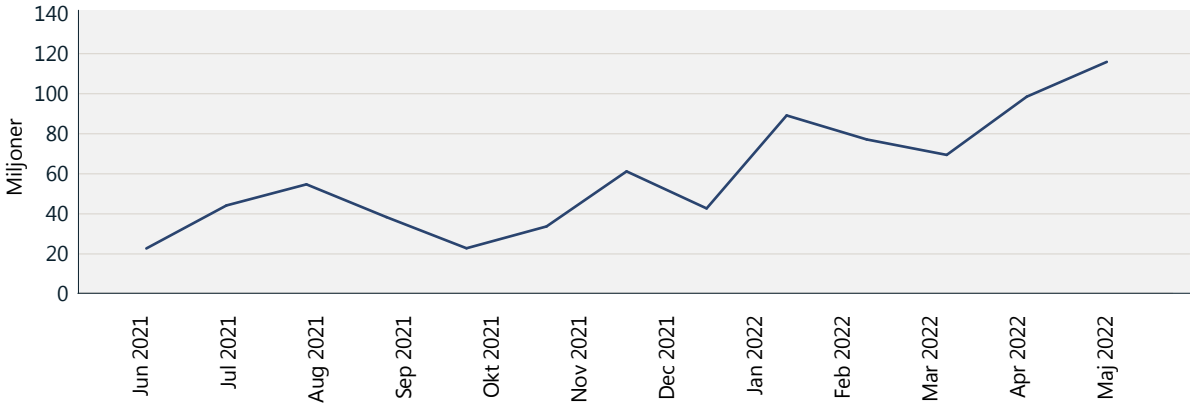
Exponerade enheter går att upptäcka via internetsökningsverktyg genom att identifiera tjänster som lyssnar på öppna nätverksportar. De här portarna används ofta för fjärrhantering av enheter. Om den inte skyddas korrekt kan en exponerad IoT-enhet användas som vändpunkt till ett annat lager i företagsnätverket, eftersom obehöriga användare kan komma åt portarna på distans. Vi har observerat att en mängd hotaktörer försöker utnyttja sårbarheter i enheter som är exponerade gentemot internet, allt från kameror till routrar och termostater. Trots risken förblir miljontals enheter exponerade eller okorrigerade.

Sammanfattning av angrepptyper mot IoT/OT



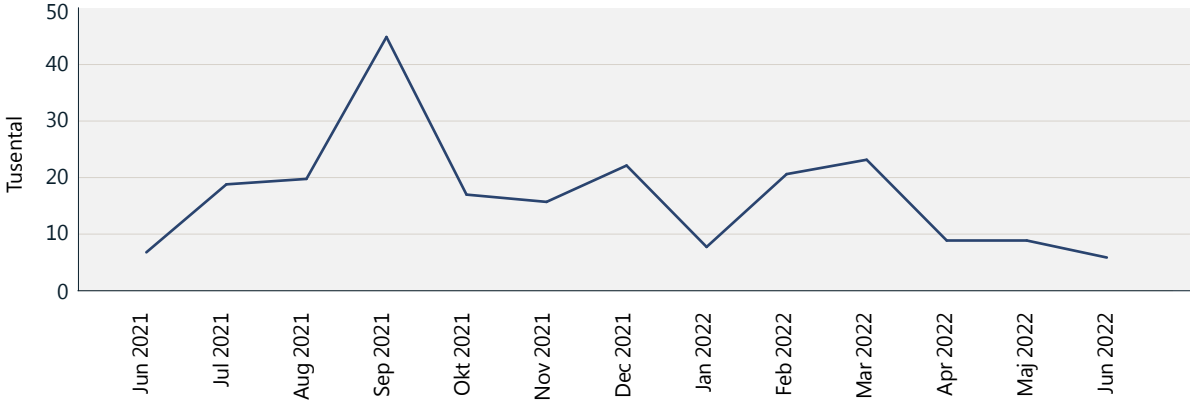
Angreppstyper som har observerats via MSTIC-sensornätverket. De vanligaste var angrepp mot fjärrhanteringsenheter, angrepp via webben och angrepp på databaser (råstyrkeattacker eller kända intrångsmöjligheter).

Angrepp mot fjärrhanteringsenheter



Ökade angrepp mot fjärrhanteringsportar över tid, vilket vi har sett i MSTIC-sensornätverket.

Webbangrepp mot IoT och OT



Volymen av webbangrepp som funktion av tiden, sett via MSTIC-sensornätverket. När antalet enheter som är direktanslutna till webben fortsätter att sjunka, kan angriparna så småningom vara mindre benägna att söka efter dem.

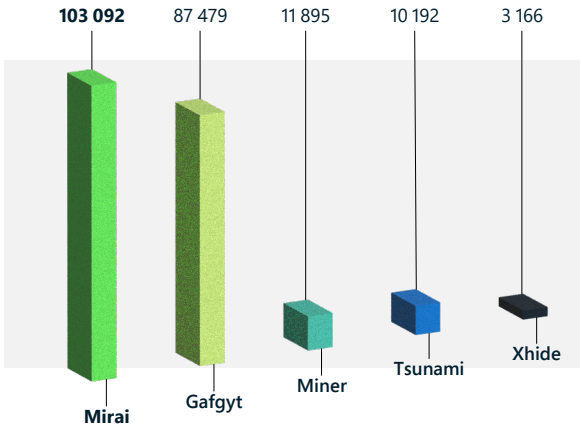
IoT och OT i blickfånget: trender och angrepp

fortsättning

Omgjort skadligt verktyg

Samtidigt som cyberbrottsgrupperna har utvecklats har deras distribution av skadlig kod och val av mål gjort detsamma. Under det senaste året har vi observerat att angrepp mot vanliga IoT-protokoll – till exempel Telnet – har minskat avsevärt, i vissa fall med så mycket som 60 procent. Samtidigt har cyberbrottsgrupper och nationella statsaktörer använt botnät till nya saker. Beständig skadlig kod, som Mirai, belyser dessa angrepps modularitet och anpassningsförmågan hos befintliga hot.

De främsta skadliga IoT-programmen som har upptäckts



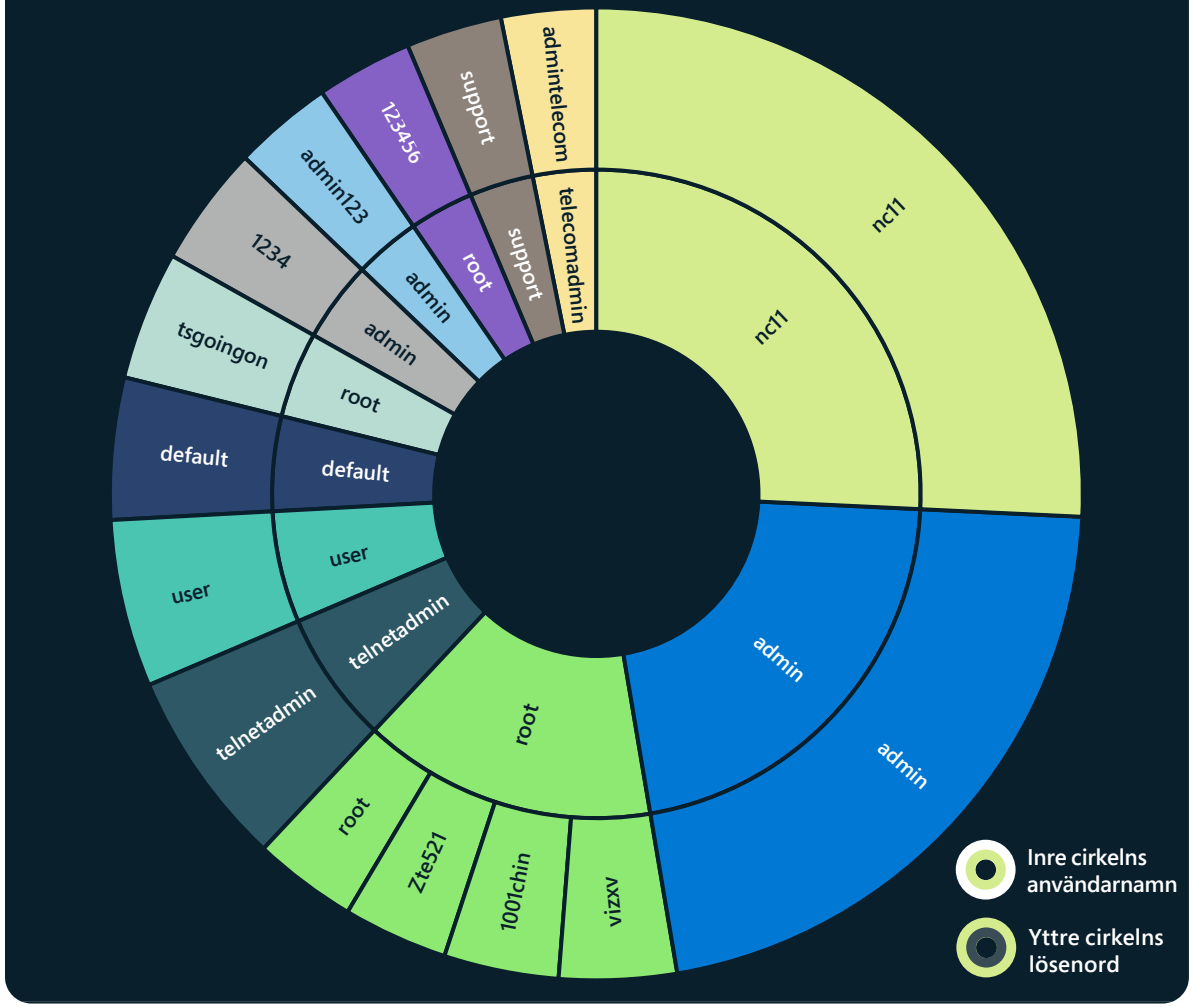
Mirai utvecklades för att infektera en hel mängd olika IoT-enheter, däribland Internet Protocol-kameror, digitala videobandspelare för säkerhetskameror och routrar. Angreppssätten kringgår gamla säkerhetskontroller och utgör en risk för slutpunkter i nätverket genom att utnyttja ytterligare sårbarheter och röra sig i sidled. Mirai har omarbetats flera gånger. Det finns varianter som anpassar sig efter olika arkitekturer och använder både kända sårbarheter och dag noll-sårbarheter för att utnyttja nya attackvektorer.

Mirai användes mer och mer för både 32- och 64-bitars x86-processorarkitekturer under det senaste året och den skadliga koden fick nya funktioner som snabbt började användas av nationalstater och kriminella grupper. Vid nationalstatsangrepp utnyttjas nu nya varianter av befintliga botnät i DDoS-angrepp mot utländska fiender.

Eftersom intäkterna från angrepp mot IoT-enheter minskade år 2022 observerade vi att flera hotbildsaktörer missbrukade sårbarheter – som Log4j och Spring4Shell – för att leverera en nyttolast mot enheter som servrar, infektera dem och rekrytera dem till stora botnät som utför DDoS-angrepp. Det omarbetade skadliga verktyget är utformat för att rikta in sig på sårbara IoT-enheter och det ger följder för både organisationer och länder, eftersom laterala förflyttningar kan exponera bakdörrar för ytterligare nyttolaster och andra enheter i nätverket.

Många industriella styrsystemprotokoll är oövervakade och därför sårbara för OT-specifika angrepp. Det kan innebära ökad risk för den kritiska infrastrukturen.

Relativ förekomst av kombinationer av användarnamn och lösenord som ses bland IoT-/OT-enheter under 45 dagars sensorsignaler



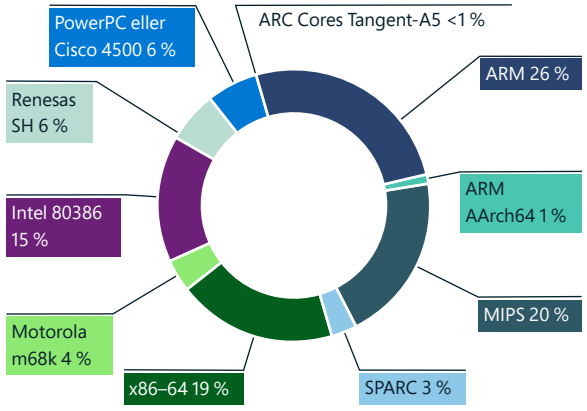
Användning av vanliga kombinationer av användarnamn och lösenord ökar risken för intrång. I en undersökning av över 39 miljoner IoT- och OT-enheter fanns det cirka 20 procent identiska användarnamn och lösenord.

IoT och OT i blickfånget: trender och angrepp

fortsättning

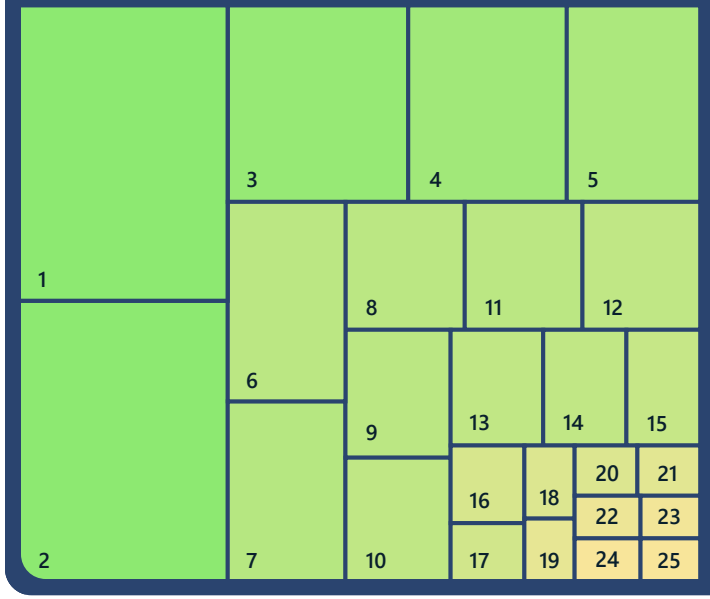
Svaga konfigurationer och standardautentiseringsuppgifter utgör visserligen fortfarande en risk för nätverk, men Microsoft observerade också många webbaserade intrång där HTTP används. Den här angreppsökningen observerades på webbaserade tjänster med äldre botnät. Samtidigt minskade antalet öppna telnet-portar på internet, vilket är positivt för nätverkssäkerheten, eftersom botnät som tidigare utgjorde en risk för enheter tappar i relevans. Trots minskningen av antalet öppna telnet-portar observerade vi fortfarande beständiga botnät i sensornätverk.

Fördelning av skadlig IoT-kod per processorarkitektur



Microsoft observerade att IoT-enheter som körs på ARM är de mest utsatta för skadlig kod, följt av MIPS, X86-64 och Intel 80386.

Förekomst av protokoll för industriella styrsystem



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet i realtid
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Siemens WinCC-agent
10. EtherNet/IP O/O
11. Honeywell Control Data Access
12. MMS
13. IEC-60870
14. Honeywell FDA Diagnostics
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

Sårbarheter i protokoll för industriella styrsystem

Vi kikade på OT-data från våra molnanslutna sensorer och avslöjade de vanligaste ICS-protokollen (industriella styrsystem). Dessa protokoll ger insikter om dessa enheters natur och deras attackyta. Detta är särskilt relevant för kritisk infrastrukturs säkerhet. Här följer några viktiga lärdomar:

1. De flesta av de protokoll som representeras är patentskyddade, så standardverktyg för IT-övervakning har inte tillräcklig insyn i säkerheten för alla enheter och protokoll. Det innebär att nätverken inte övervakas ordentligt och att de därmed är mer sårbara för OT-specifika angrepp.
2. Det finns ett stort antal leverantörsspecifika protokoll. Det betyder att leverantörsspecifika säkerhetslösningar inte kan täcka hela nätverket på ett bra sätt. Microsoft prioriterar en leverantörsagnostisk metod för att tillhandahålla säkerhet för en mängd olika enheter.
3. Organisationer bör se till att protokollen inte exponeras direkt mot internet från sina nätverk. Sådan exponering kan annars innebära stora säkerhetsrisker på grund av sårbarheter och den inneboende osäkerheten i protokollen.

Skadlig kod som Mirai blir kvar genom att utveckla ny kapacitet och används av cyberbrottsgrupper och nationella statsaktörer. De utnyttjar nya varianter av befintliga botnät i DDoS-angrepp mot utländska fiender.

Användbara insikter

1. Se till att enheterna är robusta genom att installera korrigeringar, ändra standardlösenord och SSH-standardportar.
2. Minska attackytan genom att eliminera onödiga internetanslutningar och öppna portar, begränsa fjärråtkomsten genom att blockera portar, neka fjärråtkomst och använda VPN-tjänster.
3. Använd en IoT-/OT-medveten lösning för nätverksidentifiering och reaktioner och en lösning för säkerhetsinformation och händelsehantering (SIEM)/säkerhetsinstrumentering och reaktioner (SOAR) för att övervaka avvikande eller obehöriga beteenden på enheter, till exempel kommunikation med obekanta värdar.
4. Segmentera nätverk för att begränsa angriparens förmåga att röra sig i sidled och äventyra tillgångar efter det initiala intrånget. IoT-enheter och OT-nätverk bör isoleras från företagets IT-nätverk med brandväggar.
5. Se till att ICS-protokoll inte exponeras direkt mot internet.

Hackning av försörjningskedjan och inbyggd programvara

Nästan alla internetanslutna enheter har inbyggd programvara, vilket är programvara som finns inbäddad i enhetens maskinvara eller kretskort. Under de senaste åren har vi sett ökat intresse av att utnyttja den inbyggda programvaran för att sätta i gång förödande angrepp. Eftersom inbyggd programvara sannolikt kommer att fortsätta att vara ett värdefullt mål för hotaktörer, måste alla organisationer skydda sig mot angrepp på den.

Den inbyggda programvaran ansvarar för en enhets primära funktioner, som att ansluta till ett nätverk eller lagra data. Inbyggd programvara finns i routrar, kameror, TV-apparater och andra enheter som används i företag (IoT) och i industriell styrutrustning (OT) som används i kritisk infrastruktur. Historiskt sett har den inbyggda programvaran skrivits med oskyddad kod, vilket innebär att det kan finnas betydande sårbarheter som går att utnyttja för att ta över enheten eller lägga in skadlig kod i den inbyggda programvaran.

Risken förvärras när det gäller försörjningskedjan. De flesta enheter består av programvaru- och maskinvarukomponenter från flera olika tillverkare samt bibliotek med öppen källkod. I många fall har de som använder enheterna inte insyn i maskinvarans och programvarans strukturlistor och kan därmed inte utvärdera riskerna för enheter i försörjningskedjan i sina nätverk. I juni 2020 avslöjades sårbarheter i en nätverksstack som används av många olika tillverkare och påverkar hundratals miljoner IoT-enheter inom konsument- och industriutrustningsområdet.[14] I vissa fall ändrades namnet på nätverksstacken av andra leverantörer och det fanns ingen indikation på att en enhet var sårbar. Vi ser ett växande hot från skadliga aktörer som riktar in sig på den här programvaru- och maskinvaruförsörjningskedjan med IoT-/OT-enheter för att göra intrång i organisationer.

Processen för att uppdatera inbyggd programvara varierar kraftigt mellan olika enheter och komplexiteten och den logistiska utmaningen påverkar uppdateringsfrekvensen. Det är inte alltid möjligt att avgöra om en enhet kör den senaste inbyggda programvaran, vilket gör det svårt för säkerhetsexperter att övervaka och säkerställa sina IoT- och OT-enheters säkerhetsläge. Dessutom har vissa enheter inbyggd programvara som inte är kryptografiskt signerad, vilket innebär att de kan uppdateras utan verifiering av användaren. De här bristerna öppnar enheterna än mer för angrepp i försörjningskedjan i hela produktions- och distributionskedjan.

För att komma till rätta med hoten investerar Microsoft stora pengar i att säkerställa den inbyggda programvarans säkerhet och integritet i olika stadier i försörjningskedjan och i att när som helst kunna intyga att den inte har blivit manipulerad under inmatningen eller längs vägen. Det gör att vi kan verifiera förtroendet mellan varje segment i kanalen och tillhandahålla en certifierad och bevisbar, heltäckande ansvarskedja för varje komponent som vi levererar till våra kunder. Vi samarbetar med våra partner för att börja använda den här chipp-till-moln-säkerheten på alla enheter i företags- och OT-nätverk.

”IKT-infrastruktursleverantörer blir i allt högre grad måltavlor, eftersom de möjliggör omfattande replikering av ett angrepp. Samtidigt ställs allt större krav i globala lagar och förordningar och från våra kunder på att försörjningskedjan ska vara säker och motståndskraftig. Många gånger skiljer sig kraven dessutom åt.

Lösningen är partnerskap. Tillsammans med leverantörer och länder i hela världen har Microsoft åtagit sig att ta itu med säkerheten i hela vårt ekosystem i försörjningskedjan. Vi överträffar kraven från både kunder och tillsynsmyndigheter. För att lyckas med det tillämpar vi en helhetssyn på den säkerhet och operativa återhämtning som vi distribuerar flexibelt i hela försörjningskedjan.

Nyckeln till vårt kollektiva tillvägagångssätt är att se till att den inbyggda programvaran förblir intakt från design till enhetsdrift. Att säkerställa leverantörernas SDL-rutiner och driftsätta innovationer som skapar rottillit för maskinvara är exempel på hur vi kan ”bygga in” integritet i försörjningskedjan.

Våra användare utnyttjar samfälld forskning och utveckling som spänner från nya antimanipuleringstekniker och kryptografiska mekanismer, till löpande övervakning och avvikelseidentifiering. Tillsammans gör vi framsteg för att göra försörjningskedjan till en betydligt mindre lockande attackyta.”

Edna Conway,
Vice President, Security & Risk Officer, Cloud Infrastructure

Fokus på sårbarheter i inbyggd programvara

Angriparna utnyttjar i allt högre grad sårbarheter i IoT-enheters inbyggda programvara för att infiltrera företagsnätverk. Till skillnad från traditionella IT-slutpunkter som använder XDR-agenter för att identifiera brister, är sårbarhetsidentifiering i IoT-/OT-enheter betydligt svårare att genomföra.

En nyligen genomförd undersökning från Microsoft och Ponemon Institute belyser både möjligheten och säkerhetsproblemet med IoT-/OT-enheter i företag.[15] Medan 68 procent av de svarande anser att det är nödvändigt att införa IoT/OT för den strategiska digitaliseringen menar 60 procent att IoT-/OT-säkerheten är en av de mest osäkra aspekterna av IT-/OT-infrastrukturen.

Ett exempel på angripare som utnyttjar sårbarheter i IoT-enhetens inbyggda programvara för att infiltrera nätverk är trojanen Trickbot, som använde standardlösenord och sårbarheter i Mikrotik-routrar[16] för att kringgå företags försvarssystem. Det grundläggande problemet med inbyggd IoT-programvara är bristen på insyn i enheternas säkerhetsläge och sårbarheter.

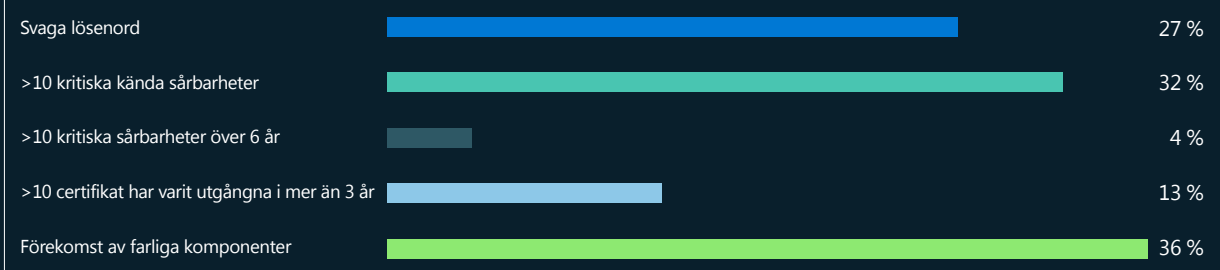
Även om det finns lösningar för att skapa säkra enheter, finns det redan miljarder enheter på marknaden och i drift hos företagen. De kallas övergivna (brownfield) enheter. 2021 köpte Microsoft ReFirm Labs för att belysa säkerheten för övergivna enheter och göra det möjligt för enhetstillverkare att förbättra sina produkters säkerhet. ReFirm Labs analyserar den binära, inbyggda programvarans avbildning för en enhet och skapar en detaljerad rapport om potentiella säkerhetsbrister.[17] Den här tekniken ska också införlivas i en kommande version av Microsoft Defender for IoT.

Under det senaste året har vi granskat samlade resultat från de unika inbyggda programvaror som våra kunder har sökt av. Även om inte varje svaghet som upptäcks är en möjlig attackrisk understryker de det grundläggande problemet med säkerheten hos enhetens inbyggda programvara.

Lägg också märke till att de typer av svagheter som finns i IoT-/OT-enheter aldrig skulle accepteras i traditionella Windows- eller Linux-slutpunkter.

- Svaga lösenord: Tjugosju procent av avbildningarna av inbyggd programvara som skannades innehöll konton med lösenord som kodats med svaga algoritmer (MD5/DES), som lätt knäcks av en angripare.

Analyserade säkerhetsbrister i avbildningar av inbyggd programvara



- Kända sårbarheter: Liksom andra system utnyttjar IoT-/OT-enhetens inbyggda programvara i stor utsträckning bibliotek med öppen källkod. Men de här enheterna levereras många gånger med gamla versioner av komponenterna. I vår analys innehöll 32 procent av avbildningarna minst tio kända sårbarheter som klassificerats som kritiska (9,0 eller högre). Fyra procent innehöll minst tio kritiska sårbarheter som var över sex år gamla.
- Utgångna certifikat: Certifikat används för att autentisera anslutningar och identiteter samt skydda känsliga data, men 13 procent av de analyserade avbildningarna innehöll minst tio certifikat som hade gått ut för mer än tre år sedan.
- Programvarukomponenter: Trettiosex procent av avbildningarna innehåller programvarukomponenter som Microsoft avråder från att inkludera i IoT-enheter, t.ex. paketinfångstverktyg (tcpdump, libpcap), som kan utnyttjas för nätverksrekognoscering som ett led i en angreppskedja.

Förekommande angrepp på inbyggd programvara

Viasat: Använder en sårbarhet i inbyggd programvara för att angripa satellitkommunikation

I februari 2022 kopplades ett strategiskt kommunikationsnätverk bort efter en incident med ett satellitnätverk, vilket påverkade hela Europa. Viasats KA-SAT-system tog emot en stor mängd trafik som kopplade bort många modem och ett DDoS-angrepp inleddes mot nätverket. När det fasta bredbandet störddes blev tusentals vindkraftverk oåtkomliga på distans för operatörerna och skadlig kod installerades på de aktuella modemen. Störningarna påverkade fler än 30 000 satellitterminaler som användes av företag och organisationer för kommunikation.

Cyclops Blink: Använder ett angrepp mot försörjningskedjan för inbyggd programvara för att rikta in sig mot brandväggsgatewayer

För hotaktörer är utvecklingen och utökningen av styrning och kontroll (C2) och angreppsinfrastrukturen avgörande för framgången. I takt med att behovet av en stabil C2-infrastruktur har växt har routrar blivit intressanta attackvektorer, eftersom de sällan är korrigerade och ofta har bristfälliga säkerhetslösningar.

Microsoft samarbetar med myndigheter och branschexperter för att utveckla analysteknik för inbyggd programvara som ger bättre insyn i enhetssäkerheten och erbjuder fullständig livscykelsäkerhet för dem som konstruerar och använder enheter.

Sedan juni 2019 har en nationalstatsanknuten avancerad beständig hotgrupp använt den modulära skadliga koden Cyclops Blink för att rikta in sig på sårbara WatchGuard-brandväggar och ASUS-routrar genom att köra skadliga uppdateringar av den inbyggda programvaran och rekrytera dem till ett stort botnät.
Den skadliga koden infekterar enheter genom att utnyttja en känd sårbarhet som tillåter en privilegieskalering, vilket gör det möjligt för hotaktörerna att hantera enheten. När den har smittats låter den skadliga koden andra moduler installeras och undviker uppdateringar av den inbyggda programvaran. Knäckta enheter har observerats ansluta till C2-servrar på andra WatchGuard-enheter. Genom att utfärda många SSL-certifikat till sin C2 på olika TCP-portar fick Cyclops Blink-operatörerna privilegierad fjärråtkomst till nätverk genom att köra skadliga uppdateringar av den inbyggda programvaran och genom att kringgå traditionella säkerhetsmetoder, till exempel genomsökning.

Så här förbättrar Microsoft säkerheten i försörjningskedjan

Microsoft samarbetar med myndigheter och branschexperter för att åtgärda säkerhetsutmaningarna för IoT- och OT-enheter (se diskussionen på sidan 66). Det gör vi till exempel genom att använda teknik för analys av inbyggd programvara som kan ge enhetsoperatörerna ökad insyn i nätverksenheternas säkerhetsläge. Det gör att kunderna kan identifiera och prioritera enheter som behöver mer skydd, uppgraderingar eller ersättas – och ökar efterfrågan på att alla som konstruerar enheter ska investera i enhetssäkerhet. Samtidigt hjälper vi konstruktörerna med omfattande lösningar för att konstruera säkra enheter och tillämpa säkra utvecklingslivscykler.

En annan viktig komponent är att ge konstruktörer och operatörer en robust infrastruktur så att enheternas inbyggda programvara kan uppdateras när säkerhetsproblem upptäcks och löses. Microsoft sammanför analysen av inbyggd programvara och Defender for IoT med Device Update for IoT Hub för att tillhandahålla en lösning som hanterar hela livscykeln för IoT- och OT-enhetssäkerhet. Det här är viktiga steg mot att realisera vår vision för att kunderna ska kunna säkra infrastrukturen genom att använda enheter med stöd för en nolltillitsstrategi för sina IoT- och OT-lösningar.[18]

Angripare riktar sig i allt högre grad mot sårbarheter i IoT-enheters inbyggda programvara för att infiltrera företagsnätverk.

Användbara insikter

1. Få djupare insyn i IoT-/OT-enheterna i nätverket och prioritera dem enligt den risk de utsätter företaget för om de knäcks.
2. Använd verktyg för genomsökning av inbyggd programvara för att förstå potentiella säkerhetsbrister och samarbeta med leverantörer för att identifiera hur det går att minska riskerna för högriskenheter.
3. Påverka IoT-/OT-enheters säkerhet positivt genom att kräva att leverantörerna använder bästa praxis för säker utveckling under livscykeln.

Länkar till mer information

- Bedömning av de kritiska försörjningskedjorna som stöder den amerikanska informations- och kommunikationsteknikindustrin

Rekognosceringsbaserade OT-angrepp

Komplexa försörjningskedjor använder specifik designinformation för att planera det faktiska systemet. Den känsligaste av alla de tillgångar som designinformationen består av är projektfilen, som definierar miljön och dess tillgångar. Den filen är ett viktigt strategiskt mål för hotaktörer som vill få tillgång till och sätta i gång ett lyckat angrepp som är helt anpassat efter miljön.

Angrepp mot industriella system för att störa driftprocesser sker i två steg.

1. Först måste angriparen komma åt OT-nätverket. Det kan ske genom att gå in via IoT-enheter på företagets sida av nätverket (Purdue Model Level 4) och korsa IT-OT-gränsen, som brukar skyddas av brandväggar och nätverksutrustning, för att ta sig vidare in i drift- och kontrollnivåerna.
2. För det andra måste nätverksenheterna identifieras. Industriella system använder standardenheter och komponenter i anpassade arkitekturer som är särskilt utformade för deras miljöer. En av standardenheterna är den programmerbara logikstyrenheten (PLC). Varje tillverkare utvecklar unika gränssnitt och funktioner för sina PLC:er, som är viktiga komponenter i industriella system. Enheterna konfigureras också med anpassade scheman som är särskilt utformade för kundens miljöer.

Varje PLC:s unika konfiguration beskrivs i projektfilen, som innehåller definitionen av miljön och dess tillgångar, steglogiken och mycket mer.

I de flesta miljöer som visar tecken på angrepp visar analysen att tidslinjen som föregår angreppet vida överstiger själva angreppets längd. Hotaktörerna lägger ofta många månader på att simulera miljön och dess tillgångar på distans och gör många försök att konstruera en modell och förbereda sitt riktade angrepp. När miljöer ständigt förändras och integrerar nya enheter, skapas sårbarheter specifikt kring data i projekt- och konfigurationsfilerna. Stölden av en projektfil kan påskynda ett angrepp med veckor eller månader och göra så att angriparna kan modellera målmiljön snabbt och korrekt, vilket ökar svårigheten att upptäcka skadlig aktivitet.

Industroyer och Incontroller

Vi har observerat fler angrepp på organisationer, kritisk infrastruktur och myndighetsmål av statligt sponsrade aktörer med hjälp av modulär skadlig kod och angreppsramverk. Nya försök att störa viktiga operationer i Ukraina understryker det växande hotet om rekognosceringsbaserade OT-angrepp som är väl anpassade till sina målmiljöer. De utökade rekognoscerings- och undersökningsfaserna som genomförs av nationella statsaktörer pekar mot en strategi om att använda cyberkrigföring för att förlama infrastruktur på distans och uppfylla specifika strategiska eller operativa mål i blandade cyber-kinetiska insatser och politisk strategi.



Vi har observerat ett växande hot om rekognosceringsbaserade OT-angrepp som är mycket anpassade till sin målmiljö.

Rekognosceringsbaserade OT-angrepp

fortsättning

I början av 2022 identifierades två anpassningsbara, kritiska OT-angrepp. Ett cyber-fysiskt angrepp mot elektriska transformatorstationer och skyddsreläer i Ukraina utfördes med anpassad skadlig kod, bland annat en variant av Industroyer, ett skadligt program som man vet orsakade strömavbrott i Ukraina efter att det sattes in 2016.

Industroyer2 är den första kända förnyade insatsen av ett skadligt OT-angrepp med ett gammalt program mot ett nytt mål. Man använde IEC104-protokollet (standardprotokollet för övervakning och kontroll av elsystem) som utvecklades för Industroyer och riktade främst in sig på PLC-liknande fjärrterminalenheter med modellnumret ABB RTU540/560. Skaparen av den skadliga koden använde sin kunskap om offrets miljö för att utfärda kommandon upprepade gånger till förutbestämda utgångar för att se till att de inte kunde slås på manuellt. Det medförde att strömavbrotten blev längre och gjorde mer skada.

Incontroller, ett modulärt angreppsramverk som identifierades under samma period, är en modulär verktygslåda som avsevärt minskar ledtiden för att tränga sig in i och angripa OT-enheter och som kringgår äldre säkerhetslösningar. Den här allmänna verktygslådan har kapacitet att samla in data, rekognoscera och angripa. Den är också mycket anpassningsbar till olika miljöer och kan påverka undersökningsfasen av ett OT-angrepp rejält. Tiden det tar att utföra rekognoscering kortas, och paketet stöder simulering av miljöer genom att extrahera information om enheter och deras konfigurationer.

Incontroller-ramverket stöder protokoll för Schneider Electrics och PLC:er från Omron och samlar in information, till exempel versionen på den inbyggda programvaran, modelltyp och anslutna enheter. Verktygslådan kan utfärda kommandon för att ändra konfigurationer och aktivera och inaktivera utgångar. När en miljö nyttjas stöder ramverket implantering av bakdörrar i enheter för leverans av fler nyttolaster, utfärdande av sårbarheter för att få fler åtkomstpunkter, uppladdning av steglogik och möjlighet att initiera DoS-angrepp. Verktygslådans generiska karaktär gör att hotaktören kan angripa en miljö snabbt, utan att behöva skriva nya angrepp för varje PLC eller plats. Det gör att aktören enkelt kan interagera med olika typer av maskiner och potentiellt i många branscher.



Användbara insikter

1. Undvik att överföra filer med systemdefinitioner via osäkra kanaler eller till icke nödvändig personal.
2. När sådana filer måste överföras ska aktiviteten övervakas i nätverket så att tillgångarna hålls säkra.
3. Skydda teknikstationer genom övervakning med EDR-lösningar.
4. Genomför proaktiv incidenthantering för OT-nätverk.
5. Använd kontinuerlig övervakning, t.ex. Defender for IoT.

Slutnoter

1. Se till exempel 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 | Nyhetsartikel | 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 – webbplats
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Se t.ex. utan titel (house.gov)
5. Cyberåterhämtningsakten | Att forma EU:s digitala framtid (europa.eu)
6. Se t.ex. Microsoft Security Development Lifecycle
7. Se t.ex. Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft—Engineering@Microsoft; se även t.ex. The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Se t.ex. https://www.microsoft.com/en-us/msrc/cvd
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill – produktsäkerhetsblad – 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. Certifiering – ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool" GitHub – Microsoft/sbom-tool: SBOM-verktyget är ett mycket skalbart och företagsklart verktyg för att skapa SPDX 2.2-kompatibla strukturlistor för programvara för alla typer av artefakter.
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 (mar 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 (maj 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 (maj 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Cyberpåverkan

Dagens utländska påverkansoperationer använder nya metoder och tekniker. Deras kampanjer är ämnade att urholka förtroendet mer effektivt.

En översikt över cyberpåverkan 72
Introduktion 73
Trender inom cyberpåverkansoperationer 74
Fokus på påverkansoperationer under covid-19 och Rysslands invasion av Ukraina 76
Hålla koll på det ryska propagandaindexet 78
Syntetiska medier 80
En helhetsmetod för att skydda mot cyberpåverkan 83

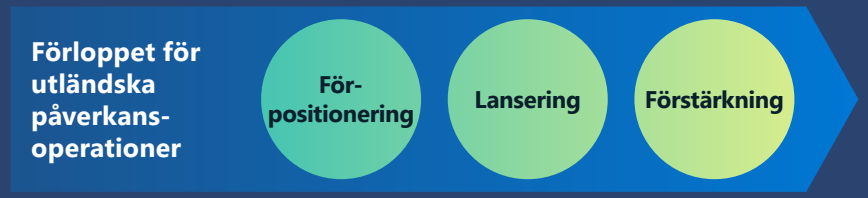
En översikt över

cyberpåverkan

Dagens utländska påverkansoperationer använder nya metoder och tekniker. Deras kampanjer är ämnade att urholka förtroendet mer effektivt.

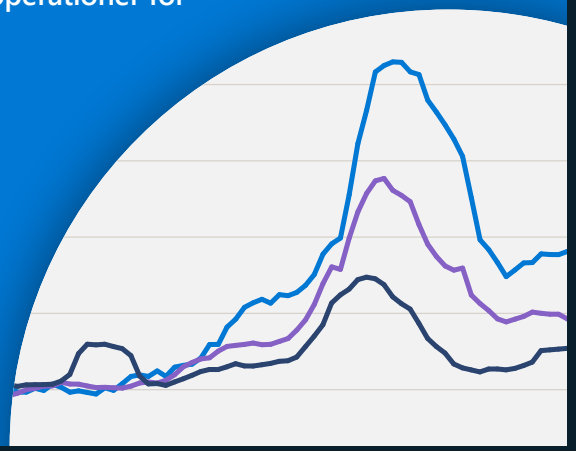
Nationalstater använder alltmer avancerade påverkansoperationer för att distribuera propaganda och påverka den allmänna opinionen både nationellt och internationellt. Kampanjerna urholkar förtroendet, ökar polariseringen och hotar demokratiska processer. Skickliga avancerade, beständiga manipulatörer använder traditionella medier och internet samt sociala medier för att kraftigt öka sina kampanjers omfattning, skala och effektivitet och den enorma påverkan de har i det globala informationsekosystemet. Under det senaste året har vi sett sådana operationer användas under Rysslands hybridkrig i Ukraina, men vi har också sett Ryssland och andra nationer, däribland Kina och Iran, i allt högre grad använda propagandainsatser i sociala medier för att utöka sitt globala inflytande.

Cyberpåverkansoperationer blir alltmer avancerade i takt med att allt fler myndigheter och nationalstater använder sig av sådana operationer för att bilda opinion, misskreditera motståndare och främja oenighet.



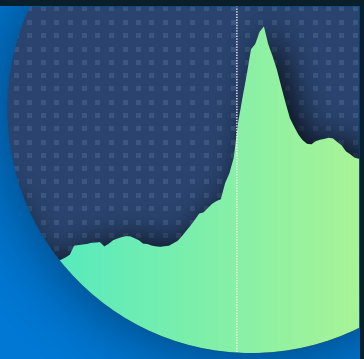
Läs mer på s. 74

Rysslands invasion av Ukraina visar hur cyberpåverkansoperationer kan integreras med mer traditionella cyberattacker och kinetiska militära operationer för maximal effekt.



Läs mer på s. 76

Ryssland, Iran och Kina nyttjade ofta propaganda- och påverkanskampanjer under hela covid-19-pandemin som en strategisk metod för att uppnå bredare politiska mål.



Läs mer på s. 76

Syntetiska medier blir allt vanligare på grund av spridningen av olika verktyg som kan användas för att enkelt skapa och sprida mycket realistiska artificiella bilder, filmer och ljud. Digital teknik för ursprungskontroll som certifierar medietillgångars ursprung kan vara ett lämpligt sätt att komma till rätta med problemet.



Läs mer på s. 80

En helhetsmetod för att skydda mot cyberpåverkan

Microsoft bygger vidare på sin redan mogna infrastruktur för cyberhotsunderrättelser för att bekämpa cyberpåverkan. Vår strategi är att identifiera, störa, försvara och avskräcka från propagandakampanjer av utländska angripare.

Läs mer på s. 83

Introduktion

Tillförlitlig information är en förutsättning för en välfungerande demokrati. Ett viktigt fokusområde för Microsoft är de påverkansoperationer som utvecklas och utförs av nationalstater. Kampanjerna urholkar förtroendet, ökar polariseringen och hotar demokratiska processer.

Påverkan från andra länder har alltid varit ett hot mot informationsekosystemet. Men den stora skillnaden i internets och de sociala mediernas tidevarv är insatsernas kraftigt ökade omfattning, skala och effektivitet och den enorma inverkan de kan ha på det globala informationsekosystemets hälsa.

Det gamla visdomsordet ”en lögn tar sig runt halva jorden innan sanningen hinner snöra på sig skorna” bekräftas nu med data. En undersökning från Massachusetts Institute of Technology (MIT)[1] visade att osanningar har 70 större chans att retweetas än sanningen och att de når de första 1 500 personerna sex gånger snabbare. Informationsekosystemet har blivit allt grumligare medan propagandakampanjerna härjar på internet och i sociala medier. De undergräver förtroendet för traditionella nyhetskanaler. I en studie från 2021[2] uppgav endast sju procent av alla vuxna i USA att de har ”stort” förtroende för tidningar, TV- och radionyheter, medan 34 procent svarade ”inget förtroende alls”.

Microsoft har arbetat för att identifiera de viktigaste aktörerna, hoten och taktikerna på det utländska cyberpåverkansområdet och dela med sig av lärdomarna. I juni i år publicerade vi en omfattande rapport om lärdomarna från Ukraina, som innehöll en detaljerad titt på Rysslands cyberpåverkan.[3]

Vi undersöker också hur avancerad teknik som deepfakes går att använda som vapen för att undergräva journalisters trovärdighet. Vi samarbetar också med industrin, myndigheter och den akademiska världen för att utveckla bättre sätt att upptäcka syntetiska medier och återställa förtroendet – till exempel AI-system som kan upptäcka förfalskningar.

Den snabbt föränderliga egenarten hos propagandan i informationsekosystemet från nationalstater – bland annat att traditionella cyberattacker smälter samman med påverkansoperationer och stör demokratiska val – kräver att hela samhället gör motstånd för att motverka hot mot demokratin både på och utanför nätet.

Microsoft är fast beslutade att stödja ett sunt informationsekosystem där betrodda nyheter och information frodas. Vi utvecklar verktyg och hotidentifieringsfunktioner för att bekämpa den föränderliga och växande risken för nationalstatsdrivna påverkansoperationer. För att underlätta arbetet köpte vi nyligen Miburo Solutions. Vi samarbetar dessutom med externa validatorer som Global Desinformation Index och NewsGuard, och vi deltar i och leder ibland partnerskap med flera intressenter, till exempel Coalition for Content Provenance and Authenticity (C2PA). Samarbete är det enda sättet som vi kan lyckas stoppa dem som försöker undergräva demokratiska processer och institutioner.

Teresa Hutson

Vice President, Technology and Corporate Responsibility

Trender inom cyber-påverkansoperationer

Cyberpåverkansoperationerna blir alltmer avancerade i takt med den tekniska utvecklingen. Vi ser ett överlapp av de verktyg som används vid traditionella cyberattacker och att de allt oftare tillämpas vid cyberpåverkansoperationer. Dessutom ser vi mer samordning och förstärkning mellan nationalstaterna.

Microsoft investerade i att bekämpa utländsk påverkan i år genom att förvärva Miburo Solutions, ett företag som har specialiserat sig på analys av utländska påverkansoperationer. Genom att kombinera de här analytikerna med Microsofts hotbildsanalytiker bildade Microsoft Digital Threat Analysis Center (DTAC). DTAC analyserar och rapporterar om hot från nationalstater, däribland både cyberattacker och påverkansoperationer. De kombinerar information och hotunderrättelser med geopolitiska analyser för att tillhandahålla insikter och informera om effektiva insatser och skydd.

Mer än tre fjärdedelar av alla människor i världen anger att de oroar sig för att information används som vapen[4] och enligt våra data är oron inte obefogad. Microsoft och dess partner har spårat hur nationella statsaktörer använder påverkansoperationer för att uppnå sina strategiska och politiska mål. Utöver destruktiva cyberattacker och cyberspionage använder auktoritära regimer allt oftare cyberpåverkan för att forma opinionen, misskreditera motståndare, ingjuta rädsla, främja oenighet och förvränga verkligheten.

Utländska cyberpåverkansoperationer sker vanligtvis i tre steg:

Förpositionering

Precis som förpositioneringen av skadlig kod i en organisations datornätverk, förpositionerar utländska cyberpåverkansoperationer falska historier i det offentliga rummet på internet. Förpositioneringstaktiker har länge underlättat mer traditionella cyberaktiviteter, särskilt om IT-administratörer skannar sin senaste nätverksaktivitet. Skadlig kod som ligger vilande under en längre tid i ett nätverk kan göra användningen senare mer effektiv. Falska berättelser som inte har uppmärksammats på internet kan få efterföljande referenser till dem att verka mer trovärdiga.

Lansering

Vid den tidpunkt då det är mest fördelaktigt för att nå aktörens mål inleds en samordnad kampanj för att sprida berättelser via myndighetsuppbackade och influerade medier och kanaler i sociala medier.

Förstärkning

Slutligen förstärker nationalstatskontrollerade medier och ställföreträdare berättelser inom särskilt utvalda målgrupper. Ofta utökar omedvetna tekniska funktioner berättelsernas räckvidd. Till exempel kan onlineannonser bidra till att finansiera aktiviteter och samordnade innehållsleveranssystem kan överbelasta sökmotorer.

Den här trestegsmetoden tillämpades i slutet av 2021 för att stödja det falska ryska narrativet om påstådda biologiska vapen och labb i Ukraina. Narrativet lades först upp på YouTube den 29 november 2021 i en vanlig engelskspråkig show av en amerikan som bor i Moskva och hävdade att USA-finansierade biologiska labb i Ukraina kunde knytas till biologiska vapen. Historien gick i stort sett obemärkt förbi i flera månader. Den 24 februari 2022, just då ryska stridsvagnar korsade gränsen, skickades berättelsen ut i strid. Ett team av dataanalytiker på Microsoft identifierade tio ryskkontrollerade eller ryskinfluerade nyhetswebbplatser som samtidigt publicerade rapporter den 24 februari och talade om ”rapporten från i fjol” och försökte göra den trovärdig. Dessutom höll ryska utrikesdepartementets tjänstemän presskonferenser där man kom med ytterligare falska påståenden om amerikanska biologiska labb i informationsmiljön. Ryssponsrade team försökte sedan förstärka narrativet på sociala medier och webbplatser i bred omfattning.

Vi ser att auktoritära regimer över hela världen samarbetar för att förorena informationsekosystemet till sin ömsesidiga fördel. Under hela covid-19-pandemin använde Ryssland, Iran och Kina propaganda- och påverkansoperationer med en blandning av öppna, halvhemliga och hemliga spridningsmetoder för att rikta in sig på demokratier och andra geopolitiska mål (som diskuteras vidare på sidan 76). De tre regimerna förstärkte varandras budskap och informationsekosystem för att hålla fram de narrativ de föredrog. En stor del av rapporterna bestod av kritik mot eller konspirationsteorier om USA och dess allierade som framfördes av statstjänstemän i officiella uttalanden samtidigt som de höll fram sina egna vacciner och reaktion på covid-19 som överlägsna USA:s och andra demokratiers. Genom att förstärka varandra gav de statliga mediekanalerna upphov till ett ekosystem där negativa texter om demokratier – eller positiva om Ryssland, Iran och Kina – som producerades av en statlig mediebyrå förstärktes av de andra.



Illustration av hur narrativ om amerikanska biologiska labb och vapen sprids via de tre breda faserna i många utländska påverkansoperationer: förpositionering, lansering och förstärkning.

Trender inom cyber-påverkansoperationer

fortsättning

Än besvärligare blir det av att privata teknikföretag kanske omedvetet möjliggör dessa kampanjer. Det kan handla om företag som registrerar internetdomäner, står värd för webbplatser, marknadsför material på sociala medier och sökwebbplatser, kanaliserar trafik och betalar för allt detta genom digital annonsering. Det är viktigt att organisationer känner till vilka verktyg och metoder som används av auktoritära regimer för cyberpåverkan, så att de kan upptäcka och sedan förhindra att kampanjerna sprids. Det finns också ett växande behov av att hjälpa konsumenterna att utveckla bättre förmåga att identifiera andra länders påverkansoperationer och begränsa mötena med deras narrativ eller innehåll.

Cyberpåverkansoperationer, däribland auktoritär propaganda, är ett hot mot demokratier i hela världen eftersom de urholkar förtroendet, ökar polariseringen och hotar demokratiska processer.

Ökad samordning och informationsutbyte mellan myndigheter, den privata sektorn och civilsamhället behövs för att öka insynen och exponera och störa påverkanskampanjerna.

Globalt oroar sig mer än tre fjärdedelar av alla människor för hur information används som vapen.



Fokus på påverkansoperationer under covid-19 och Rysslands invasion av Ukraina

Nationalstater som försökte styra över informationsmiljön under hela pandemin och under den ryska invasionen av Ukraina är goda exempel på hur auktoritära regimer blandar samman cyber- och informationsverksamhet.

Covid-19-propaganda

Ryssland, Iran och Kina använde propaganda och påverkanskampanjer under hela covid-19-pandemin. Covid-19 förekom ofta i de här kampanjerna på två centrala vis:

1. Representationer av själva pandemin.
2. Kampanjer som använde covid-19 som en strategisk faktor för att uppnå bredare politiska mål.

Det finns två allmänna syften med de här typerna av kampanjer: det första syftet är att undergräva demokratier, demokratiska institutioner och bilden av USA och dess allierade på den globala scenen och det andra är att stärka sin egen ställning i och utanför landet.

Ett exempel på det här framgår av skillnaden mellan budskapen från kända ryska konton och medieorganisationer som vänder sig till engelska läsare och den ryska statens budskap till sitt eget folk om vaccinet och hur allvarligt covid-19 är.

Ämnena för de tio mest visade coronavirushistorierna på RT.com (oktober 2021–april 2022)

Antivaccinpropaganda riktas mot icke-ryska läsare

Ryska	Engelska
"Nedstängningar och extra vaccineringar hindrar smitta"	"Vaccinationer lyckas inte bromsa smittspridningen och är ineffektiva mot nya varianter"
"Ryska offentliga personer testar positivt"	"Pfizers vaccin har farliga biverkningar"
"Antalet fall och dödsfall ökar i Ryssland"	"Massvaccinering är politiskt motiverat"
"Spu tnik V-vaccinet är mycket effektivt"	"Pfizer och Moderna genomför oreglerade försök"
"Vaccinpass behövs för att få åka kollektivtrafik"	

Ryska budskap om covid-19 skiljer sig åt beroende på språk.

Kampanjer som försökte dölja covid-19-virusets ursprung är ett annat exempel. Sedan pandemins inledning har den ryska, iranska och kinesiska covid-19-propagandan återberättat vad de andra säger för att förstärka dessa centrala teman. Mycket av presstäckningen bestod av att främja kritik mot eller konspirationsteorier om USA. Genom att återberätta vad de andra sade utvecklade statliga mediekanaler ett ekosystem där negativa texter om demokratier eller positiva om Ryssland, Iran och Kina som producerades av en statlig mediebyrå förstärktes av de andra om och om igen.

Ett sådant exempel är det tidiga förslaget från ryska och iranska statliga medier att covid-19 skulle kunna vara ett biovapen som framställts av USA. Det här påståendet cirkulerade på konspirationswebbplatser tidigt under pandemin efter en intervju med en juridikprofessor som hävdade att han trodde att covid-19 hade skapats som ett vapen.[6] Efter att intervjun publicerades på några webbplatser med begränsad räckvidd togs berättelsen upp av statliga medier. PressTV, en nyhetsbyrå med material på persiska, engelska och franska som sponsras av den iranska staten[7] publicerade en engelskspråkig berättelse i februari 2020 med titeln "Är coronavirus ett amerikanskt biologiskt vapen som Francis Boyle tror?" I artikeln påstods att USA låg bakom covid-19-utbrottet och man skrev "i alla amerikanska krig används radiologiska, kemiska, biologiska och andra förbjudna vapen som ger förödande verkan på människor i de utsatta områdena".[8] Ryska statliga medier och kinesiska statliga konton sade samma sak. Russia Today (RT) – en statsägd nyhetsbyrå som är känd för att sprida Kremls propaganda[9] – publicerade minst en berättelse med uttalanden från iranska tjänstemän som hävdar att covid-19 kan vara en "produkt av amerikanska biologiska angrepp riktade mot Iran och Kina"[10] och skrev inlägg i sociala medier som antydde det. En tweet från RT den 27 februari 2020 lyder: "Show of hands, who isn't going to be surprised if it ever gets revealed that #coronavirus is a bioweapon?"[11]

Kriget i Ukraina – propaganda som vapen

Rysslands invasion av Ukraina är ett tydligt exempel på hur cyberpåverkansoperationer kan kombineras med mer traditionella cyberattacker och militära markoperationer för att maximera inverkan.

Under uppbyggnaden inför invasionen av Ukraina upptäckte Microsofts hotunderrättelseanalytiker minst sex separata ryssvänliga aktörer inleda fler än 237 cyberattacker mot Ukraina. Med kampanjerna försökte man försvaga tjänster och institutioner, störa ukrainarnas tillgång till tillförlitlig information och så tvivel om landets ledning.

Fokus på påverkansoperationer under covid-19 och Rysslands invasion av Ukraina

fortsättning

I en rapport från Microsoft som släpptes i april 2022 visade vi att Ryssland i ett uppenbart försök att kontrollera informationsmiljön i Kiev genomförde ett missilangrepp mot ett TV-torn i Kiev samma dag som landet satte in destruktiv skadlig kod mot ett stort ukrainskt medieföretag.[12]

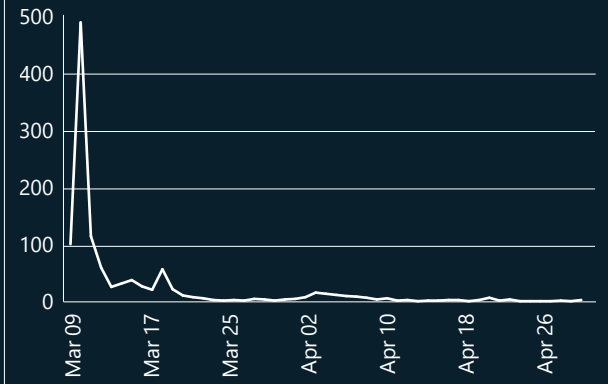
I ett annat exempel på hur cyberattacker och påverkansoperationer sammanstrålar skickade en rysk hotaktör e-postmeddelanden till ukrainska medborgare som påstods komma från invånare i Mariupol och som anklagade den ukrainska regeringen för krigsupptrappningen och uppmanade sina landsmän att kämpa mot regeringen. De här e-postmeddelandena var specifikt adresserade (med namn) till dem som fick e-postmeddelandet, vilket tyder på att de kan ha fått sina uppgifter stulna i en tidigare spionagerelaterad cyberattack. Inga skadliga länkar ingick, vilket tyder på att avsikten var ren påverkan.

Påstått hackat, läckt eller på annat sätt känsligt material är en vanlig taktik som används av ryska aktörer under påverkansoperationer. Under kriget i Ukraina har proryska sociala medier främjat vad de påstår är läckt eller på annat sätt känsligt material från ukrainska källor. Läckt eller känsligt material används av proryska kanaler i sociala medier och på andra ställen som ett led i en bredare påverkansstrategi för att försämra förtroendet för institutioner och skapa tvivel kring de normala narrativen. Sådan information kan manipuleras för att skapa propaganda med inriktning på Ukraina och väst, minska förtroendet för den digitala säkerheten och urholka stödet för västerländskt stöd till Ukraina.

Ryssland använde andra informationsangrepp för att påverka den allmänna opinionen efter händelser på marken för att dölja eller undergräva fakta. Den 7 mars offentliggjorde Ryssland t.ex. på förhand ett narrativ genom att anmäla till Förenta nationerna (FN) att ett BB i Mariupol i Ukraina hade tömts och användes som en militäranläggning. Den 9 mars bombade Ryssland sjukhuset. När nyheten om bombningen blev känd twittrade Rysslands FN-representant Dmitrij Poljanskij att rapportering om bombningen var ”falska nyheter” och citerade Rysslands tidigare påståenden om att det användes som en militäranläggning. Ryssland ställde sig sedan bakom narrativet på bred front på ryskkontrollerade webbplatser i två veckor efter angreppet mot sjukhuset.



Domäner med trafik
(9 mars 2022–30 april 2022)



Propagandawebbplatser publicerade berättelser om BB i omkring två veckor med ett kort förnyat uppsving med början 1 april 2022. Källa: Microsoft AI for Good Lab.

Satellitbilder från ett BB i Mariupol i februari och mars 2022





Microsoft egen analys av satellitbilder visade att BB:t bombades. Det första fotot är från 24 februari 2022 och det andra är från 24 mars 2022. Bildkälla: Planet Labs.

Rysslands försköning av sina grymheter har fortsatt under krigets gång. I slutet av juni 2022 beskrev till exempel ryska medier och influerare bombningen av ett köpcentrum som motiverad och nödvändig. De hävdade felaktigt att det inte användes som köpcenter utan var ett vapenlager för den ukrainska försvarsmakten.[13] Flera bloggare som står bakom Kreml lade upp och förstärkte på Telegram innehåll som stärkte ”krigslistnarrativet” och bloggare pekade på påstådda indikatorer på tillverkning, däribland att det förekom människor i uniform i bilder från platsen[14] och att det saknades kvinnor på bilderna.[15] Ryssland lanserade kampanjer genom att förlita sig på ett inbyggt system av propagandabudbärare och propagandamedier. Förstärkningen av narrativen på nätet ger Ryssland möjlighet att skjuta ifrån sig skulden på den internationella scenen och undvika ansvar.

Nationalstater som Ryssland förstår värdet av att använda information som härrör från slutna källor för att påverka allmänhetens uppfattning och använder hack-and-leak-kampanjer för att sprida alternativa berättelser och så misstro.

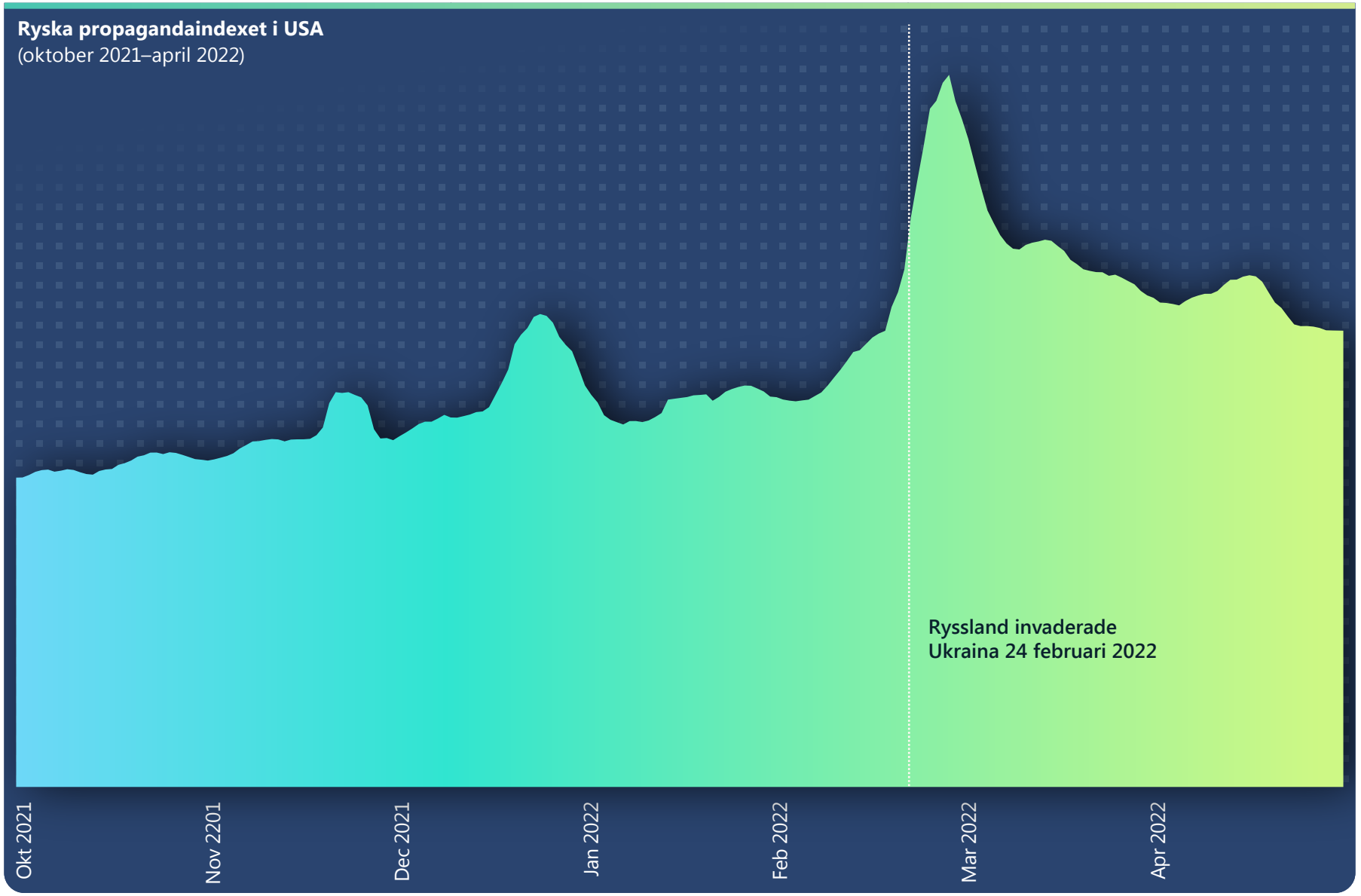
Länkar till mer information

- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- An overview of Russia’s cyberattack activity in Ukraine | Microsoft Special Report
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues

Hålla koll på det ryska propagandaindexet

I januari 2022 hänvisade nästan tusen amerikanska webbplatser trafik till ryska propagandawebbplatser. De vanligaste ämnena för ryska propagandawebbplatser som riktade sig mot amerikaner var kriget i Ukraina, USA:s inrikespolitik (antingen för Trump eller för Biden) och covid-19 och vaccinrelaterade berättelser.

Det ryska propagandaindexet (RPI) övervakar nyhetsflödet från ryska statskontrollerade och sponsrade nyhetskanaler och talesmän som en andel av den totala nyhetstrafiken på internet. RPI kan användas för att kartlägga konsumtionen av rysk propaganda på internet och i olika geografiska områden på en exakt tidslinje. Microsoft konstaterar dock att vi bara kan observera den ryska propaganda som publiceras på tidigare identifierade webbplatser. Vi har inte inblick i propaganda på andra typer av webbplatser, däribland auktoritativa nyhetswebbplatser, oidentifierade webbplatser och grupper i sociala nätverk.



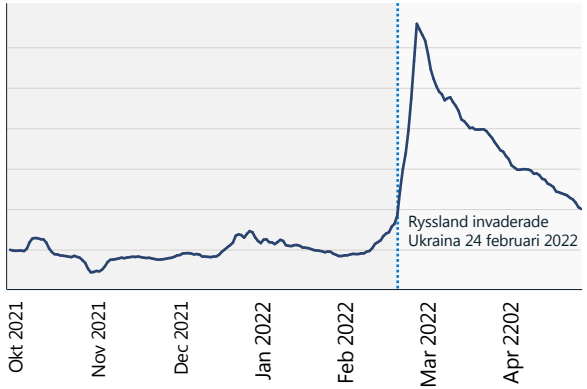
Hålla koll på det ryska propagandaindexet

fortsättning

Ryska propagandaindexet: Ukraina

När kriget i Ukraina inleddes såg vi en ökning med 216 procent av den ryska propagandan, som nådde sin höjdpunkt 2 mars. Diagrammet nedan visar hur denna plötsliga ökning sammanföll med invasionen. De två graferna visar hur rysk propaganda ökade markant strax efter att invasionen började.

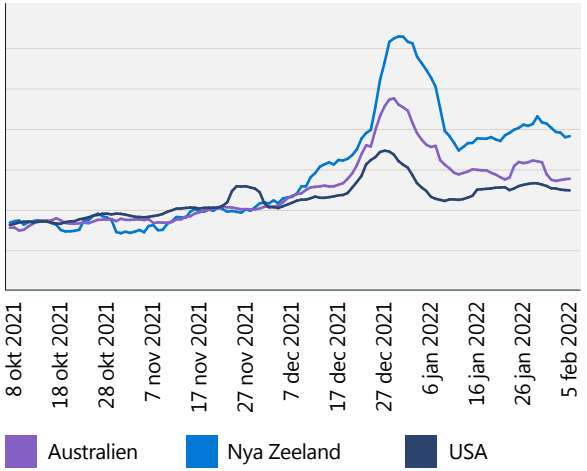
RPI, Ukraina
(7 oktober 2021–30 april 2022)



Ryska propagandaindexet: Nya Zeeland kontra Australien och USA

En bedömning av RPI i Nya Zeeland visade en topp i slutet av 2021 som gällde covid-19-propaganda. Denna topp i konsumtionen av rysk propaganda i Nya Zeeland föregick en ökning av allmänhetens protester i början av 2022 i Wellington. En andra topp var tydligt relaterad till den ryska invasionen av Ukraina och överskred RPI:erna i Australien och USA.

RPI, Nya Zeeland kontra Australien och USA



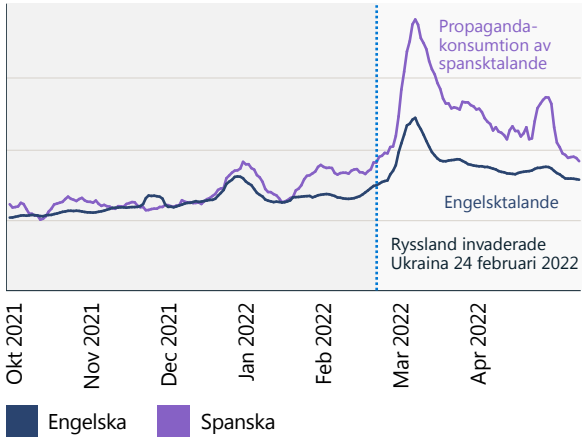
Konsumtionen av rysk propaganda i Nya Zeeland liknar den i Australien fram till den första veckan i december 2021. Efter december ökade konsumtionen av rysk propaganda i Nya Zeeland med över 30 procent i förhållande till konsumtionen i Australien och USA.

Ryska propagandaindexet i USA: engelska och spanska

RPI spårar även propaganda på olika språk. Flera nyhetsbyråer, däribland RT och Sputnik News, finns på över 20 språk. Dessa inkluderar engelska, spanska, tyska, franska, grekiska, italienska, tjeckiska, polska, serbiska, lettiska, litauiska, moldaviska, belarusiska, armeniska, ossetiska, georgiska, azerbajdzjanska, arabiska, turkiska, persiska och dari.

Följande diagram visar att RPI för spansktalande nyheter i USA är mycket högre än för engelskspråkiga nyheter.

Konsumtionen av rysk propaganda är två gånger högre bland spansktalande



Konsumtionen av rysk propaganda i USA är två gånger högre bland spansktalande.

Det finns mycket rysk propaganda i Latinamerika



RT på spanska är det internationella nyhetsorgan som har flest sidvisningar och Facebook-följare.

Källa: Microsoft AI for Good Research Lab

Syntetiska medier

Vi är på väg in i en gyllene era för AI-medieskapande och AI-manipulation. Microsofts analytiker noterar att två viktiga trender står bakom det här: spridningen av lättanvända verktyg och tjänster för att på konstgjord väg skapa mycket realistiska syntetiska bilder, filmer, ljud och text, och förmågan att snabbt sprida innehåll som är optimerat för specifika målgrupper.

Ingen av de här utvecklingarna är egentligen problematiska i sig. AI-baserad teknik kan användas för att skapa roligt och spännande digitalt innehåll, oavsett om det gäller att skapa rent syntetiskt eller förbättra befintligt material. Verktygen används i stor utsträckning av företag för marknadsföring och kommunikation och av enskilda personer för att skapa engagerande innehåll till sina följare. Men syntetiska medier som skapas och distribueras med avsikt att göra skada kan leda till allvarliga skador för individer, företag, institutioner och samhället. Microsoft har varit en drivande kraft bakom att utveckla teknik och praxis, både internt och i det sammantagna medieekosystemet, för att begränsa sådana skador.

I det här avsnittet undersöker vi insikter från Microsofts analyser om den toppmoderna tekniken för att skapa skadligt syntetiskt innehåll, de skador som kan uppstå om innehållet sprids vitt och brett, samt tekniska åtgärder som kan försvara oss mot cyberhot från syntetiska medier.

Skapa syntetiska medier

Fältet för syntetisk text och syntetiska medier utvecklas otroligt snabbt, eftersom tekniker som en gång bara var möjliga med enorma datorresurser i stora filmstudior nu finns inbyggda i mobilappar. Samtidigt blir verktygen enklare att använda och kan generera innehåll som är så realistiska att de till och med kan lura mediespecialisterna. Vi är mycket nära att nå den punkt där vem som helst kan skapa en syntetisk video av vem som helst som säger eller gör vad som helst. Det är inte orimligt att tro att vi går mot en era där en betydande mängd av det innehåll vi ser på nätet är helt eller delvis syntetiskt och skapat med hjälp av AI-teknik.

> Eftersom avancerade och lättanvända verktyg är allmänt tillgängliga skapas mer syntetiskt innehåll och snart kommer det att vara omöjligt att skilja det från verkligheten.

Det finns många kostnadsfria och kommersiella bild-, film- och ljudredigeringsverktyg av hög kvalitet. Verktygen kan användas för att skapa enkla, men potentiellt skadliga ändringar i digitalt innehåll, som att lägga till vilseledande text, byta ut ansikten och ta bort eller ändra sammanhang. Sådana ”billiga förfalskningar” används ofta för att sprida skändligt material, främja politiska ideologier och skada personers rykte. Ett välkänt exempel är 2019 års[16] film med talmannen i det amerikanska representanthuset, Nancy Pelosi, som sluddrar och verkar berusad. Även om det snabbt framgick att filmen hade saktats ned för att skapa effekten, spreds den ”billiga förfalskningen” vitt och brett innan den ursprungliga videon och kontexten hade dykt upp.

Mer avancerade metoder för att ändra medieinnehåll omfattar användning av avancerade AI-tekniker för att (a) skapa rent syntetiska medier och (b) göra mer raffinerade ändringar i befintliga medier. Ordet ”deepfake” används ofta för syntetiska medier som har skapats med den senaste AI-tekniken (namnet kommer från de djupa neurala nätverk som ibland används). De här teknikerna utvecklas som fristående appar, verktyg och tjänster och integreras i etablerade redigeringsverktyg från kommersiella och öppna källor.

Sådan teknik kan användas som vapen av illasinnade aktörer som hoppas kunna skada individer och institutioner. Här är några exempel på deepfake-tekniker:

- **Ansiktsbyten (film, bilder) –** ersätta ett ansikte i en film med ett annat. Tekniken kan användas för att försöka utpressa en person, ett företag eller en institution, eller för att placera individer på pinsamma platser eller i pinsamma situationer.
- **Dockspel (film, bilder) –** att använda en film för att animera en stillbild eller en annan film. Tekniken kan få det att se ut som om en person har sagt något pinsamt eller missvisande.
- **Generativa motståndarnätverk (film, bilder) –** en teknikkategori för att generera fotorealistiska bilder.
- **Transformmodeller (film, bilder, text) –** skapa innehållsrika bilder från textbeskrivningar.

Sådana avancerade AI-tekniker används inte i särskilt stor utsträckning i cyberpåverkanskampanjer ännu, men vi förväntar oss att problemet växer när verktygen blir enklare att använda och mer allmänt tillgängliga.

Effekten av manipulation med syntetiska medier

Användningen av informationsverksamhet för att orsaka skada eller öka sitt inflytande är inte något nytt. Men med tanke på hur fort informationen kan spridas och vår oförmåga att snabbt skilja fakta från påhitt, innebär det att effekten och skadan som orsakas av förfalskningar och andra syntetiskt genererade skadliga medier kan bli mycket större, vilket framgår av Pelosi-exemplet.

Det finns flera kategorier av skador att ta hänsyn till: marknadsmanipulation, betalningsbedrägerier, samtalsfiske, personifieringar, varumärkesskador, renommésskador och botnät. Många av kategorierna har ofta rapporterade verkliga exempel, vilket kan göra det ännu svårare att skilja fakta från påhitt.

Ett mer långsiktigt och lömskt hot är vår syn på vad som är sant om vi inte längre kan lita på det vi ser och hör. Det skulle kunna göra det enklare att avfärda eventuella kompromitterande bilder, ljud eller filmer av offentliga personer eller privatpersoner som falska – precis som sensmoralen i berättelsen om Peter och vargen.[17] Ny forskning[18] visar att det här teknikmissbruket redan används för att angripa finansiella system, även om många andra missbrukssscenarier är rimliga.

Syntetiska medier

fortsättning

Identifiera syntetiska medier

Det pågår insatser inom industrin, hos myndigheter och i den akademiska världen för att utveckla bättre sätt att identifiera och mildra effekterna av syntetiska medier och återställa förtroendet. Det finns flera lovande vägar framåt, men också hinder som behöver övervägas.

Ett sätt är att bygga AI-baserade system som kan upptäcka förfalskningar – i huvudsak "defensiva" AI-system för att motverka de offensiva AI-systemen. Det är ett aktivt forskningsområde där de nuvarande systemen för att skapa syntetiskt ljud och syntetisk film efterlämnar artefakter som utbildade medieanalytiker och automatiserade verktyg kan upptäcka.

Men även om de nuvarande förfalskningarna har avslöjande brister, tenderar de exakta artefakterna tyvärr att vara specifika för ett visst verktyg eller en viss algoritm. Det betyder att utbildning om kända förfalskningar vanligtvis inte går att generalisera till andra algoritmer, vilket visades under en öppen tävling 2020 för att skapa bilddetektorer som kan identifiera deepfakes.[19] Det är frestande att öka investeringarna i att utveckla mer avancerade detektorer, men av två anledningar tror Microsoft inte att sådana investeringar kommer att leda till några betydande förbättringar:

För det första har vi utmärkta fysiska modeller som återspeglar verkligheten. De som nu skapar falska bilder tar genvägar, vilket leder till detekterbara artefakter, men framtida modeller kommer att bli alltmer realistiska. Det finns egentligen inget särskilt med en verklig scen som registreras av en kamera som inte går att modellera med en dator.

För det andra använder avancerade algoritmer för att skapa falska bilder en teknik som kallas generativa motståndarnätverk (GM). Ett GM ställer två AI-system mot varandra med hjälp av en generator för att skapa den falska bilden och en detektor som hittar falska bilder och tränar generatorn. Alla investeringar i att utveckla en bättre detektor kommer bara att medföra att generatorn kan förbättra kvaliteten på förfalskningarna.



Syntetiska medier

fortsättning

Härkomst för digitala tillgångar

Men vad kan man då göra för att skydda mot skadlig användning av syntetiska medier, om det inte går att avslöja förfalskningarna på ett effektivt sätt? En viktig ny teknik är digital härkomst, en mekanism som gör att de som skapar digitala medier kan certifiera en tillgång och hjälpa konsumenterna att avgöra om den digitala tillgången har manipulerats eller inte. Digital härkomst är särskilt viktigt i samband med dagens sociala medienätverk, med tanke på hur snabbt innehåll kan spridas på internet och möjligheten för illasinnade att enkelt manipulera innehåll.

900 %

ökning av deepfakes per år sedan 2019.[20]

Digital Provenance Technology är en modern version av kryptografisk dokumentsignering. Tekniken är avsedd att registrera källan, redigeringshistoriken och metadata för objekt när de flödar genom den moderna webben. Visionen och de tekniska metoderna för att möjliggöra den här typen av heltäckande manipulationssäker certifiering av medier har utvecklats av ett tvärvetenskapligt team med forskare och vetenskapsmän på Microsoft. Vi är med och leder ett branschöverskridande samarbete som syftar till att bringa liv i tekniken för mediehärkomst i Project Origin (som grundades av Microsoft, BBC, CBC/Radio-Canada och New York Times) och engagerar oss i Content Authenticity Initiative (som grundades av Adobe). Microsoft samarbetade också med partner inom teknik- och medietjänster för att inrätta Coalition for Content Provenance and Authenticity (C2PA). C2PA är en standardorganisation som nyligen publicerade den mest avancerade specifikationen för digital härkomst som är tänkt att användas med medietillgångar som bilder, filmer, ljud och text.

Ett C2PA-objekt bär med sig ett manifest som skyddar det och dess metadata från manipulation, och det medföljande certifikatet identifierar utgivaren.

Syntetiska medier var ursprungligen inte avsedda att skada någon, men de görs till vapen av illasinnade för att undergräva förtroendet för individer och institutioner.

Digital härkomst är en lovande ny teknik som skulle kunna bidra till att återställa människors förtroende för medieinnehåll online genom att certifiera en medietillgångs ursprung.

Offentligt tillgängliga lösningar som bygger på C2PA-specifikationen dyker antingen upp som en ny funktion i befintliga produkter eller nya fristående appar och tjänster. Vi förväntar oss att de flesta av de vanligaste registrerings-, redigerings- och skapandeverktygen ska kunna använda C2PA om några år. Detta innebär en möjlighet för företag att fastställa sina behov och användningsområden för digital härkomst i dag, och att kräva detta ytterligare skyddslager i de verktyg de använder i befintliga arbetsflöden.

Användbara insikter

1. Vidta proaktiva åtgärder för att skydda organisationen mot desinformationshot genom proaktiva överväganden av era PR- och kommunikationsinsatser.
2. Använd härkomstteknik för att skydda officiell kommunikation.

Länkar till mer information

- A promising step forward on disinformation | Microsoft On the Issues
- A Milestone Reached, 31 januari, 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Utforska tekniska detaljer om det system Project Origin använder för autentisering av medier | Microsoft ALT Innovation

En helhetsmetod för att skydda mot cyberpåverkan

Microsoft bygger vidare på den redan mogna infrastrukturen för cyberhotsunderrättelser för att ta fram en bredare och mer inkluderande syn på cyberpåverkan.

För att bekämpa det hot som operationerna utgör använder vi ett ramverk med förslag på åtgärder och begränsningsstrategier. Ramverket har fyra huvudpelare: identifiera, störa, försvara och avskräcka.

Dessutom har Microsoft antagit fyra principer för att förankra vårt arbete inom det här området. Den första är ett åtagande om att respektera yttrandefriheten och upprätthålla våra kunders förmåga att skapa, publicera och söka efter information via våra plattformar, produkter och tjänster. Den andra är att vi arbetar proaktivt för att förhindra att våra plattformar och produkter används för att förstärka utländska webbplatser och innehåll för cyberpåverkan. Den tredje är att vi inte medvetet kommer att dra nytta av utländskt cyberpåverkande innehåll eller aktörer. Slutligen prioriterar vi att visa upp innehåll för att motverka utländsk cyberpåverkan genom att använda interna och betrodda data från tredje man i våra produkter.

Identifiera

Precis som vid cyberförsvar är det första steget för att motverka utländska cyberpåverkansoperationer att utveckla vår förmåga att upptäcka dem. Inget enskilt företag eller enskild organisation kan på egen hand lyckas åstadkomma de framsteg som behövs. Ett nytt, omfattande samarbete inom den tekniska sektorn kommer att vara nödvändigt. Framstegen när det gäller att analysera och rapportera cyberpåverkan är starkt avhängiga av civilsamhället, till exempel via akademiska institutioner och ideella organisationer.

Forskarna Jake Shapiro och Alicia Wanless vid Princeton University respektive Carnegie Endowment for International Peace planerar att lansera det nya Institute for Research on the Information Environment (IRIE). Med stöd från Microsoft, Knight Foundation och Craig Newmark Philanthropies kommer IRIE att utarbeta en inkluderande forskningsinstitution för många intressenter, med CERN som modell. Den kommer att kombinera expertis inom databehandling och dataanalys för att påskynda och skalanpassa nya upptäckter inom området. Resultaten kommer att publiceras för att informera beslutsfattare, teknikföretag och konsumenter.

Försvara

Den andra strategiska pelaren är att främja och försvara demokratin. Det har länge varit högprioriterat, men det behövs mer investeringar och innovationer. Strategierna måste ta hänsyn till de utmaningar som tekniken har skapat för demokratin och de möjligheter som tekniken har skapat för att försvara demokratiska samhällen på ett mer effektivt sätt.

Microsofts strategiramverk syftar till att hjälpa intressenter i olika sektorer att identifiera, störa, försvara och avskräcka från propaganda – särskilt kampanjer från utländska angripare.

En lämplig startpunkt är en av de stora tekniska utmaningarna i vår tid – den påverkan som internet och digital reklam har på den traditionella journalistiken. Ända sedan 1700-talet har en fri och oberoende press haft en särskild roll att spela för att främja och stödja alla världens demokratier. Pressen avslöjar korruption, dokumenterar krig och belyser de största samhälleliga utmaningarna i vår tid och alla andra tider. Men internet har skapat stora utmaningar för lokala medier genom att suga upp reklamintäkterna och locka bort betalande prenumeranter. Många lokala tidningar har kollapsat. En av många insikter vi har fått av vårt arbete på sistone är att städer som saknar en tidning omedvetet och oundvikligen exponeras för en större genomsnittlig volym av utländsk propaganda. Därför är en av demokratins nödvändiga försvarsspelare att stärka den traditionella journalistiken och den fria pressen, särskilt lokalt. Det kräver löpande investeringar och innovationer som måste återspegla de lokala behoven i olika länder och på olika kontinenter. De här frågorna är inte lätta att hantera och kräver insatser från många intressenter, och Microsoft och andra teknikföretag riktar alltmer stöd åt frågan.

En annan prioriterad fråga är politiskt nytänkande. Det kan till exempel handla om lagar som gör att utgivare kan förhandla om annonsintäkter kollektivt med teknikföretag och lagstiftning som ger skattelättnader för att befria lokala nyhetsredaktioner från en del av sina löneskatter för de journalister de anlitar. Journalister behöver många andra verktyg för sitt värv, däribland möjlighet att skilja mellan innehåll från legitima och bedrägliga källor.

Det finns också ett snabbt föränderligt behov av att hjälpa konsumenter att bli bättre på att upptäcka nationalstatsdriven informationsverksamhet. Även om det här kan verka svårt påminner det på många sätt om det arbete som teknikSektorn sedan länge har bedrivit för att bekämpa andra cyberhot. Tänk bara på arbetet för att utbilda konsumenter att titta närmare på e-postadressen i sina e-postmeddelanden för att avgöra om det kan vara skräppost eller annan bedräglig kommunikation. Initiativ i USA, till exempel News Literacy Project och Trusted Journalism Program

Ett mer långsiktigt och lömskt hot är vår syn på vad som är sant om vi inte längre kan lita på det vi ser och hör.

En helhetsmetod för att skydda mot cyberpåverkan

fortsättning

bidrar till utvecklingen av mer välinformerade konsumenter av nyheter och information. Globalt kan ny teknik som webbläsarinstickspogrammet från NewsGuard hjälpa till att utveckla den här insatsen mycket snabbare.

Det här understryker också att en del av demokratins grunder ligger i medborgarnas utbildning. Som vanligt måste insatserna inledas i skolan. Men i dagens värld behöver utbildningen i medborgarkunskap pågå under hela livet. Det nya Civics at Work-initiativet, som leds av Center for Strategic and International Studies och som Microsoft undertecknade och var med om från början, syftar till att stärka medborgarnas samhällskunskaper på företag. Det är ett bra exempel på alla möjligheter som finns för att stärka försvaret av demokratin.

Störa

På senare år har Microsoft Digital Crimes Unit (DCU) förfinat sina taktiker och utvecklat verktyg för att störa alla cyberhot från utpressningstrojaner till botnät och angrepp från nationalstater. Vi har fått många viktiga lärdomar, till att börja med den roll som aktiva störningar spelar för att motverka en mängd olika cyberattacker.

När vi funderar på att motverka cyberpåverkansoperationer kan störningar spela en ännu viktigare roll och vi är på god väg att komma fram till den bästa störningsmetoden. Det mest effektiva motgiftet mot omfattande bedrägeri är öppenhet. Det var därför Microsoft ökade sin kapacitet att upptäcka och störa nationalstaters påverkansoperationer genom att köpa Miburo Solutions, ett ledande cyberhotsanalys- och forskningsföretag som har specialiserat sig på att identifiera och reagera på utländska cyberpåverkansoperationer.

Vår erfarenhet visar att myndigheter, teknikföretag och icke-statliga organisationer bör tillskriva cyberattacker noggrant och med goda underlag. Att förstå effekterna av sådana störningar är viktigt och kan vara ännu mer användbart för att störa cyberpåverkan. Se bara på USA:s sätt att dela information inför Rysslands invasion av Ukraina. Där gjorde man effektiv nytta genom öppenheten, som att exponera Rysslands planer, däribland specifika kampanjer som en plan att använda en falsk, målande video.

Som förra sommarens publikation från CyberPeace Institute i Genève visade om pågående cyberattacker i och utanför Ukraina är det möjligt att genom ett brett spektrum från civilsamhället och organisationer i den privata sektorn främja öppenheten i samband med cyberpåverkansoperationer. Tillförlitliga rapporter om nyligen upptäckta och väldokumenterade angrepp kan hjälpa allmänheten att bli bättre på att utvärdera vad de läser, ser och hör, särskilt på internet. I det syftet tänker Microsoft bygga vidare på och utöka sina befintliga cyberrapporter och släppa nya rapporter, data och uppdateringar om vad vi upptäcker om cyberpåverkansoperationer, till exempel tillskrivningar i lämpliga fall. Vi kommer att publicera en årsrapport där vi använder en datadriven metod för att i hela företaget se på förekomsten av utländsk informationsverksamhet och vad vi kan göra härnäst för att säkerställa olika förbättringar. Vi kommer också att överväga ytterligare åtgärder som bygger på den här typen av öppenhet och insyn.

Den digitala marknadsföringens roll är särskilt viktig, till exempel eftersom reklam kan delfinansiera utländska operationer och samtidigt ge ett legitimt sken åt propagandawebbplatser som sponsras av andra länder. Nya insatser kommer att behövas för att störa de här finansiella flödena.

Avskräcka

Slutligen kan vi inte vänta oss att några länder ändrar sitt beteende om inget ansvar utkrävs för brott mot internationella regler. Att genomdriva ett sådant ansvar faller enbart på länder. Men i allt högre grad spelar insatser från många intressenter en viktig roll för att stärka och utöka de internationella normerna. Fler än 30 onlineplattformar, annonsörer och utgivare – däribland Microsoft – har undertecknat Europeiska kommissionens nyligen uppdaterade uppförandekod om desinformation och har gått med på att stärka sitt åtagande om att hantera det här växande problemet. Precis som i de på senare tid slutna samarbetsavtalen Paris Call, Christchurch Call och Declaration on the Future of the Internet kan multilaterala åtgärder av många intressenter samla länder och allmänheten i demokratiska nationer. Länderna kan sedan bygga vidare på normer och lagar för att ställa sig bakom det ansvar som världens demokratier behöver och förtjänar.

Genom snabb och radikal öppenhet kan demokratiska länder och samhällen effektivt avtrubba påverkanskampanjer genom att nämna källan till nationalstatsangrepp, informera allmänheten och bygga upp förtroende för institutioner.

> Vi har ökad teknisk kapacitet att upptäcka och störa utländska påverkansoperationer och arbetar aktivt för att öppet rapportera om sådana operationer, precis som vi rapporterar om cyberattacker.

Användbara insikter

1. Inför goda rutiner för digital hygien i hela organisationen.
2. Överväg sätt att minska allt oavsiktligt underlättande av cyberpåverkanskampanjer av era medarbetare eller genom era affärsmetoder. Det inkluderar att minska tillförseln till kända utländska propagandawebbplatser.
3. Stöd informationskompetens och kampanjer för medborgerligt engagemang som en viktig komponent för att hjälpa samhällen att försvara sig mot propaganda och utländskt inflytande.
4. Engagera er direkt i grupper som är relevanta för er bransch och som jobbar för att hantera påverkansoperationer.

Slutnoter

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. Defending Ukraine: Early Lessons from the Cyber War (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Ryska utrikesministeriets talesperson Maria Zakharova: https://tass.com/politics/1401777; Labrov: 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. Påståendena från Kremenchuk i Ryssland kontra bevisen – bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Fact check: "Drunk" Nancy Pelosi video is manipulated | 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. Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas och Kristjan Peterson, oktober 2020

Cyberåterhämtning

Att förstå riskerna och fördelarna med modernisering är avgörande för en helhetssyn på återhämtning.

En översikt över cyberåterhämtning	87
Introduktion	88
Cyberåterhämtning: En förutsättning i ett uppkopplat samhälle	89
Vikten av att modernisera system och arkitektur	90
Det grundläggande säkerhetsläget är en avgörande faktor för avancerade lösningars effektivitet	92
Att upprätthålla identitetshälsan är avgörande för organisationers välbefinnande	93
Standardsäkerhetsinställningar för operativsystemet	96
Centralitet i försörjningskedjan för programvara	97
Skapa motståndskraft mot nya DDoS-, webbprogram- och nätverksangrepp	98
Utveckla en balanserad strategi för datasäkerhet och cyberåterhämtning	101
Motståndskraft mot cyberpåverkan: den mänskliga dimensionen	102
Stärka den mänskliga faktorn med kompetenshöjning	103
Insikter från vårt program för att undanröja utpressningstrojaner	104
Åtgärda säkerhetskonsekvenserna av kvantdatorer nu	105
Integrera företag, säkerhet och IT för bättre motståndskraft	106
Klockkurvan för cybermotståndskraft	108

En översikt över

cyberåterhämtning

Cybersäkerhet är en viktig faktor för teknisk framgång. Innovation och ökad produktivitet går bara att uppnå genom att införa säkerhetsåtgärder som gör organisationer så motståndskraftiga som möjligt mot moderna angrepp.

Pandemin har utmanat oss att göra om våra säkerhetsrutiner och säkerhetstekniker för att skydda Microsofts medarbetare var de än arbetar. Det senaste året har hotaktörer fortsatt att utnyttja de sårbarheter som exponerades under pandemin och övergången till en hybridarbetsmiljö. Sedan dess har vårt främsta problem varit att hantera förekomsten och komplexiteten av olika angreppsmetoder och den ökade nationalstatsaktiviteten.

Effektiv cyberåterhämtning kräver en holistisk, adaptiv strategi för att motstå föränderliga hot mot kärntjänster och infrastruktur.

Läs mer på s. 89

Moderniserade system och en moderniserad arkitektur är viktiga för att hantera hot i en hypersammankopplad värld.

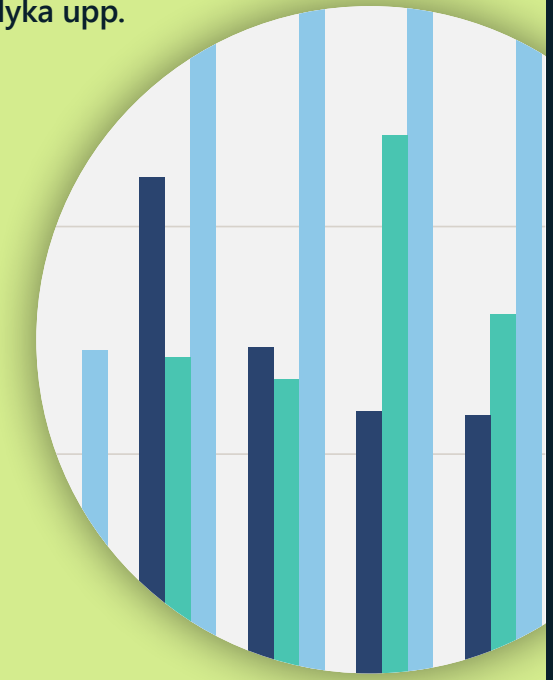


Läs mer på s. 90

Det grundläggande säkerhetsläget är en avgörande faktor för avancerade lösningars effektivitet.

Läs mer på s. 92

Även om lösenordsbaserade angrepp fortfarande är den främsta anledningen till knäckta identiteter börjar andra typer av angrepp dyka upp.



Läs mer på s. 93

Den mänskliga dimensionen av motståndskraften mot cyberpåverkan är vår förmåga att samarbeta.

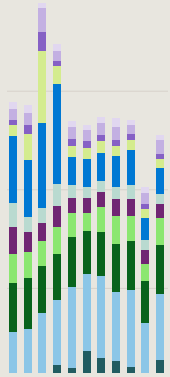
Läs mer på s. 102

De allra flesta framgångsrika cyberattacker skulle kunna förhindras med hjälp av grundläggande säkerhetshygien.

Läs mer på s. 108

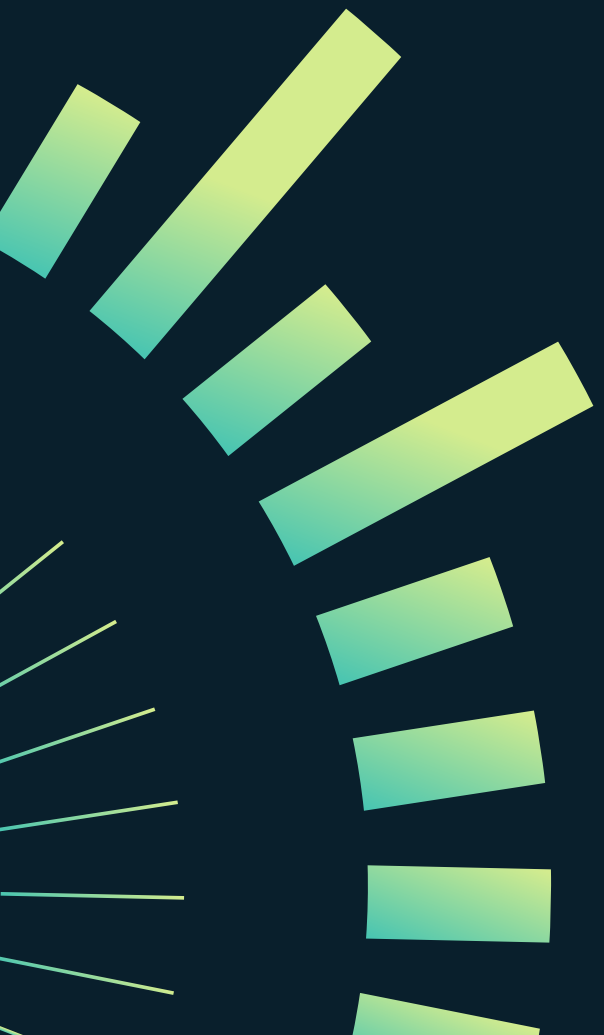


Under det senaste året har världens DDoS-aktiviteter ökat till större volym, komplexitet och frekvens än någonsin förut.



Läs mer på s. 98

Introduktion



Pandemin har utmanat oss att göra om våra säkerhetsrutiner och säkerhetstekniker för att skydda Microsofts medarbetare var de än arbetar. Det senaste året har hotaktörer fortsatt att utnyttja de sårbarheter som exponerades under pandemin och övergången till en hybridarbetsmiljö. Sedan dess har vårt främsta problem varit att hantera förekomsten och komplexiteten av olika angreppsmetoder och den ökade nationalstatsaktiviteten.

Den digitala hotaktiviteten och nivån på hur avancerade cyberattackerna är ökar för varje dag som går. Många av dagens komplexa angrepp fokuserar på att knäcka identitetsarkitekturer, försörjningskedjor och tredje man med varierande grad av säkerhetskontroller. Vi har i synnerhet observerat identitetsnätfiske som ett tydligt och närvarande hot. De här typerna av angrepp misslyckas dock i allmänhet om det finns god identitetshantering, nätfiskekontroll och metoder för att hantera slutpunkter. Därför får vi aldrig glömma bort grunden: nittioåtta procent av alla angrepp går att stoppa om rätt grundläggande hygienåtgärder finns på plats. På Microsoft hanterar vi identiteter och enheter i vår nolltillitsstrategi, som omfattar minsta privilegierad åtkomst och nätfiskeresistenta autentiseringsuppgifter för att effektivt stoppa hotaktörerna och skydda våra data.

I dag kan till och med hotaktörer som saknar avancerad teknisk kompetens inleda oerhört destruktiva angrepp, eftersom cyberbrottslighetsekonomin har gett vem som helst tillgång till avancerad taktik, teknik och förfaranden. Kriget i Ukraina visade hur nationella statsaktörer har eskalerat sin offensiva cyberverksamhet genom ökad användning av utpressningstrojaner. Utpressningstrojaner är nu en välutvecklad bransch där hotaktörer använder dubbla eller tredubbla utpressningsmetoder för att få ut pengar och utvecklare erbjuder utpressningstrojaner som tjänst (RaaS). Med RaaS nyttjar hotaktörerna ett nätverk med anknutna organisationer för att utföra angrepp, vilket sänker barriären för mindre skickliga cyberbrottslingar att genomföra angrepp och i slutänden innebär det fler möjliga angripare.

Därför har Microsoft konstruerat ett program för att eliminera utpressningstrojaner. Målet är att åtgärda brister i kontroller och täckning, bidra till funktionsförbättringar för tjänster och utveckla återställningsmetoder för vårt säkerhetscenter och våra teknikerteam i händelse av en utpressningstrojanattack.

De senaste angreppen mot försörjningskedjor och tredje man tyder på en stor förändring i branschen. De störningar som angreppen orsakar våra kunder, partner, myndigheter och Microsoft fortsätter att öka, vilket visar vikten av att ha fokus på cyberåterhämtning och samarbete mellan säkerhetsintressenter. Angripare riktar också in sig mot lokala system, vilket underblåser behovet av att organisationer hanterar sårbarheter som uppstår med äldre system genom att modernisera och flytta infrastruktur till molnet, där säkerheten är mer robust.

Vi lever i en tid då säkerhet är en viktig faktor för teknisk framgång. Innovation och ökad produktivitet går bara att uppnå genom att införa säkerhetsåtgärder som gör organisationer så motståndskraftiga som möjligt mot moderna angrepp. I takt med att de digitala hoten ökar i omfattning och utvecklas är det viktigt att bygga in cyberåterhämtning i varje organisations struktur.

Bret Arsenault
Informationssäkerhetschef

Cyberåterhämtning: En förutsättning i ett uppkopplat samhälle

Revolutionen inom digital teknik har gjort att organisationer har blivit alltmer uppkopplade, både i fråga om hur de arbetar och de tjänster de erbjuder. I takt med att hoten i cyberlandskapet ökar hat inbyggd cyberåterhämtning blivit lika viktig för organisationen som den ekonomiska och operativa motståndsskraften.

Digitaliseringen har för alltid förändrat hur organisationer interagerar med kunder, partner, anställda och andra intressenter. Ny teknik ger tillgång till enorma möjligheter att interagera med människor, göra om produkter och optimera verksamheten. Pandemin påskyndade digitaliseringen genom att underblåsa innovativ teknik som låter människor samarbeta på nya sätt och från valfri plats.

När cyberhot blir endemiska är det svårare att hindra dem från att påverka en organisation, i dagens ständigt uppkopplade värld. Cyberåterhämtning handlar om organisationens förmåga att fortsätta sin verksamhet och upprätthålla tillväxten trots angrepp. Förebyggande åtgärder måste balanseras med överlevnads- och återställningskapaciteten och som ett led i cyberåterhämtningen utvecklar både länder och företag kompletta modeller som omfattar mer än bara säkerhet och integritet för att skydda sina tillgångar, data och andra resurser.

Utveckla en helhetssyn på cyberåterhämtning

Cyberåterhämtning kräver en holistisk, adaptiv och global metod som kan motstå föränderliga hot mot kärntjänster och infrastruktur, däribland

- enkel cyberhygien som beskrivs i vår cyberåterhämtningsklockkurva
- att förstå och hantera avvägningen mellan risken av/vinsterna från digitaliseringen
- kapacitet att reagera i realtid som möjliggör proaktiv identifiering av hot och sårbarheter
- skydd mot kända angrepp och förebyggande aktivitet mot nya och förväntade attackvektorer, däribland möjlighet att åtgärda automatiskt
- minskad effekt av angrepp och katastrofer genom felisolering och segmentering
- automatiserad återställning och redundans vid störningar
- prioritering av operativa tester för att hitta luckor och förstå gemensamma ansvarsområden och beroenden av externa resurser som molnbaserade säkerhetslösningar.

Ett effektivt cyberåterhämtningsprogram utgår från grundläggande resursförståelse, som att förstå tillgängliga tjänster och att ha en tillförlitlig katalog med resurser som kan anropas i händelse av störningar. Från den grunden måste programmet kunna bedöma hur effektivt det är, mäta prestanda för kritiska tjänster och deras beroenden, testa och validera funktioner i lokala tjänster och molntjänster samt främja kontinuerliga förbättringar under organisationens digitala livscykel.

För att skapa en helhetsbild samarbetar vi med organisationer för att identifiera deras mest kritiska lokala tjänster och onlinetjänster, affärsprocesser, beroenden, medarbetare, säljare och leverantörer. Vi försöker också identifiera tillgångar och resurser som är kopplade till kundernas och marknadens förväntningar, lag- och kontraktsenliga förpliktelser samt intern drift. Samtidigt som de kritiska resurserna identifieras bör parallella insatser identifiera och övervaka hot, störningar, potentiella attackvektorer samt system- och processårbarheter. För att lyckas göra det trots dagens kompetensbrist krävs noggranna prioriteringar baserat på den övergripande risken för organisationen.

Den här typen av helhetssyn måste anpassas mot bakgrund av en ständigt föränderlig hotbild. Målet är att driva på mätbara prestandaförbättringar, kortare tid för att identifiera, reagera och återhämta sig och minskad påverkan om störningar ändå inträffar. Strategin måste också ta hänsyn till att hoten allt oftare kommer från nätet. En säkerhetsincident kan till exempel leda till ett dataintrång med konsekvenser för integriteten, vilket kräver att många interna och externa team samarbetar för att reagera snabbt och minimera påverkan.

> Cyberåterhämtning handlar om företagets förmåga att fortsätta sin verksamhet och upprätthålla tillväxten trots störningar, inklusive cyberattacker.

Användbara insikter

1. Skapa och hantera tekniska system som begränsar effekten av ett intrång så att systemet kan fortsätta att fungera tryggt och effektivt, även om ett intrång lyckas. Fokusera på vanliga kritiska tillgångar, stöd smidighet och konstruera för anpassningsförmåga (till exempel hybrid- och multimoln, flera plattformar), minska attackytorna (ta t.ex. bort oanvända appar och onödigt stora åtkomsträttigheter), anta att tillgångar har knäckts och förvänta er att angriparna utvecklas.
2. När ni planerar digitala projekt bör ni ta hänsyn till både potentiella hot och möjligheter och delat ansvar för att skapa återhämtningskapacitet i hela försörjningskedjan för digital teknik, till exempel med molnbaserade säkerhetslösningar.
3. Skapa system för att bädda in säkerhet per design och vidta åtgärder för att förutse, identifiera, stå emot, anpassa er och reagera på framtida föränderliga hot.
4. Se till att företagets ledning rådgör med säkerhetsteamen efter behov för att förstå riskerna med nya skeenden. Samtidigt måste säkerhetsteamen också ta hänsyn till affärssyften och ge råd till ledningen om hur de kan gå att uppnå på ett säkert sätt.
5. Ta fram tydliga operativa rutiner och procedurer för organisationens återhämtningskapacitet vid cyberincidenter.

Vikten av att modernisera system och arkitektur

När vi utvecklar ny kapacitet i en hyperansluten värld måste vi samtidigt hantera hoten från äldre system och programvara.

Äldre system – som utvecklades innan moderna anslutningsverktyg som mobiler, surfplattor och molntjänster blev normen – utgör en risk för organisationer som fortfarande använder dem. Riskexponeringen bekräftas av resultaten från Microsoft-teamet för Security Service for Incident Response, en säkerhetsexpertgrupp som hjälper kunderna att reagera på och återhämta sig från angrepp.

De problem som upptäcktes hos kunder som återhämtar sig från angrepp under det senaste året kan delas in i sex kategorier, som diagrammet på den här sidan visar. På följande sida beskrivs åtgärder som kan vidtas för att förbättra återhämtningskapaciteten.

Över 80 procent av alla säkerhetsincidenter går att härleda till några element som saknas och kan åtgärdas med hjälp av moderna säkerhetsstrategier.

Viktiga frågor som påverkar cyberåterhämtningen



I diagrammet visas andelen påverkade kunder som saknar grundläggande säkerhetskontroller som är avgörande för att öka organisationens cyberåterhämtning. Resultaten bygger på Microsoft engagemang under det senaste året.

”Ledare bör se cyberåterhämtning som en avgörande del av företagets återhämtningskapacitet. De bör planera för cyberstörningar på samma sätt som naturkatastrofer eller andra oförutsedda händelser och sammanföra interna intressenter inom drift, kommunikation, juridiska frågor och andra områden för att formulera strategier. De organisationer som gör det kan snabbare få ut sina kritiska affärssystem på nätet igen och återuppta den normala affärsverksamheten.

Men det är inte allt. Eftersom många organisationer använder externa leverantörer och tjänsteleverantörer måste ledningen utöka cyberåterhämtningsplaneringen till hela värdekedjan för att säkerställa kontinuitet och återhämtningskapacitet i verksamheten.”

Ann Johnson,
Corporate Vice President of Security, Compliance, Identity, and Management Business Development

Vikten av att modernisera system och arkitektur

fortsättning

Det finns tydliga områden som organisationer kan ta itu med för att modernisera sin strategi och skydda sig mot hot:

Problem	Konkreta åtgärder
Osäker konfiguration av identitetsleverantören Felaktig konfiguration och exponering av identitetsplattformar och dess komponenter är ett vanligt sätt för angripare att få obehörig åtkomst med hög behörighet.	Följ grundläggande säkerhetskonfiguration och bästa praxis när ni installerar och underhåller identitetssystem som AD- och Azure AD-infrastrukturen. Inför åtkomstbegränsningar genom att genomdriva segregering av behörighet, minst privilegierad åtkomst och användning av arbetsstationer med privilegierad åtkomst för hantering av identitetssystem.
Otillräckliga kontroller av behörighet och laterala förflyttningar Administratörer har för stora behörigheter i den digitala miljön och använder ofta administrativa autentiseringsuppgifter på arbetsstationer som kan kopplas till internet- och produktivitetsrisker.	Säkra och begränsa den administrativa åtkomsten för att göra miljön mer motståndskraftig och begränsa omfattningen av angrepp. Använd Privilege Access Management-kontroller som just-in-time-åtkomst och just-enough-administration.
Ingen flerfaktorsautentisering (MFA) Moderna angripare bryter sig inte in, de loggar in.	MFA är en mycket viktig och grundläggande användaråtkomstkontroll som alla organisationer bör använda. I kombination med villkorsstyrd åtkomst kan MFA vara ovärderlig för att bekämpa cyberhot.
Säkerhetsåtgärder med låg mognad De flesta organisationer som har råkat ut för intrång använde traditionella verktyg för hotidentifiering och saknade relevanta insikter för snabba insatser och åtgärder.	En omfattande hotidentifieringsstrategi kräver investeringar i utökad identifiering och respons (XDR) samt moderna molnverktyg som använder maskininlärning för att skilja brus från signaler. Modernisera säkerhetshanteringsverktygen genom att införliva XDR, vilket kan ge djupa säkerhetsinsikter i hela det digitala landskapet.
Brist på informationsskyddskontroll Organisationer fortsätter att kämpa med att utforma holistiska informationsskyddskontroller som har full täckning på alla platser med data och är effektiva under hela informationslivscykeln samt anpassade till hur affärskritisk informationen är.	Identifiera era affärskritiska data och var de finns. Granska informationslivscykelns processer och upprätthåll dataskyddet samtidigt som kontinuiteten i verksamheten säkerställs.
Begränsad användning av moderna säkerhetsramverk Identitetsskydd är det nya säkerhetsområdet, eftersom identiteter ger tillgång till olika digitala tjänster och datormiljöer. Genom integrerade nolltillitsprinciper, applikationssäkerhet och andra moderna cyberramverk kan organisationen proaktivt hantera risker som den annars kan ha svårt att föreställa sig.	Nolltillitsramverk upprätthåller koncepten minst privilegierad åtkomst, explicit verifiering av all åtkomst och förutsätter alltid intrång. Organisationen bör också införa säkerhetskontroller och säkerhetsrutiner i DevOps- och applivscykelns rutiner för ökad säkerhetsgaranti i sina affärssystem.

Det grundläggande säkerhetsläget är en avgörande faktor för avancerade lösningars effektivitet

Genom vår analys upptäckte vi vanliga blinda fläckar i organisationernas försvar som gör det möjligt för angripare att bryta sig in initialt, upprätta ett brohuvud och genomföra ett angrepp, även när avancerade säkerhetslösningar används.

I många fall bestäms resultatet av en cyberattack långt innan attacken inleds. Angriparna utnyttjar sårbara miljöer för att ta sig in, övervaka och orsaka förödelse via laterala rörelser och kryptering eller exfiltrering. Om angriparen kan stoppas i ett tidigt skede ökar det avsevärt chansen att minska den totala effekten.

Microsoft har studerat specifika säkerhetskonfigurationer för att identifiera de vanligaste bristerna i praktiken i de här miljöerna. Det gjorde att vi kunde se vilka sårbarheter som utnyttjas oftast under utpressningstrojanattacker som leds av människor och som gjorde att hotaktörerna kunde få tillgång till och ta sig genom ett nätverk utan att bli upptäckta.

Grundläggande säkerhetskonfigurationer måste aktiveras

En organisations enheter som inte har utrustats enligt specifikation eller är föråldrade (både i förhållande till sårbarheter och säkerhetsagentstatus) är potentiella ingångsställen och åtkomstställen för angripare. Det är visserligen viktigt att organisationens enheter utrustas med en uppdaterad EDR-[1] (identifiering av och reaktion på slutpunkter) och EPP-lösning[2] (plattform för slutpunktsskydd), men det garanterar inte att utpressningstrojaner stoppas.

Avancerade lösningar som EDR och EPP är mycket viktiga för att upptäcka angripare tidigt i angreppsflödet och genomföra automatiska reparationer och skyddsåtgärder. Men eftersom de här avancerade lösningarna förlitar sig på en grundläggande förmåga att upptäcka angrepp, kräver de att grundläggande säkerhetskonfigurationer är aktiverade. Faktum är att vi observerade en massa scenarier där avancerade lösningar användes, men undergrävdes av att grundläggande säkerhetskonfigurationer saknades.

Bästa praxis i säkerhetskonfigurationer är en bättre indikation på motståndskraft än säkerhetscentrets reaktionstid

Vi observerade en 70-procentig minskning av den tid det tar en SOC-analytiker att granska och hantera en relevant avisering under en sexmånadersperiod bland alla våra kunder och partner. Den här ökade medvetenheten är ett gott tecken. Men även om säkerhetskonfigurationers synlighet har förbättrat SOC-analytikers arbetsresultat var produktsynligheten genom att man tog in och uppdaterade organisationens enheter ett bättre tecken på framgångsrikt förebyggande arbete.

Risker med okända enheter

Till skillnad från molnnätverk, där kunderna vet vilka tillgångar som körs på vilka operativsystem, kan lokala nätverk innehålla en mängd olika enheter som IoT, stationära datorer, servrar och nätverksenheter som inte övervakas eller hanteras av organisationen.

Ett genomsnittligt företagsnätverk har över 3 500 anslutna enheter som inte skyddas av en EDR-agent och skulle kunna ha tillgång till företagsresurser eller till och med mycket värdefulla tillgångar. Microsoft Defender för Endpoint (MDE) använder nätverksinspektion för att hitta enheter och tillhandahålla information om enhetsklassificeringar för dem som är anslutna till nätverket, t.ex. enhetsnamn, operativsystemdistribution och enhetstyp.

3 500

anslutna enheter i snitt i ett företag som inte skyddas av en agent för slutpunktsidentifiering och svar.

Enheter som inte stöds av någon EDR-agent bör du åtminstone vara medveten om att de finns och handla för att skydda dem genom att bedöma sårbarheter och begränsa nätverksåtkomsten.

Användbara insikter

1. Även avancerade lösningar kan undergrävas av att enkla säkerhetskonfigurationer inte används.
2. Investera i bästa praxis i fråga om säkerhetskonfigurationer för att skydda mot framtida angrepp. De här grundläggande inställningarna ger enorm avkastning när det gäller organisationens förmåga att försvara sig mot angrepp.
3. Låt alla aktuella enheter få en EDR-lösning.
4. Var noga med att uppdatera säkerhetsagenter och säkerställa skyddet mot manipulation för att få större insyn och kompletta skyddsfördelar med produkter.

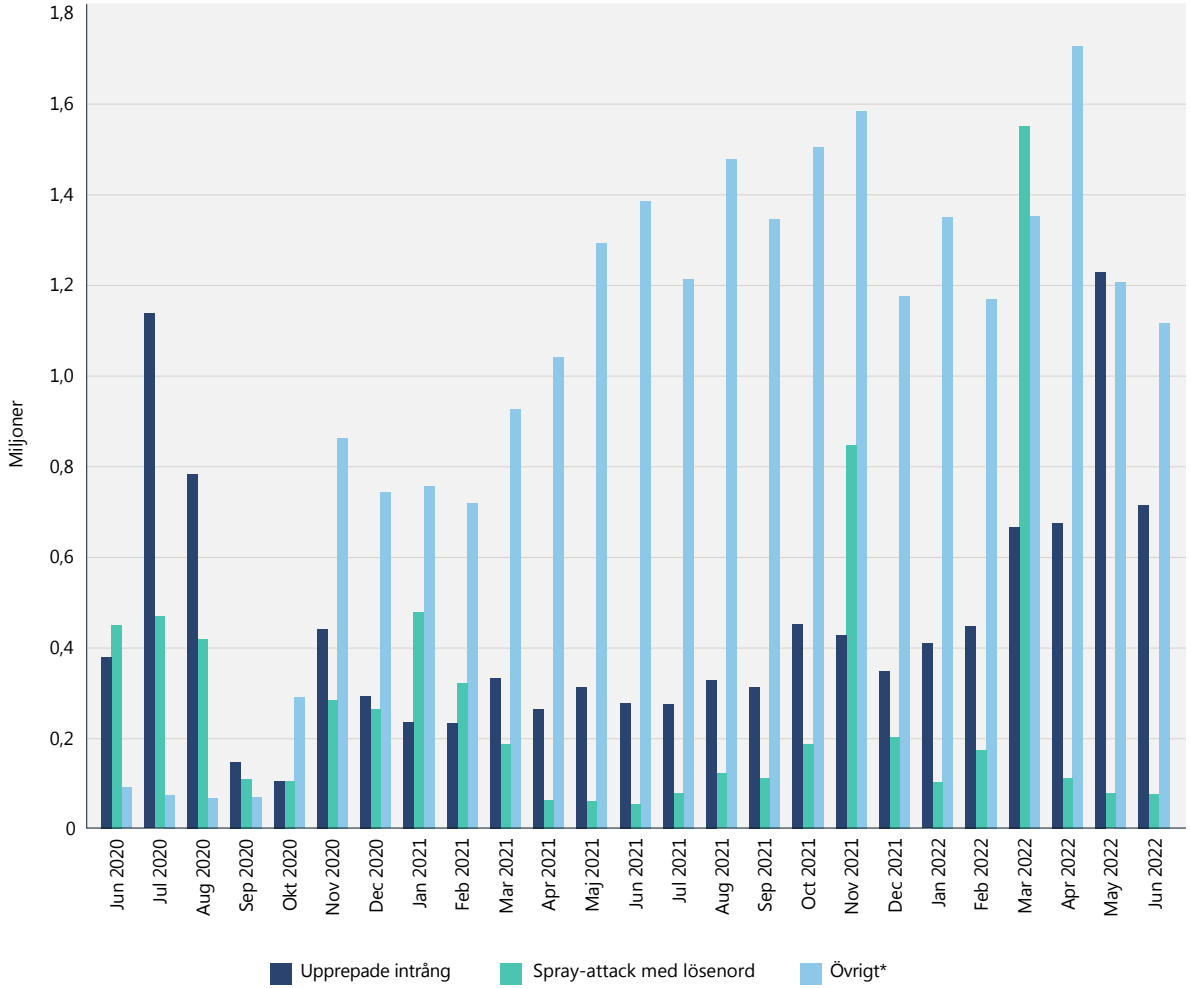
Att upprätthålla identitetshälsan är avgörande för organisationers välbefinnande

Det är viktigare än någonsin att skydda identiteter. Även om lösenordsbaserade angrepp fortfarande är den främsta anledningen till knäckta identiteter börjar andra typer av angrepp dyka upp. Antalet avancerade angrepp fortsätter att öka i förhållande till den tidigare normen med lösenordsattacker och upprepade intrång.

Lösenordsbaserade angrepp är fortfarande vanliga och över 90 procent av de konton som knäcks med sådana metoder skyddas inte med stark autentisering. Med stark autentisering används mer än en faktor för autentisering, till exempel lösenord + SMS och FIDO2-säkerhetsnycklar.

Vi har sett en ökning av riktade spray-attacker med lösenord med mycket stora toppar i angripartrafikvolymen spridda över tusentals IP-adresser.

Användare som har råkat illa ut per angreppskategori



Användare som har råkat illa ut per månad och angreppskategori. Volymen för spray-attacker med lösenord varierade mycket, vilket framgår av topparna i november 2021 och mars 2022. Topparna representerar tusentals användare och tusentals berörda IP-adresser. *"Övrigt" indikerar andra angrepp än spray-attacker med lösenord och upprepade intrång, däribland nätfiske, skadlig kod, mellanhandsangrepp, lokala tokenutgivarintrång och annat. Källa: Azure AD Identity Protection.

4 500

Under den tid det tar dig att läsa den här meningen har vi försvarat oss mot 4 500 lösenordsangrepp.

Att upprätthålla identitetshälsan är avgörande för organisationers välbefinnande

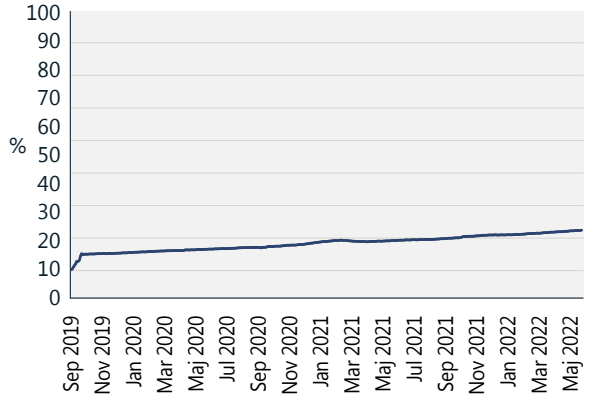
fortsättning

Implementering av stark autentisering

Vi ser en positiv utveckling i den stadigt ökande användningen av stark autentisering bland våra Azure Active Directory-företagskunder (Azure AD). För Azure AD ökade månadsanvändarna av stark autentisering från 19 till 26 procent under det senaste året, medan användarna av stark autentisering varje månad för administrativa konton ökade från 30 till cirka 33 procent.

Trenden är positiv, men många fler behöver lägga till stark autentisering innan flertalet använder det. Kunder som inte redan använder stark autentisering i sin miljö bör börja planera och implementera stark autentisering för att skydda sina användare.[3] Samtidigt som man planerar inför implementering av stark autentisering bör lösenordslös autentisering övervägas, eftersom det ger den säkraste praktiska upplevelsen och undanröjer risken för lösenordsangrepp.

Användning av stark autentisering
(september 2019–maj 2022)

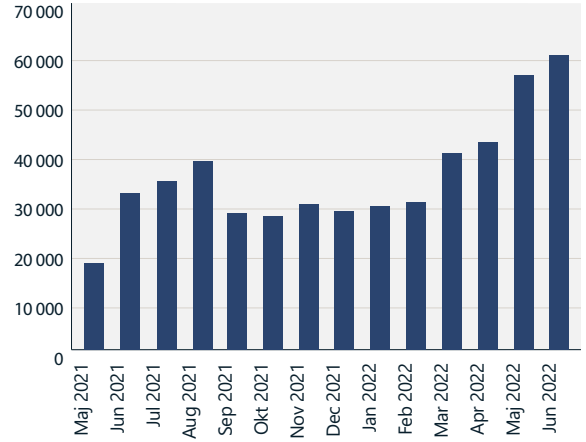


Även om användningen av stark autentisering har fördubblats sedan 2019, är det bara 26 procent av användarna och 33 procent av administratörerna som använder det. Källa: Azure Active Directory.

Stadig ökning av tokenrepetitionsattacker

Antalet andra former av angrepp ökade 2022. De riktade angreppen som specifikt undviker lösenordsbaserad autentisering ökade, vilket minskar risken för identifiering. Vid sådana angrepp utnyttjas cookies för enkel inloggning (SSO) i webbläsaren eller uppdateringstoken som erhållits via skadlig kod, nätfiske eller andra metoder. I vissa fall väljer angriparna infrastruktur på platser nära det tilltänkta offret för att ytterligare minska risken för upptäckt. Vi har sett en stadig ökning av antalet tokenrepetitionsattacker. Antalet har överstigit 40 000 varje månad i Azure AD Identity Protection. Tokenrepetitioner innebär att en angripare som har tillgång till token återanvänder dem som utfärdats till en legitim användare. Token brukar erhållas via skadlig kod, till exempel genom att exfiltrera cookies från användarens webbläsare eller genom avancerade nätfiskemetoder.

Volymen av upptäckta tokenrepetitionsattacker



Identifierade tokenrepetitionsattacker per månad. Källa: Azure AD Identity Protection, unika sessioner som har flaggats på grund av identifiering av avvikande token.

Att upprätthålla identitetshälsan är avgörande för organisationers välbefinnande

fortsättning

Extrahera token

Angripare behöver autentiseringsuppgifter mer än skadlig kod för att uppnå sina mål. Faktum är att samtliga utpressningstrojanattacker med människor bakom använder stulna autentiseringsuppgifter. Många avancerade intrång omfattar autentiseringsuppgifter som har inhandlats från den mörka webben. De stals ursprungligen av osofistikerad skadlig kod som stjäl autentiseringsuppgifter som många har tillgång till. Den här klassen av skadlig kod har utvecklats för att stjäla token, däribland sessionsinformation och MFA-anspråk. Det innebär att infektioner i hemsystem, varifrån användare loggar in till ett företags tillgångar, kan leda till allvarliga incidenter i företagsnätverk.

Angripare kan också extrahera token från offrens enheter genom mellanhandsangrepp, som innebär att offret klickar på en skadlig länk i ett nätfiskemeddelande eller ett snabbmeddelande och hamnar på en webbplats som ser ut som identitetsleverantörens legitima inloggningssida. Men i själva verket är det en webbtjänst som angriparen har ordnat med och som vidarebefordrar och avlyssnar all trafik mellan användaren och identitetsleverantören. Angriparen kan snappa upp användarnamn och lösenord och även vidarebefordra MFA-utmaningar. De token som då utfärdas av identitetsleverantören snappas upp av angriparen och kan innehålla MFA-anspråk som angriparen kan använda för att uppfylla MFA-krav.

Microsoft Defender for Cloud Apps har identifierat i snitt 895 sådana angrepp per månad sedan början av 2022. Den här formen av angrepp kan förhindras genom att använda nätfiskeresistenta MFA-faktorer, till exempel certifikatbaserad autentisering, Windows Hello för företag eller FIDO2-säkerhetsnycklar.

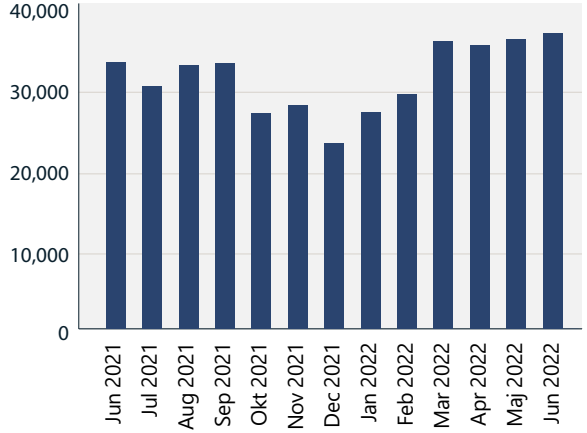
> Lösenordsbaserade angrepp är den primära metoden för att knäcka konton.

MFA-utmattning

Konceptet MFA-utmattning betyder att angripare genererar många MFA-förfrågningar till offrets enhet i hopp om att offret ska acceptera begäran antingen oavsiktligt eller till följd av leda. Sådana angrepp går att förhindra genom att använda moderna autentiseringsappar som Microsoft Authenticator i kombination med funktioner som siffermatchning[4] och tillgängliggöra ytterligare kontext.[5] Azure AD Identity Protection uppskattade att 30 000 MFA-utmattningsangrepp sker varje månad.

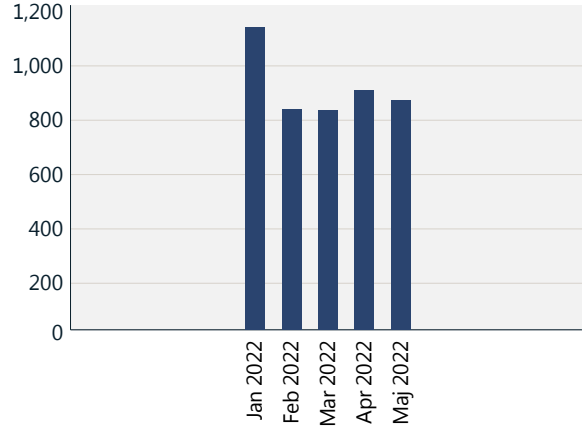
> Andelen sofistikerade angrepp fortsätter att öka, vilket verkligen visar behovet av nätfiskeresistenta faktorer för multifaktorautentisering.

Uppskattade instanser av MFA-utmattningsangrepp



Källa: Azure AD Identity Protection.

Identifierade fall av nätfiske följt av mellanhandsangrepp



Källa: Microsoft Defender for Cloud Apps.

Användbara insikter

1. Se till att alla konton i organisationen skyddas av starka autentiseringsåtgärder.
2. Lösenordslös autentisering är den säkraste och mest användarvänliga upplevelsen och eliminerar risken för lösenordsangrepp.
3. Inaktivera äldre autentisering i hela organisationen.
4. Skydda mycket värdefulla och administrativa konton med nätfiskeresistenta former av stark autentisering.
5. Modernisera från en lokal identitetsleverantör till en molnidentitetsleverantör. Anslut alla appar till den molnbaserade identitetsleverantören för konsekventa användarupplevelser och säkerhet.

Länkar till mer information

› This World Password Day consider ditching passwords altogether | Microsoft Security

Standardsäkerhets-inställningar operativsystemet

Med den ständigt föränderliga säkerhetshotbilden finns det ett ökande behov av standardkonfigurerad datorsäkerhet för att förbättra cyberåterhämtningen. Även om operativsystemssäkerhet är mer brådskande, komplex och affärskritisk än någonsin förut, kan det vara svårt att göra rätt och hantera.

Tidigare hade dator- och enhetssäkerheten inbyggda säkerhetsfunktioner som kunden eller IT-proffsen förväntades konfigurera till sin egen önskade nivå. Den här metoden räcker inte längre, eftersom angriparna använder mer avancerade verktyg inom automatisering, molninfrastruktur och fjärråtkomstteknik för att uppnå sina mål. Det har blivit absolut nödvändigt att alla säkerhetslager, från kretskort till moln, är konfigurerade som standard. Microsoft konfigurerar nu Windows-operativsystemssäkerheten som standard.[6]

Kunder som satsar på att försvara sig – på djupet med en skiktad säkerhetsinställning, nya säkerhetsfunktioner, regelbundna och konsekventa korrigeringar och uppdateringar samt säkerhetsutbildning och säkerhetsmedvetenhet för att rapportera nätfiske och andra bedrägerier – kan förvänta sig mindre skadlig kod.

För att förenkla försvaret på djupet har Windows 11 tätt integrerade maskinvaru- och programvaruskydd som är på som standard, däribland minnesintegritet, Secure Boot och Trusted Platform Module 2.0. Windows 10-användare på kompatibel maskinvara kan också aktivera de här funktionerna i Windows inställningsapp eller på BIOS-menyn.

Äldre enheter har i allmänhet ofta inte lika god anpassning mellan maskinvarusäkerhet och säkerhetstekniker för programvara. För enheter där säkerheten inte är aktiverad som standard kan den konfigureras manuellt med inställningar där det är möjligt.[7]

För enheter där säkerheten inte är aktiverad som standard rekommenderar Microsoft att den konfigureras manuellt med inställningar där det är möjligt.

Var proaktiv vid tillämpningen av kontinuerliga operativsystemuppdateringar och säkerhetskorrigeringar som skyddar under hela maskinvaru- och programvarulivscykeln.

Användbara insikter

1. Använd en lösning utan lösenord som binder inloggningsuppgifter i Trusted Platform Module. Leta specifikt efter en lösenordslös lösning som uppfyller Faster Identity Online (FIDO) Alliances[8] branschstandard.
2. Rensa bort alla oanvända och inaktuella körbara filer som lagras på organisationers enheter i god tid.
3. Skydda avancerade angrepp mot inbyggd programvara genom att aktivera minnesintegritet, Secure Boot och Trusted Platform Module 2.0, om det inte är aktiverat som standard. Det härdar starten av datorn med funktioner som är inbyggda i moderna processorer.
4. Slå på datakryptering och autentiseringsskydd.
5. Aktivera app- och webbläsarkontroller för utökat skydd mot obetrodda appar och andra inbyggda intrångsskydd.
6. Aktivera skydd mot minnesåtkomst för att skydda mot fysiska angrepp, t.ex. att någon ansluter en skadlig enhet till externt tillgängliga portar.

Länkar till mer information

- Bok om Windows-säkerhet | Kommersiell
- New security features for Windows 11 will help protect hybrid work | Microsoft Security Blog

Centralitet i försörjningskedjan för programvara

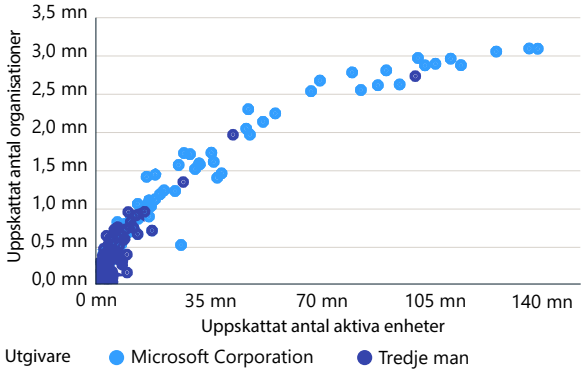
Angrepp mot appar, insticksprogram och tillägg från tredje man kan urholka kundernas förtroende för leverantörer som spelar en central roll i försörjningsekosystemet. Genom att använda nätverksteori för att titta på programvarans centralitet blir det lättare att se hur viktigt det är med korrigeringar, särskilt för centrala appar.

Windows App Network som består av 18 miljoner körbara program installeras och används av fem miljoner organisationer och ger oss översikt över vårt programvaruekosystem. Av de 100 000 mest använda programmen produceras 97 % av externa organisationer vars uppdateringar och säkerhetskorrigeringar underhålls av dem. Det illustrerar två viktiga egenskaper i vårt ekosystem med kommersiella appar.

För det första finns det centralitet i Windows ekosystem med kommersiella program. Bara de 100 000 (av 18 miljoner) främsta programmen används på 1 000 eller fler enheter. Med andra ord har drygt en halv procent av de här programmen en sådan bredspektrig effekt på enhetsekosystemet.

För det andra hanteras programmen på en mängd olika sätt. De 10 000 programleverantörerna hanterar uppdateringar och säkerhetskorrigeringar av de här mest använda kommersiella programmen. Det visar det ömsesidiga beroende som ett företag har av en mängd olika programvaruleverantörers säkerhets-, efterlevnads- och hanteringskontroller.

Kommersiellt avtryck av de mest använda programmen



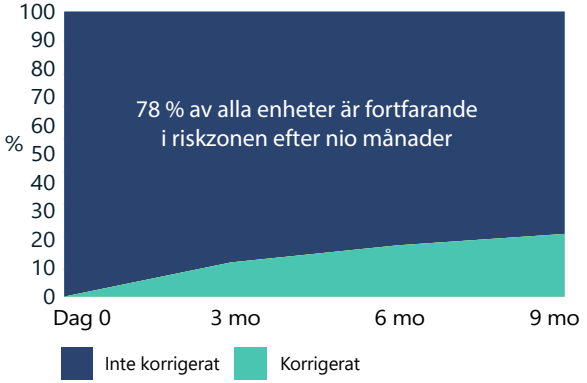
De främsta programmen används av miljontals organisationer och på tiotals miljoner enheter. Eftersom de finns nästan överallt är brottsliga aktörer ständigt på jakt efter sårbarheter i de här programmen, som kan påverka miljontals användares enheter.

Vi ser att miljontals kommersiella enheter fortfarande använder sårbara programversioner många månader efter publiceringen av en korrigering eller till och med år efter att produktsupporten har upphört. Det finns till exempel fler än en miljon aktiva kommersiella Windows-enheter som kör en version av en PDF-läsare som inte har stötts sedan 2017.

Gamla programversioner som inte stöds används fortfarande aktivt på miljontals kommersiella enheter. Det innebär att organisationerna riskerar att ha kvar sårbarheter som inte blir korrigerade.

För programversioner som stöds ser vi att hastigheten med vilken kritiska korrigeringar används uppnår en platå, vilket är motsatsen till den trend som ger återhämtningsförmåga. Kurvan borde visa en exponentiell användning av korrigeringar från månad till månad för att den återhämtning som krävs ska uppnås.

Hastighet för installation av kritiska korrigeringar



Efter att ha undersökt en kritisk sårbarhet som påverkade 134 versioner av en viss uppsättning webbläsare upptäckte vi att 78 procent, miljontals enheter, fortfarande använde en av de berörda versionerna nio månader efter att korrigeringsfilen släpptes.

Vi använde verktygslådan InterpretML[9] för att identifiera egenskaper som är korrelerade med organisationer som är mer benägna att ha enheter med äldre appversioner. De viktigaste egenskaperna var kort användningstid för enheter, geografiska områden som Asien och Stillahavsområdet och Latinamerika samt branscher som fordonsindustrin, kemikalier, telekommunikation, transport och logistik, hälso- och sjukvårdsgivare (skadehanterare) och försäkringsbranschen.

Underhållet av programvarors återhämtningskapacitet bör omfatta regelbunden inaktivering eller avinstallation av appar som inte används.

En organisations säkerhet och efterlevnad beror på företagets egna ansträngningar och på programvaruleverantörernas insatser.

Användbara insikter

1. Uppdatera alla program och slutpunkter i rätt tid via din organisation.
2. Rensa bort alla oanvända och inaktuella körbara filer som lagras på organisationers enheter i god tid.

Länkar till mer information

- Microsoft Intune-dokumentation | Microsoft Docs
- Hantera appar | Microsoft Docs
- Microsoft Defender för Endpoint | Microsoft Security
- OSS Secure Supply Chain Framework | Microsoft Security Engineering
- Microsoft Open Source Software Secure Supply Chain Framework | GitHub

Skapa motståndskraft mot nya DDoS-, webbprogram- och nätverksangrepp

Den accelererade digitaliseringen har omintetgjort den traditionella modellen för nätverk och säkerhetsperimetern. Flytten till molnet innebär att företagen måste införa molnbaserad nätverkssäkerhet för att skydda digitala tillgångar.

Angreppens komplexitet, frekvens och volym växer stadigt och är inte längre begränsad till semestertider utan sker numera året runt. Det belyser vikten av kontinuerligt skydd bortom traditionella trafiktoppar.

DDoS-angrepp (Distributed Denial of Service)

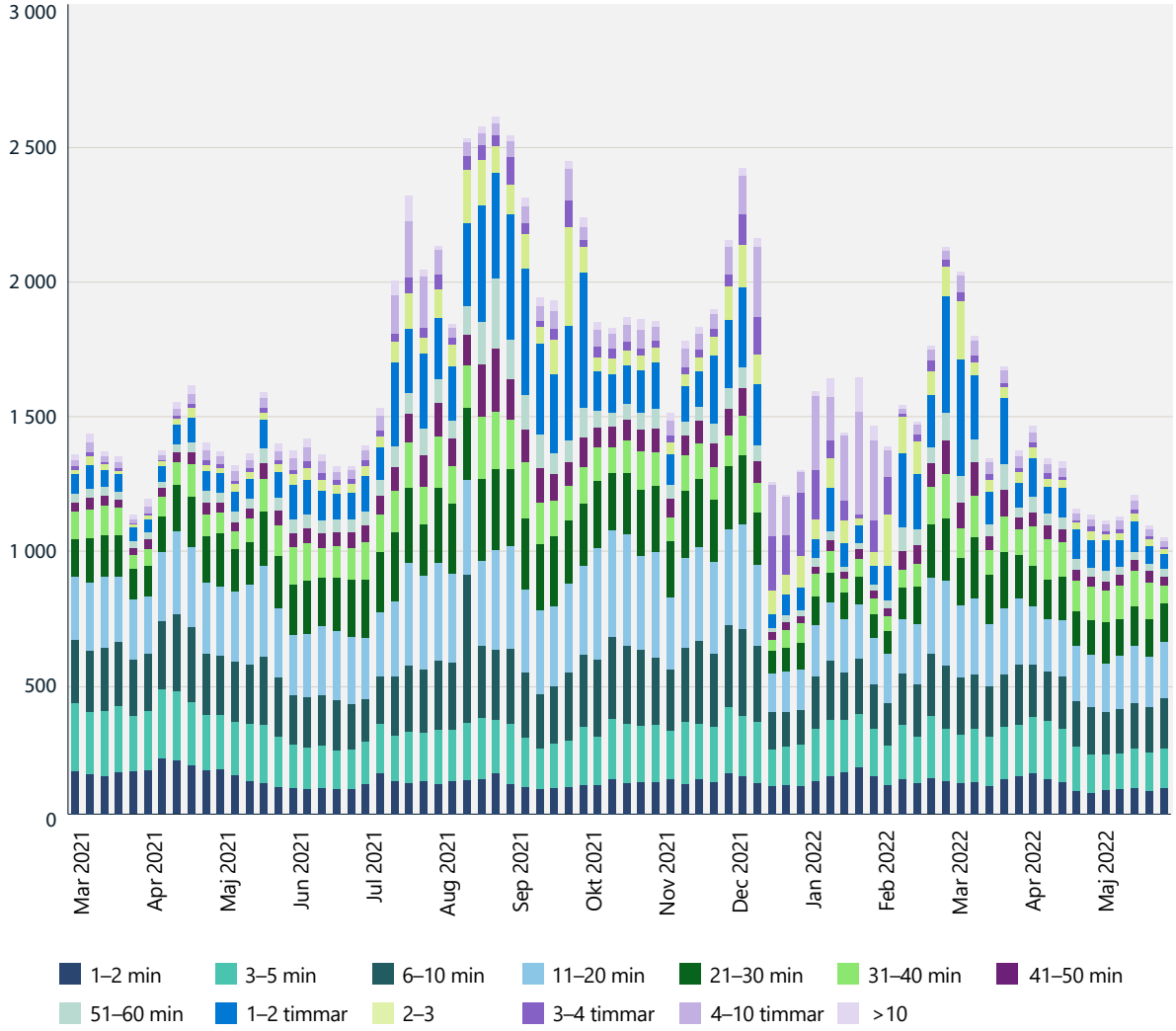
Under det senaste året har världens DDoS-aktiviteter ökat till större volym, komplexitet och frekvens än någonsin förut. Den här DDoS-explosionen drevs på av en avsevärd ökning av angrepp från nationalstater och ett stort utbud av tillgängliga DDoS-tjänster till lågt pris. Microsoft hanterade i snitt 1 955 angrepp per dag, en ökning med 40 procent jämfört med föregående år. Tidigare inträffade det maximala antalet angrepp normalt mellan jul och nyår. Men i år inträffade toppen den 10 augusti 2021. Det här kan tyda på en övergång till angrepp året runt och belyser vikten av löpande skydd utöver traditionella högtrafiksäsonger.

I november 2021 satte Microsoft stopp för ett voluminöst DDoS-angrepp med en genomströmning på 3,4 TB/sekund från omkring 10 000 källor i flera länder. Liknande högvolymsangrepp över 2 Tbit/s hanterades under 2022 och belyste att det inte bara är komplexiteten och angreppsfrekvensen som ökar, utan även angreppens volym (bandbredd).

Angrepps varaktighet

De flesta angrepp som observerades under det senaste året var kortlivade. Ungefär 28 procent av angreppen varade mindre än 10 minuter, 26 procent varade 10–30 minuter och 14 procent varade 31–60 minuter. 32 procent av angreppen var mer än en timme långa.

Antalet DDoS-angrepp och fördelningen av deras varaktighet
(mars 2021–maj 2022)



De flesta angreppen under det senaste året var kortlivade. Ungefär 28 procent av angreppen varade mindre än tio minuter.

Skapa motståndskraft mot nya DDoS-, webbprogram- och nätverksangrepp

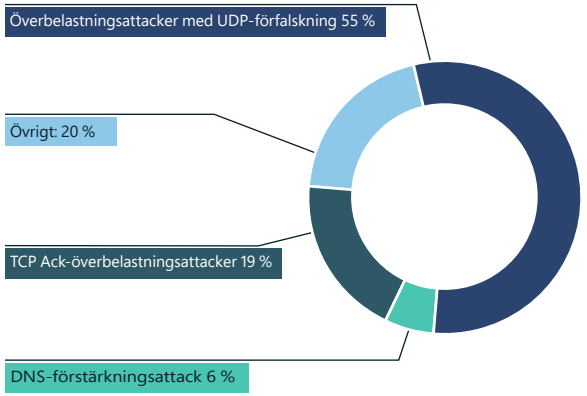
Fortsättning

DDoS-attackvektorer

Under det gångna året var de vanligast använda attackvektorerna UDP-reflektion (User Datagram Protocol) på port 80 med hjälp av SSDP (Simple Service Discovery Protocol), CLDAP (Connectionless Lightweight Directory Access Protocol), DNS (Domain Name System) och NTP (Network Time Protocol) med en enda topp. Vi såg också ett ökat antal DDoS-angrepp i applikationslagret som riktade sig mot webbplatser med 16,3 miljoner förfrågningar per sekund som mest och 9,89 Tbit/s trafik som mest.

År 2022 hanterade Microsoft nästan 2 000 DDoS-angrepp per dag och omintetgjorde det största DDoS-angreppet som någonsin hade rapporterats.

DDoS-attackvektorer



Överbelastningsattacker med UDP-förfalskning växte till den viktigaste angreppsmetoden under första halvåret 2022, från 16 till 55 procent. TCP Ack-överbelastningsattackerna minskade från 54 till 19 procent.

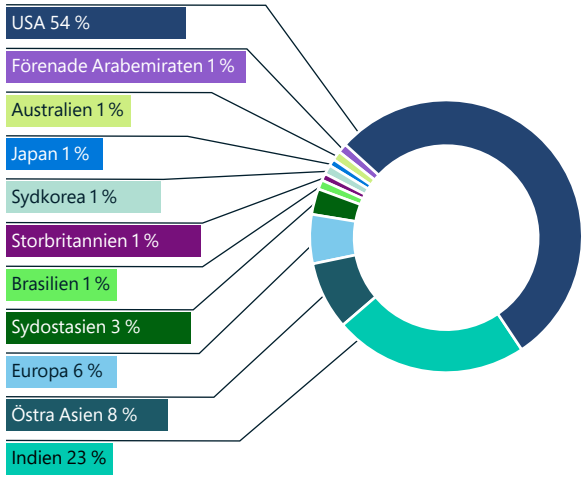


Spelindustrin fortsätter att vara det främsta målet för DDoS-angrepp, främst genom mutationer av Mirai-botnätet och UDP-protokollangrepp med låg volym. Eftersom UDP ofta används i spel- och streamingappar var en överväldigande majoritet av attackvektorerna överbelastningsattacker med UDP-förfalskningar, medan en liten del var UDP-reflektions- och förstärkningsangrepp.

Geografiska målregioner

Av de DDoS-angrepp som upptäcktes i fjol genomfördes 54 procent mot mål i USA, en trend som delvis kan förklaras av det faktum att de flesta Azure- och Microsoft-kunder finns i USA. Vi såg också en kraftig ökning av angreppen mot Indien, från bara 2 procent av alla angrepp under andra halvåret 2021 till 23 procent under första halvåret 2022. Östra Asien, särskilt Hongkong, är fortfarande ett populärt mål på 8 procent. I Europa var angreppen koncentrerade mot Amsterdam, Wien, Paris och Frankfurt.

DDoS-angreppsmål

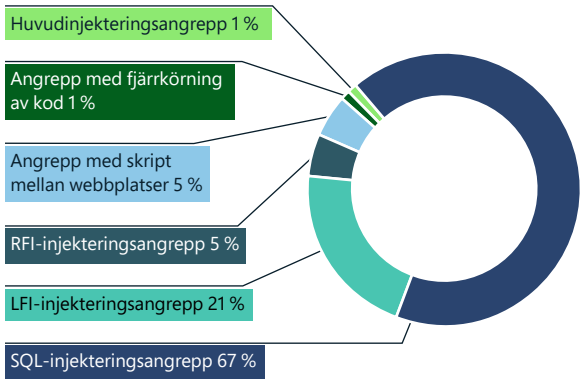


Vi tillskriver den stora mängden angrepp i Asien till regionens enorma spelmarknad, särskilt i Kina, Japan, Sydkorea och Indien. Den marknaden kommer att fortsätta att växa eftersom ökande mobilanvändning också ökar användningen av mobilspel. Det tyder på att Asien som geografiskt mål bara kommer att fortsätta att växa.

Angrepp på webbprogram

Web Application Firewall (WAF) i kombination med DDoS-skydd utgör en integrerad del av strategin för försvar på djupet för att skydda webb- och API-tillgångar. Microsoft observerade uppemot 300 miljarder WAF-regler som utlöstes per månad via Azures WAF.

Fördelning av de vanligaste angreppstyperna



Azure WAF identifierar miljardtals av Open Web Application Security Project (OWASP) tio främsta[10] angrepp varje dag. Enligt våra signaler försöka angriparna mest med SQL-injekteringsangrepp följt av lokala filinjekterings- och fjärrfilinjekteringsangrepp. Det överensstämmer med att OWASP:s tio-i-topp-lista visar injekteringsangrepp som den tredje vanligaste typen av webbangrepp.

Botangreppen mot Azure-webbappar har också ökat med i snitt 1,7 miljarder botförfrågningar per månad. 4,6 procent av den trafiken består av illasinnade botar.

Skapa motståndskraft mot nya DDoS-, webbprogram- och nätverksangrepp

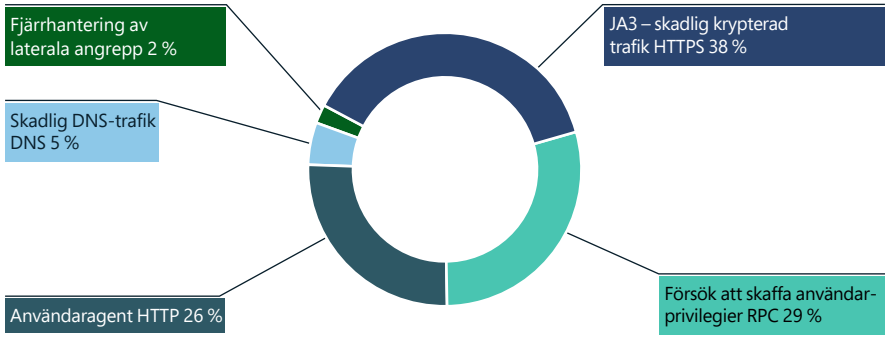
fortsättning

På grund av att ett ökande antal botar utför angrepp med stulna autentiseringsuppgifter, kreditkortsbedrägerier, cyberpåverkanskampanjer och angrepp på försörjningskedjan, väntar vi oss att se en stadig ökning av botangrepp mot webbappar.

Nätverksintrång: identifiering och förebyggande

Vi såg en betydande ökning av angreppen mot nätverksskiktet, särskilt skadlig kod, under 2022. Azure Firewalls intrångsdetekterings- och skyddssystem (IDPS) blockerade mer än 150 miljoner anslutningar enbart under juni.

Orsaker till IDPS Deny-trafik



Orsaker till IDPS-trafikvarningar



Analys av IDPS-varnings- och Deny-trafik visar följande metoder som användes av angripare. I Deny-trafiken ser vi angripare som använder SSL för att dölja sin aktivitet och fjärrkörningsangrepp blir allt vanligare. I Alert-trafiken ser vi att SMB/SMB2-protokoll används för att utföra fjärrkörningsangrepp.

Användbara insikter

1. Inspektera all trafik mellan system i ett datacenter eller en molntjänst och trafik som försöker komma åt dem.
2. Utveckla en robust strategi för nätverkssäkerhetsinsatser året runt.
3. Använd molnbaserade säkerhetstjänster för att implementera robust nätverkssäkerhet med nolltillit.

Länkar till mer information

- Improve your security defenses for ransomware attacks with Azure Firewall | Azure-bloggen och uppdateringar | Microsoft Azure
- Anatomy of a DDoS amplification attack | Microsoft Security-bloggen
- Intelligent application protection from edge to cloud with Azure Web Application Firewall | Azure-bloggen och uppdateringar | Microsoft Azure

Utveckla en balanserad strategi för datasäkerhet och cyberåterhämtning

Digitaliseringen har gett bränsle åt en enorm ökning av antalet datatillgångar och mer säkerhets-, efterlevnads- och integritetsrisker. Motståndskraftiga organisationer måste balansera sina investeringar i dataskydd, efterlevnad och återställningsfunktioner och integrera dem med särskilda rutiner för hantering av regleringar för att hantera olika typer av intrång.

Dataintrång kommer att inträffa, frågan är bara när. IBM och Ponemon Institutes studie Cost of a Data Breach, 2021, visar att kostnaden för ett genomsnittligt dataintrång är 4;24 miljoner USD (en ökning med tio procent från föregående år) och 9,05 miljoner USD i USA. Bristande efterlevnad befanns vara den främsta faktorn som ökade kostnaderna. Omvänt sågs ett samband mellan minskade kostnader för intrång och tillämpning av bästa praxis, till exempel incidenthanteringsplanering, driftsättningsmognad med nolltillit, AI för säkerhet och automatisering samt användning av kryptering.

Dataintrång är oundvikliga.
Men organisationer med en balanserad syn på motståndskraft kan minska frekvensen av, effekten av och kostnaden för intrången.

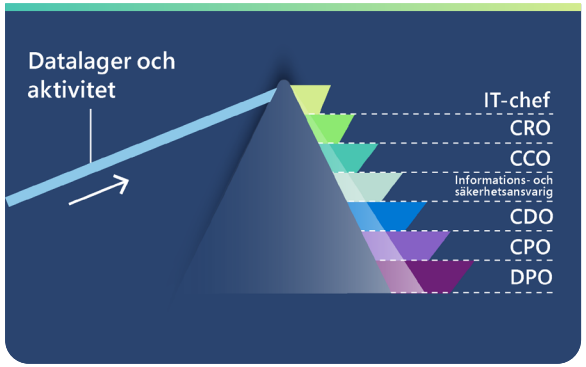
Datastyrning, säkerhet, efterlevnad och integritet är beroende av varandra

Vi har sett data få en framträdande plats under de senaste åren som en avgörande värdeskapande motor. Samtidigt har alltfler integritetsförordningar som kräver både datastyrning och säkerhet suddat ut linjerna mellan riskroller. Även om nya ledande roller på företag som Chief Data Officer (CDO) eller Chief Privacy Officers (CPO) har ett egenintresse av säkerhet och efterlevnad, förlitar sig implementeringen och organisationen av dataskydd ofta på team som leds av Chief Information Officers (CIO) och/eller Chief Information Security Officer (CISO). Det är inte en enkelriktad väg, eftersom datastyrningsinitiativ som leds av CDO:er också har säkerhetsfördelar. På grund av denna sammanlänkning måste IT-, datastyrnings-, säkerhets-, efterlevnads- och integritetsteamen jobba allt närmre varandra för att uppnå effektivitet och hantera risker.

Enhetliga plattformar för datariskhantering i hela organisationens dataegendomar är framtiden

Det är svårt att anpassa IT-, datastyrnings-, säkerhets-, efterlevnads- och sekretesshanteringsprocessen i en miljö med skräddarsydda program för varje disciplin och inkonsekvent täckning i en vanlig organisations hybridiserade dataspridning i flera moln. Vi anser att organisationer behöver ett enda ”fönster” för att hitta och lära känna sina data, skydda sina data, styra åtkomsten, användningen och livscykeln för data och förhindra dataförlust.

Att arbeta med samma datalager- och aktivitetsinformation underlättar teamoberoende processer, ger en mer omfattande riskbild och gör det möjligt för organisationer att förbereda och effektivisera sina reaktioner på intrång bättre.



Det enda ”fönstret” bör fungera som ett prisma. Team som jobbar med datasäkerhet, efterlevnad och integritet behöver olika men konsekventa inblickar i samma datalager och aktiviteter för att komma överens och samarbeta. Dataaktivitet omfattar dataåtkomst, ändrings- och förflyttningshändelser, som är en värdefull del av datasäkerhetsekvationen.

Effektiv datastyrning, säkerhet, efterlevnad och integritet är beroende av varandra och kräver samarbete mellan olika team.

Användbara insikter

1. Balansera försvar med återställning och minimera påverkan av dataintrång genom att investera i efterlevnad, dataskydd och svarsfunktioner.
2. Utveckla och implementera processer och verktyg som fungerar för alla datarisksilor och gäller alla data.

Länkar till mer information

- Microsoft Purview—Data Protection Solutions | Microsoft Security
- The future of compliance and data governance is here: Introducing Microsoft Purview | Microsoft Security-bloggen

Motståndskraft mot cyberpåverkan: den mänskliga dimensionen

Under de senaste fem åren har framsteg inom grafik och maskininlärning gett lättanvända verktyg som snabbt kan generera högkvalitativt, realistiskt innehåll som kan spridas vitt och brett över hela internet på några sekunder.

När det gäller händelser som rapporteras via text, ljud och visuellt innehåll har vi nått en punkt där varken människor eller algoritmer på ett tillförlitligt sätt kan skilja mellan fakta och påhitt. Alla dessa verktyg och deras resultat sår tvivel om digitala mediers trovärdighet, vilket orsakar kaos för vår förståelse av lokala och internationella händelser. Nya former av påverkansoperationer som har möjliggjorts av tekniska framsteg får allvarliga konsekvenser för demokratiska processer.[11]

Frågan uppstår om vad vi kan göra för att förbereda oss på en framtid där vi är mer motståndskraftiga mot cyberpåverkansoperationer. Teknik är bara en del av pusslet. Det kommer att krävas insatser på flera områden, däribland utbildning som syftar till högre mediekompetens, medvetenhet och vaksamhet, investeringar i kvalitetsjournalistik – med välrenommerade reportrar på plats, lokalt, nationellt och internationellt – nätverk för att berätta och varna om påverkansoperationer samt nya typer av förordningar som straffar illvilliga aktörer som genererar eller manipulerar digitala medier i syfte att lura andra.



Vi inser också att det är ett ambitiöst mål att försöka återställa förtroendet för digitalt innehåll och att det kommer att kräva många olika perspektiv och delaktighet. Ett företag, en institution eller en myndighet kan inte lösa de här hoten på egen hand. Vår superkraft som människor är vår förmåga att samarbeta. Det är särskilt viktigt nu eftersom alla – myndigheter i hela världen, branscher, den akademiska världen och i synnerhet nyhets-, sociala och medieorganisationer – måste samarbeta för att vi ska lyckas förbättra och vårda vårt samhälle.

Länkar till mer information

- Applications for artificial intelligence in Department of Defense cyber missions | Microsoft On the Issues
- Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions. Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the Subcommittee on Cybersecurity, of the Senate Armed Services Committee, 117th Congress (3 maj 2022; vittnesmål av Eric Horvitz)

Stärka den mänskliga faktorn med kompetenshöjning

Hanteringen av den mänskliga faktorn är en viktig komponent i alla strategier för att öka cybersäkerhetskompetensen. Enligt en undersökning i serien Kaspersky Human Factor in IT Security[12] involverar 46 procent av alla cybersäkerhetsincidenter slarvig eller okunnig personal som oavsiktligt underlättar attacken.

Microsofts utbildnings- och medvetenhetsteam i organisationen Digital Security and Resilience ansvarar för att stärka den mänskliga faktorn inom cybersäkerhet genom att ge medarbetarna möjlighet att säkra våra egna och våra kunders system och data. Våra mål är att

- minska risken för Microsoft och våra kunder genom att bygga upp en central uppsättning säkerhetskompetenser för hela personalen
- öka medarbetarnas säkerhetskunskaper genom en utbildning i flera faser som stöder önskade beteenderesultat
- främja kulturella förändringar genom att göra säkerhetstänkande till en central del av företagskulturen på Microsoft genom obligatoriska säkerhetsutbildningar och säkerhetsevenemang varje år
- marknadsföra en central webbresurs där vi pratar om bästa praxis, har information om företagets policyer och rapporterar incidenter om allt som rör cybersäkerhet.

Ett målinriktat, centraliserat kompetensprogram för cybersäkerhet hamnar på Microsoft-medarbetares bord minst en gång per år. Utbildningarna är optimerade för att stödja aktuella cybersäkerhetsinitiativ och leverera mätbara beteenderesultat. Microsofts Information Risk Management Council (IRMC) spelar en viktig roll när det gäller att identifiera viktiga resultat av beteendeförändringar inom cybersäkerhet som utbildningen är tänkt att hantera.

Med alla våra kompetensprogram inom cybersäkerhet mäter vi lösningens effektivitet, verkan och resultat då det är möjligt. Vår utbildning om insiderhot genomfördes till exempel av 95 procent. De som gått kursen är väldigt nöjda och den har lett till att betydligt fler mellanchefer rapporterar eventuella insiderhot via företagets verktyg Report It Now. Programmet omfattar följande:

Grunden för säkerhet: Centraliserad, företagsomfattande utbildning i medvetenhet om cybersäkerhet och efterlevnad som tar upp grundläggande säkerhets- och integritetsrutiner. Den här mycket efterlängtade utbildningsserien har utformats enligt en edutainment-modell för att göra utbildningen om cybersäkerhet engagerande och intressant.

STRIKE: Microsofts obligatoriska tekniska utbildning för tekniker som bygger och underhåller affärslösningar. Den här utbildningen som enbart erbjuds för inbjudna deltagare tar upp aktuell och kritisk bästa praxis för cybersäkerhetshygien. Vi använder en modell för hybridleverans som är anpassad efter målgruppens behov.

Programspecifikt: Riktade utbildningsprogram stöder specifika cybersäkerhetsinitiativ som Shadow IT, Insider Threat och Microsoft Federal. De här utbildningarna är tätt knutna till den övergripande engagemangsstrategin för sina respektive cybersäkerhetsinitiativ genom sponsring av ledningen och rapportering av poängprotokoll för att förhindra en utbildningsmetod som enbart går ut på att kryssa i rutor.

MSProtect: Microsofts centrala webbresurs tar upp bästa praxis, information om företagets policyer och incidentrapportering om allt som rör cybersäkerhet. Den här on-demand-resursen är den som gäller för medarbetare som inte deltar i formella utbildningar.

Kompetenshöjning inom säkerhet handlar inte om att bara genomföra utbildningen och bocka av punkterna. Fokusera i stället på beteendeförändringar så att resultaten går att stämma av mot identifierade målbeteenden och inrätta lyssningssystem för att avgöra effekten av utbildningen.

Användbara insikter

1. Ge säkerhetsutbildning och resurser till medarbetarna när och där de behöver det.
2. Ta fram en kompetensstrategi centralt med utgångspunkt från vad intressenter i hela företaget säger.
3. Håll reda på effekten av utbildningen och analysera dess effektivitet (kvantitet), verkan (kvalitet) och resultat (inverkan på verksamheten).

Länkar till mer information

- Microsoft lanserar nästa steg av ett kompetensinitiativ efter att ha hjälpt 30 miljoner människor

Insikter från vårt program för att undanröja utpressningstrojaner

Microsoft har varit ute på sin egen nolltillitsfärd[13] under de senaste fem åren för att se till att identiteter och enheter hanteras robust och hälsosamt. I takt med att risken för utpressningstrojaner har ökat har vi utvecklat inblicken för att stödja vår metod att skydda oss själva och våra kunder.

Efter en djuplodande intern utvärdering tog vi fram ett program för att eliminera utpressningstrojaner för att åtgärda luckor i våra kontroller och täckning, bidra till funktionsförbättringar av tjänster som Defender for Endpoint, Azure och M365 samt för att utveckla regler för våra SOC- och teknikteam om de bästa återhämtningsmetoderna efter en utpressningstrojanattack.

Det första steget var att förstå omfattningen av vårt skydd mot utpressningstrojanattacker som riktades mot Microsoft. Arbetet pågick redan med att införa Defender for Endpoint och se till att alla enheter hanteras och följer våra nolltillitspolicyer, men vi behövde hitta ett sätt att förstå alla aspekter av den viktigare frågan om huruvida vi effektivt skulle kunna återhämta oss från ett angrepp. För att få reda på mer utvärderade vi NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile[14], som överensstämmer med vår övergripande företagspolicy mot vår kända lista med kontroller. Analysen visade snabbt på luckor i täckningen.

Därefter prioriterade vi luckor i CSF-funktionerna Identifiera, Detektera, Skydda, Reagera och Återställ. Vi upptäckte strategisk anpassning till nolltillit och andra program och även luckor som inte hade någon befintlig arbetsmetod. Efter att ha bedömt det arbete och de insatser som krävs för att åtgärda dessa luckor, delade vi in allt i två pelare:

- **Skydda företaget (SF):** Definiera arbetsområden som vi behöver hantera i hela företaget för att skydda oss och kunna återhämta oss från ett framgångsrikt angrepp.
- **Skydda kunden (SK):** Bygg in kapacitet i våra produkter för att skydda våra kunder och vår verksamhet.

Bädda in resultat i vårt eget företag

För att åtgärda de största riskerna och skydda våra kritiska tjänster mot utpressningstrojanattacker tänker vi under de kommande sex till tolv månaderna fokusera investeringarna på att lyckas med de fem scenarierna nedan som en del av ett särskilt program för hantering av utpressningstrojaner. När vi har lyckats för alla scenarier kommer vi gradvis att utöka omfattningen av programmet så att det når alla delar av företaget.

Scenario 1: Medlemmar av säkerhetsteamet förstår den övergripande risken med utpressningstrojanattacker och har en inrättad rutin för att göra ledningen medveten om kontrollbrister och riskstatusen.

Scenario 2: Medlemmar av säkerhetsteamet har tillgång till rutiner som är utformade för att hjälpa dem och andra team på Microsoft att reagera på och återställa viktiga tjänster efter utpressningstrojanattacker.

Scenario 3: Medlemmar av Enterprise Resilience-teamet har en standard att följa för säkerhetskopiering av kritiska system. Det finns rutiner och regelbundna säkerhetskopierings- och återställningsövningar genomförs för att säkerställa att data kan återställas om en utpressningstrojanattack inträffar.

Scenario 4: Serviceägare förstår och inför de nödvändiga säkerhets- och driftkontrollerna och policyerna för att skydda sina tjänster, kunddata, slutpunkter och nätverkstillgångar mot utpressningstrojanattacker med särskilt fokus på tjänster som prioriteras som Microsofts kritiska tjänster.

Scenario 5: Alla anställda kan använda utbildnings- och träningsresurser som beskriver hur man känner igen ett utpressningstrojanattacker och hur man aviserar säkerhetsteamet och inleder motarbetet.

Användbara insikter

1. Dokumentera och validera kompletta återställnings- och reparationsaktiviteter som rör utpressningstrojanattacker mot kritiska tjänster.
2. Be intressenterna om hjälp att uppdatera företagets rutiner för krishantering så att de inkluderar utpressningstrojanspecifika aktiviteter och en beslutsprocess och råd för att avgöra om och när man ska betala för utpressningstrojaner.
3. Förbättra identifieringen och skyddet genom att införa funktioner som är tillgängliga i de säkerhetsprodukter ni använder (t.ex. Defender for Endpoint Attack Surface Reduction-regler).
4. Samarbeta med säkerhetsstandardteamet om att definiera en grundnivå för skyddet mot utpressningstrojanattacker och ge utbildning och dokumentation till de tekniska teamen om hur man skyddar sig mot utpressningstrojanattacker.
5. Använd automatisering för att förenkla införandet av säkerhets- och driftpolicyer för DevOps-teamen och se till att system som börjar avvika från reglerna snabbt uppmärksammas och åtgärdas.

Länkar till mer information

› Sharing how Microsoft protects against ransomware | Microsoft Inside Track

Åtgärda säkerhetskonsekvenserna av kvantdatorer nu

Pressen ökar för att hantera det hot som kvantdatorer utgör för modern kryptografi och allt den skyddar. Det nyligen utfärdade Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15] utgår från presidentorder 10 428[16], Improving the Nation's Cybersecurity. Den belyser att säkerheten i programvarors försörjningskedja är avgörande för att hantera framtida angrepp från nationalstater.

Vad är kvantdatorer?

Kvantdatorer är maskiner som använder kvantfysikens egenskaper för att lagra data och utföra beräkningar. Det kan vara extremt fördelaktigt för vissa arbetsuppgifter där de skulle kunna överträffa även våra bästa superdatorer enormt. Kvantberäkningar visar redan nya horisonter för datakryptering och databearbetning. Studier förutspår att kvantdatorer kommer att bli en industri värd många miljarder dollar redan 2030.[17] Kvantdatorer och kvantkommunikation kommer att få en transformerande inverkan inom en rad branscher, allt från hälso- och sjukvård och energi till ekonomi och säkerhet.

Kvantdatorer är ett hot mot dagens kryptografi och allt den skyddar.

Hotet mot dagens kryptografi

Med Shors algoritm från 1994 och en kvantdator i industriell skala med flera miljoner fysiska qubits kan alla våra nuvarande, allmänt distribuerade krypteringsalgoritmer med offentliga nycklar knäckas hur lätt som helst. Det är oerhört viktigt att överväga, utvärdera och standardisera "kvantsäkra" kryptosystem som är effektiva, smidiga och säkra mot fientliga, kvantbaserade angrepp. Migreringen av programvara till kryptografin efter införandet av kvantdatorer, nämligen befintliga klassiska algoritmer och protokoll som står pall för kvantangrepp, kommer att ta år – kanske ett decennium eller mer – att uppnå.[18]

Det innebär att pressen ökar för att hantera hotet mot den moderna kryptografin och allt den skyddar. Fienden kan spara krypterade data nu och utnyttja dem senare när en kvantdator är tillgänglig. Det är för sent att vänta på att kvantdatorer ska bli realitet innan de kryptografiska konsekvenserna åtgärdas.

Eftersom kryptografi används i hela cyberekosystemet innebär det att våra kryptografiska säkerhetstjänster skulle kunna knäckas. Det omfattar till exempel kommunikationstjänster (TLS, IPSec), meddelanden (e-post, webbkonferenser), identitets- och åtkomsthantering, webbläsning, kodsignering, betalningstransaktioner och andra tjänster som är beroende av kryptografi för skydd.

När kvantdatorer väl blir en realitet kommer programvarukomponenter från tredje man med implementeringar av kryptografiska algoritmer och funktioner också att behöva synas i sömmarna. Det kräver att alla organisationer i värdekedjan gör sin del av arbetet för att säkerställa att kedjan förblir säker. Branschorgan och myndigheter ökar sina ansträngningar att definiera säkerhetskrav för programvaruförsörjningskedjan och i vissa fall inför man nya regler för att säkra kedjan. National Security Memorandum NSM-8[19] fastställer krav och tidsfrister för att införa kryptografi efter införandet av kvantdatorer i National Security Systems (NSS). Där nämns tidsförväntningar om 180 dagar för "moderniseringsplanering, användning av kryptering som inte stöds, godkända uppdragsspecifika protokoll, kvantresistenta protokoll och planering för användning av kvantresistent kryptografi vid behov".

Standardisering är en aktivitet med lång ledtid vid övergången till kvantsäker kryptografi. Standardiseringsorgan som arbetar med standarder som rör kryptering med offentliga nycklar måste börja experimentera med och anpassa sig till kvantalgoritmer redan nu.

Nya algoritmer som fungerar efter att kvantdatorer blir tillgängliga – klassiska algoritmer som tros kunna stå emot kvantangrepp – granskas nu i NIST:s Post-Quantum Standardization Project.[20] Det arbetet kommer att påverka globala insatser inom standardiseringsorgan. Även om det kommer att finnas ett visst överlapp med amerikanska myndigheters val av algoritmer, kan olika nationella organs/förvaltningsorgans val av kompatibla algoritmer utgöra problem internationellt. Fragmenteringen kommer i sin tur att komplicera produkt- och servicetekniken.

Nya krypteringsalgoritmer som fungerar efter införandet av kvantdatorer granskas i NIST:s program Post-Quantum Cryptography Standardization. Arbetet kommer att påverka globala insatser inom standardiseringsorgan.

Användbara insikter

Tillsammans med SAFECode och partnermedlemmar bör branschen vidta omedelbara åtgärder på kort sikt för att förbereda sig för övergången till ett kvantdatorsamhälle.[21] Detta inbegrips:

1. Inventera era produkter/kod där kryptografi används.
2. Inför en strategi för kryptosmidighet i organisationen som omfattar att minimera omsättningen av kod som krävs när kryptografin ändras.
3. Gör en pilotstudie av bruket av kvantdatorsäkra algoritmer i era produkter eller tjänster där kryptografi används.
4. Var beredda på att använda olika algoritmer med offentliga nycklar för kryptering, nyckelutbyte och signaturer.
5. Testa era appars hantering av mycket stora nyckelstorlekar, chiffer och signaturer.

Länkar till mer information

- Microsoft has demonstrated the underlying physics required to create a new kind of qubit | Microsoft Research

Integrera företag, säkerhet och IT för bättre motståndskraft

Robust cyberåterhämtning är beroende av att företagsledare samarbetar med säkerhetsteamen för att införa säkerhet. Enligt Microsofts erfarenhet är det svårt att vara ledande på säkerhet, eftersom det kräver stöd från organisationens ledare att skydda organisationen på bästa sätt.

Säkerhetsledare navigerar i en skärgård av dynamiska problem med grynnor som rör risker, teknik, ekonomi, organisatoriska processer, affärsmodeller, kulturomdaning, geopolitiska intressen, spionage och efterlevnad av internationella sanktioner. Samtliga innebär nyanser som måste granskas, förstås och hanteras noga.

Säkerhetsledare har också till uppgift att klara av angrepp från både intelligenta, välfinansierade och mycket motiverade mänskliga angripare och lågutbildade men effektiva cyberbrottslingar. Teamen måste försvara komplexa tekniska egendomar som ofta har byggts upp i små steg under 30 år eller mer då säkerhet prioriterades lågt eller inte alls. Beslut som fattades för många år sedan kan innebära risker i dag, tills vi betalar av den tekniska skulden och tar itu med säkerhetsbristerna.

Organisationens ledare och beslutsfattare kan ha en betydande positiv inverkan på säkerheten genom att aktivt stödja säkerhetsledare och hjälpa dem att slå en bro mellan inbyggd säkerhet och resten av organisationen. När Microsoft arbetar med kunder som har den synen på sin säkerhet märker vi att de har större framgångar i att bygga upp en motståndskraftig organisation och samtidigt är bättre på att anpassa och förnya sig.

Organisationens ledning kan stödja säkerhetsledare genom att fokusera på tre viktiga områden:

1. Skapa säkerhet genom design

Säkerhet ses ibland som ett hinder eller en eftertanke i affärsprocesserna och övervägs många gånger bara när det är för sent att undvika en risk eller åtgärda den billigt och enkelt.

Organisationens ledare och beslutsfattare bör tillse detta:

Ta med säkerhetsaspekten tidigt vid nya initiativ. Nya digitala initiativ och molnanvändning bör prioritera säkerheten för att se till att riskerna som organisationen löper inte ökar för varje ny app eller digital kapacitet. Om säkerhet är tillförlitligt inkluderat går det att använda de här processerna för att modernisera äldre system och få både säkerhets- och produktivitetsfördelar på samma gång.

Normalisera förebyggande underhåll för säkerhet. Säkerställ att grundläggande säkerhetsunderhåll – som att tillämpa säkerhetsuppdateringar och korrigeringar och säkra konfigurationer – stöds fullständigt av organisationen (inklusive budgetar, planerade driftstopp och inköpskrav för leverantörers produktsupport).

Tyvärr fördröjer eller väntar många organisationer med de här metoderna, eller tillämpar dem bara delvis. Det ger angriparna omfattande möjligheter att utnyttja. Behovet av säkerhetsnormalisering omnämns i US NIST 800-40.[22]

2. Engagera sig i säkerhet

Organisationens ledare bör aktivt delta i och sponsra viktiga säkerhetsprocesser för att säkerställa att resurser och beredskapen inför säkerhetskatastrofer prioriteras. Följande bör de engagera sig i:

Identifiera viktiga affärstillgångar. Säkerhetsledare och säkerhetsteam behöver veta vilka tillgångar som är affärskritiska för att fokusera säkerhetsresurserna på det viktigaste. Det här är ofta ett nytt arbetsfält som omfattar att ställa och besvara nya frågor som inte har behandlats tidigare.

Övningar för affärskontinuitet och haveriberedskap på cybersäkerhetsområdet. Cyberattacker kan vara allvarliga händelser som stör eller stoppar den mesta eller all affärsverksamhet. Genom att se till att teamen i hela organisationen är beredda att hantera den här typen av situationer minskas tiden för att återställa verksamheten samtidigt som skadan på organisationen begränsas och förtroendet och tilliten hos kunder, medborgare och intressenter upprätthålls. Det här bör integreras i en befintlig process för affärskontinuitet och katastrofåterställning.

Beslut om säkerhetsrisker fattas bäst av affärs- eller uppdragsägare som har full insyn i alla risker och möjligheter.



Integrera företaget, säkerheten och IT för bättre motståndskraft

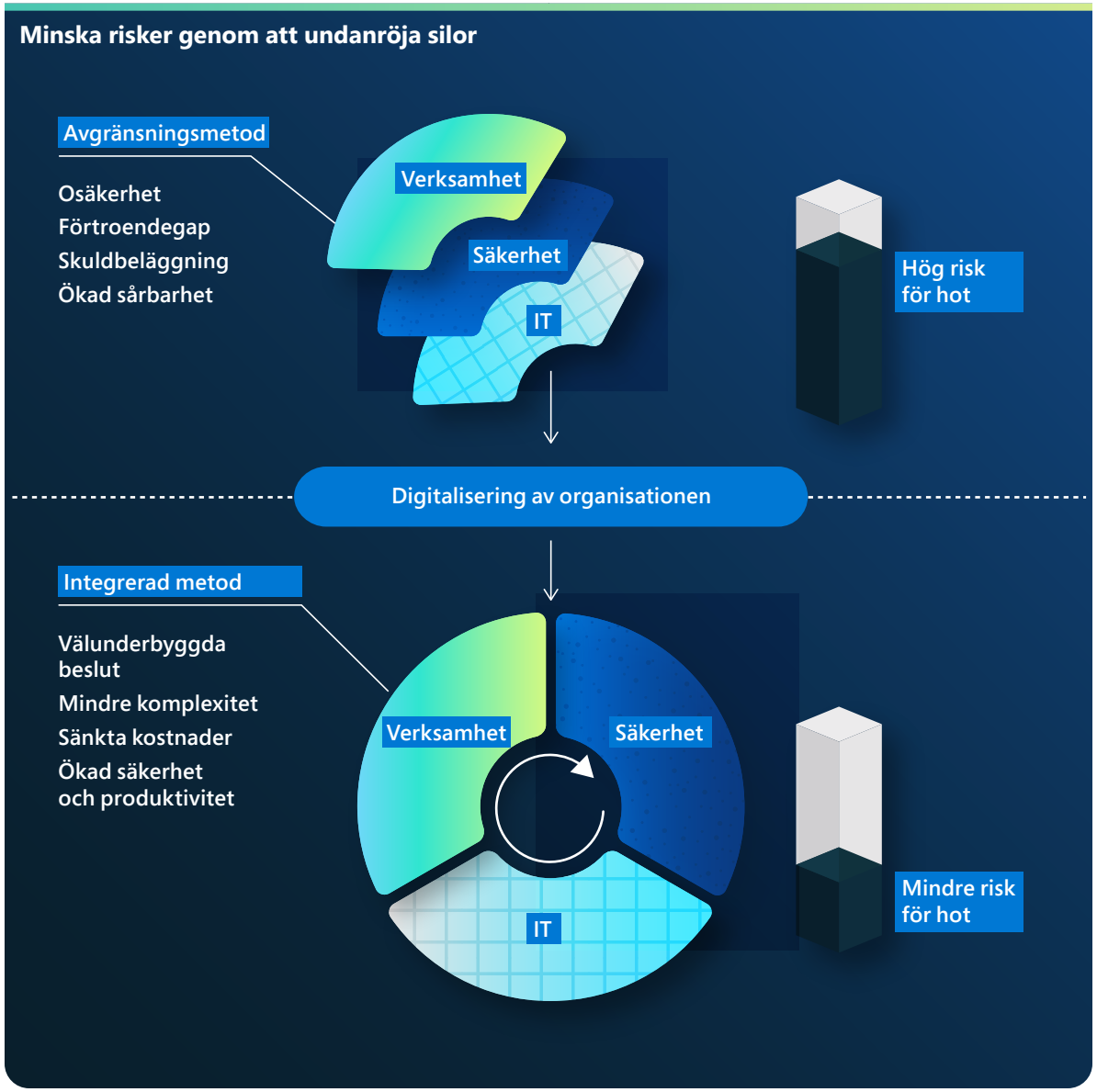
fortsättning

3. Positionera säkerheten korrekt

Organisationernas sätt att strukturera ansvaret för säkerhetsrisker gör många gånger att de blir dåliga på att fatta beslut om säkerhetsrisker. Riskbeslut fattas bäst av affärs- eller uppdragsägare som har full insyn i alla risker och möjligheter, men många organisationer tilldelar (implicit eller uttryckligen) säkerhetsriskansvaret på ämnesexperter i säkerhetsteamet i stället. Det lägger en tung börda på säkerhetsteamen och berövar affärsägarna insyn och kontroll över en viktig risk som deras verksamhet löper. Så här kan organisationen åtgärda problemet:

Förbered affärsägarna: Utbilda affärsägarna om övergripande säkerhetsrisker och hur hoten kan och kommer att påverka deras verksamhet. Om säkerhetsteamen är direkt inblandade i det här arbetet ökar även samarbetet mellan säkerhetsavdelningen och den övergripande affärsflexibiliteten.

Tilldela säkerhetsrisker till affärsägare: När affärsägarna vet tillräckligt för att förstå och acceptera säkerhetsrisker, bör organisationen uttryckligen lägga över ansvaret för säkerhetsrisker på dem, samtidigt som säkerhetsteamen fortfarande hålls ansvariga för att hantera riskerna och ge välgrundade expertråd och andra råd till ägaren.



"Cyberåterhämtning befinner sig på en glidande skala från klassisk affärskontinuitet och haveriberedskap med bra rutiner för säkerhetskopiering av data till återställningskapacitet för processer, teknik och deras beroenden (inklusive personer och externa parter), samt att övergå till tjänster som alltid är på och läker sig själva, motståndskraftiga kritiska roller och redundans för viktiga tredje parter. De mest motståndskraftiga organisationerna arbetar för att integrera IT, företagsledare och säkerhetspersonal. God återhämtning omfattar att designa för motståndskraft från början, att ha säker ändringshantering och detaljerad felisolering. Cyberåterhämtning är bara ett scenario i ett bra program där man planerar för alla risker. I takt med att cyberriskerna ökar och överlappet mellan cybersäkerhet och motståndskraft blir allt viktigare, blir kopplingen mellan informationssäkerhetschefen (CISO) och programmet för företagets motståndskraft starkare. Varje år tar fler informationssäkerhetschefer på sig ansvaret för företagets hela motståndskraft."

Lisa Reshaur
General Manager, Risk Management, Microsoft

Länkar till mer information

- From resilience to digital perseverance: How organizations are using digital technology to turn the corner in unprecedented times | Officiell Microsoft-blogg
- How IT and security teams can work together to improve endpoint security | Microsoft Security

Klockkurvan för cybermotståndskraft

Framgångsfaktorer för återhämtning som varje organisation bör använda

Som vi har sett lyckas många cyberattacker helt enkelt på grund av att grundläggande säkerhetshygien inte har följts. Följande minimistandarder bör varje organisation ha:

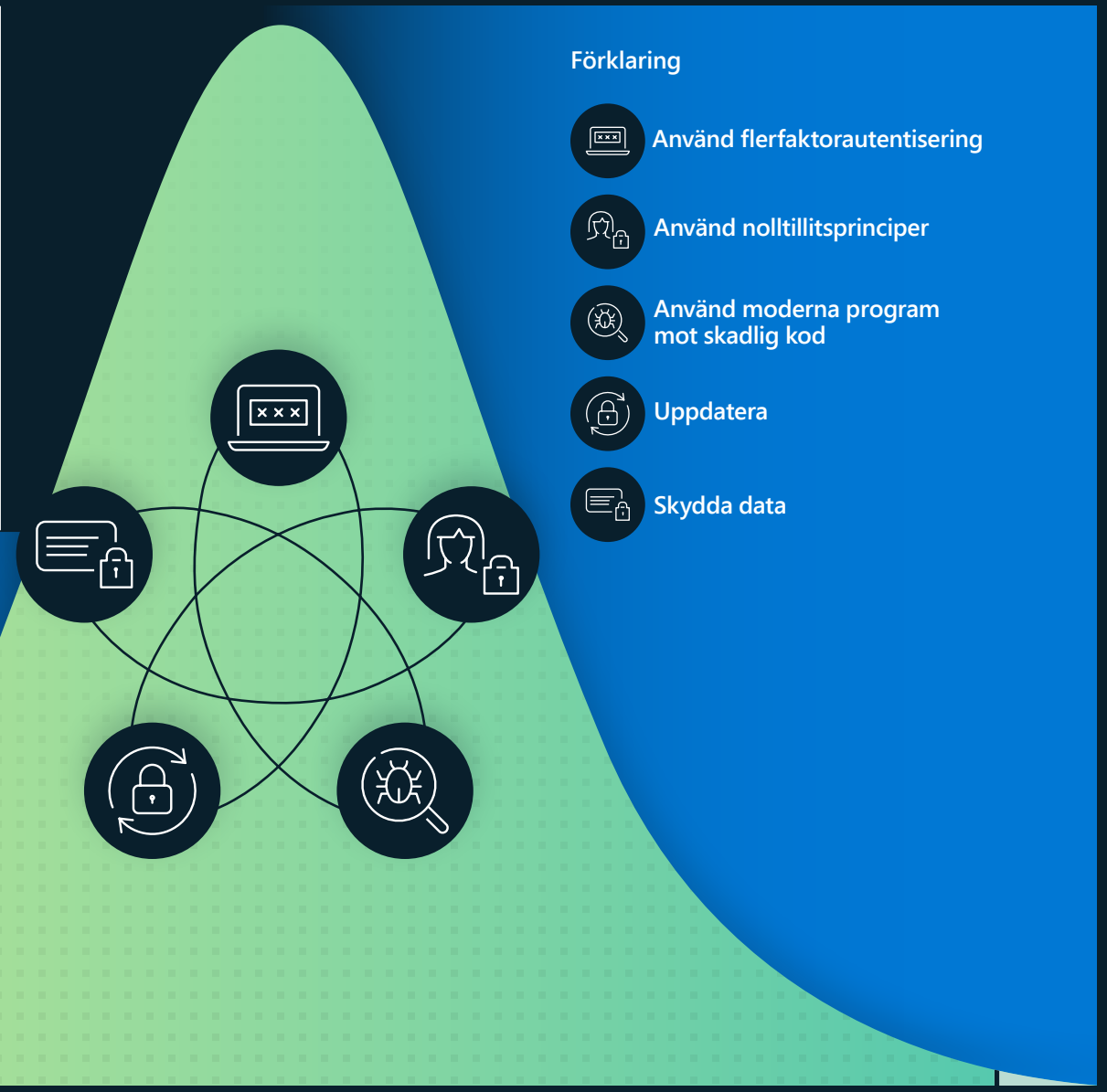
- **Aktivera multifaktorautentisering (MFA):** Det skyddar mot knäckta användarlösenord och gör identiteter mer motståndskraftiga.
- **Använd nolltillitsprinciper:** Hörnstenen i en motståndsplan som begränsar effekten på organisationen. Principerna är följande:

1. – Verifiera explicit – se till att användare och enheter är i ett bra tillstånd innan de får använda resurser.
2. – Använd minst privilegierad åtkomst – tillåt bara den behörighet som krävs för åtkomst till en resurs, inte mer.
3. – Förutsätt intrång – förutsätt att systemets försvar inte har räckt och att system kan ha knäckts. Det innebär att miljön ständigt ska övervakas efter möjliga angrepp.

- **Använd program mot skadlig kod med utökade identifierings- och svarsmöjligheter:** Använd programvara för att upptäcka och automatiskt blockera angrepp och ge insikter till säkerhetsåtgärder. Det är viktigt att ha koll på insikter från hotidentifieringssystem för att kunna reagera på hot snabbt.
- **Håll allt uppdaterat:** Okorrigerade och föråldrade system är en viktig orsak till att många organisationer råkar ut för angrepp. Se till att alla system hålls uppdaterade, däribland inbyggd programvara, operativsystemet och apparna.
- **Skydda data:** Att känna till era viktiga data, var de finns och om rätt system har införts är helt avgörande för att kunna implementera lämpligt skydd.

98 %

Grundläggande säkerhetshygien skyddar fortfarande mot 98 procent av angreppen



Slutnoter

1. Endpoint Detection and Response (EDR) är en säkerhetsplattform för företagsslutpunkter som har utformats för att hjälpa företagsnätverk att förhindra, upptäcka, undersöka och reagera på avancerade hot. EDR-insatser är ett avancerat sätt att identifiera angrepp nära nog i realtid med åtgärdsmöjligheter. Säkerhetsanalytiker kan prioritera varningar effektivt, få insyn i ett intrångs hela omfattning och vidta åtgärder för att åtgärda hot.
2. En EPP (Endpoint Protection Platform) är en lösning som installeras på slutpunktsenheter för att förhindra filbaserad skadlig kod, identifiera och blockera skadlig aktivitet från betrodda och opålitliga appar samt tillhandahålla de undersöknings- och reparationsfunktioner som krävs för att dynamiskt reagera på säkerhetsincidenter och varningar.
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. Bok om Windows-säkerhet: Kommersiell
7. New security features for Windows 11 will help protect hybrid work | Microsoft Security Blog
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
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. Executive Order 14028 Improving the Nation's Cybersecurity
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

Bidragande team

Bidragande team

Informationen och insikterna i den här rapporten kommer från en mängd säkerhetsfokuserade proffs som arbetar i många olika team på Microsoft. Deras gemensamma mål är att skydda Microsoft, dess kunder och hela världen från hot om cyberattacker. Vi är stolta över att dela med oss av våra insikter i denna anda av öppenhet, med det gemensamma målet att göra världen till en säkrare plats för alla.

AI for Good Research Lab: Utnyttjar kraften i data och AI för att hantera många av världens utmaningar. Labbet samarbetar med organisationer utanför Microsoft och tillämpar AI för att förbättra försörjningsmöjligheter och miljöer. Fokusområdena är onlinesäkerhet (desinformation, cybersäkerhet, barns säkerhet), katastrofinsatser, hållbarhet och AI för hälsa.

Azure Edge & Platform, Enterprise & OS Security: Ansvariga för grundläggande operativsystem- och plattformssäkerhet i Windows, Azure och andra Microsoft-produkter. Teamet skapar branschledande säkerhets- och maskinvarulösningar till Microsofts plattformar för att få ned antalet intrångsmöjligheter och intrång genom identiteter och skadlig kod från chip till moln. Det här är teamet bakom till exempel Microsofts Secured-core-plattform för datorer, nätverksgräns och servrar och Microsoft Pluton Security-processorn.

Azure Networking, Core: Ett molnnätverksteam som fokuserar på Microsofts WAN, datacenternätverk och den programvarudefinierade nätverksinfrastrukturen i Azure, däribland DDoS-plattformen, nätverksgränsplattformen och nätverkssäkerhetsprodukter som Azure WAF, Azure Firewall och Azure DDoS Protection Standard.

Cloud Security Research-teamet: Genom att säkra Microsofts moln, skapa innovativa säkerhetsfunktioner och säkerhetsprodukter och bedriva forskning skyddar och ger detta team Microsofts kunder möjlighet att utveckla sina organisationer säkert.

Customer Security and Trust (CST): Ett team som ständigt arbetar för att höja kundsäkerheten i Microsofts produkter och onlinetjänster. CST arbetar med teknik- och säkerhetsteam från hela företaget och garanterar efterlevnad, stärker säkerheten och ger mer insyn för att skydda våra kunder och främja globalt förtroende för Microsoft.

Customer Success: Säkerhetsteam i Customer Success samarbetar direkt med kunderna för att berätta om bästa praxis, lärdomar och råd för att påskynda säkerhetsomvandlingen och moderniseringen. Det här teamet sammanställer och ordnar bästa praxis och de lärdomar vi har dragit under Microsofts – liksom våra kunders – resa mot referensstrategier, referensarkitekturer, referensplaner med mera.

Cyber Defense Operations Center (CDOC): Microsofts cybersäkerhets- och försvarsanläggning är ett samlingscenter där säkerhetsexperter från hela företaget samlas för att skydda vår företagsinfrastruktur och den molninfrastruktur som kunderna har tillgång till. Vår incidentpersonal arbetar tillsammans med datavetare och säkerhetstekniker från Microsofts olika tjänster, produkter och enhetsgrupper för att skydda, upptäcka och reagera på hot dygnet runt.

Democracy Forward Initiative: Ett Microsoft-team som arbetar för att bevara, skydda och främja demokratins grunder genom att främja ett sunt informationsekosystem, skydda öppna och säkra demokratiska processer samt förespråka företagens samhällsansvar.

Digital Crimes Unit (DCU): Ett team som består av advokater, utredare, dataloger, tekniker, analytiker och affärsfolk som arbetar med att bekämpa cyberbrott i global skala med hjälp av teknik, kriminalteknik, civilrättsliga åtgärder, överlämna material till brottsutredare och både offentliga och privata partnerskap.

Digital Diplomacy: Ett internationellt team som består av före detta diplomater, beslutsfattare och juridiska experter som arbetar för att främja en fredlig, stabil och säker cyberrymd inför hotet av ökande konflikter mellan nationalstater.

Digital Security & Resilience (DSR): En organisation som arbetar för att Microsoft ska kunna ta fram de mest betrodda enheterna och tjänsterna, samtidigt som vårt företag säkras och både våra och kundernas data skyddas.

Digital Security Unit (DSU): Ett team av cybersäkerhetsadvokater och analytiker som står bakom juridisk, geopolitisk och teknisk expertis för att skydda Microsoft och dess kunder. DSU bygger upp förtroendet för Microsofts säkerhetsförsvar mot avancerade cyberfiender över hela världen.

Digital Threat Analysis Center (DTAC): Ett expertteam som analyserar och rapporterar hot från nationalstater, däribland cyberattacker och påverkansoperationer. Teamet kombinerar informations- och cyberhotsunderrättelser med geopolitiska analyser för att ge våra kunder och Microsoft insikter som ska användas för effektiva insatser och skydd.

Enterprise and Security: Ett team som fokuserar på att tillhandahålla en modern, säker och hanterbar plattform för det intelligenta molnet och den intelligenta närverksgränsen.

Enterprise Mobility: Ett team som hjälper till att leverera den moderna arbetsplatsen och modern hantering för att hålla data säkra i molnet och lokalt. Endpoint Manager omfattar de tjänster och verktyg som Microsoft och företagets kunder använder för att hantera och övervaka mobila enheter, stationära datorer, virtuella maskiner, inbäddade enheter och servrar.

Bidragande team

fortsättning

Enterprise Risk Management: Ett team som arbetar med olika affärsenheter för att prioritera riskdiskussioner med Microsoft ledande befattningshavare. ERM är navet för flera operativa riskteam, hanterar Microsofts riskramverk och underlättar företagets interna säkerhetsbedömning med NIST Cybersecurity Framework.

Global Cybersecurity Policy: Ett team som jobbar med myndigheter, ideella organisationer och branschpartner för att främja en offentlig cybersäkerhetspolicy som ger kunderna möjlighet att stärka sin säkerhet och motståndskraft när de tar till sig och använder Microsoft-teknik.

Identity and Network Access (IDNA) Security: Ett team som arbetar för att skydda alla Microsofts kunder från obehörig åtkomst och bedrägerier. IDNA Security är ett allomfattande team som består av tekniker, produktchefer, dataloger och säkerhetsutredare.

M365 Security: En organisation som utvecklar säkerhetslösningar som Microsoft Defender för Endpoint (MDE), Microsoft Defender for Identity (MDI) och andra för att skydda företagskunder.

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): Ett rådgivande organ på Microsoft med uppdraget att se till att ny teknik utvecklas och sätts in på ett ansvarsfullt sätt.

Microsoft Bing Search and Distribution: Ett team som enbart jobbar med att tillhandahålla en sökmotor i världsklass med vilken användare runtom i världen snabbt kan få tillförlitliga sökresultat och information, däribland att hålla reda på ämnen och trender som är viktiga för dem, samtidigt som användarna får kontroll över sin integritet.

Microsoft Customer and Partner Solutions: Microsofts enhetliga organisation för kommersialisering av varor som ansvarar för fältroller som säkerhets- och tekniska säljspecialister och rådgivare.

Microsoft Defender Experts: Microsofts största globala organisation med produktfokuserade säkerhetsforskare, forskare på tillämpningsområden och hotunderrättelseanalytiker. Defender Experts levererar innovativa detekterings- och svarsfunktioner i Microsoft 365:s säkerhetsprodukter och hanterade Microsoft Defender Experts-tjänster.

Microsoft Defender for IoT: Ett team som består av ämnesområdesexperter som har specialiserat sig på att i grund studera skadlig IoT-/OT-kod, protokoll och inbyggd programvara. Teamet jagar efter IoT-/OT-hot för att upptäcka skadliga trender och kampanjer.

Microsoft Defender Threat Intelligence (RiskIQ): Ett team som framställer taktiska underrättelser genom analys av Microsofts omfattande externa telemetrisamling. De kartlägger hotbilden i takt med att den utvecklas för att upptäcka tidigare okänd hotinfrastruktur och lägga till kontext som rör hotaktörer och kampanjer. Teamet publicerar regelbundet aktuella och särskiljande forskningsresultat för att leverera livsavgörande taktisk information till försvarare.

Microsoft Security Business Development Team: Ett team som leder Microsoft tillväxtstrategi, partnerskap och strategiska investeringar på cybersäkerhetsområdet.

Microsoft Security Response Center (MSRC): Ett team som samarbetar med säkerhetsforskare som jobbar för att skydda Microsoft kunder och partnerekosystem. MSRC är en viktig del av Microsofts Cyber Defense Operations Center (CDOC) och samlar experter på säkerhetsrespons för att upptäcka och reagera på hot i realtid.

Microsoft Security Services for Incident Response: Ett team med cybersäkerhetsexperter som hjälper kunderna under cyberattacker med allt från utredning till inneslutning och återställningsrelaterad verksamhet. Tjänsterna erbjuds via två mycket integrerade team, Detection and Response Team (DART) med fokus på utredning och grundarbete för återställning, samt Compromise Recovery Security Practice (CRSP), som fokuserar på inneslutnings- och återställningsaspekter.

Microsoft Threat Intelligence Center (MSTIC): Ett team som fokuserar på att identifiera, spåra och samla information som rör de mest sofistikerade angriparna som påverkar Microsofts kunder, däribland hot från nationalstater, skadlig kod och nätfiske.

One Engineering System (1ES): Ett team med uppdrag att leverera verktyg i världsklass för att hjälpa Microsofts utvecklare att vara så produktiva och säkra som möjligt. Teamet leder den centrala strategin för att säkra Microsoft i hela försörjningskedjan för programvara.

Operational Threat Intelligence Center (OpTIC): Teamet som ansvarar för att hantera och sprida information om cyberhot som stöder Microsoft Cyber Defense Operation Centers (CDOC) uppdrag att skydda Microsoft och våra kunder.

Microsoft

Belyser hotbilden och stärker ett digitalt försvar.

- Läs mer: **https://microsoft.com/mddr**
- Djupdykning: **https://blogs.microsoft.com/on-the-issues/**
- Håll kontakten: **@msftissues och @msftsecurity**

© 2022 Microsoft. Med ensamrätt.