Microsoft

Raport Microsoft dotyczący bezpieczeństwa cyfrowego (2022 r.)

Omówienie krajobrazu zagrożeń
i wzmocnienie cyfrowej obrony.

Spis treści

Dane, analizy i wydarzenia podane w tym raporcie pochodzą z okresu od lipca 2021 r. do czerwca 2022 r. (rok podatkowy 2022), chyba że zaznaczono inaczej.

Ten raport najlepiej wyświetlać w Adobe Reader (można go pobrać za darmo z witryny Adobe).

Wprowadzenie — Tom Burt

Wiceprezes ds. bezpieczeństwa i zaufania klientów

„Biliony sygnałów, które analizujemy z naszego światowego ekosystemu produktów i usług, ujawniają gwałtowność, zakres i skalę zagrożeń cyfrowych”

Migawka z naszych analiz...

Zakres i skala zagrożeń
Wolumen ataków opartych na hasłach wzrósł do szacunkowo 921 ataków na sekundę — o 74% w ciągu zaledwie roku.

Walka z cyberprzestępczością
Do tej pory Microsoft usunął ponad 10 000 domen wykorzystywanych przez cyberprzestępców i 600 wykorzystywanych przez atakujące państwa.

Usuwanie luk w zabezpieczeniach
Reagując na incydenty związane z oprogramowaniem wymuszającym okup, w 93% przypadków odkryliśmy niewystarczającą kontrolę uprawnień dostępu i penetracji sieci.

23 lutego 2022 r. świat cyberbezpieczeństwa wkroczył w nową erę: wojny hybrydowej. Tego dnia, na godziny przed wystrzeleniem rakiet i przejazdem czołgów przez granice, grupy powiązane z Rosją rozpoczęły masowy, niszczycielski cyberatak na administrację publiczną, infrastrukturę technologiczną i sektor finansowy Ukrainy. Więcej o tych atakach przeczytasz w rozdziale „Zagrożenia ze strony państw” w niniejszym, trzecim wydaniu corocznego „Raportu Microsoft dotyczącego bezpieczeństwa cyfrowego”. Kluczowym wnioskiem jest to, że najlepsze fizyczne i logiczne zabezpieczenie przed cyberatakami zapewnia chmura. Umożliwia ona lepszą analitykę zagrożeń i ochronę urządzeń klienckich, co zostało udowodnione na Ukrainie.

Tegoroczny raport zawiera jednak o wiele więcej konkluzji. W pierwszym rozdziale skupiamy się na działaniach cyberprzestępców, a w drugim na zagrożeniach ze strony państw. W obu kategoriach ataków znacznie zwiększono wyrafinowanie, co znacząco poprawiło ich skuteczność. Gdy Rosja znalazła się na pierwszych stronach gazet, Iran po zmianie prezydenta nasilił ataki na Izrael, a także operacje wymuszania okupu oraz „hakowania i publikowania wykradzionych danych” wymierzone w infrastrukturę krytyczną w Stanach Zjednoczonych. Również Chiny poszerzyły swoje działania szpiegowskie w Azji Południowo-Wschodniej i innych miejscach na półkuli południowej, starając się przeciwdziałać wpływom Stanów Zjednoczonych oraz wykradać krytyczne dane i informacje.

Państwa realizują również na całym świecie operacje wpływu propagandowego z użyciem wysoce skutecznych technik (rozdział trzeci). Na przykład Rosja poświęciła dużo wysiłku, aby przekonać obywateli swoich i wielu innych krajów, że jej inwazja na Ukrainę była usprawiedliwiona — jednocześnie siejąc propagandę dyskredytującą szczepionki COVID na Zachodzie, ale promując ich skuteczność u siebie. Ponadto coraz częściej obierane są za cel urządzenia IoT (Internetu rzeczy) oraz urządzenia sterujące OT (technologii operacyjnej), gdyż mogą służyć jako punkty wejścia do sieci i infrastruktury krytycznej (rozdział czwarty). Wreszcie, w ostatnim rozdziale przedstawiamy wnioski, które wyciągnęliśmy w ubiegłym roku, broniąc się przed atakami na Microsoft i naszych klientów, a także dokonujemy przeglądu tegorocznych postępów w zakresie cyberodporności.

Każdy rozdział zawiera ważne spostrzeżenia wynikające z unikalnego punktu widzenia Microsoft. Biliony sygnałów, które analizujemy z naszego światowego ekosystemu produktów i usług, ujawniają gwałtowność, zakres i skalę zagrożeń cyfrowych. Microsoft podejmuje działania mające na celu ochronę klientów i ekosystemu cyfrowego przed tymi zagrożeniami. Nasze technologie identyfikują i blokują miliardy prób wyłudzania informacji, kradzieży tożsamości i innych zagrożeń.

Wprowadzenie — Tom Burt

Ciąg dalszy

Wykorzystujemy również środki prawne i techniczne do konfiskowania i wyłączania infrastruktury wykorzystywanej przez cyberprzestępców i państwa. Powiadamiamy również naszych klientów w przypadku zagrożenia lub ataku ze strony państwa. Pracujemy nad rozwojem efektywnych funkcji i usług z technologiami AI/ML pozwalających na szybsze i skuteczniejsze identyfikowanie i blokowanie cyberzagrożeń. Specjaliści ds. bezpieczeństwa coraz skuteczniej chronią przed cyberwłamaniami i je identyfikują.

Co najważniejsze, przedstawiamy tutaj nasze najlepsze rady dotyczące kroków, które osoby prywatne, organizacje i przedsiębiorstwa mogą podjąć w celu ochrony przed zagrożeniami cyfrowymi. Przyjęcie dobrych praktyk w zakresie cyberhigieny jest najlepszą obroną i może znacznie zmniejszyć ryzyko cyberataków.

Stan cyberprzestępczości

Cyberprzestępcy nadal działają jak zaawansowane przedsiębiorstwa nastawione na zysk. Atakujący dostosowują się i zwiększają złożoność tego, jak i gdzie hostują infrastrukturę operacyjną kampanii. Jednocześnie stają się bardziej oszczędni. Aby obniżyć koszty i zwiększyć pozory legalności, atakujący hostują kampanie wyłudzania informacji i złośliwe oprogramowanie, a nawet wydobywają kryptowaluty, wykorzystując sieci i urządzenia legalnych firm.

Więcej informacji na str. 6

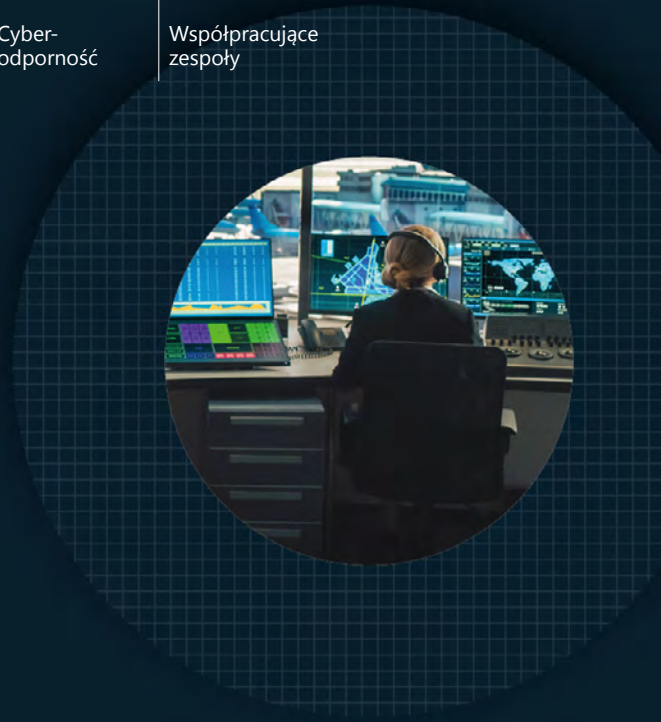
„Pojawienie się cyberbroni na wojnie hybrydowej na Ukrainie to początek nowej ery konfliktów”.

Zagrożenia ze strony państw

Państwa przeprowadzają coraz bardziej wyrafinowane cyberataki zaprojektowane tak, by uniknąć wykrycia i zrealizować swoje strategiczne cele. Pojawienie się cyberbroni na wojnie hybrydowej na Ukrainie to początek nowej ery konfliktów. W ramach wojny Rosja realizowała również operacje wpływu informacyjnego, manipulując opiniami w Rosji, na Ukrainie i na świecie za pomocą propagandy. Atakujące państwa zwiększyły aktywność również poza Ukrainą — zaczęły wykorzystywać nowości w zakresie automatyzacji, infrastruktury chmurowej i technologii zdalnego dostępu, aby atakować szerszą gamę celów. Często atakowane były korporacyjne łańcuchy dostaw IT, które umożliwiają dostęp do ostatecznych ofiar. Cyberhigiena stała się jeszcze bardziej krytyczna, ponieważ atakujący szybko wykorzystywali niezaktualizowane luki, stosowali zarówno wyrafinowane techniki kradzieży poświadczeń, jak i ataki siłowe (brute-force), a także ukrywali swoje działania, wykorzystując legalne oprogramowanie lub typu open-source. Iran dołączył do Rosji w stosowaniu destrukcyjnej cyberbroni, w tym oprogramowania wymuszającego okup.

Zmiany te wymagają pilnego przyjęcia spójnych, globalnych ram, które nadadzą priorytet prawom człowieka i będą chronić ludzi przed lekkomyślnym zachowaniem czynników państwowych w sieci. Wszystkie narody muszą współpracować w celu wdrożenia norm odpowiedzialnego postępowania państw.

Więcej informacji na str. 30



Urządzenia i infrastruktura

Pandemia, w połączeniu z szybkim wdrożeniem wszelkiego rodzaju urządzeń z dostępem do Internetu w ramach przyspieszającej transformacji cyfrowej, znacznie zwiększyła obszar podatny na ataki naszego cyfrowego świata. Cyberprzestępcy i atakujące państwa szybko to wykorzystały. Chociaż zabezpieczenia sprzętu i oprogramowania IT w ostatnich latach się poprawiły, to urządzeń IoT i OT już nie. Atakujący wykorzystują te urządzenia do uzyskiwania dostępu do sieci i ich penetracji, zdobywania przyczółków w łańcuchach dostaw czy zakłócania operacji OT organizacji-ofiar.

Więcej informacji na str. 56

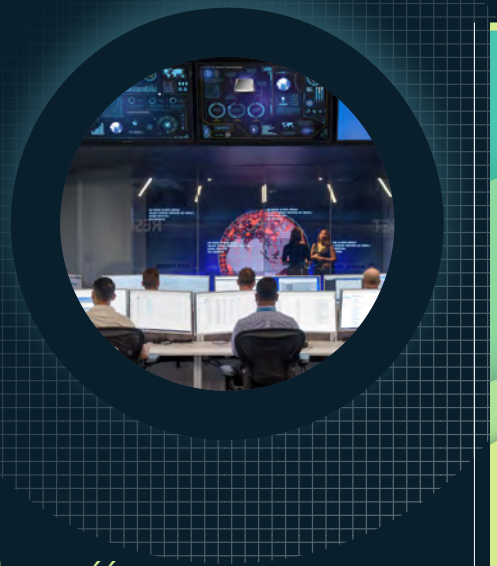
Wprowadzenie — Tom Burt

Ciąg dalszy

Operacje wpływu

Państwa coraz częściej stosują wyrafinowane operacje wpływu w celu rozpowszechniania propagandy i kształtowania opinii publicznej zarówno wewnętrznie, jak i za granicą. Kampanie te podkopują zaufanie, zwiększają polaryzację społeczną i zagrażają demokracji. Zaawansowani i zdeterminowani manipulatorzy wykorzystują tradycyjne media oraz Internet i media społecznościowe, aby znacznie zwiększyć zakres, skalę i skuteczność swoich kampanii oraz i tak już ogromny wpływ, jaki wywierają na globalny ekosystem informacyjny. W zeszłym roku tego typu operacje były realizowane w ramach rosyjskiej wojny hybrydowej na Ukrainie. Rosja i inne kraje, w tym Chiny i Iran, coraz częściej stosowały operacje propagandowe przez media społecznościowe, aby rozszerzyć swój globalny wpływ na szereg obszarów.

Więcej informacji na str. 71



Cyberodporność

Bezpieczeństwo jest kluczowym czynnikiem sukcesu technologicznego. Innowacyjność i wysoką produktywność można osiągnąć jedynie poprzez wprowadzenie zabezpieczeń, które zwiększą odporność organizacji na nowoczesne ataki. Wskutek pandemii musieliśmy zmienić praktyki i technologie bezpieczeństwa Microsoft, aby chronić naszych pracowników niezależnie od tego, gdzie pracują. W minionym roku atakujący nadal wykorzystywali luki ujawnione w okresie pandemii i przechodzenia na pracę hybrydową. Od tego czasu naszą główną troską jest masowość i złożoność ataków oraz zwiększona aktywność atakujących państw. W tym rozdziale opisujemy wyzwania, przed którymi stanęliśmy, oraz środki obrony, które wdrożyliśmy wraz z ponad 15 000 partnerami.

Więcej informacji na str. 86

Nasz wyjątkowy punkt widzenia

37 mld
zablokowanych zagrożeń e-mail

34,7 mld
zablokowanych zagrożeń dla tożsamości

43 bln
sygnałów przetwarzanych codziennie z użyciem zaawansowanej analityki danych i algorytmów AI w celu zrozumienia zagrożeń i cyberaktywności przestępców oraz ochrony przed nimi.

2,5 mld
codziennie analizowanych sygnałów z urządzeń klienckich

Ponad 8500
inżynierów, badaczy, analityków danych, ekspertów ds. cyberbezpieczeństwa, poszukiwaczy zagrożeń, analityków geopolitycznych, śledczych i pracowników pierwszego kontaktu w 77 krajach.

Ponad 15 000
partnerów w naszym ekosystemie bezpieczeństwa, którzy zwiększają cyberodporność naszych klientów.

Od 1 lipca 2021 r. do 30 czerwca 2022 r.

Wprowadzenie — Tom Burt

Ciąg dalszy

Wierzymy, że Microsoft — samodzielnie i poprzez bliskie partnerstwa z innymi podmiotami z sektora prywatnego, administracji publicznej i społeczeństwa obywatelskiego — ma obowiązek chronić systemy cyfrowe, które stanowią podstawę tkanki społecznej, oraz promować bezpieczne środowiska komputerowe dla każdej osoby, niezależnie od tego, gdzie się znajduje. W ramach tej odpowiedzialności od 2020 r. publikujemy corocznie raport dotyczący cyberbezpieczeństwa. Oparty jest on na ogromie danych i dogłębnych badaniach Microsoft. Zawiera nasze unikalne spostrzeżenia na temat tego, jak ewoluuje krajobraz zagrożeń cyfrowych i jakie kluczowe działania można podjąć już dziś, aby poprawić bezpieczeństwo ekosystemu.

Mamy nadzieję, że uda nam się wzbudzić poczucie pilności, aby czytelnicy podjęli natychmiastowe działania w oparciu o dane i spostrzeżenia, które prezentujemy zarówno tutaj, jak i w naszych publikacjach dotyczących cyberbezpieczeństwa. Cyberzagrożenia to poważny problem. Dlatego wszyscy powinniśmy działać na rzecz ochrony siebie oraz naszych organizacji i przedsiębiorstw.

Dziękujemy za poświęcenie czasu na zapoznanie się z tegorocznym „Raportem Microsoft dotyczącym bezpieczeństwa cyfrowego”. Zawiera on cenne spostrzeżenia i zalecenia, które pomogą nam wspólnie chronić ekosystem cyfrowy.

Tom Burt
Wiceprezes ds. bezpieczeństwa i zaufania klientów

Cel tego raportu jest dwojaki:

1. Przedstawić naszym klientom, partnerom i interesariuszom z całego ekosystemu zmieniający się krajobraz zagrożeń cyfrowych, rzucając światło zarówno na nowe cyberataki, jak i zmieniające się trendy w występujących od dawna zagrożeniach.
2. Umożliwić naszym klientom i partnerom poprawę cyberodporności i reakcji na zagrożenia.

Stan cyber-przestępczości

Atakujący ulepszają swoje techniki w obliczu wzmacniania się cyberobrony i coraz większej liczby organizacji proaktywnie podejmujących działania zapobiegawcze.

Przegląd

stanu cyberprzestępczości

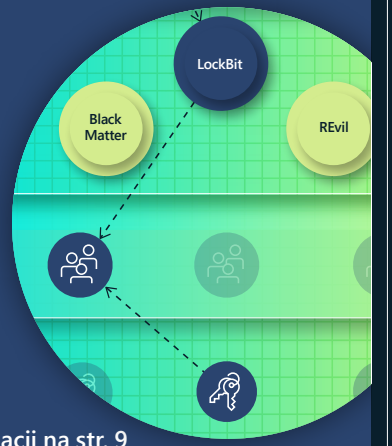
Atakujący ulepszają swoje techniki w obliczu wzmacniania się cyberobrony i coraz większej liczby organizacji proaktywnie podejmujących działania zapobiegawcze.

Cyberprzestępcy nadal działają jak zaawansowane przedsiębiorstwa nastawione na zysk. Atakujący dostosowują się i zwiększają złożoność tego, jak i gdzie hostują infrastrukturę operacyjną kampanii. Jednocześnie stają się bardziej oszczędni. Aby obniżyć koszty i zwiększyć pozory legalności, atakujący hostują kampanie wyłudzania informacji i złośliwe oprogramowanie, a nawet wydobywają kryptowaluty, wykorzystując sieci i urządzenia legalnych firm.

Cyberprzestępczość „uprzemysławia się” — ułatwienie dostępu do narzędzi i infrastruktury powoduje obniżenie bariery wejścia pod względem wymaganych umiejętności.

Więcej informacji na str. 18

Celem ataków oprogramowania wymuszającego okup jest coraz częściej administracja publiczna, przedsiębiorstwa i infrastruktura krytyczna.

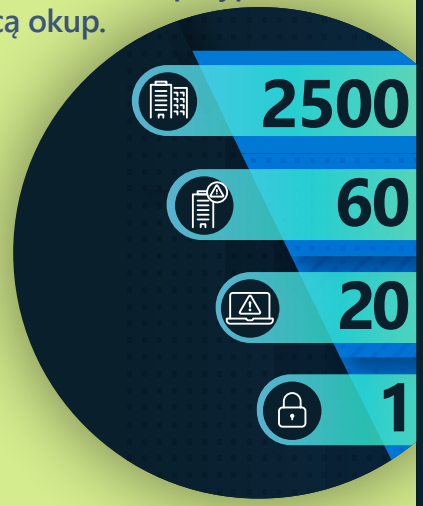


Więcej informacji na str. 9

Atakujący coraz częściej grożą ujawnieniem danych wrażliwych, aby wymusić okup.

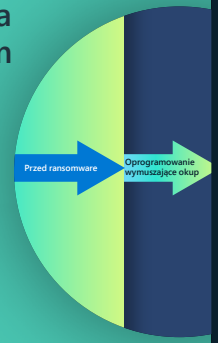
Więcej informacji na str. 10

Najbardziej rozpowszechnione jest oprogramowanie wymuszające okup obsługiwane przez człowieka — w jego przypadku jedna trzecia ataków jest skuteczna, a w 5% przypadków ofiary płacą okup.



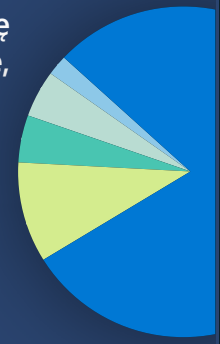
Więcej informacji na str. 9

Najskuteczniejsza obrona przed oprogramowaniem wymuszającym okup to uwierzytelnianie wieloskładnikowe, regularne stosowanie poprawek zabezpieczeń oraz zasady Zero Trust w całej sieci.



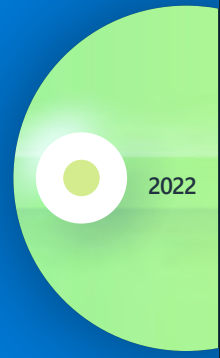
Więcej informacji na str. 13

Kampanie wyłudzania informacji (phishing), w tym głównie poświadczeń, kierowane na skrzynki pocztowe są masowe. Ataki na pocztę elektroniczną w biznesie, w tym oszustwa związane z fakturami, stanowią poważne cyberzagrożenie dla przedsiębiorstw.



Więcej informacji na str. 21

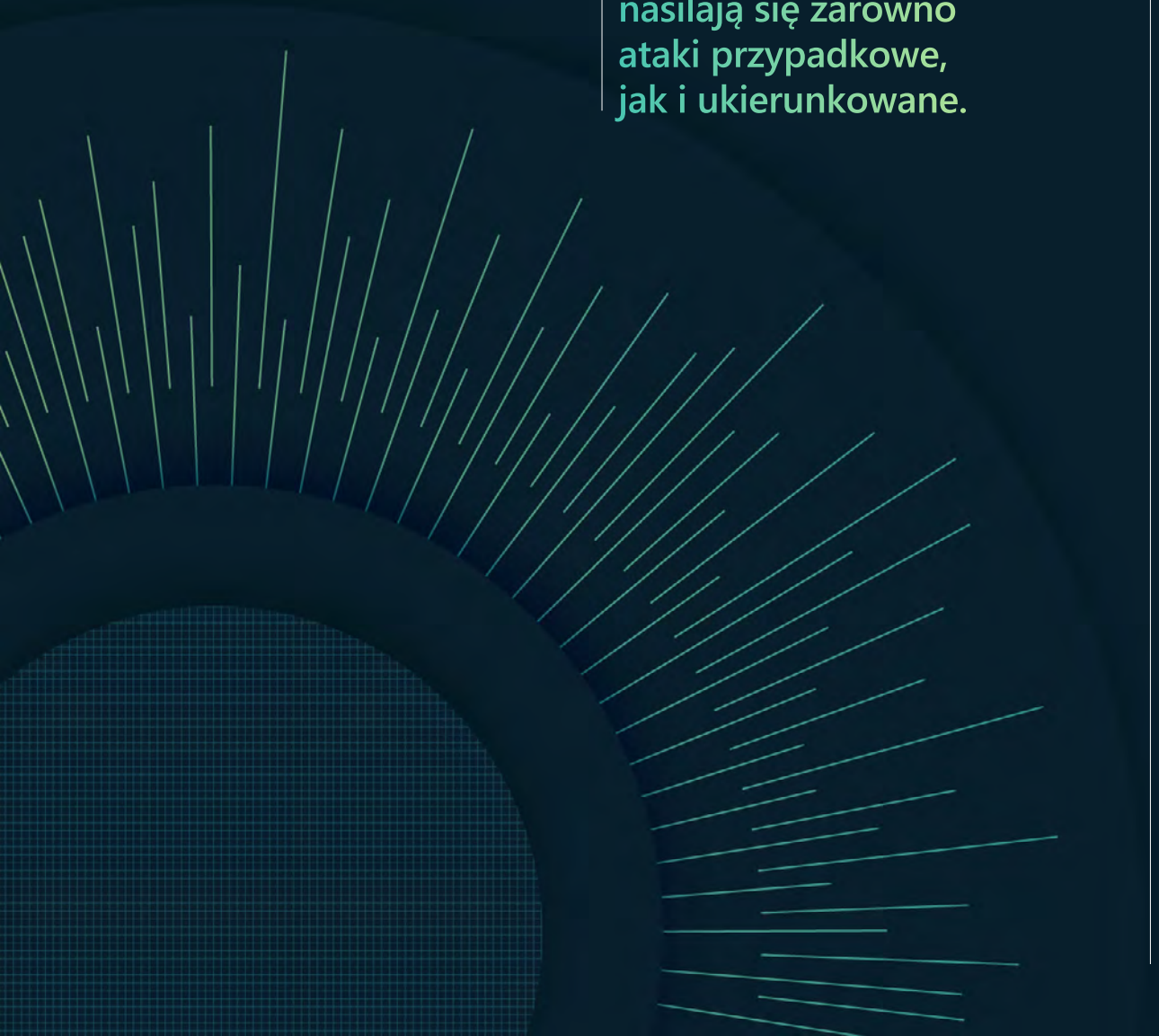
Microsoft stara się zakłócić działanie infrastruktur cyberprzestępców i atakujących państw, wykorzystując innowacyjne podejścia prawne oraz partnerstwa publiczne i prywatne.



Więcej informacji na str. 25

Wprowadzenie

Cyberprzestępczość nadal rośnie, przy czym nasilają się zarówno ataki przypadkowe, jak i ukierunkowane.



Ponieważ cyberobrona się umacnia, a coraz więcej instytucji administracji publicznej i firm przyjmuje proaktywne podejście do ochrony, napastnicy stosują dwie strategie, aby uzyskać dostęp niezbędny do dalszych działań przestępczych. Jednym z podejść są masowe, szerokie kampanie. Drugim podejściem jest selektywna analiza celów i dobieranie ich pod kątem maksymalizacji „stopy zwrotu". Nawet jeśli generowanie przychodów nie jest celem — jak w przypadku atakujących państw, którym chodzi o cele geopolityczne — stosowane są zarówno ataki losowe, jak i ukierunkowane. W ubiegłym roku cyberprzestępcy nadal wykorzystywali inżynierię społeczną i aktualnie popularne tematy, by zwiększyć skuteczność kampanii. Na przykład w atakach wyłudzania informacji przynęty na temat COVID były rzadsze, za to zaobserwowaliśmy wzrost liczby takich, w których zachęcano do przekazywania darowizn na rzecz obywateli Ukrainy.

Atakujący dostosowują się i zwiększają złożoność tego, jak i gdzie hostują infrastrukturę operacyjną kampanii. Zauważyliśmy, że cyberprzestępcy stają się bardziej oszczędni i nie płacą już za technologię. Aby obniżyć koszty i zwiększyć pozory legalności, niektórzy atakujący hostują kampanie wyłudzania informacji i złośliwe oprogramowanie, a nawet wydobywają kryptowaluty, wykorzystując systemy legalnych firm.

W tym rozdziale omawiamy również wzrost haktywizmu, czyli zakłóceń spowodowanych przez obywateli przeprowadzających cyberataki w celu realizacji celów społecznych lub politycznych. Tysiące osób na całym świecie, zarówno ekspertów, jak i nowicjuszy, zmobilizowało się od lutego 2022 r. do przeprowadzenia ataków w ramach wojny rosyjsko-ukraińskiej, np. wyłączania witryn internetowych czy wycieków wykradzionych danych. Nie wiadomo, czy ta tendencja utrzyma się po zakończeniu aktywnych działań wojennych.

Organizacje, w celu obrony przed cyberatakami, muszą regularnie przeglądać i poprawiać mechanizmy kontroli dostępu oraz wdrażać strategie bezpieczeństwa. Jednak to nie wszystko. Omówimy, jak nasz Digital Crimes Unit (DCU, Zespół ds. przestępstw cyfrowych) na gruncie prawa cywilnego spowodował skonfiskowanie złośliwej infrastruktury wykorzystywanej przez cyberprzestępców i atakujące państwa. Musimy wspólnie walczyć z tym zagrożeniem przez partnerstwo zarówno publiczne, jak i prywatne. Mamy nadzieję, że dzieląc się tym, czego nauczyliśmy się w ciągu ostatnich 10 lat, pomożemy innym zrozumieć i wdrożyć proaktywne środki, dzięki którym ochronią siebie i cały ekosystem przed rosnącymi cyberzagrożeniami.

Amy Hogan-Burney
Dyrektor generalny, Digital Crimes Unit

Oprogramowanie wymuszające okup: zagrożenie ze strony państw

Oprogramowanie wymuszające okup (ransomware) to duże zagrożenie dla wszystkich obywateli, ponieważ przestępcy, wykorzystując rosnący ekosystem cyberprzestępczy, atakują infrastrukturę krytyczną, przedsiębiorstwa każdej wielkości oraz administrację zarówno rządową, jak i samorządową.

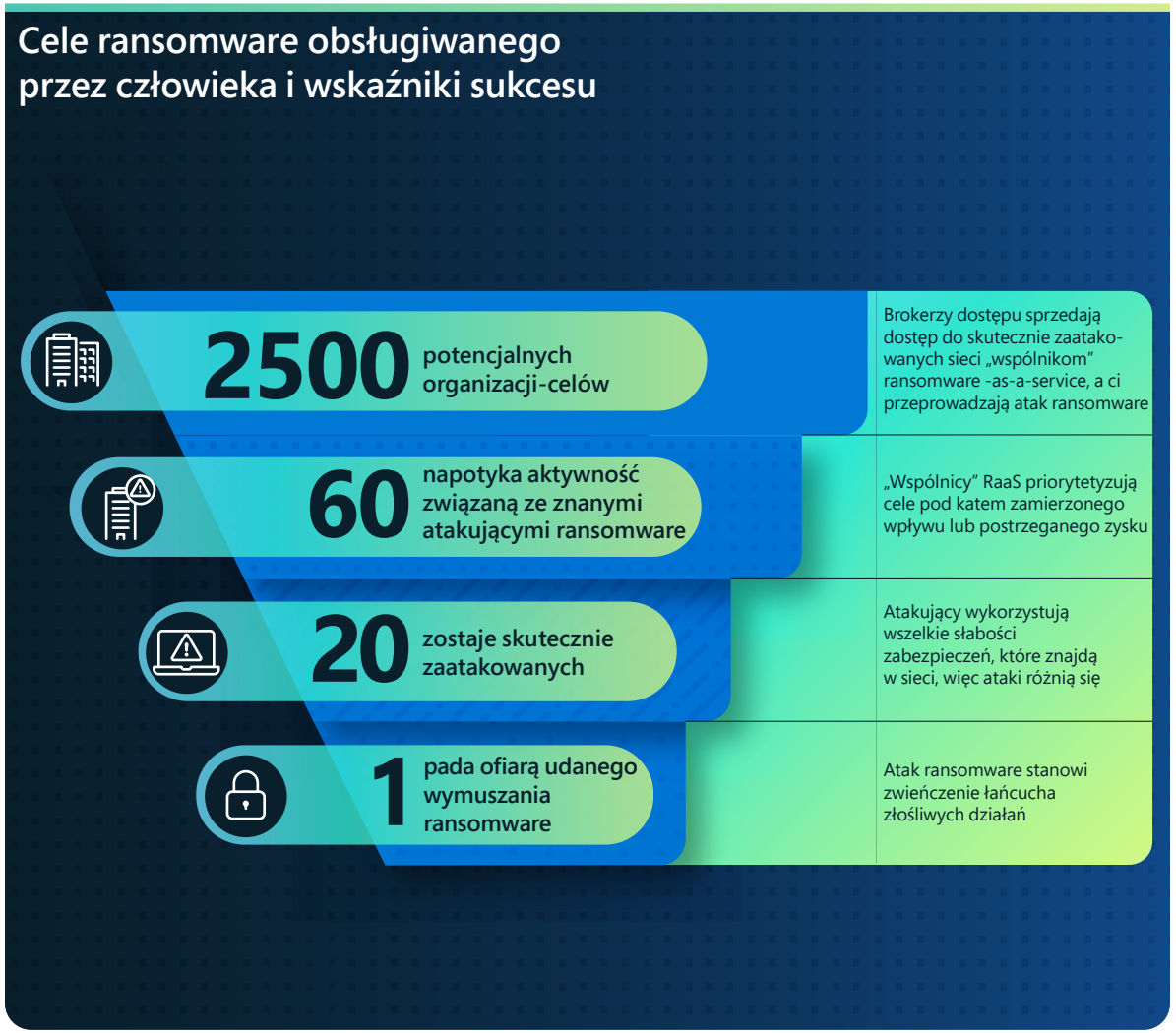
W ciągu ostatnich dwóch lat głośne incydenty związane z oprogramowaniem wymuszającym okup (ransomware) — np. dotyczące infrastruktury krytycznej, opieki zdrowotnej czy dostawców usług IT — przyciągnęły uwagę opinii publicznej. Ataki ransomware stają się coraz bardziej zuchwałe, a ich skutki są coraz bardziej doniosłe. Poniżej przedstawiamy przykłady ataków z 2022 r.:

- W lutym atak na dwie firmy wpłynął na systemy przetwarzania płatności setek stacji benzynowych w północnych Niemczech[1].
- W marcu atak na greckie usługi pocztowe tymczasowo zakłócił dostarczanie poczty i wpłynął na przetwarzanie transakcji finansowych[2].
- Pod koniec maja atak ransomware na kostarykańskie instytucje administracji publicznej zmusił do ogłoszenia stanu wyjątkowego w kraju po zamknięciu szpitali i zakłóceniu poboru ceł i podatków[3].
- Również w maju atak spowodował opóźnienia i odwołania lotów jednej z największych indyjskich linii lotniczych, pozostawiając setki pasażerów na pastwę losu[4].

Skuteczność tych ataków i ich masowość są wynikiem „uprzemysłowienia" gospodarki cyberprzestępczej. Dostęp do narzędzi i infrastruktury stał się łatwiejszy oraz nastąpiło obniżenie bariery wejścia pod względem wymaganych umiejętności.

W ostatnich latach oprogramowanie ransomware przeszło od modelu, w którym pojedynczy „gang" zarówno opracowywał, jak i wdrażał ładunek ransomware, do modelu oprogramowania wymuszającego okup jako usługi (RaaS). W modelu RaaS dwie grupy dzielą się zyskami: pierwsza tworzy ładunek ransomware oraz obsługuje płatności i środowisko wymuszania, używając wycieków danych. Druga grupa zwana „wspólnikami" (affiliates) przeprowadza same ataki. Tego typu „franczyza" w gospodarce cyberprzestępczości poszerzyła grono atakujących. „Uprzemysłowienie" narzędzi cyberprzestępców ułatwiło atakującym przeprowadzanie włamań, eksfiltrację danych i wdrażanie ransomware.

Ransomware obsługiwany przez człowieka[5] pozostaje istotnym zagrożeniem dla organizacji. Pojęcie to wprowadzili badacze Microsoft na opisanie ataków, w których to ludzie na każdym etapie podejmują decyzje w oparciu o to, co odkryją w złamanej sieci. Termin ten odróżnia zagrożenia tego typu od ataków automatycznych.



Model oparty na danych Ochrony punktu końcowego w usłudze Microsoft Defender (EDR) (styczeń–czerwiec 2022 r.).

Oprogramowanie wymuszające okup: zagrożenie ze strony państw

(c.d.)

Ataki ransomware stały się jeszcze bardziej destrukcyjne, gdy standardową praktyką stało się zarabianie na podwójnym wymuszaniu. Na złamanych urządzeniach przestępcy eksfiltrują dane, szyfrują je, a następnie publicznie je udostępniają lub grożą tym, aby zmusić ofiary do zapłacenia okupu.

Przy większości ataków, ransomware jest wdrażany w każdej sieci, do której atakujący uzyskają dostęp. W niektórych przypadkach intruzi kupują dostęp od innych cyberprzestępców, wykorzystując kontakty między brokerami dostępu a operatorami ransomware.

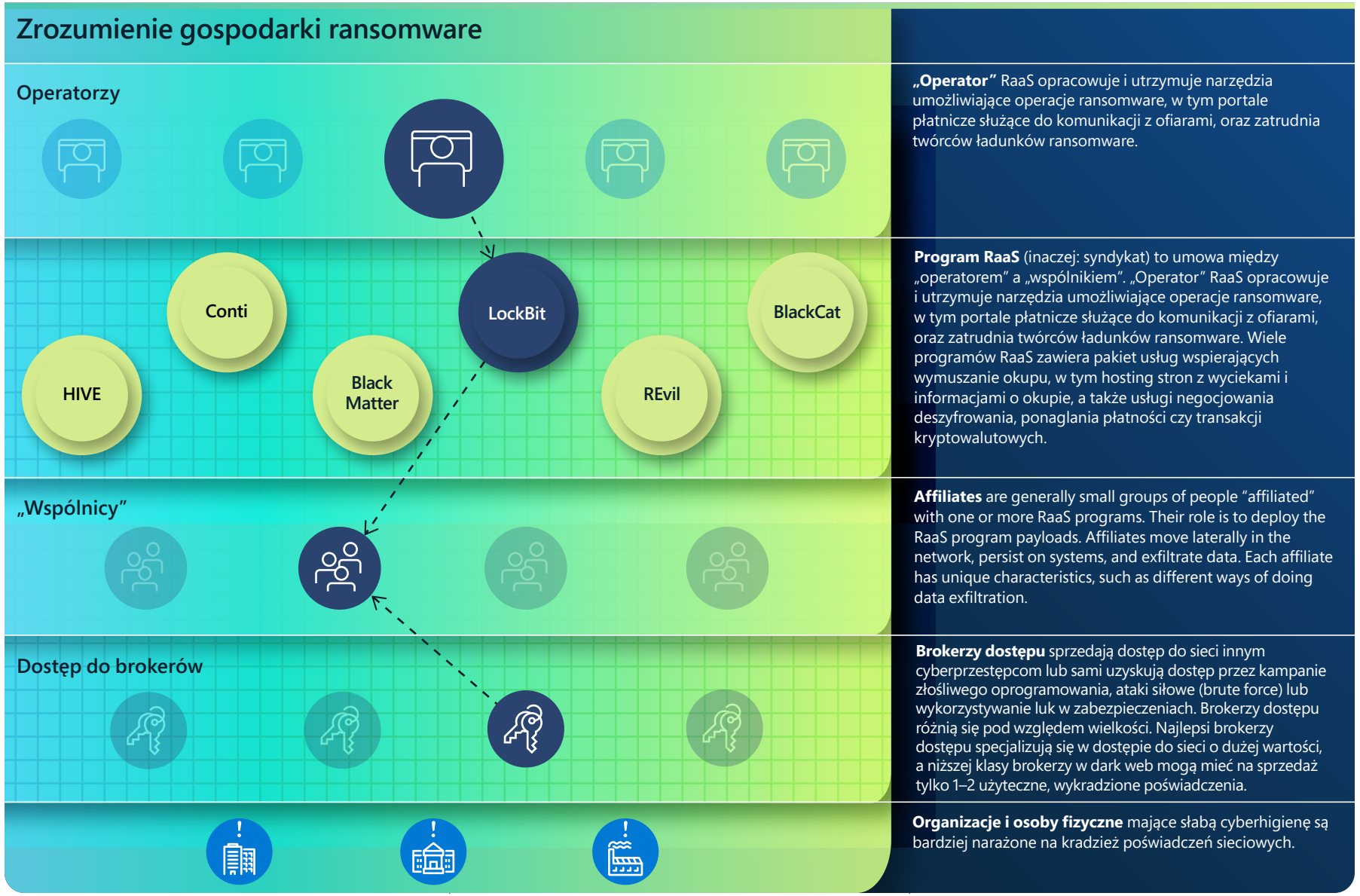
Nasza unikalna, szeroka analityka sygnałowa jest zbierana z wielu źródeł — tożsamości, poczty elektronicznej, urządzeń klienckich oraz chmury — zapewniając wgląd w rosnącą gospodarkę ransomware i model „wspólników", w którym narzędziami dysponują nawet mniej zaawansowani technicznie przestępcy.

Rozszerzające się relacje między wyspecjalizowanymi cyberprzestępcami zwiększyły tempo, wyrafinowanie i skuteczność ataków ransomware. Spowodowało to ewolucję ekosystemu cyberprzestępczego — przestępcy o różnych technikach, celach i umiejętnościach łączą i wspierają się nawzajem, pomagając sobie wstępnie przełamywać zabezpieczenia systemów ofiar, a także udostępniając usługi płatnicze oraz narzędzia lub strony do deszyfrowania czy publikowania danych.

Operatorzy ransomware mogą obecnie kupować dostęp do organizacji lub sieci administracji publicznej online lub uzyskiwać poświadczenia i dostęp przez znajomość z „brokerami", których głównym celem jest zarabianie na raz zdobytym dostępie.

Operatorzy następnie wykorzystują zakupiony dostęp, aby wdrożyć ładunek ransomware, który kupują na platformach handlowych lub forach w dark web. W wielu przypadkach negocjacje z ofiarami prowadzi zespół RaaS, a nie sami operatorzy. Przestępcze transakcje są najczęściej bezproblemowe, a ich uczestnicy w małym stopniu ryzykują aresztowaniem i postawieniem zarzutów ze względu na anonimowość dark web i trudności w egzekwowaniu prawa w skali międzynarodowej.

Trwałe i skuteczne działania przeciwko temu zagrożeniu będą wymagały strategii całej administracji publicznej realizowanej w ścisłym partnerstwie z sektorem prywatnym.



W przeciwieństwie do tego, jak oprogramowanie wymuszające okup jest przedstawiane w mediach, niewiele jest samodzielnych, wszechstronnych „gangów ransomware". To w rzeczywistości zlepek oddzielnych grup: inne zespoły tworzą złośliwe oprogramowanie, uzyskują dostęp do systemów ofiar, wdrażają ransomware i prowadzą negocjacje dotyczące wymuszeń. „Uprzemysłowienie" ekosystemu przestępczego spowodowało podział zadań:

- „Brokerzy dostępu" włamują się i przekazują dostęp dalej („dostęp jako usługa").
- Twórcy złośliwego oprogramowania sprzedają narzędzia.
- „Operatorzy" i „wspólnicy" przeprowadzają włamania.
- „Dostawcy" usług szyfrowania i wymuszania przejmują operację od „wspólników" i zajmują się jej „spieniężeniem" (model RaaS).

Wszystkie kampanie ransomware obsługiwanego przez człowieka są możliwe dzięki typowym lukom w zabezpieczeniach. W szczególności, napastnicy zazwyczaj wykorzystują niską cyberhigienę organizacji, np. rzadkie stosowanie poprawek czy brak uwierzytelniania wieloskładnikowego (MFA).

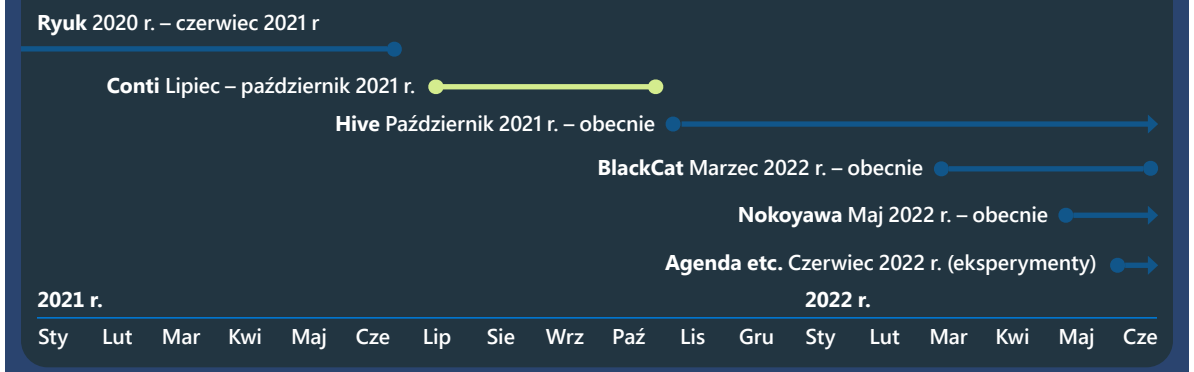
Analiza przypadku: Zanik odmiany Conti

Conti, jeden z czołowych wariantów ransomware w ciągu ostatnich dwóch lat, zaczął zanikać w połowie 2022 r. Microsoft Threat Intelligence Center (MSTIC) zaobserwował znaczny spadek aktywności pod koniec marca i na początku kwietnia. Ostatnie wdrożenia ransomware Conti obserwowaliśmy w połowie kwietnia. Jednak, podobnie jak w przypadku zamknięcia innych operacji związanych z ransomware, zanik Conti nie miał znaczącego wpływu na ataki ransomware. MSTIC zaobserwował, że „wspólnicy" używający Conti przechodzili na inne ładunki ransomware, w tym BlackBasta, Lockbit 2.0, LockbitBlack czy HIVE. Jest to zgodne z danymi z poprzednich lat i sugeruje, że gdy gangi ransomware wstrzymują działalność, pojawiają się ponownie miesiące później lub przekazują swoje zasoby i możliwości techniczne nowym grupom.

Zespoły ds. analizy zagrożeń Microsoft śledzą grupy ransomware (nazywane DEV) w oparciu o używane przez nich narzędzia, a nie złośliwe oprogramowanie. Dlatego kiedy „wspólnicy" Conti rozproszyli się, mogliśmy kontynuować śledzenie tych DEV na podstawie używanych przez nich narzędzi lub zestawów RaaS. Na przykład:

- DEV-0230, który jest powiązany z Trickbot, był użytkownikiem Conti. Pod koniec kwietnia MSTIC zaobserwował to przy użyciu QuantumLocker.
- DEV-0237 przeszedł z zestawu ransomware Conti na HIVE i Nokoyawa, np. użył HIVE w ataku z 31 maja na instytucje administracji publicznej w Kostaryce.
- DEV-0506, kolejny użytkownik zestawu ransomware Conti, zaczął używać BlackBasta.

Przykład „wspólnika" (DEV-0237), który szybko zmienił narzędzia RaaS



Po zamknięciu programu RaaS, takiego jak Conti, „wspólnik" niemal natychmiast przechodzi na inny program (np. Hive).

RaaS zmienia ekosystem ransomware i utrudnia ustalanie sprawców

Ponieważ ransomware obsługiwany przez człowieka jest sterowany przez indywidualnych operatorów, wzorce ataku różnią się w zależności od celu i mogą ulegać zmianie w trakcie ataku. W przeszłości w każdej kampanii w ramach pojedynczej odmiany ransomware obserwowaliśmy ścisłą korelację między początkowym wektorem wniknięcia do systemu, narzędziami i ustawionymi opcjami ładunku ransomware. Ułatwiało to ustalanie sprawców. Model „wspólników" RaaS rozłącza jednak tę korelację. W rezultacie Microsoft śledzi „wspólników" ransomware wdrażających ładunki w konkretnych atakach, a nie śledzi twórców ładunków ransomware jako operatorów.

Innymi słowy, nie zakładamy już, że programista HIVE jest operatorem stojącym za atakiem ransomware HIVE. Atak prawdopodobnie realizuje „wspólnik".

Branża cyberbezpieczeństwa miała trudności z właściwym zrozumieniem tego podziału między programistami a operatorami. Na przykład incydenty związane z ransomware są często zgłaszane na podstawie nazwy ładunku. Daje to fałszywe wrażenie, że za wszystkimi atakami z wykorzystaniem konkretnego ładunku ransomware stoi jeden podmiot lub gang, a wszystkie incydenty z nim związane mają wspólne techniki i składniki infrastruktury. Aby wesprzeć obrońców sieci, należy dowiedzieć się więcej o etapach poprzedzających ataki różnych „wspólników" — takich jak eksfiltracja danych i sposoby utrzymywania się w naruszonych systemach — oraz o możliwościach wykrywania i ochrony.

Aby odnieść sukces, atakujący bardziej niż złośliwego oprogramowania potrzebują poświadczeń. Skuteczne zainfekowanie całej organizacji za pomocą ransomware obsługiwanego przez człowieka zależy od dostępu do konta z wysokimi uprawnieniami.

Ataki ransomware obsługiwanym przez człowieka

W ciągu ostatniego roku eksperci Microsoft ds. ransomware przeprowadzili dogłębne badania ponad 100 incydentów związanych z ransomware obsługiwanym przez człowieka, aby poznać techniki atakujących i zrozumieć, jak lepiej się bronić.

Należy zaznaczyć, że analiza, którą się tu dzielimy, dotyczy tylko urządzeń z wdrożonymi użytkownikami i zarządzanych. Urządzenia niezarządzane stanowią najmniej bezpieczną część zasobów sprzętowych organizacji.

Najpopularniejsze techniki w atakach ransomware:

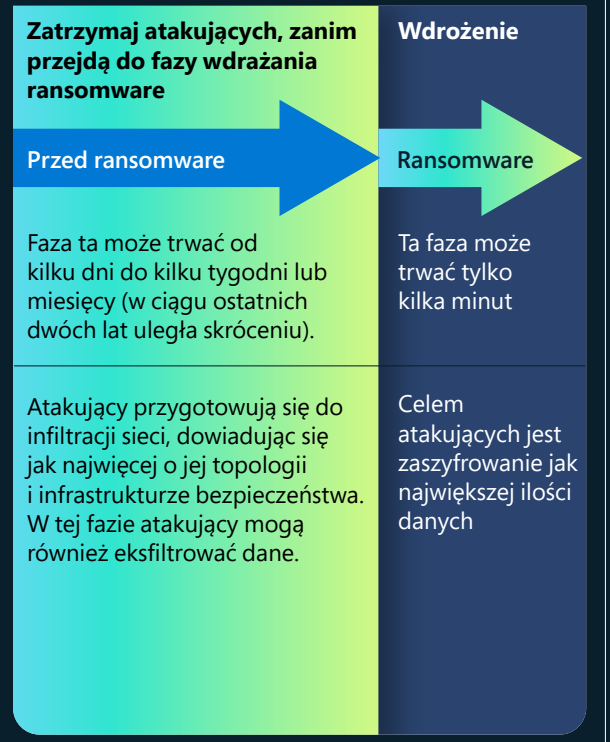
75%
używa narzędzi administracyjnych.

75%
wykorzystuje kupione konta użytkowników z wysokimi uprawnieniami w celu rozprzestrzeniania złośliwych ładunków za pomocą protokołu SMB.

99%
próbuje manipulować wykrytymi produktami zabezpieczającymi i do tworzenia kopii zapasowych przy użyciu narzędzi wbudowanych w system operacyjny.

Typowy atak obsługiwany przez człowieka

Ataki ransomware obsługiwanym przez człowieka można podzielić na fazę poprzedzającą wdrożenie ransomware i fazę wdrożenia ransomware. W fazie przed wdrożeniem ransomware napastnicy przygotowują się do infiltracji sieci, poznając topologię organizacji i infrastrukturę bezpieczeństwa.



Nasze badania wykazały, że większość ataków ransomware obsługiwanym przez człowieka wykorzystuje podobne słabości zabezpieczeń oraz stosuje wspólne wzorce i techniki ataku.

Trwała strategia bezpieczeństwa

Zwalczanie ataków tego rodzaju i zapobieganie im wymaga zmiany sposobu myślenia organizacji, aby skupić się na kompleksowej ochronie wymaganej do spowolnienia i powstrzymania napastników, zanim przejdą oni z fazy poprzedzającej wdrożenie ransomware do fazy jego wdrożenia.

Przedsiębiorstwa muszą konsekwentnie i zdecydowanie stosować najlepsze praktyki bezpieczeństwa w swoich sieciach, aby przeciwdziałać całym klasom ataków. Ze względu na ludzki proces decyzyjny ataki ransomware mogą generować wiele pozornie rozbieżnych alertów bezpieczeństwa, które łatwo mogą zostać przeoczone lub na które nie można zareagować na czas. Zmęczenie alertami jest realne. Centra operacji bezpieczeństwa (SOC) mogą ułatwić sobie pracę, analizując trendy w alertach lub grupując je w zdarzenia, aby zobaczyć szerszy obraz. SOC mogą następnie minimalizować problemy z alertami, stosując odpowiednie funkcje wzmacniania ochrony, takie jak reguły ograniczające obszar podatny na ataki. Wzmacnianie ochrony przed typowymi zagrożeniami może nie tylko zmniejszyć liczbę alertów, ale także powstrzymać wielu atakujących, zanim uzyskają dostęp do sieci.

Organizacje muszą stale utrzymywać wysokie standardy bezpieczeństwa i higieny sieci, aby chronić się przed atakami ransomware obsługiwanym przez człowieka.

Praktyczne wskazówki

Cyberprzestępcy atakujący za pomocą ransomware chcą łatwych zysków, dlatego podniesienie ich kosztów przez wzmocnienie zabezpieczeń ma kluczowe znaczenie dla zakłócenia ich modelu działania.

1. Dbaj o bezpieczeństwo poświadczeń. Aby odnieść sukces, atakujący bardziej niż złośliwego oprogramowania potrzebują poświadczeń. Skuteczne zainfekowanie całej organizacji przez ransomware obsługiwany przez człowieka zależy od dostępu do konta z wysokimi uprawnieniami, takiego jak administrator domeny, lub możliwości edycji zasady grupy.
2. Przeprowadzaj inspekcje narażenia poświadczeń.
3. Priorytetowo wdrażaj aktualizacje Active Directory.
4. Nadaj priorytet wzmacnianiu ochrony chmury.
5. Ogranicz obszar podatny na ataki.
6. Wzmocnij ochronę zasobów z dostępem do Internetu i określ, gdzie jest granica.
7. Ogranicz liczbę alertów SOC przez wzmocnienie ochrony sieci w celu oszczędzenia zasobów na ważne incydenty.

Linki do dalszych informacji

- RaaS: Zrozumienie nowego modelu cyberprzestępczości i sposoby ochrony | Blog Microsoft Security
- Ataki ransomware obsługiwanym przez człowieka: katastrofa, której można uniknąć | Blog Microsoft Security

Oprogramowanie wymuszające okup: relacje osób z pierwszej linii

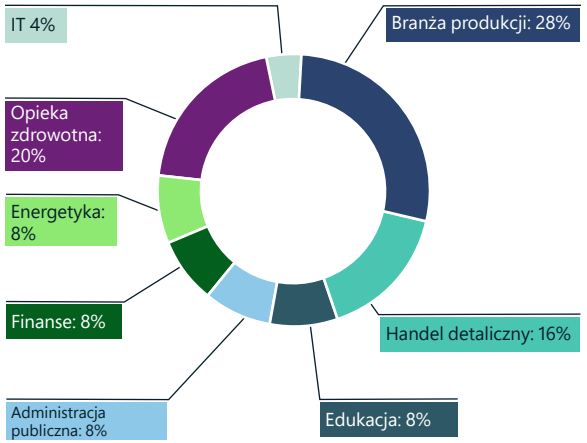
Organizacje na całym świecie doświadczyły wzrostu liczby ataków ransomware obsługiwanego przez człowieka na początku 2019 r. Jednak działania organów ścigania i wydarzenia geopolityczne w ubiegłym roku miały znaczący wpływ na organizacje cyberprzestępcze.

Linia usług bezpieczeństwa (Security Service Line) Microsoft wspiera klientów w trakcie całego cyberataku, od badania po skuteczne powstrzymywanie i działania naprawcze. Usługi reagowania i odzyskiwania są oferowane przez dwa zunifikowane zespoły, z których jeden koncentruje się na badaniach i przygotowaniach do odzyskiwania, a drugi na powstrzymywaniu i odzyskiwaniu. Ta sekcja zawiera podsumowanie wniosków na podstawie doświadczeń z ransomware w ostatnim roku.

93%

badań przeprowadzonych przez Microsoft w ramach odzyskiwania po atakach ransomware wykazało niewystarczającą kontrolę uprawnień dostępu i penetracji sieci.

Incydenty związane z ransomware i odzyskiwaniem danych według branż

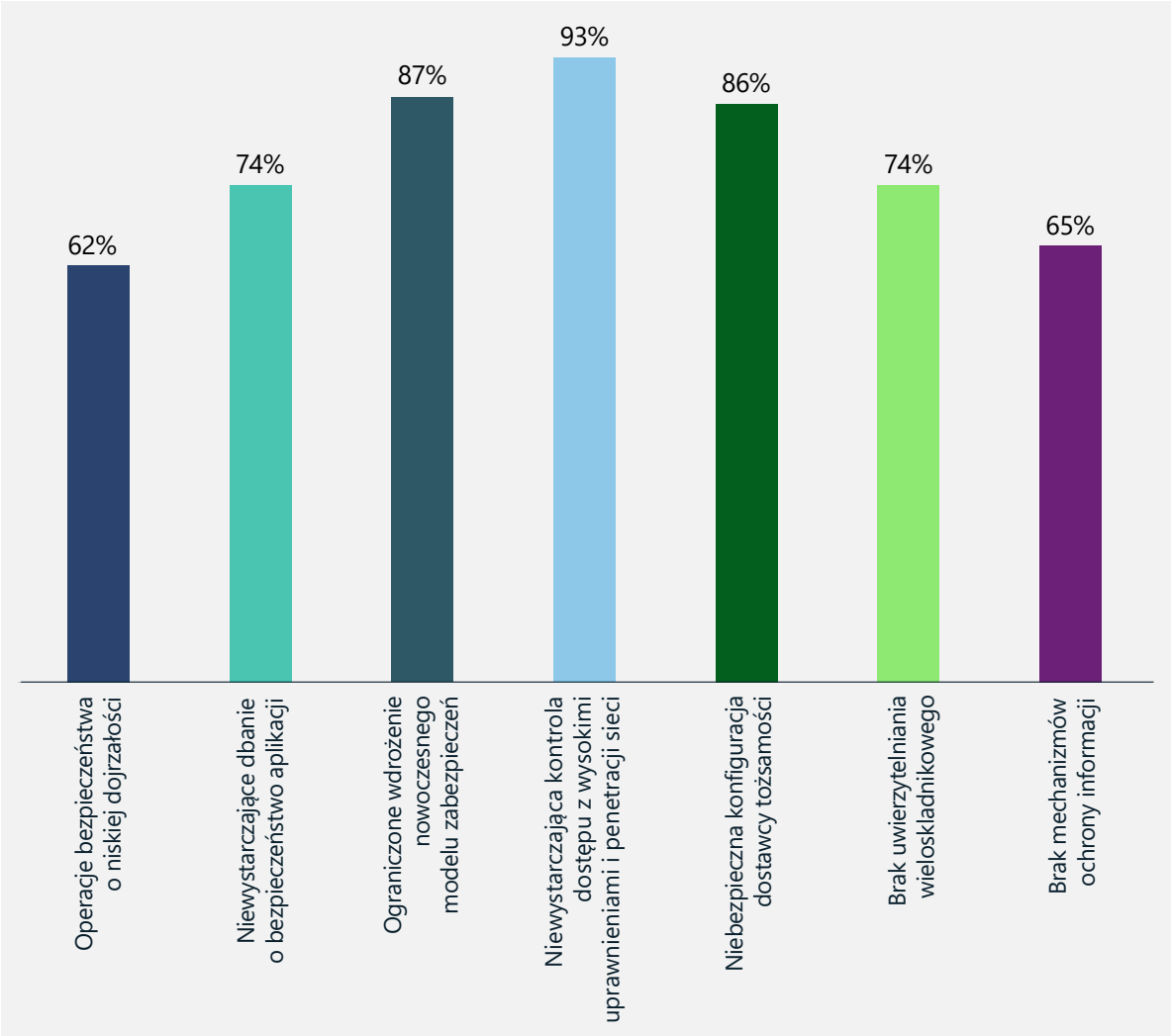


Ponieważ powstają nowe, małe grupy, zespoły ds. bezpieczeństwa muszą być świadome ewoluujących zagrożeń ransomware, a jednocześnie bronić się przed wcześniej nieznanymi rodzinami oprogramowania ransomware. Podejście szybkiego rozwoju stosowane przez grupy przestępcze doprowadziło do stworzenia inteligentnego oprogramowania ransomware spakowanego w łatwe do użycia zestawy. Pozwala to na większą elastyczność w przeprowadzaniu rozległych ataków na większą liczbę celów.

Na kolejnych stronach przedstawiono głębsze spojrzenie na najczęściej obserwowane czynniki przyczyniające się do słabej ochrony przed ransomware, pogrupowane w trzy kategorie ustaleń:

1. Słaba kontrola tożsamości
2. Nieefektywne operacje bezpieczeństwa
3. Ograniczona ochrona danych

Podsumowanie najczęstszych ustaleń dotyczących reakcji na ransomware



Najczęstszym wnioskiem z incydentów ransomware była niewystarczająca kontrola uprawnień dostępu i penetracji sieci.

Oprogramowanie wymuszające okup: relacje osób z pierwszej linii

(c.d.)

Trzy główne czynniki przyczyniające się, które obserwujemy u ofiar:

① **Słaba kontrola tożsamości:** Ataki polegające na kradzieży poświadczeń pozostają jednym z głównych czynników przyczyniających się

② **Nieefektywne operacje bezpieczeństwa** nie tylko stanowią okazję dla atakujących, ale mają znaczący wpływ na czas odzyskiwania.

③ Wszystko sprowadza się do danych — organizacje mają trudności z wdrożeniem skutecznej **strategii ochrony danych** odpowiadającej ich potrzebom biznesowym.

① Słaba kontrola tożsamości

Ransomware obsługiwany przez człowieka nadal ewoluuje i wykorzystuje metody kradzieży poświadczeń oraz penetracji sieci, które są tradycyjnie związane z atakami ukierunkowanymi. Udane ataki są często wynikiem długotrwałych kampanii naruszania systemów tożsamości takich jak Active Directory (AD), które pozwalają ludziom-operatorom na kradzież poświadczeń, dostęp do systemów i utrzymywanie się w naruszonych sieciach.

Zabezpieczenia Azure AD i Active Directory (AD)

88%

klientów, których dotyczy problem, nie zastosowało najlepszych rozwiązań w zakresie bezpieczeństwa AD i Azure AD. Stało się to powszechnym wektorem ataku — napastnicy wykorzystują błędne konfiguracje i słabsze zabezpieczenia w krytycznych systemach tożsamości, aby uzyskać szerszy dostęp.

Przyznawanie dostępu z minimalnymi uprawnieniami i korzystanie ze stacji roboczych o dostępie uprzywilejowanym (PAW)

Żadna ze skutecznie zaatakowanych organizacji nie wdrożyła odpowiedniej segregacji poświadczeń administracyjnych ani zasady przyznawania dostępu z minimalnymi uprawnieniami za pośrednictwem dedykowanych stacji roboczych w swoich krytycznych zasobach tożsamości i o wysokiej wartości, takich jak systemy zastrzeżone i aplikacje krytyczne.

Bezpieczeństwo kont z wysokimi uprawnieniami

88%

W większości przypadków dla kont wrażliwych i z wysokimi uprawieniami nie wdrożono uwierzytelniania wieloskładnikowego, co pozostawiało lukę w zabezpieczeniach, która umożliwiała napastnikom przechwytywanie prawdziwych poświadczeń i przeprowadzanie dalszych ataków z ich użyciem.

84%

Administratorzy w 84% organizacji nie stosowali mechanizmów kontroli kont administratorów, takich jak dostęp „just-in-time”, co pozwoliłoby zapobiec wrogiemu wykorzystaniu tego typu kont po ewentualnym przejęciu.

Oprogramowanie wymuszające okup: relacje osób z pierwszej linii

(c.d.)

② Nieefektywne operacje bezpieczeństwa

Z naszych danych wynika, że organizacje, które ucierpiały w wyniku ataków ransomware, miały znaczące luki w operacjach bezpieczeństwa, narzędziach i zarządzaniu cyklem życia zasobów informatycznych. Zaobserwowano następujące braki:

Stosowanie poprawek:

68%

skutecznie zaatakowanych organizacji nie miało efektywnego procesu zarządzania lukami i poprawkami, a duża zależność od procesów ręcznych w porównaniu do automatycznego stosowania poprawek doprowadziła do powstania krytycznych luk bezpieczeństwa. Branża produkcyjna i infrastruktura krytyczna nadal borykają się z problemem konserwacji i stosowania poprawek względem starszych systemów OT (technologii operacyjnych).

Brak narzędzi do operacji bezpieczeństwa:

Większość organizacji zgłosiła brak kompleksowej widoczności bezpieczeństwa z powodu braku lub błędnej konfiguracji narzędzi zabezpieczających, co prowadziło do spadku skuteczności wykrywania i reagowania.

60%

organizacji zgłosiło, że nie korzysta z narzędzi EDR[6], czyli podstawowej technologii służącej do wykrywania i reagowania.

60%

organizacji nie zainwestowało w technologię SIEM (Zarządzanie informacjami i zdarzeniami zabezpieczeń), co doprowadziło do powstania barier między odrębnymi systemami monitorowania, ograniczonej zdolności do kompleksowego wykrywania zagrożeń i nieefektywnych operacji bezpieczeństwa. Automatyzacja pozostaje kluczową luką w narzędziach i procesach SOC, co zmusza ich pracowników do spędzania niezliczonych godzin na analizowaniu telemetrii zabezpieczeń.

84%

dotkniętych organizacji nie umożliwiło integracji swoich środowisk wielochmurowych z narzędziami do operacji bezpieczeństwa.

Procesy reagowania i odzyskiwania:

76%

Brak skutecznego planu reagowania stanowił krytyczny problem w 76% dotkniętych organizacji, przez co nie było odpowiedniej gotowości organizacyjnej na kryzys, a czas reakcji i powrotu do sprawności był długi.

③ Ograniczona ochrona danych

Wiele skutecznie zaatakowanych organizacji nie miało odpowiednich procesów ochrony danych, co poważnie wpływało na czas odzyskiwania i przywracanie operacji biznesowych. Do najczęściej spotykanych braków należały:

Niezmienialna kopia zapasowa:

44%

organizacji nie miało niezmienialnych kopii zapasowych dotkniętych systemów. Dane pokazują również, że administratorzy nie mieli kopii zapasowych ani planów odzyskiwania danych dla krytycznych zasobów takich jak AD.

Ochrona przed utratą danych:

Atakujący zazwyczaj znajdują drogę do naruszania systemów przez wykorzystanie luk w organizacji, eksfiltrując krytyczne dane w celu wymuszenia, kradzieży własności intelektualnej lub zarobku.

92%

dotkniętych organizacji nie wdrożyło skutecznych mechanizmów zapobiegania utracie danych w celu ograniczenia tego ryzyka, co doprowadziło do utraty krytycznych danych.

Liczba przypadków ransomware w niektórych regionach spadła, a w innych wzrosła

W tym roku zaobserwowaliśmy spadek ogólnej liczby przypadków ransomware zgłoszonych do naszych zespołów reagowania w Ameryce Północnej i Europie w porównaniu z rokiem poprzednim. Jednocześnie wzrosła liczba przypadków zgłoszonych w Ameryce Łacińskiej.

Jedną z interpretacji jest to, że cyberprzestępcy odeszli od obszarów postrzeganych jako obarczone wyższym ryzykiem wywołania reakcji organów ścigania na rzecz bardziej „miękkich" celów. Ponieważ Microsoft nie zaobserwował znaczącej poprawy zabezpieczeń sieci przedsiębiorstw na całym świecie, najbardziej prawdopodobnym wyjaśnieniem spadku zgłoszeń związanych z ransomware jest nałożenie się działań organów ścigania w 2021 i 2022 r., które zwiększyły koszty działalności przestępczej, oraz wydarzeń geopolitycznych z 2022 r.

Jedna z największych operacji RaaS została przeprowadzona przez rosyjskojęzyczną grupę przestępczą REvil (zwaną również Sodinokibi), która jest aktywna od 2019 r. W październiku 2021 r. serwery REvil zostały zamknięte wskutek międzynarodowej operacji organów ścigania GoldDust[7]. W styczniu 2022 r. Rosja aresztowała 14 domniemanych członków REvil i przeprowadziła nalot na 25 miejsc z nimi związanych[8]. Był to pierwszy raz, gdy Rosja podjęła działania przeciwko operatorom ransomware na swoim terytorium.

Chociaż działania organów ścigania prawdopodobnie zmniejszyły częstotliwość ataków w 2022 r., przestępcy mogą opracować nowe strategie, aby uniknąć złapania w przyszłości. Ponadto napięcie między Rosją a Stanami Zjednoczonymi w związku z inwazją Rosji na Ukrainę położyło kres rodzącej się współpracy Rosji w globalnej walce z ransomware. Po krótkim okresie niepewności po aresztowaniu REvil Stany Zjednoczone i Rosja zaprzestały współpracy w ściganiu przestępców zajmujących się ransomware — cyberprzestępcy mogą ponownie postrzegać Rosję jako „bezpieczną przystań".

Przewidujemy, że intensywność ataków ransomware będzie zależeć od kilku kluczowych aspektów:

1. Czy rządy podejmą działania przeciwko grupom ransomware operującym na ich terytorium, a także grupom z zagranicy?
2. Czy grupy zajmujące się ransomware zmienią taktykę — wyeliminują potrzebę stosowania modelu ransomware i będą uciekać się do samych wymuszeń?
3. Czy organizacje będą w stanie modernizować i przekształcać swoje operacje IT szybciej niż przestępcy będą wykorzystywać luki?
4. Czy postępy w śledzeniu i namierzaniu płatności okupów zmuszą odbiorców okupów do zmiany taktyki i sposobów negocjacji?

Chociaż działania organów ścigania prawdopodobnie zmniejszyły częstotliwość ataków w 2022 r., przestępcy mogą opracować nowe strategie, aby uniknąć złapania w przyszłości.

2x

Liczba ataków ransomware spadła w niektórych regionach, ale żądania okupu wzrosły ponad dwukrotnie.

Praktyczne wskazówki

1. Wszystkie rodziny oprogramowania ransomware wykorzystują te same słabości zabezpieczeń, a więc należy skoncentrować się na kompleksowych strategiach bezpieczeństwa.
2. Aktualizuj i utrzymuj podstawy zabezpieczeń w celu zwiększenia podstawowego poziomu ochrony dogłębnej i modernizacji operacji bezpieczeństwa. Przejście do chmury pozwala na szybsze wykrywanie zagrożeń i szybszą reakcję.

Linki do dalszych informacji

- Chroń swoją organizację przed ransomware | Microsoft Security
- 7 sposobów, aby chronić środowisko przed zagrożeniami | Blog Microsoft Security
- Poprawa ochrony opartej na AI w celu przeciwdziałania ransomware obsługiwanemu przez człowieka | Microsoft 365 Defender Research Team
- Security Insider: Zapoznaj się z snajnowszymi spostrzeżeniami i aktualnościami dotyczącymi cyberbezpieczeństwa | Microsoft Security

Cyberprzestępczość jako usługa

Cyberprzestępczość jako usługa (CaaS) jest rosnącym i ewoluującym zagrożeniem na całym świecie. Microsoft Digital Crimes Unit (DCU) Microsoft zaobserwował ciągły rozwój ekosystemu CaaS z rosnącą liczbą usług online ułatwiających popełnianie różnych cyberprzestępstw, w tym BEC i ransomware obsługiwanego przez człowieka. Wyłudzanie informacji jest nadal preferowaną metodą ataku. Udana kradzież i sprzedaż dostępu do wykradzionych kont jest dla cyberprzestępców bardzo zyskowna.

W odpowiedzi na rozwijający się rynek CaaS, DCU usprawnił używane systemy nasłuchu, aby wykrywać i identyfikować oferty CaaS w całym ekosystemie — w Internecie, deep web, forach z weryfikacją[9], dedykowanych witrynach internetowych, internetowych forach dyskusyjnych i platformach komunikacyjnych.

Cyberprzestępcy współpracują obecnie ponad strefami czasowymi i językami. Na przykład jedna z witryn CaaS administrowana przez osobę z Azji prowadzi działalność w Europie, a w Afryce tworzy złośliwe konta. Wielojurysdykcyjny charakter tych operacji stanowi złożone wyzwanie dla prawa i jego egzekwowania. W odpowiedzi DCU koncentruje swoje wysiłki na wyłączaniu złośliwej infrastruktury przestępczej wykorzystywanej do ataków CaaS oraz współpracuje z organami ścigania na całym świecie, by pociągnąć przestępców do odpowiedzialności.

Cyberprzestępcy coraz częściej wykorzystują analitykę do maksymalizacji zasięgu i zakresu operacji oraz zysków. Podobnie jak legalne firmy witryny CaaS muszą zapewnić wiarygodność i reputację „produktów i usług". Na przykład witryny CaaS zazwyczaj automatyzują dostęp do przejętych kont, aby udowodnić poprawność wykradzionych poświadczeń. Cyberprzestępcy zaprzestają sprzedaży konkretnych kont, gdy hasła zostaną zresetowane albo luki usunięte aktualizacjami. Coraz częściej witryny CaaS umożliwiają „kupującym" weryfikację na żądanie w ramach „gwarancji jakości". W rezultacie „kupujący" mogą mieć pewność, że witryna CaaS sprzedaje aktywne konta i hasła. Zmniejsza to również potencjalne koszty ponoszone przez sprzedawcę CaaS, jeśli skradzione poświadczenia zostaną zmienione przed sprzedażą.

DCU zaobserwował również witryny CaaS oferujące nabywcom możliwość zakupu przejętych kont z określonych lokalizacji geograficznych, wyznaczonych dostawców usług online czy konkretnie wybranych osób, zawodów i branż. Często zamawiane są konta specjalistów lub działów, które przetwarzają faktury (np. CFO czy „rozrachunki z odbiorcami"). Celami również są branże uczestniczące w zamówieniach publicznych ze względu na ilość informacji udostępnianych w ramach przetargów.

Badania DCU dotyczące CaaS ujawniły kilka kluczowych trendów:

Rośnie liczba i stopień zaawansowania „usług".

Jednym z przykładów jest ewolucja powłok internetowych, które zazwyczaj składają się z naruszonych serwerów www wykorzystywanych do automatyzowania ataków wyłudzania informacji. DCU zaobserwował, że odsprzedawcy CaaS upraszczają przesyłanie zestawów do wyłudzania informacji lub złośliwego oprogramowania przez specjalistyczne pulpity zarządcze www. Sprzedawcy CaaS często próbują następnie sprzedać przestępcy dodatkowe usługi za pośrednictwem pulpitu zarządczego, takie jak usługi wysyłania wiadomości spam czy wyselekcjonowane listy odbiorców spamu oparte na zdefiniowanych atrybutach, np. lokalizacji geograficznej czy zawodzie. W niektórych przypadkach zaobserwowaliśmy, że pojedyncza powłoka internetowa jest wykorzystywana w wielu kampaniach ataku, co sugeruje, że przestępcy mogą stale utrzymywać się na naruszonym serwerze. Zaobserwowaliśmy również wzrost usług anonimizacji dostępnych w ekosystemie CaaS, a także oferty kont VPN (wirtualnych sieci prywatnych) i VPS (wirtualnych serwerów prywatnych). W większości przypadków oferowane VPN/VPS były początkowo nabywane za pomocą skradzionych kart kredytowych. Witryny CaaS oferowały również coraz więcej usług RDP, SSH i cPanel do wykorzystania jako platformy organizowania cyberataków. Sprzedawcy CaaS konfigurują RDP, SSH i cPanel za pomocą odpowiednich narzędzi i skryptów, aby ułatwić różnego rodzaju cyberataki.

Usługi tworzenia domen homoglificznych coraz częściej wymagają płatności w kryptowalutach.

Domeny homoglificzne są podobne do nazw oryginalnych domen — wykorzystują znaki, które wyglądają identyczne lub prawie identyczne. Celem jest oszukanie użytkownika, aby myślał, że domena homoglificzna jest prawdziwa. Domeny te są wszechobecnym zagrożeniem i umożliwiają wiele cyberprzestępstw. Witryny CaaS sprzedają teraz niestandardowe nazwy domen homoglificznych. Kupujący mogą podać konkretną nazwę firmy lub domeny, pod którą chcą się podszyć. Po otrzymaniu płatności sprzedawcy CaaS za pomocą generatora homoglifów wybierają nazwę domeny, a następnie rejestrują ten złośliwy homoglif. Płatność odbywa się niemal wyłącznie w kryptowalutach.

2 750 000

rejestracji witryn internetowych zostało skutecznie zablokowanych w tym roku przez DCU, co pozwoliło uprzedzić atakujących planujących ich wykorzystanie do przestępstw na całym świecie.

Cyberprzestępczość jako usługa

(c.d.)

Sprzedawcy CaaS coraz częściej oferują zakup wykradzionych poświadczeń.

Wykradzione poświadczenia umożliwiają nieautoryzowany dostęp do kont użytkowników, w tym do usług e-mail, zasobów udostępniania plików przedsiębiorstwa czy OneDrive dla firm. Jeśli poświadczenia administratora zostaną wykradzione, nieautoryzowani użytkownicy mogą uzyskać dostęp do poufnych plików, zasobów Azure czy firmowych kont użytkowników. W wielu badaniach obserwowaliśmy automatyzację weryfikowania poświadczeń poprzez nieautoryzowane użycie tego samego poświadczenia na wielu serwerach. Ten schemat działania sugeruje, że skutecznie zaatakowany użytkownik mógł być ofiarą wielokrotnych ataków wyłudzania informacji lub mieć na swoim urządzeniu złośliwe oprogramowanie umożliwiające zbieranie poświadczeń rejestratorom klawiszy (keyloggers) działającym w sieci botnet.

Pojawiają się „usługi i produkty" CaaS z rozszerzonymi funkcjami pozwalającymi na uniknięcie wykrycia.

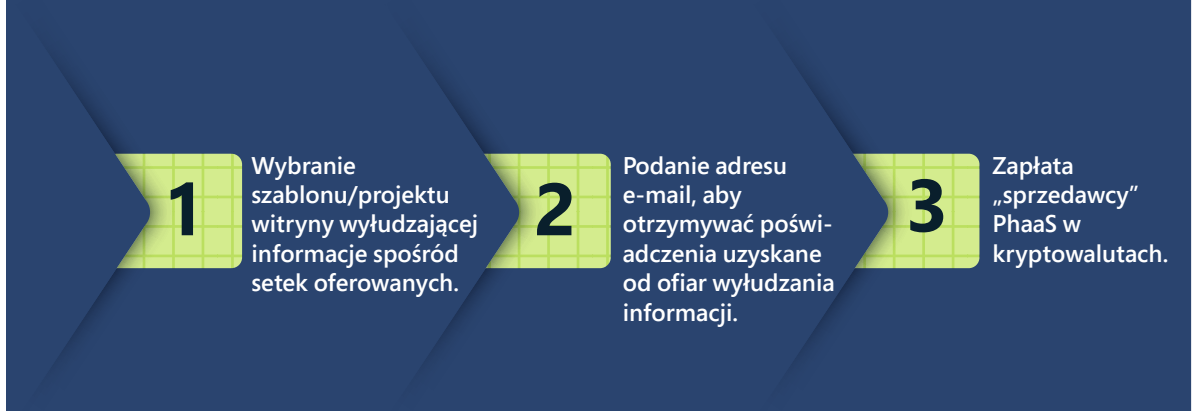
Jeden ze sprzedawców CaaS oferuje zaawansowane zestawy do wyłudzania informacji z funkcjami anonimizacji umożliwiające obchodzenie systemów wykrywania i zapobiegania. Cena to tylko 6 USD dziennie. Usługa oferuje serię przekierowań, które dokonują inteligentnych sprawdzeń przed przejściem do następnej warstwy lub kolejnego zasobu. Przykładem jest ponad 90 sprawdzeń identyfikujących unikalną charakterystykę urządzenia, w tym czy jest to maszyna wirtualna oraz szczegóły przeglądarki i sprzętu. Jeśli wszystkie sprawdzenia przejdą pomyślnie, ruch jest wysyłany do strony docelowej używanej do wyłudzania informacji.

Cyberprzestępcy oferujący kompleksowe usługi sprzedają abonamenty na usługi zarządzane.

Zazwyczaj każdy etap popełniania przestępstwa internetowego może zdemaskować przestępców. Ryzyko ich ujawnienia i zidentyfikowania wzrasta, jeśli usługi są kupowane z wielu witryn CaaS. DCU zaobserwował niepokojący trend w dark web polegający na wzroście liczby usług oferujących anonimizację kodu oprogramowania i generalizację tekstu strony internetowej w celu zmniejszenia możliwości tego typu identyfikacji. Dostawcy kompleksowych usług cyberprzestępczości w modelu subskrypcyjnym zarządzają wszystkimi usługami i gwarantują konkretne wyniki, co dodatkowo zmniejsza ryzyko zidentyfikowania kupującego. Zmniejszone ryzyko spowodowało wzrost popularności tych kompleksowych usług.

Jednym z przykładów kompleksowej usługi cyberprzestępczej jest wyłudzanie informacji jako usługa (PhaaS). PhaaS stanowi ewolucję wcześniejszych usług znanych jako usługi w pełni niewykrywalne (FUD) i jest oferowany w subskrypcji. Typowa oferta PhaaS obejmuje utrzymywanie przez miesiąc aktywnych witryn wyłudzania informacji.

Cyberprzestępcy PhaaS oferują wiele usług w jednym abonamencie. Nabywca musi podjąć tylko trzy działania:



Po wykonaniu tych kroków sprzedawca PhaaS tworzy usługi z trzema lub czterema warstwami przekierowań zawierające zasoby hostingowe pod kątem konkretnych ofiar. Kampania jest rozpoczynana, a poświadczenia ofiar są zbierane, weryfikowane i wysyłane na e-mail podany przez kupującego. Za specjalną opłatą wielu sprzedawców PhaaS oferuje hostowanie stron wyłudzających informacje na publicznym blockchainie, dzięki czemu można uzyskiwać do nich dostęp za pomocą dowolnej przeglądarki, a przekierowania mogą prowadzić użytkowników do zasobów w księdze rozproszonej (distributed ledger).

DCU zidentyfikował również sprzedawcę CaaS oferującego ataki DDoS w subskrypcji. W tym modelu tworzenie i utrzymywanie botnetu niezbędnego do przeprowadzania ataków jest po stronie sprzedawcy CaaS. Każdy subskrybent DDoS otrzymuje szyfrowaną usługę zwiększającą bezpieczeństwo operacyjne oraz rok całodobowego wsparcia. Usługa subskrypcji DDoS oferuje różne architektury i metody ataku, więc nabywca jedynie wybiera zasób do zaatakowania, a sprzedawca zapewnia dostęp do szeregu naruszonych urządzeń w swoim botnecie w celu przeprowadzenia ataku. Koszt susbskrypcji DDoS to zaledwie 500 USD.

Trwają prace DCU nad opracowaniem narzędzi i technik, które będą identyfikować i zakłócać działania cyberprzestępców CaaS. Ewolucja usług CaaS wiąże się z poważnymi wyzwaniami, np. jak przeciwdziałać płatnościom w kryptowalutach.

Przestępcze wykorzystanie kryptowalut

W miarę jak kryptowaluty wchodzą do głównego nurtu, atakujący coraz częściej wykorzystują je do unikania organów ścigania i przepisów dotyczących przeciwdziałania praniu pieniędzy (AML). Utrudnia to śledzenie płatności cyberprzestępców przez organy ścigania.

Światowe wydatki na rozwiązania blockchain wzrosły o około 340% w ciągu ostatnich czterech lat, podczas gdy nowe portfele kryptowalutowe wzrosły o około 270%. Na świecie istnieje ponad 83 miliony unikalnych portfeli, a łączna kapitalizacja rynkowa wszystkich kryptowalut wynosiła 28 lipca 2022 r. około 1,1 biliona USD[10].

Źródło: Twitter.com — @PeckShieldAlert (PeckShield to chińska firma zajmująca się bezpieczeństwem blockchain).

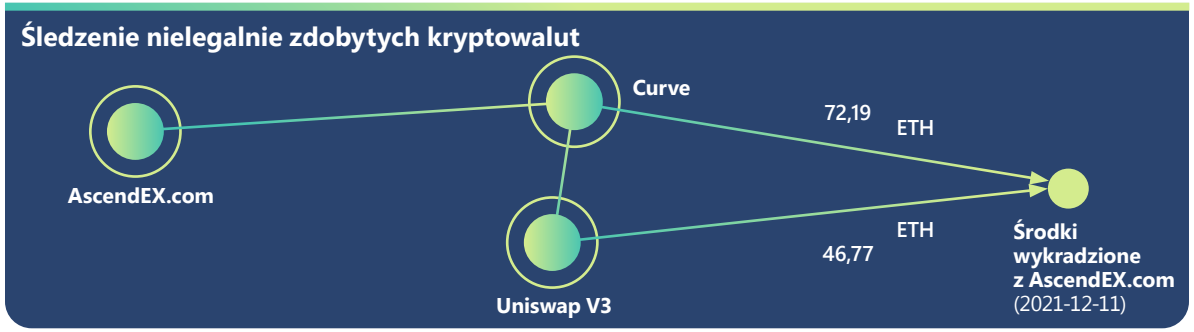
Śledzenie płatności za ransomware

Ransomware jest jednym z największych źródeł nielegalnie zdobywanych kryptowalut. W ramach przeciwdziałania infrastrukturze technicznej wykorzystywanej przez przestępców w atakach ransomware (przykładem jest zakłócenie działania Zloader w kwietniu 2022 r.[11]) DCU Microsoft śledzi portfele przestępców, aby umożliwić odzyskiwanie kryptowalut.

Śledczy DCU zaobserwowali, że przestępcy ransomware modyfikują swoje taktyki komunikacji z ofiarami w celu ukrycia ścieżki przepływu pieniędzy. Początkowo cyberprzestępcy umieszczali adresy Bitcoin w informacjach o okupie. Ułatwiło to jednak śledzenie transakcji płatniczych w blockchain, więc przestali oni dołączać adresy portfeli, a zamiast tego dołączali adresy e-mail lub linki do witryn czatu. Dopiero tam przekazywali adresy płatności ofiarom okupu. Niektórzy tworzyli nawet unikalne witryny internetowe i loginy dla każdej ofiary, aby uniemożliwić badaczom bezpieczeństwa i organom ścigania uzyskanie adresów portfeli przestępców przez udawanie ofiar. Pomimo wysiłków przestępców, aby ukryć ślady, niektóre płatności okupu mogą być odzyskane dzięki współpracy z organami ścigania i firmami zajmującymi się analizą kryptowalut, które śledzą ruch w blockchain.

Trendy: Pranie nielegalnych pieniędzy przez giełdy DEX

Kluczowym problemem dla cyberprzestępców jest konwersja kryptowalut na walutę fiducjarną. Mają oni kilka potencjalnych dróg konwersji. Każda niesie inny stopień ryzyka. Jedną z metod stosowanych w celu zmniejszenia ryzyka jest pranie wpływów przez zdecentralizowaną giełdę (DEX), a następnie dokonywanie wypłaty w różny sposób, np. przez giełdę scentralizowaną (CEX) czy peer-to-peer (P2P) albo w ramach obrotu pozagiełdowego (OTC). DEX to atrakcyjne platformy do prania pieniędzy, ponieważ często nie stosują zaleceń AML.



Korzystając z narzędzia do analizy kryptowalut Chainalysis, DCU Microsoft odkrył, że hakerzy AcendEX oprócz Uniswap wymienili skradzione środki w mniejszym DEX o nazwie Curve. Ten diagram ilustruje odkryte przez zespół ścieżki prania. Każde koło reprezentuje klaster portfeli, a liczby w każdej linii reprezentują całkowitą ilość Ethereum przekazaną w ramach prania.

W grudniu 2021 r. hakerzy zaatakowali globalną platformę handlu kryptowalutami AscendEx, kradnąc około 77,7 mln USD w kryptowalutach należących do jej klientów[12]. AscendEx zatrudnił firmy analityczne blockchain i zwrócił się do innych CEX, aby portfele otrzymujące skradzione środki trafiały na czarną listę. Ponadto adresy, na które zostały wysłane środki, zostały specjalnie oznaczone w eksploratorze blockchain sieci Ethereum (Etherscan)[13]. W celu obejścia ostrzeżeń i czarnej listy 18 lutego 2022 r. hakerzy wysłali 1,5 mln USD w Ethereum na Uniswap, jeden z największych na świecie DEX[14].

Przyjęcie ściślejszych zaleceń AML przez giełdy DEX mogłoby ograniczyć pranie pieniędzy na ich platformach i zmusić cyberprzestępców do korzystania z innych metod maskowania, takich jak „miksowanie kryptowalut" (coin tumbling) czy nielicencjonowane giełdy. Na przykład Uniswap niedawno ogłosił, że zacznie używać czarnych list do uniemożliwiania transakcji portfelom zaangażowanym w nielegalną działalność[15].

Praktyczne wskazówki

1. Jeśli jesteś ofiarą cyberprzestępstwa, która zapłaciła przestępcy kryptowalutą, skontaktuj się z lokalnymi organami ścigania, które mogą prześledzić i odzyskać utracone środki.
2. Wybierając DEX, zapoznaj się z zaleceniami ALM.

Linki do dalszych informacji

- Sprzętowa ochrona przed coraz bardziej zaawansowanymi atakami kopania kryptowalut | Microsoft 365 Defender Research Team

Ewoluujący krajobraz ataków wyłudzania informacji

Wyłudzanie informacji (phishing), w tym głównie poświadczeń, przybiera na sile i stanowi istotne zagrożenie dla użytkowników na całym świecie. Celem tego typu kampanii są wszystkie skrzynki pocztowe. Wśród zagrożeń, które nasi badacze śledzą i przed którymi chronią, liczba ataków wyłudzania informacji jest o rzędy wielkości większa niż wszystkich innych zagrożeń.

W danych z Ochrony usługi Office w usłudze Defender obserwujemy aktywność związaną ze złośliwymi wiadomościami e-mail i wykradzionymi tożsamościami. Azure Active Directory Identity Protection dostarcza jeszcze więcej informacji dzięki alertom o wykradzionych tożsamościach. W ramach Defender for Cloud Apps obserwujemy uzyskiwanie dostępu do danych z użyciem wykradzionych tożsamości. Microsoft 365 Defender (M365D) zapewnia korelację międzyproduktową. Dane dotyczące penetracji sieci pochodzą z Ochrony punktu końcowego w usłudze Microsoft Defender (alerty i zdarzenia dotyczące ataku), Ochrony usługi Office w usłudze Defender (złośliwe wiadomości e-mail) i Microsoft 365 Defender (korelacja między produktami).

710 mln

wiadomości e-mail wyłudzających informacje blokowanych tygodniowo.

1 godz. 12 min

Mediana czasu potrzebnego atakującemu na uzyskanie dostępu do Twoich prywatnych danych, jeśli padniesz ofiarą e-maila wyłudzającego informacje[16].

1 godz. 42 min

Średni czas, po którym atakujący zaczyna penetrować sieć przedsiębiorstwa po włamaniu się do urządzenia[17].

Poświadczenia Microsoft 365 pozostają jednym z najbardziej poszukiwanych przez atakujących typów kont. Używając wykradzionych poświadczeń, przestępcy mogą zalogować się do systemów komputerowych powiązanych z firmą, aby ułatwić infekcję złośliwym oprogramowaniem i ransomware, wykraść poufne dane firmowe przez uzyskanie dostępu do plików SharePoint, a także m.in. rozpowszechniać atak dalej przez wysyłanie dodatkowych złośliwych wiadomości e-mail przy użyciu Outlook.

Oprócz szerokich kampanii wyłudzania poświadczeń, darowizn i danych osobowych, atakujący wybierają konkretne firmy, by zwiększyć zyski. E-mailowe ataki wyłudzania informacji na firmy w celu uzyskania korzyści finansowych są wspólnie określane jako ataki BEC.

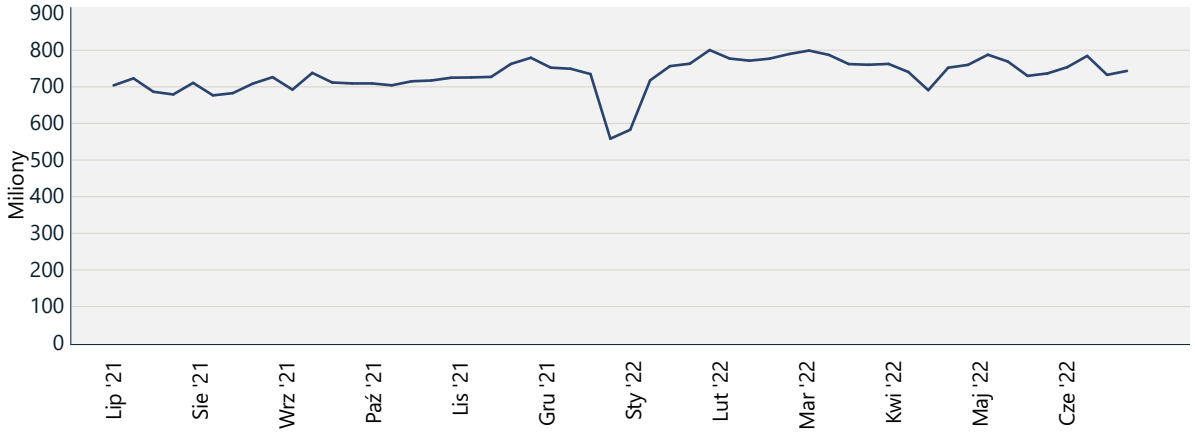
Microsoft co miesiąc wykrywa miliony e-maili BEC, co odpowiada 0,6% wszystkich zaobserwowanych e-maili wyłudzających informacje. Raport IC3[18] opublikowany w maju 2022 r. wskazuje na tendencję wzrostową strat spowodowanych atakami BEC.

Techniki stosowane w atakach wyłudzania informacji są coraz bardziej złożone. W odpowiedzi na środki zaradcze atakujący zwiększają złożoność tego, jak i gdzie hostują infrastrukturę operacyjną kampanii. Oznacza to, że organizacje muszą regularnie modyfikować swoją strategię rozwiązań bezpieczeństwa tak, aby blokować złośliwe wiadomości e-mail i wzmacniać kontrolę dostępu do poszczególnych kont użytkowników.

531 000

Oprócz adresów URL zablokowanych przez Ochronę usługi Office w usłudze Defender nasz DCU usunął 531 000 unikalnych adresów URL służących do wyłudzania informacji hostowanych poza Microsoft.

Wykryte e-maile wyłudzające informacje



Liczba wykrytych ataków wyłudzania informacji nadal rośnie. Spadek na przełomie grudnia i stycznia to oczekiwany spadek sezonowy, odnotowany również w ubiegłorocznym raporcie. Źródło: „Exchange Online Protection signals".

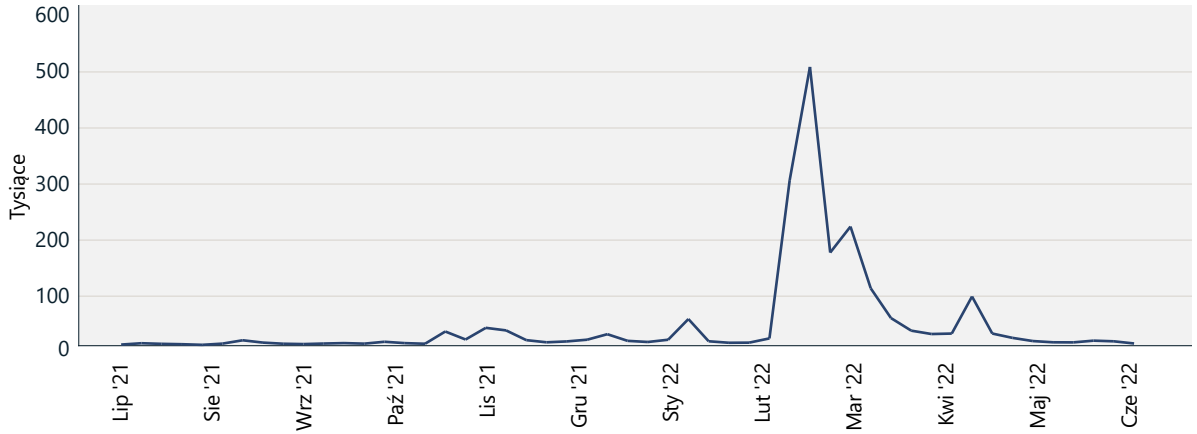
Ewoluujący krajobraz ataków wyłudzania informacji

(c.d.)

Nadal obserwujemy stały wzrost liczby e-maili wyłudzających informacje. W związku z przejściem na pracę zdalną w latach 2020 i 2021 nastąpił znaczny wzrost liczby ataków wyłudzania informacji mających na celu wykorzystanie zmieniającego się środowiska pracy. Operatorzy ataków wyłudzania informacji szybko wprowadzają nowe szablony e-maili, wykorzystując przynęty związane z ważnymi wydarzeniami na świecie, takimi jak pandemia COVID-19, oraz tematy związane z narzędziami do współpracy i zwiększającymi produktywność, takimi jak Google Drive czy OneDrive do udostępniania plików. Liczba tematów COVID-19 zmniejszyła się, jednak od początku marca 2022 r. wojna na Ukrainie stała się nową przynętą. Nasi badacze zaobserwowali ogromny wzrost liczby e-maili podszywających się pod legalne organizacje, które zabiegały o darowizny kryptowalutowe w Bitcoin i Ethereum rzekomo na sparcie obywateli Ukrainy.

Zaledwie kilka dni po rozpoczęciu wojny na Ukrainie, pod koniec lutego 2022 r., liczba wykrytych e-maili wyłudzających informacje, zawierających adresy Ethereum, odbieranych w przedsiębiorstwach gwałtownie wzrosła. Całkowita liczba przypadków osiągnęła szczyt w pierwszym tygodniu marca, gdy pół miliona e-maili wyłudzających informacje zawierało adres portfela Ethereum. Przed wojną wykrywano znacznie mniej e-maili wyłudzających informacje z adresami portfeli Ethereum (średnio kilka tysięcy e-maili dziennie).

E-maile wyłudzające informacje z adresami portfela Ethereum



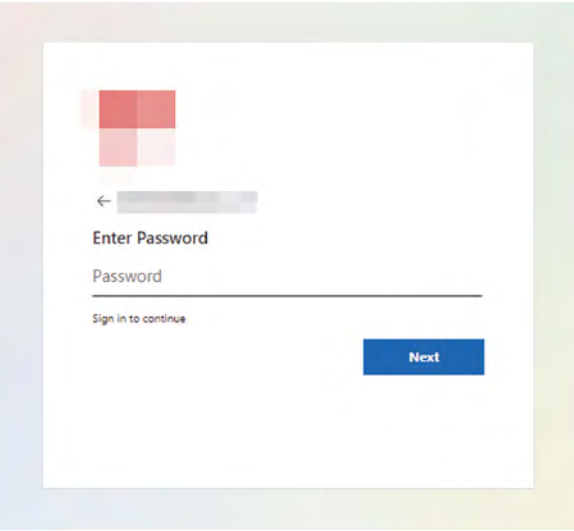
Całkowita liczba e-maili wykrytych jako wyłudzanie informacji, zawierających adresy portfeli Ethereum wzrosła na początku konfliktu ukraińsko-rosyjskiego, a następnie spadała.

Częściej niż wcześniej wyłudzanie informacji działa na legalnej infrastrukturze, aby atakujący nie musieli kupować, wynajmować lub obsługiwać własnej. Sprzyja to wzrostowi liczby kampanii tego typu. Na przykład złośliwe wiadomości e-mail mogą pochodzić z przejętych kont nadawców. Atakujący korzystają z tych adresów e-mail, które mają wyższy wskaźnik reputacji i są postrzegane jako bardziej godne zaufania niż nowo utworzone konta i domeny. W niektórych, bardziej zaawansowanych kampaniach wyłudzania informacji zaobserwowaliśmy, że atakujący preferują wysyłkę z domen, które mają nieprawidłowo ustawiony parametr DMARC[19] na zasadę „no action", co otwiera drzwi dla fałszowania e-maili.

W operacjach wyłudzania informacji na dużą skalę częściej wykorzystywane są usługi chmurowe i maszyny wirtualne w chmurze (VM). Atakujący mogą w pełni zautomatyzować proces wdrażania i dostarczania wiadomości e-mail z maszyn wirtualnych przy użyciu przekaźników poczty SMTP lub infrastruktury poczty e-mail w chmurze, aby skorzystać z wysokich wskaźników dostarczalności i pozytywnej reputacji tych legalnych usług. Jeśli złośliwe wiadomości e-mail mogą być wysyłane za pośrednictwem tych usług w chmurze, obrońcy muszą polegać na silnych możliwościach filtrowania wiadomości e-mail, by zablokować wiadomości e-mail przed wejściem do ich środowiska.

Konta Microsoft pozostają głównym celem operatorów wyłudzania informacji, o czym świadczą liczne strony docelowe podszywające się pod witrynę logowania Microsoft 365. Na przykład próbują oni dopasować się do wyglądu środowiska logowania Microsoft poprzez wygenerowanie unikalnego adresu URL dostosowanego do odbiorcy. Ten adres URL przekierowuje na złośliwą witrynę opracowaną w celu zbierania poświadczeń, przy czym parametr w adresie URL zawiera adres e-mail konkretnego odbiorcy. Gdy użytkownik przejdzie na stronę, zestaw wyłudzania informacji wstawi dane logowania użytkownika i logo firmy dostosowane do odbiorcy wiadomości e-mail, odzwierciedlając wygląd niestandardowej strony logowania Microsoft 365 firmy użytkownika.

Strona wyłudzania informacji podszywająca się pod środowisko logowania Microsoft z dynamiczną zawartością

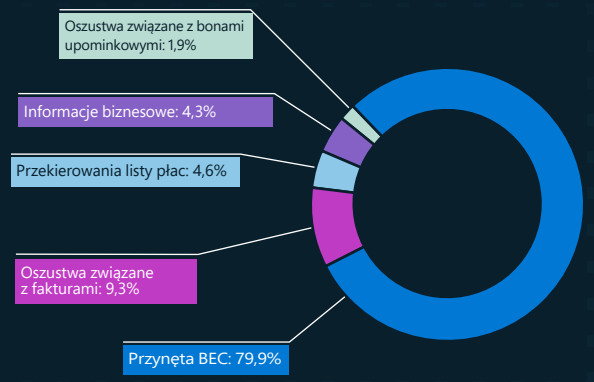


Włamania do biznesowej poczty e-mail

Cyberprzestępcy opracowują coraz bardziej skomplikowane schematy i techniki, aby pokonać zabezpieczenia osób prywatnych, firm i organizacji. W odpowiedzi na to inwestujemy znaczne środki w celu dalszego rozwoju naszego programu zwalczania BEC.

BEC to najbardziej kosztowne cyberprzestępstwo finansowe, którego skorygowane straty w 2021 r. szacuje się na 2,4 mld USD, co stanowi ponad 59% strat z pierwszej piątki przestępstw internetowych na świecie[20]. Aby zrozumieć zakres problemu i jak najlepiej chronić użytkowników przed BEC, badacze bezpieczeństwa Microsoft śledzili najczęstsze motywy wykorzystywane w atakach.

Motywy BEC (styczeń–czerwiec 2022 r.)



Motywy BEC według procentu występowania

Trendy BEC

Na początku atakujący BEC zazwyczaj próbują rozpocząć rozmowę z potencjalnymi ofiarami. Podając się za współpracownika, atakujący stopniowo prowadzi rozmowę w kierunku przelewu pieniężnego. Wstępne wiadomości e-mail, które obserwujemy jako przynęty BEC, reprezentują blisko 80% wykrytych e-maili BEC. Inne trendy zidentyfikowane przez Microsoft w ciągu ostatniego roku to:

- W atakach BEC w 2022 r. najczęściej fałszowano tożsamość[21] i podszywano się pod inne osoby[22].
- Podtypem BEC powodującym największe szkody finansowe u ofiar (w oparciu o liczbę przypadków i żądane kwoty) były oszustwa związane z fakturami.
- Przekonujące oszustwo związane z fakturami jest możliwe np. dzięki kradzieży informacji biznesowych takich jak raporty zobowiązań czy dane o klientach.
- Większość żądań przekierowań listy płac była wysyłana z darmowych usług e-mail, a rzadko z przejętych kont. Liczba e-maili z tych źródeł wzrastała w okolicach pierwszego i piętnastego dnia każdego miesiąca, czyli w najczęstszych terminach wypłat.
- Oszustwa związane z bonami upominkowymi są dobrze znane, ale stanowiły jedynie 1,9% wykrytych ataków BEC.

Praktyczne wskazówki

Ochrona przed wyłudzaniem informacji

Aby ograniczyć ryzyko udanego ataku wyłudzenia informacji na organizację, zachęca się administratorów IT do wdrażania następujących zasad i funkcji:

1. Wymagaj użycia uwierzytelniania wieloskładnikowego na wszystkich kontach, aby ograniczyć nieautoryzowany dostęp.
2. Włącz funkcje dostępu warunkowego dla kont z wysokimi uprawnieniami, aby zablokować dostęp z krajów, regionów i adresów IP, które zazwyczaj nie generują ruchu w Twojej organizacji.
3. Rozważ użycie fizycznych kluczy bezpieczeństwa dla kadry kierowniczej, pracowników zaangażowanych w działania związane z płatnościami lub zakupami oraz innych kont z wysokimi uprawnieniami.
4. Wymuszaj używanie przeglądarek, które obsługują usługi takie jak Microsoft SmartScreen analizujące adresy URL pod kątem podejrzanych zachowań i blokujące dostęp do znanych złośliwych stron internetowych[23].
5. Stosuj rozwiązania bezpieczeństwa oparte na uczeniu maszynowym, które poddają kwarantannie elementy oceniane jako prawdopodobne wyłudzanie informacji oraz otwierają adresy URL i załączniki w piaskownicy, zanim e-mail dotrze do skrzynki odbiorczej, jak np. Ochrona usługi Office 365 w usłudze Microsoft Defender[24].
6. Włącz funkcje ochrony przed podszywaniem się i fałszowaniem tożsamości w całej organizacji.
7. Skonfiguruj zasady DKIM (DomainKeys Identified Mail) oraz DMARC (Domain-based Message Authentication Reporting & Conformance), aby zapobiec dostarczaniu nieautentycznych e-maili, które mogą podszywać się pod prawdziwych nadawców.
8. Przeprowadzaj inspekcje reguł dopuszczających utworzonych przez dzierżawców i użytkowników oraz usuń szerokie wyjątki oparte na domenach i adresach IP. Reguły te często mają pierwszeństwo. Umożliwiają one filtrowanie znanych złośliwych wiadomości e-mail.
9. Regularnie przeprowadzaj symulacje wyłudzania informacji, aby oceniać ryzyko w całej organizacji oraz identyfikować i edukować użytkowników, którzy mogliby się poddać tego typu atakom.

Linki do dalszych informacji

- Od kradzieży plików cookie do BEC: atakujący wykorzystują witryny wyłudzania informacji AiTM jako punkt wejścia do dalszych oszustw finansowych | Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

Oszustwo homoglificzne

BEC i wyłudzanie informacji to typowe taktyki socjotechniki. Socjotechnika odgrywa istotną rolę w cyberprzestępczości. Atakujący zdobywa zaufanie użytkownika, by ten wykonał oczekiwane działania.

W handlu stacjonarnym znaki towarowe uosabiają zaufanie do pochodzenia produktu lub usługi. Podrobione produkty to nadużycie. Podobnie, podczas ataku wyłudzania informacji cyberprzestępcy podają się za kontakt znany użytkownikowi, oszukując ofiary za pomocą homoglifów.

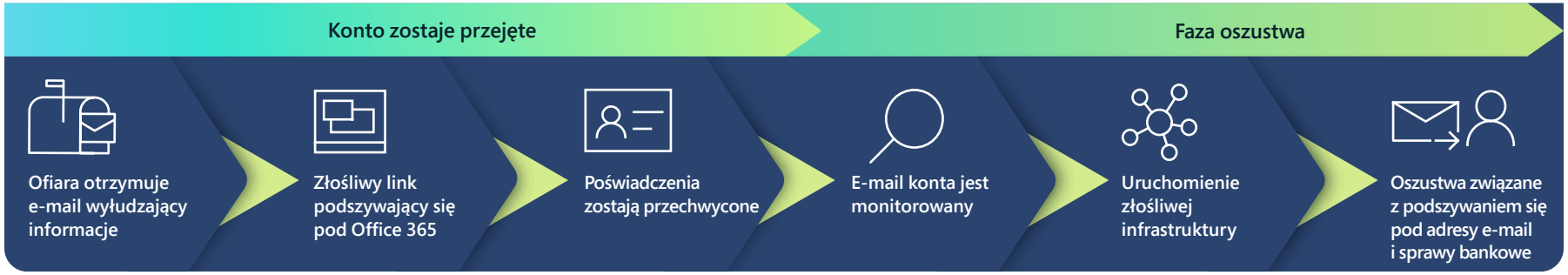
Homoglif to nazwa domeny wykorzystywana w komunikacji e-mailowej w atakach BEC, w której znak jest zastępowany przez taki, który ma identyczny lub prawie identyczny wygląd, aby oszukać użytkownika.

Techniki homoglifów stosowane w atakach BEC

BEC składa się zazwyczaj z dwóch faz, z których pierwsza obejmuje wykradanie poświadczeń. Tego typu wycieki poświadczeń mogą być wynikiem ataków wyłudzania informacji lub dużych kradzieży danych. Poświadczeniami następnie handluje się w dark web.

Drugi etap to faza oszustwa — atakujący na bazie wykradzionych poświadczeń stosują wyrafinowaną socjotechnikę z wykorzystaniem homoglificznych domen e-mail.

Postęp ataku BEC



Technika	% domen wykazujących technikę homoglifu
podstawienie l za I	25%
podstawienie i za l	12%
podstawienie q za g	7%
podstawienie rn za m	6%
podstawienie .cam za .com	6%
podstawienie 0 za o	5%
podstawienie ll za l	3%
podstawienie ii za i	2%
podstawienie vv za w	2%
podstawienie l za ll	2%
podstawienie e za a	2%
podstawienie nn za m	1%
podstawienie ll za I, podstawienie l za i	1%
podstawienie o za u	1%

Analiza ponad 1700 domen homoglificznych w okresie styczeń-lipiec 2022 r. Wykorzystano łącznie 170 technik homoglificznych, jednak w przypadku 75% domen użyto jedynie 14 technik.

Homoglif w akcji

Domena homoglificzna, która wygląda dla ofiary jak znajoma domena e-mail, jest zarejestrowana u dostawcy poczty z identyczną nazwą użytkownika. Następnie z przejętej domeny jest wysyłany e-mail z nowymi instrukcjami dotyczącymi płatności.

Wykorzystując „biały wywiad" i dostęp do wątków e-mailowych, przestępca identyfikuje osoby, które są odpowiedzialne za fakturowanie i płatności. Następnie podszywa się pod adres e-mail osoby wysyłającej faktury. To podszycie składa się z identycznej nazwy użytkownika i domeny e-mail będącej homoglifem prawdziwego nadawcy.

Atakujący kopiuje łańcuch e-maili zawierający legalną fakturę, a następnie zmienia ją tak, aby zawierała jego własne dane bankowe. Ta nowa, zmodyfikowana faktura jest następnie ponownie wysyłana z fałszywego, homoglificznego e-maila do osoby będącej celem. Ponieważ kontekst ma sens, a e-mail wygląda autentycznie, często osoba będąca celem wykonuje fałszywe instrukcje.

Praktyczne wskazówki

1. Wymuszaj używanie przeglądarek, które obsługują usługi takie jak Safe Links czy SmartScreen analizujące adresy URL pod kątem podejrzanych zachowań i blokujące dostęp do znanych złośliwych stron internetowych[25].
2. Używaj rozwiązania bezpieczeństwa oparte na uczeniu maszynowym, które poddają kwarantannie elementy oceniane jako prawdopodobne wyłudzanie informacji oraz otwierają adresy URL i załączniki w piaskownicy, zanim e-mail dotrze do skrzynki odbiorczej.

Linki do dalszych informacji

- Internet Crime Complaint Center (IC3) | Naruszenia e-maili biznesowych: 43 mld USD strat
- Analiza fałszowania tożsamości — Office 365 | Microsoft Docs
- Analiza podszywania się — Office 365 | Microsoft Docs

Harmonogram: przeciwdziałanie botnetom przez Microsoft

Od ponad dekady DCU proaktywnie powstrzymuje cyberprzestępczość. Efektem było przeciwdziałanie 26 atakom złośliwego oprogramowania i grupom powiązanym z państwami. Zespół DCU stosuje coraz bardziej zaawansowane taktyki i narzędzia do zamykania nielegalnych operacji, jednak cyberprzestępcy również ewoluują, próbując pozostać o krok przed nami. Oto harmonogram zwalczania przykładowych botnetów przez DCU i strategie ich likwidacji przyjęte przez Microsoft.

2008 r.

Botnet Conficker

Opis: Szybko rozprzestrzeniający się robak wymierzony w system operacyjny Windows, infekujący miliony komputerów i urządzeń we wspólnej sieci, spowodował przerwy w działaniu sieci na całym świecie.

Współpraca: Utworzenie Conficker Working Group, pierwszego tego typu konsorcjum. Microsoft, aby pokonać bota, nawiązał współpracę z 16 organizacjami na całym świecie.

Reakcja Microsoft: Grupa współpracowała międzynarodowo — udało się jej doprowadzić do likwidacji Conficker.

2009 r.

Botnet Waledac

Opis: Złożony botnet spamowy z domenami w Stanach Zjednoczonych, który zbierał adresy e-mail i rozprowadzał spam oraz zainfekował do 90 000 komputerów na całym świecie[26].

Współpraca: Utworzenie kolejnego konsorcjum, Microsoft Malware Protection Center (MMPC), z naciskiem na ścisłą współpracę z ośrodkami akademickimi[27].

Reakcja Microsoft: Microsoft zastosował podejście warstwowe do zwalczania systemów sterowania i kontroli, a także zaskoczył przestępców, konfiskując bez uprzedzenia domeny ze Stanów Zjednoczonych[28]. Microsoft tymczasowo przejął niemal 280 domen używanych przez serwery Waledac.

2011 r.

Powstaje Microsoft Digital Crimes Unit

Współpraca: Udaremnianie cyberprzestępczości wpływającej na ekosystem Microsoft przez ścisłą integrację zespołów śledczych, prawników i inżynierów.

Podejście Microsoft: Celem jest lepsze zrozumienie technicznych aspektów różnego typu złośliwego oprogramowania i dostarczenie tych spostrzeżeń zespołowi prawnemu Microsoft, aby opracować skuteczną strategię przeciwdziałania.

2013 r.

Botnet Rustock

Opis: Bot spamujący typu „backdoor trojan" wykorzystujący dostawców Internetu jako główne składniki sterowania i kontroli. Jego celem była sprzedaż farmaceutyków.

Współpraca: Microsoft nawiązał współpracę z Pfizer Pharmaceuticals, aby poznać leki sprzedawane przez Rustock, i ściśle współpracował z holenderskimi organami ścigania[29].

Reakcja Microsoft: Microsoft współpracował z US Marshalls i organami ścigania w Holandii, aby zlikwidować serwery sterowania i kontroli w tym kraju. Zarejestrowano i zablokowano wszystkie przyszłe DGA (algorytmy generowania domen).

Botnet Zero Access/Sirefef

Opis: Botnet reklamowy zaprojektowany w celu kierowania ludzi na niebezpieczne strony internetowe, które instalują złośliwe oprogramowanie lub wykradają informacje osobiste. Zainfekował ponad dwa miliony komputerów i kosztował reklamodawców ponad 2,7 mln USD miesięcznie, głównie w Stanach Zjednoczonych i Europie Zachodniej.

Współpraca: Ścisła współpraca z FBI i Cybercrime Center w ramach Europolu, aby wyeliminować infrastrukturę peer-to-peer.

Reakcja Microsoft: Dołączono do sieci Zero Access, podmieniono przestępcze serwery sterowania i kontroli oraz skonfiskowano domeny serwerów pobierania.

2019 r.

Botnet Trickbot

Opis: Wyrafinowany botnet z rozdrobnioną infrastrukturą na całym świecie, którego celem była branża usług finansowych. Skutecznie zaatakował urządzenia IoT.

Współpraca: Microsoft w celu zlikwidowania Trickbot współpracował z Financial Services Information Sharing and Analysis Center (FS-ISAC)[30].

Reakcja Microsoft: DCU zbudował system do identyfikowania i śledzenia infrastruktury botów oraz wygenerował powiadomienia dla aktywnych dostawców Internetu, biorąc pod uwagę specyficzne prawa w różnych krajach.

2022 r.

Ciągła koncentracja na zakłóceniach

Opis: Microsoft w ciągu ostatniego roku zakłócił działanie infrastruktury siedmiu grup przestępczych, uniemożliwiając im dalszą dystrybucję złośliwego oprogramowania, kontrolowanie komputerów ofiar oraz namierzanie kolejnych.

Współpraca: We współpracy z dostawcami usług internetowych, administracją publiczną, organami ścigania i sektorem prywatnym Microsoft udostępnił informacje, które pomogły ponad 17 milionom ofiar złośliwego oprogramowania na całym świecie.

Patrząc w przyszłość

DCU nadal wprowadza innowacje. Na bazie doświadczenia przeciwdziałania botnetom będzie prowadzić skoordynowane operacje wykraczające poza złośliwe oprogramowanie. Nasz dalszy sukces wymaga kreatywnej inżynierii, dzielenia się informacjami, innowacyjnych teorii prawnych oraz partnerstw publicznych oraz prywatnych.

Przestępcze nadużycie infrastruktury

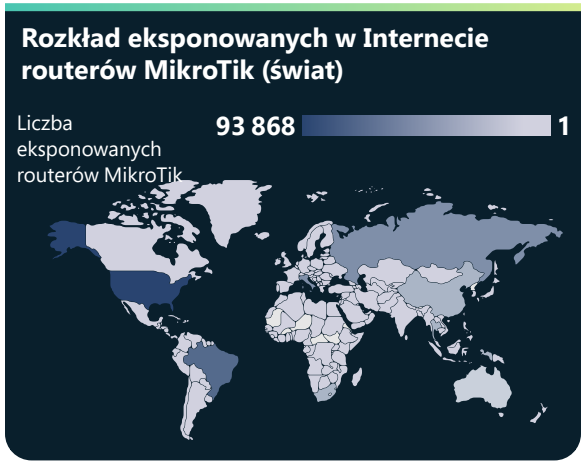
Bramy internetowe jako przestępcza infrastruktura sterowania i kontroli

Urządzenia IoT stają się coraz popularniejszym celem dla cyberprzestępców wykorzystujących rozległe botnety. Gdy routery są niezaktualizowane i eksponowane w Internecie, przestępcy mogą je wykorzystywać do uzyskiwania dostępu do sieci, przeprowadzania złośliwych ataków, a nawet realizowania swoich operacji.

Zespół Microsoft Defender dla IoT prowadzi badania nad różnymi typami sprzętu, od starszych kontrolerów przemysłowych systemów sterowania po najnowocześniejsze czujniki IoT. Zespół bada złośliwe oprogramowanie związane z IoT i OT w celu opracowania wspólnej listy wskaźników naruszenia bezpieczeństwa.

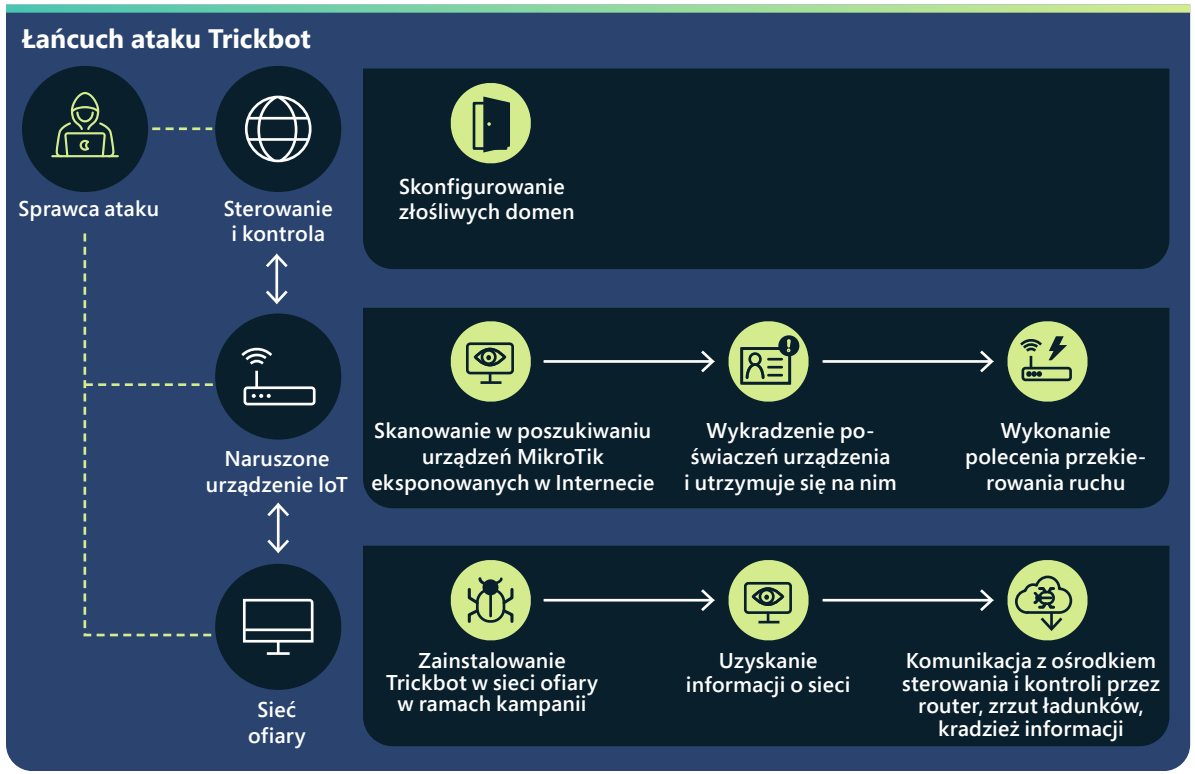
Routery są szczególnie podatnym wektorem ataku, ponieważ są wszechobecne w podłączonych do Internetu domach i organizacjach. Śledziliśmy aktywność routerów MikroTik popularnych na całym świecie zarówno w domach, jak i w organizacjach, identyfikując, jak są one wykorzystywane do sterowania i kontroli (C2), ataków na DNS oraz wymuszonego kopania kryptowalut.

W szczególności zidentyfikowaliśmy sposób, w jaki operatorzy Trickbot wykorzystują naruszone routery MikroTik i rekonfigurują je tak, aby działały jako część ich infrastruktury sterowania i kontroli. Popularność tych urządzeń potęguje stopień ich wykorzystania przez Trickbot, a ich unikalne oprogramowanie i sprzęt pozwalają przestępcom na omijanie tradycyjnych zabezpieczeń, rozbudowę infrastruktury i atakowanie kolejnych urządzeń i sieci.



Eksponowane w Internecie routery są narażone na ryzyko wykorzystania potencjalnych luk w zabezpieczeniach.

Śledząc i analizując ruch zawierający polecenia SSH, zaobserwowaliśmy, że napastnicy wykorzystują routery MikroTik do komunikacji z infrastrukturą Trickbot po zdobyciu poświadczeń urządzeń. Te poświadczenia mogą być uzyskane przez ataki siłowe (brute force), wykorzystanie znanych luk w zabezpieczeniach czy wskutek stosowania domyślnych haseł. Po uzyskaniu dostępu do urządzenia atakujący wydaje unikalne polecenie, które przekierowuje



Łańcuch ataku Trickbot ilustrujący wykorzystanie urządzeń MikroTik IoT jako serwerów proxy na potrzeby sterowania i kontroli.

ruch pomiędzy dwoma portami w routerze, ustanawiając linię komunikacji pomiędzy urządzeniami zaatakowanymi przez Trickbot a systemami sterowania i kontroli.

Na podstawie wiedzy o różnych metodach ataku na urządzenia MikroTik (poza samym Trickbot) oraz znanych, typowych luk i zagrożeń (CVE) stworzyliśmy narzędzie open-source dla urządzeń MikroTik, które umożliwia wydobycie śladów kryminalistycznych związanych z atakami na te urządzenia[31].

Urządzenia działające jako zwrotne serwery proxy w systemach sterowania i kontroli złośliwego oprogramowania nie są unikatowe tylko dla routerów Trickbot i MikroTik. We współpracy z zespołem Microsoft RiskIQ wyśledziliśmy systemy użyte do sterowania i kontroli. Poprzez obserwację certyfikatów SSL zidentyfikowaliśmy urządzenia Ubiquiti i LigoWave, które również były naruszone[32]. Świadczy to, że urządzenia IoT stają się składnikami ataków organizowanych przez państwa i popularnym celem dla cyberprzestępców wykorzystujących rozległe botnety.

Przestępcy kryptowalutowi wykorzystują urządzenia IoT

Urządzenia typu brama stają się coraz bardziej wartościowym celem dla przestępców — liczba znanych luk w zabezpieczeniach rośnie z roku na rok. Są one wykorzystywane do wydobywania kryptowalut i innych rodzajów przestępczej działalności.

Kiedy kryptowaluty stały się popularne, wiele osób i organizacji użyło mocy obliczeniowej i zasobów sieciowych z urządzeń takich jak routery do wydobywania „monet" na blockchainie. Jednak kopanie kryptowalut to czasochłonny i zasobochłonny proces o niskim prawdopodobieństwie sukcesu. Aby zwiększyć prawdopodobieństwo wydobycia kryptowaluty, górnicy łączą się w rozproszone, kooperacyjne sieci, otrzymując hashe proporcjonalnie do procentu środków, które udało im się wydobyć za pomocą połączonych zasobów.

W ubiegłym roku Microsoft zaobserwował rosnącą liczbę ataków wykorzystujących routery do przekierowywania mocy wydobywania kryptowalut. Cyberprzestępcy atakują routery podłączone do pul górniczych i przekierowują ruch górniczy na powiązane z nimi adresy IP za pomocą ataków DNS poisoning, które zmieniają ustawienia DNS docelowych urządzeń. Dotknięte routery rejestrują niewłaściwy adres IP do danej nazwy domeny, wysyłając swoje zasoby kopania (hashe) do pul wykorzystywanych przez przestępców. Pule te mogą wydobywać anonimowe monety związane z działalnością przestępczą lub wykorzystywać legalne hashe generowane przez górników, aby zdobyć procent wydobytej przez nich monety, czerpiąc w ten sposób korzyści.

W związku z tym, że ponad połowa znanych luk znalezionych w 2021 r. nie została usunięta, aktualizacja i zabezpieczenie routerów w sieciach firmowych i prywatnych pozostaje poważnym wyzwaniem dla właścicieli i administratorów urządzeń.

Atakowanie urządzeń w celu nielegalnego kopania kryptowalut

Część hashy z pierwotnej puli jest wykradana przez atakujących lub zasoby są przenoszone do ich puli, lub routery mają złośliwe oprogramowanie, które wykorzystuje ich zasoby do kopania.

Ataki DNS poisoning na bramy zagrażają legalnym kopalniom kryptowalut i przekierowują zasoby na przestępcze operacje kopania.

Maszyny wirtualne jako infrastruktura przestępcza

Powszechne przenoszenie się do chmury obejmuje cyberprzestępców, którzy wykorzystują prywatne zasoby nieświadomych ofiar uzyskane w wyniku wyłudzania informacji lub dystrybucji złośliwego oprogramowania wykradającego poświadczenia. Wielu cyberprzestępców decyduje się na tworzenie złośliwych infrastruktur opartych na chmurowych maszynach wirtualnych, kontenerach i mikrousługach.

Po uzyskaniu dostępu przez atakujących może nastąpić seria działań mających na celu skonfigurowanie infrastruktury (np. grupy maszyn wirtualnych) za pomocą skryptów i zautomatyzowanych procesów. Te oskryptowane, zautomatyzowane procesy są wykorzystywane do złośliwych działań, w tym ataków spamowych na dużą skalę czy wyłudzania informacji, a także do hostowania stron internetowych zawierających szkodliwe treści. Zdarzają się nawet skalowane środowiska wirtualne wydobywające kryptowaluty. Skutki u ofiary to rachunek na setki tysięcy dolarów za miesiąc.

Cyberprzestępcy wiedzą, że mają ograniczony czas, zanim zostaną wykryci i zablokowani. Dlatego zwiększają skalę i obecnie działają już proaktywnie, z góry przygotowując się na nieoczekiwane sytuacje. Zaobserwowano, że przygotowują z wyprzedzeniem naruszone konta i monitorują ich środowiska. Gdy tylko konto skonfigurowane na setki tysięcy maszyn wirtualnych zostanie wykryte, przechodzą na kolejne konto — już przygotowane przez skrypty do natychmiastowej aktywacji. Ich przestępcze operacje są kontynuowane bez przerwy.

Infrastruktura lokalna, podobnie jak chmurowa, może być wykorzystywana w atakach z użyciem wirtualnych środowisk lokalnych, które nie są znane użytkownikowi lokalnemu. Wymaga to, aby przyczółek dostępu pozostał otwarty i dostępny. Lokalne zasoby prywatne były również wykorzystywane przez cyberprzestępców do inicjowania dalszego łańcucha infrastruktury chmurowej skonfigurowanego tak, aby ukryć ich pochodzenie w celu uniknięcia wykrycia podejrzanej infrastruktury.

Praktyczne wskazówki

1. Promuj cyberhigienę i zapewnij pracownikom szkolenia z zakresu cyberbezpieczeństwa ze wskazówkami dotyczącymi obrony przed socjotechniką.
2. Przeprowadzaj regularne, zautomatyzowane kontrole anomalii aktywności użytkowników przez wykrywanie na dużą skalę, aby ograniczyć tego typu ataki.
3. Aktualizuj i zabezpieczaj routery w sieciach firmowych i prywatnych.

Czy haktywizm pozostanie?

Haktywizm nie jest nowym zjawiskiem, jednak wojna na Ukrainie spowodowała wzrost liczby hakerów-ochotników, niekiedy kierowanych przez rządy, którzy za pomocą cybernarzędzi niszczą reputację lub zasoby przeciwników politycznych, organizacji, a nawet państw.

W lutym 2022 r. ukraiński rząd wezwał cywilów na całym świecie do przeprowadzania cyberataków na Rosję w ramach 300-tysięcznej „armii IT"[33]. W tym samym czasie grupy haktywistów, takie jak Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans czy RaidForum2, zaczęły przeprowadzać ataki w celu wsparcia Ukrainy. Inne grupy, w tym część gangu ransomware Conti, stanęły po stronie Rosji[34].

W kolejnych miesiącach działalność Anonymous była bardzo widoczna. Hakerzy działający w imieniu grupy wyłączyli tymczasowo tysiące rosyjskich i białoruskich stron internetowych, ujawnili setki gigabajtów skradzionych danych, włamali się do rosyjskich kanałów telewizyjnych i odtworzyli proukraińskie treści, a nawet zaoferowali zapłatę w bitcoinach za poddane rosyjskie czołgi.

Powstanie hakerów obywatelskich

Platformy mediów społecznościowych umożliwiły szybką organizację i mobilizację tysięcy niedoszłych hakerów obywatelskich, którzy otrzymywali wskazówki dotyczące przeprowadzania łatwych do wykonania ataków, takich jak DDoS. Organizatorzy wykorzystali Twitter, Telegram i prywatne fora, aby zebrać hakerów, zorganizować operacje i rozpowszechniać instrukcje hakerskie.

Jednak większość z tych hakerów wprawdzie ma odpowiednie instrukcje, ale ich umiejętności są ograniczone. Sugeruje to dwie możliwości: jedną, w której setki lub tysiące osób o podstawowych umiejętnościach technicznych wykorzystują szablony ataków do przeprowadzania przyszłych skoordynowanych lub odosobnionych ataków haktywistycznych, i drugą, w której ostateczne zakończenie działań wojennych na Ukrainie sprawi, że osoby te porzucają haktywizm, przynajmniej do czasu, gdy kolejna kwestia polityczna lub społeczna nie zainspiruje ich do działania.

Upolitycznienie hakerów

Większym zagrożeniem wynikającym z tej politycznej mobilizacji jest wprowadzenie do akcji zaawansowanych technicznie hakerów, którzy mogą nadal przeprowadzać cyberataki na zagraniczne cele administracji publicznej, aby wspierać strategię swojego kraju: z własnej inicjatywy lub na polecenie rządu swojego kraju.

Iran, Chiny i Rosja już teraz wykorzystują haktywizm jako pożywkę dla rekrutacji do swoich państwowych grup hakerskich. Na przykład w kwietniu 2022 r. prorosyjska grupa hakerska Killnet przeprowadziła ataki DDoS przeciwko czeskim liniom kolejowym, regionalnym lotniskom i serwerowi czeskiej służby cywilnej, mimo że Czechy nie są bezpośrednio zaangażowane w wojnę[35]. Jednocześnie niektóre rządy mogą wykorzystywać haktywizm jako przykrywkę dla tradycyjnych operacji cybernetycznych lub sabotażowych — przykładem mogą być irańskie działania przeciwko Izraelowi.

W środowisku wzmożonych ataków DDoS związanych z haktywizmem branża technologiczna staje przed wyzwaniem szybkiego rozszyfrowania różnicy między normalnym a nienormalnym przepływem ruchu do strony internetowej. Microsoft i jego partnerzy opracowali zbiór narzędzi, które rozróżniają złośliwy ruch DDoS i śledzą jego pochodzenie. Ponadto Microsoft Azure może identyfikować działające na tej platformie maszyny, które generują wyjątkowo wysoki ruch wychodzący i wyłączać je.

Pojawienie się „oprogramowania protestacyjnego"

„Oprogramowanie protestacyjne" (protestware) pojawiło się jako bezpośredni efekt emocjonalnych reakcji na wojnę między Rosją a Ukrainą. Niektórzy twórcy oprogramowania open-source wykorzystali popularność swojego oprogramowania jako środek do wypowiedzenia się lub podjęcia działań przeciwko aktualnej sytuacji geopolitycznej. Były to nieszkodliwe pliki tekstowe otwierane na pulpicie lub w przeglądarce w celu szerzenia wiadomości o pokoju, ale również ukierunkowane ataki oparte na geolokalizacji adresu IP oraz działania destrukcyjne, takie jak wymazywanie dysku twardego. W miarę rozwoju innych, globalnych wydarzeń, możemy spodziewać się, że w przyszłości protestware ponownie się pojawi. Ponieważ są to zazwyczaj przypadki, w których szanowani opiekunowie open-source decydują się na osobiste wypowiedzi za pośrednictwem kontrolowanych przez siebie komponentów, nie ma obecnie żadnej ochrony, która powstrzymałaby tego typu zmiany w pakietach plików źródłowych. Użytkownicy powinni mieć świadomość potencjalnych zagrożeń.

Platformy mediów społecznościowych umożliwiły organizację i mobilizację tysięcy niedoszłych hakerów obywatelskich, którzy otrzymywali wskazówki dotyczące przeprowadzania łatwych do wykonania ataków, takich jak DDoS.

Praktyczne wskazówki

1. Branża technologiczna musi się zjednoczyć, aby opracować kompleksową odpowiedź na to nowe zagrożenie.
2. Wiodące firmy technologiczne, w tym Microsoft, dysponują narzędziami umożliwiającymi identyfikację złośliwego ruchu związanego z atakami DDoS i wyłączenie odpowiedzialnych za to maszyn.
3. Użytkownicy open-source powinni zachować wzmożoną czujność w czasach konfliktów geopolitycznych.

Przypisy końcowe

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. Wykrywanie i reagowanie w ramach ochrony punktów końcowych. 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. Forum z weryfikacją to internetowe forum dyskusyjne, na którym nowy członek musi mieć poręczenie dotychczasowego.
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. Źródło danych: Ochrona usługi Office w usłudze Microsoft Defender (złośliwe e-maile/działalność związana z wykradzionymi tożsamościami), Azure Active Directory Identity Protection (alerty/zdarzenia związane z wykradzioną tożsamością), Defender for Cloud Apps (zdarzenia związane z dostępem do danych z użyciem wykradzionych tożsamości) oraz M365D (korelacja między produktami).
17. Źródło danych: Ochrona punktu końcowego w usłudze Defender (zdarzenia/alerty związane z atakiem), Ochrona usługi Office w usłudze Defender (złośliwe wiadomość e-mail) i M365D (korelacja między produktami).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Domain-based Message Authentication, Reporting and Conformance (Zgodność, raportowanie i uwierzytelnianie wiadomości oparte na domenie): protokół uwierzytelniania wiadomości e-mail i zasad oraz protokół raportowania, który umożliwia właścicielom domen poczty e-mail ich ochronę przed nieautoryzowanym użyciem.
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 przeciw John Does 1-27 i inne, nr 1:10CV156, (E.D.Va., 22 lutego 2010 r.).
27. Patrz Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27 września 2011 r.
28. W szczególności art. 65 federalnych zasad postępowania cywilnego (Federal Rules of Civil Procedure) zezwala stronie na skorzystanie z takiego środka, jeśli: 1) strona poniesie natychmiastową i nieodwracalną szkodę, a roszczenia nie zostaną zaspokojone, oraz 2) strona podejmie próbę przekazania drugiej stronie powiadomienia na czas. Ponadto prawo wymaga zastosowania testu bilansującego, aby wziąć pod uwagę jednocześnie prawo pozwanego do powiadomienia i wielkość szkody ponoszonej przez społeczeństwo.
29. Microsoft Corporation przeciw John Does 1-11 i inne, No. 2:11cv222, (W.D. Wa., 9 lutego 2011 r.).
30. Microsoft Corp. przeciwko Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va., 12 sierpnia 2021 r.).
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

Zagrożenia ze strony państw

Państwa przeprowadzają coraz bardziej wyrafinowane cyberataki tak, aby uniknąć wykrycia i zrealizować swoje strategiczne cele.

Przegląd

zagrożeń ze strony państw

Państwa przeprowadzają coraz bardziej wyrafinowane cyberataki tak, aby uniknąć wykrycia i zrealizować swoje strategiczne cele. Pojawienie się cyberbroni na wojnie hybrydowej na Ukrainie to początek nowej ery konfliktów.

W ramach wojny Rosja realizowała również operacje wpływu informacyjnego, manipulując opiniami w Rosji, na Ukrainie i na świecie za pomocą propagandy. Ten pierwszy pełnowymiarowy konflikt hybrydowy przyniósł inne ważne wnioski. Po pierwsze, operacje cyfrowe i dane można najlepiej chronić — zarówno w cyberprzestrzeni, jak i w przestrzeni fizycznej — przenosząc się do chmury. Początkowe rosyjskie ataki za pomocą złośliwego oprogramowania wiper były wymierzone w usługi lokalne, a jeden z pierwszych wystrzelonych pocisków był wycelowany w fizyczne centrum danych.

Ukraina odpowiedziała szybkim przeniesieniem obciążeń i danych do hiperskalowych chmur hostowanych w centrach danych poza Ukrainą. Po drugie, postępy w zakresie analityki cyberzagrożeń i ochrony urządzeń klienckich oparte na danych oraz zaawansowanych usługach AI i ML w chmurze pomogły Ukrainie obronić się przed rosyjskimi cyberatakami.

Również poza Ukrainą czynniki państwowe zwiększyły aktywność — zaczęły wykorzystywać nowości w zakresie automatyzacji, infrastruktury chmurowej i technologii zdalnego dostępu, aby atakować szerszą gamę celów. Często atakowane były korporacyjne łańcuchy dostaw IT, które umożliwiają dostęp do ostatecznych ofiar. Cyberhigiena stała się jeszcze bardziej krytyczna, ponieważ atakujący szybko wykorzystywali niezaktualizowane luki, stosowali zarówno wyrafinowane techniki kradzieży poświadczeń, jak i ataki siłowe (brute-force), a także ukrywali swoje działania, wykorzystując legalne oprogramowanie lub typu open-source. Ponadto Iran dołączył do Rosji w stosowaniu destrukcyjnej cyberbroni, w tym oprogramowania wymuszającego okup (ransomware).

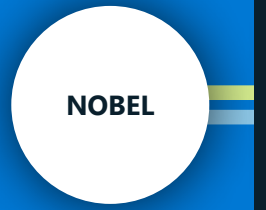
Zmiany te wymagają pilnego przyjęcia spójnych, globalnych ram, które nadadzą priorytet prawom człowieka i będą chronić ludzi przed lekkomyślnym zachowaniem czynników państwowych w sieci. Wszystkie narody muszą współpracować w celu wdrożenia norm odpowiedzialnego postępowania państw.

Obrona Ukrainy: pierwsze lekcje z cyberwojny — Microsoft On the Issues

Zwiększone ukierunkowanie na infrastrukturę krytyczną, zwłaszcza sektor IT, usługi finansowe, systemy transportowe i infrastrukturę komunikacyjną.

Więcej informacji na str. 35

Łańcuch dostaw IT jest wykorzystywany jako brama dostępu do ofiar.



Więcej informacji na str. 36

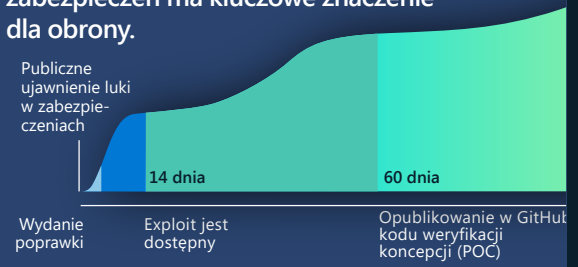
Chiny rozszerzają globalne działania, szczególnie na mniejsze kraje w Azji Południowo-Wschodniej, w celu zdobywania informacji i przewagi konkurencyjnej.

Więcej informacji na str. 44

Iran po zmianie władzy zwiększył agresywność działań. Rozszerzył ataki ransomware z regionalnych przeciwników na Stany Zjednoczone i UE. Atakuje także amerykańską infrastrukturę krytyczną.

Więcej informacji na str. 46

Kluczową taktyką stało się identyfikowanie i szybkie wykorzystywanie niezaktualizowanych luk. Szybkie stosowanie aktualizacji zabezpieczeń ma kluczowe znaczenie dla obrony.



Więcej informacji na str 39

Korea Północna obrała sobie za cel firmy z branży obronnej i lotniczej, kryptowaluty, serwisy informacyjne, uciekinierów i organizacje pomocowe, aby osiągnąć cele reżimu: wzmocnić sektor obronności, gospodarkę i stabilność wewnętrzną.

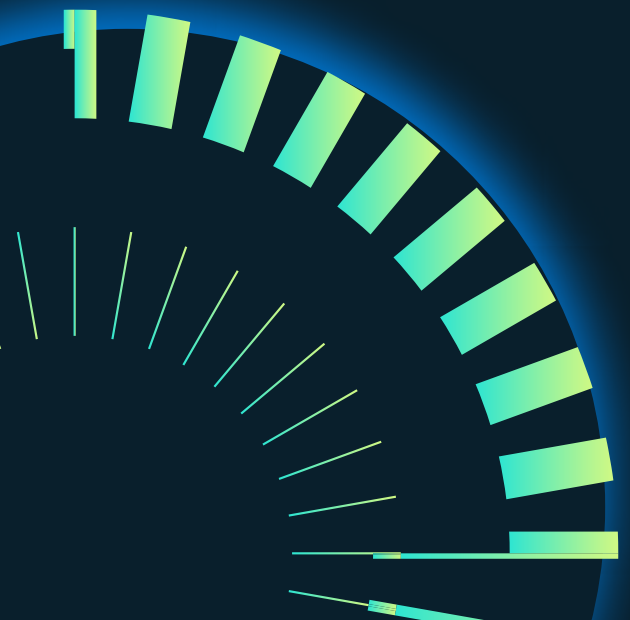
Więcej informacji na str. 49

Cybernajemnicy zagrażają stabilności cyberprzestrzeni — ta rosnąca branża prywatnych firm opracowuje i sprzedaje zaawansowane narzędzia, techniki i usługi, aby umożliwić swoim klientom (często rządom) włamywanie się do sieci i urządzeń.

Więcej informacji na str. 52

Wprowadzenie

Po głośnych atakach w latach 2020 i 2021 atakujące państwa wydały znaczne środki na przełamywanie nowych zabezpieczeń wdrożonych przez organizacje w celu obrony przed wyrafinowanymi zagrożeniami.



Podobnie jak w przypadku firm atakujący zaczęli wykorzystywać postępy w zakresie automatyzacji, infrastruktury chmurowej i technologii zdalnego dostępu, aby rozszerzyć swoje ataki na szerszą gamę celów. Skutkiem były nowe podejścia i ataki na dużą skalę na firmowe łańcuchy dostaw. Cyberhigiena IT nabrała jeszcze większego znaczenia, ponieważ atakujący opracowali nowe sposoby szybkiego wykorzystywania niezaktualizowanych luk, rozszerzyli techniki naruszania sieci firmowych oraz ukrywali swoje działania, wykorzystując oprogramowanie open-source lub legalne. Nowe techniki ataków dostarczyły nowych, trudniejszych do wykrycia wektorów umożliwiających uzyskanie dostępu do sieci ofiary. Wreszcie zaobserwowaliśmy, że w działalności wojskowej — wraz z eskalacją fizycznych działań — znaczącą rolę odgrywają cyberataki.

Wojna na Ukrainie stała się sugestywnym przykładem, że cyberataki wpływają na rzeczywistość równolegle z konfliktem zbrojnym w terenie. Systemy energetyczne i telekomunikacyjne, usługi komunalne oraz innego typu infrastruktura krytyczna stały się celem zarówno ataków fizycznych, jak i cybernetycznych. Próby włamań do sieci, powszechnie obserwowane jako część kampanii szpiegowskich i eksfiltracji informacji, skupiły się w wojnie hybrydowej na destrukcyjnych atakach złośliwego oprogramowania typu wiper na systemy infrastruktury krytycznej. Podłączenie zabezpieczeń tych systemów do chmury zaowocowało wczesnym wykryciem i przerwaniem potencjalnie niszczycielskich ataków[1].

Po raz pierwszy w przypadku dużego cyberataku mechanizmy wykrywania behawioralnego wykorzystujące uczenie maszynowe na podstawie znanych wzorców ataków skutecznie zidentyfikowały i powstrzymały dalsze ataki bez wcześniejszej znajomości leżącego u ich podstaw złośliwego oprogramowania — nawet zanim ludzie uświadomili sobie zagrożenie. Potwierdziliśmy również wartość dzielenia się informacjami o zagrożeniach w czasie rzeczywistym z obrońcami chroniącymi te systemy. Mają oni istotne informacje umożliwiające przewidywanie i obronę przed aktywnymi atakami.

Atakujące państwa rozszerzają swoje działania na całym świecie na nowe i stare sposoby. Chiny, Korea Północna, Iran i Rosja przeprowadzały ataki na klientów Microsoft. Łańcuch dostaw IT stał się typowym celem — atakujący przenieśli uwagę na usługi na górze łańcucha, które mogą zapewnić wejście do wielu organizacji. Spodziewamy się, że atakujący będą nadal wykorzystywać zaufane relacje w łańcuchach dostaw przedsiębiorstw. Tym większe będzie znaczenie kompleksowego egzekwowania zasad uwierzytelniania, szybkiego stosowania poprawek i konfiguracji kont w infrastrukturze dostępu zdalnego, a także częstej kontroli relacji partnerskich w celu weryfikacji autentyczności.

Atakujący powiązani z państwami oraz operatorzy oprogramowania ransomware i przestępczego zareagowali na te zmiany, przekierowując ataki na słabo skonfigurowane lub niezaktualizowane systemy firmowe (infrastrukturę VPN/VPS, serwery lokalne czy oprogramowanie innych firm) i wykorzystując taktykę „living-off-the-land" (dokonując złośliwych działań za pośrednictwem natywnych funkcji tych systemów). Wielu z nich zwiększyło wykorzystanie dostępnego na rynku złośliwego oprogramowania oraz narzędzi open-source dla czerwonych zespołów (red team) w celu ukrycia swoich przestępczych działań.

W rezultacie podstawami aktywnej obrony przed wyrafinowanymi atakującymi stały się: utrzymywanie higieny cyberbezpieczeństwa IT przez nadanie priorytetu stosowaniu poprawek, włączanie funkcji ochrony przed naruszeniami, używanie narzędzi do zarządzania obszarem podatnym na ataki takich jak RiskIQ, aby zapewnić sobie ogólny widok obszaru podatnego na ataki, oraz włączanie uwierzytelniania wieloskładnikowego w całym przedsiębiorstwie.

Atakujące państwa w coraz większym stopniu wykorzystują oprogramowanie ransomware, często ponownie wykorzystując ransomware stworzony przez ekosystem przestępczy. Wykryliśmy, że grupy powiązane z Iranem i Koreą Północną niszczyły systemy u regionalnych rywali, w tym infrastrukturę krytyczną, z użyciem dostępnych na rynku narzędzi ransomware. Wreszcie, zaobserwowaliśmy rosnące zagrożenie ze strony cybernajemników, którzy opracowują i sprzedają narzędzia, techniki i usługi służące do atakowania luk w systemach podmiotów trzecich. Zaawansowanie ataków dokonywanych przez państwa będzie z każdym rokiem coraz większe. Organizacje muszą reagować — śledzić krajobraz zagrożeń i dostosowywać swoją obronę.

John Lambert
Wiceprezes i inżynier, Microsoft Threat Intelligence Center

Kontekst danych o działaniach państw

Zagrożenia ze strony państw to działania cyberprzestępcze, które mają źródło w konkretnym kraju, a ich celem jest wspieranie interesów narodowych. Atakujące państwa stanowią jedne z najbardziej zaawansowanych i trwałych zagrożeń dla naszych klientów. Realizują one kradzieże własności intelektualnej, szpiegostwo, inwigilację, kradzieże poświadczeń, ataki destrukcyjne i inne.

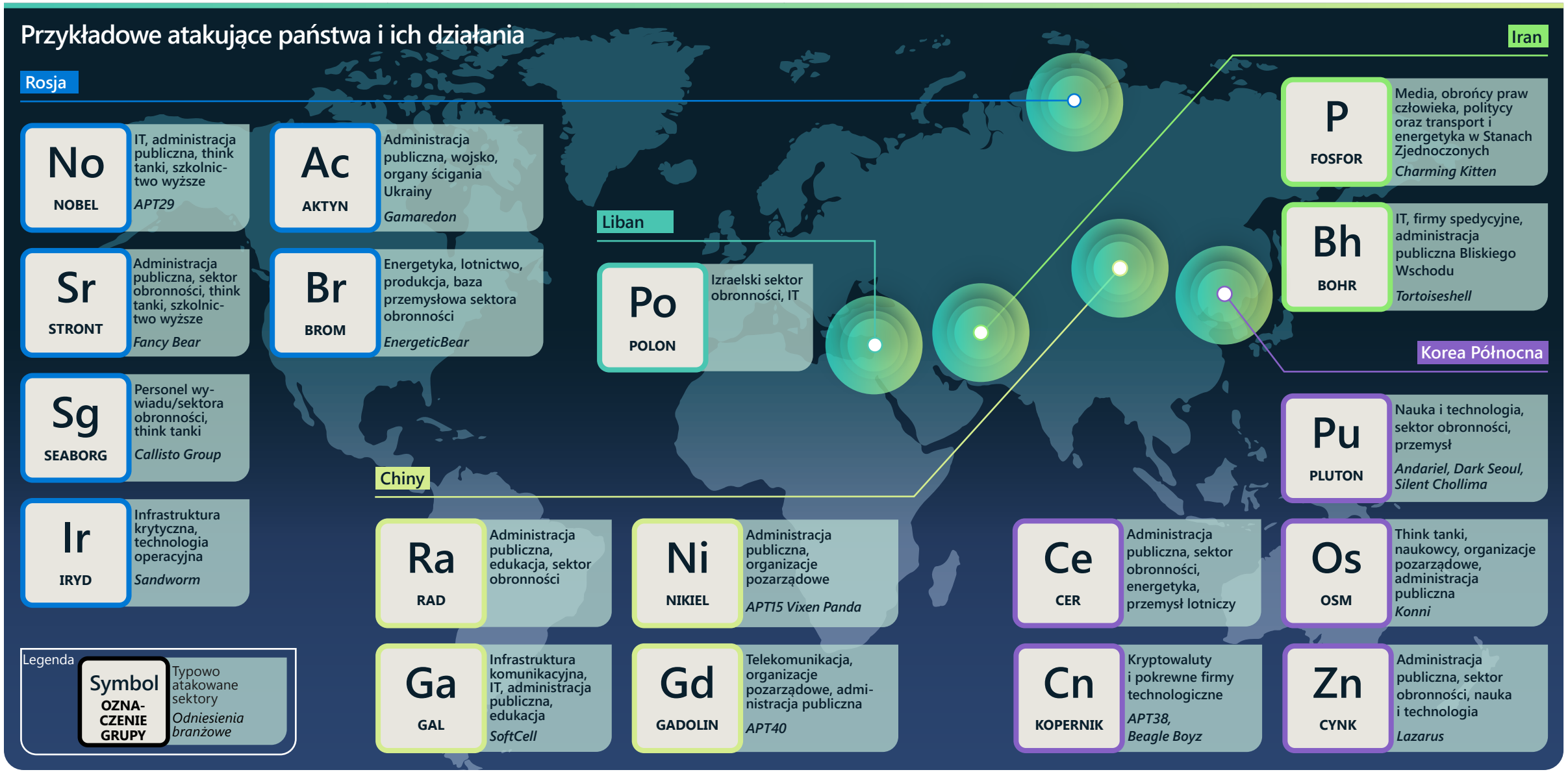
Inwestujemy znaczne środki w wykrywanie tych zagrożeń, ich poznawanie oraz przeciwdziałanie im. Gdy organizacja lub indywidualny posiadacz konta są atakowani przez państwo, Microsoft przesyła klientowi powiadomienie o ataku ze strony państwa (NSN, Nation state notification) wraz z informacjami potrzebnymi do zbadania aktywności. Od kiedy uruchomiliśmy ten system w 2018 r. do czerwca 2022 r. dostarczyliśmy ponad 67 000 powiadomień NSN.

W tym rozdziale przedstawiamy dane z alertów Microsoft NSN, które obrazują mierzalną aktywność. Poziom aktywności państw przedstawiony na wykresach opiera się na liczbie powiadomień NSN wysłanych przez Microsoft klientom w odpowiedzi na wykrycie ataku ze strony państwa, którego celem było co najmniej jedno konto w organizacji klienta.

Cztery główne państwa, których ataki omawiamy w tym raporcie, to Rosja, Chiny, Iran i Korea Północna. Są to miejsca pochodzenia najczęściej obserwowanych ataków, których celem byli klienci Microsoft w ciągu ostatniego roku. Raport zawiera również nasze spostrzeżenia dotyczące grup atakujących z Libanu oraz cybernajemników, czyli podmiotów atakujących wynajętych z sektora prywatnego.

Microsoft określa ataki państw nazwami pierwiastków chemicznych (np. NOBEL), z których część przedstawiono na kolejnej stronie. Używamy też oznaczeń DEV-#### jako tymczasowych nazw nadawanych nieznanym, pojawiającym się lub rozwijającym się grupom zagrożeń, dopóki nie uzyskamy pewności co do ich pochodzenia lub tożsamości.

Po ustaleniu, kim jest DEV, jest on przekształcany w nazwany podmiot lub włączany do już zidentyfikowanej grupy. W rozdziale przytaczamy konkretne przykłady państw i grup DEV, aby zapewnić szersze spojrzenie na cele ataków oraz ich techniki i motywacje. Wiele z tych grup korzysta z identycznych narzędzi, co cyberprzestępcy, jednak stanowią one wyjątkowe zagrożenie z uwagi na używanie również złośliwego oprogramowania szytego na miarę, zdolność do odkrywania i wykorzystywania luk zero-day oraz bezkarność prawną.


Przykładowe atakujące państwa i ich działania
Rosja
No
NOBEL
IT, administracja publiczna, think tanki, szkolnictwo wyższe
APT29
Ac
AKTYN
Administracja publiczna, wojsko, organy ścigania Ukrainy
Gamaredon
Sr
STRONT
Administracja publiczna, sektor obronności, think tanki, szkolnictwo wyższe
Fancy Bear
Br
BROM
Energetyka, lotnictwo, produkcja, baza przemysłowa sektora obronności
EnergeticBear
Sg
SEABORG
Personel wywiadu/sektora obronności, think tanki
Callisto Group
Ir
IRYD
Infrastruktura krytyczna, technologia operacyjna
Sandworm
Liban
Po
POLON
Izraelski sektor obronności, IT
Iran
P
FOSFOR
Media, obrońcy praw człowieka, politycy oraz transport i energetyka w Stanach Zjednoczonych
Charming Kitten
Bh
BOHR
IT, firmy spedycyjne, administracja publiczna Bliskiego Wschodu
Tortoiseshell
Korea Północna
Pu
PLUTON
Nauka i technologia, sektor obronności, przemysł
Andariel, Dark Seoul, Silent Chollima
Chiny
Ra
RAD
Administracja publiczna, edukacja, sektor obronności
Ni
NIKIEL
Administracja publiczna, organizacje pozarządowe
APT15 Vixen Panda
Ce
CER
Administracja publiczna, sektor obronności, energetyka, przemysł lotniczy
Os
OSM
Think tanki, naukowcy, organizacje pozarządowe, administracja publiczna
Konni
Ga
GAL
Infrastruktura komunikacyjna, IT, administracja publiczna, edukacja
SoftCell
Gd
GADOLIN
Telekomunikacja, organizacje pozarządowe, administracja publiczna
APT40
Cn
KOPERNIK
Kryptowaluty i pokrewne firmy technologiczne
APT38, Beagle Boyz
Zn
CYNK
Administracja publiczna, sektor obronności, nauka i technologia
Lazarus
Legenda
Symbol
OZNACZENIE GRUPY
Typowo atakowane sektory
Odniesienia branżowe

Ewoluujący krajobraz zagrożeń

Misją Microsoft w zakresie ochrony klientów przed atakami jest śledzenie aktywności państw i powiadamianie użytkowników, gdy zostaną zaatakowani.

Te powiadamiania są kluczową częścią naszego zobowiązania do informowania klientów o tym, czy zaobserwowanym atakom skutecznie zapobiegają nasze produkty zabezpieczające, czy też ataki są skuteczne z powodu nieznanych jeszcze podatności. Śledzenie zgłoszeń w czasie pomaga Microsoft identyfikować ewoluujące trendy zagrożeń według grup atakujących i skupiać zabezpieczenia produktów na proaktywnym reagowaniu na zagrożenia dla klientów w naszych usługach w chmurze.

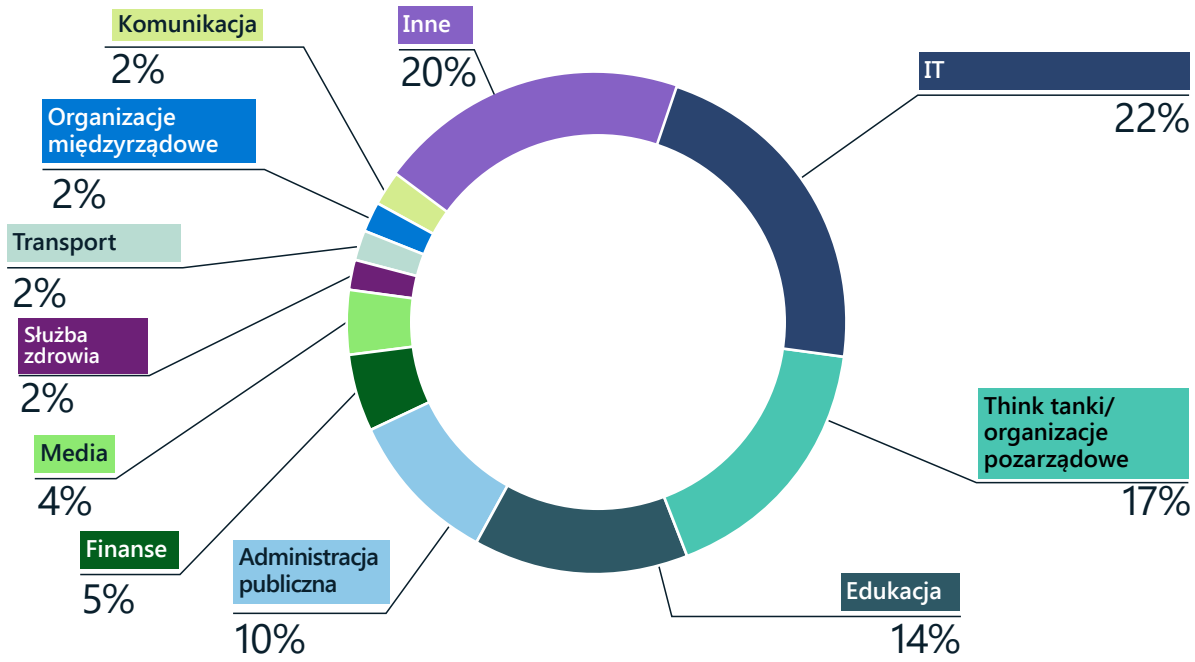
Takie śledzenie pozwala nam również na udostępnianie danych i analiz dotyczących tego, co widzimy. Analitycy śledzący te grupy i ich ataki korelują wskaźniki techniczne (kontekst techniczny) i wiedzę geopolityczną (kontekst globalny), aby zrozumieć ich motywacje. Te analizy zapewniają unikalny wgląd w priorytety atakujących państw oraz w to, że działania grup powiązanych z państwami odzwierciedlają polityczne, wojskowe i ekonomiczne priorytety państw-zleceniodawców.

Wydarzenia polityczne w ubiegłym roku ukształtowały priorytety atakujących państw. Ponieważ relacje geopolityczne uległy załamaniu, a w niektórych państwach władzę przejęły radykalne nurty polityczne, cyberatakujący stali się bardziej agresywni. Na przykład:

- Rosja oprócz działań wojskowych nieustannie atakowała ukraińską administrację publiczną i infrastrukturę krytyczną[2].
- Iran agresywnie dążył do ataku na infrastrukturę krytyczną Stanów Zjednoczonych, np. na porty.
- Korea Północna kontynuowała kampanię kradzieży kryptowalut od firm finansowych i technologicznych.
- Chiny rozszerzyły globalne operacje cyberszpiegowskie.

Chociaż atakujący powiązani z państwami mogą być zaawansowani technicznie i stosować szeroką gamę taktyk, do odparcia ich ataków często wystarczy sama cyberhigiena. Wielu z tych atakujących, aby wdrożyć wyrafinowane złośliwe oprogramowanie, wcale nie tworzy zaawansowanych exploitów ani nie wykorzystuje ukierunkowanej inżynierii społecznej. Zamiast tego polegają oni na stosunkowo mało zaawansowanych środkach, takich jak wiadomości e-mail wyłudzające informacje.

Sektory atakowane przez państwa



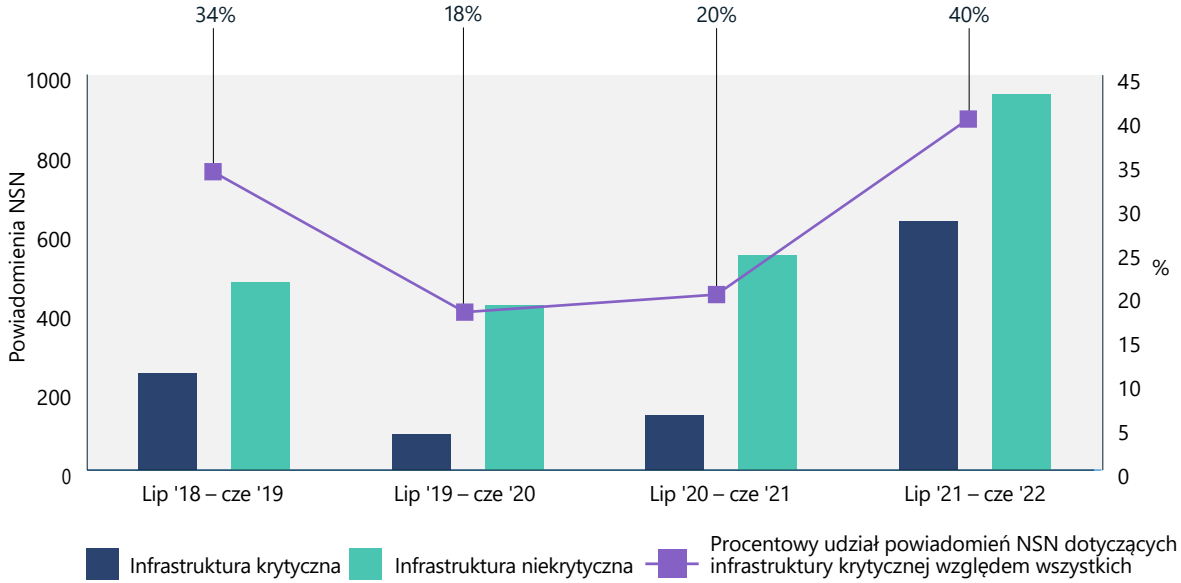
Grupy państw atakują szereg sektorów. Napastnicy powiązani z Rosją i Iranem obrali sobie za cel branżę IT jako sposób na uzyskanie dostępu do klientów firm IT. Think tanki, organizacje pozarządowe (NGO), uniwersytety i instytucje administracji publicznej to inne częste cele ataków ze strony państw.

Państwa mają różne cele, które mogą skutkować atakowaniem konkretnych organizacji lub osób. W ostatnim roku nasiliły się naruszenia łańcuchów dostaw, ze szczególnym uwzględnieniem firm IT. Atakując dostawców usług IT, napastnicy często są w stanie wniknąć do systemów ofiary, wykorzystując jej zaufaną relację z firmą, która zarządza podłączonymi systemami, lub przeprowadzić działania na znacznie większą skalę, naruszając setki klientów na dole łańcucha w pojedynczym ataku. Po sektorze IT najczęściej atakowanymi podmiotami były think tanki, pracownicy naukowi na uczelniach oraz urzędnicy administracji publicznej. Są to pożądane „miękkie cele" dla szpiegostwa pozwalające na zbieranie informacji wywiadowczych na tematy geopolityczne.

Ewoluujący krajobraz zagrożeń

(c.d.)

Trendy dotyczące infrastruktury krytycznej

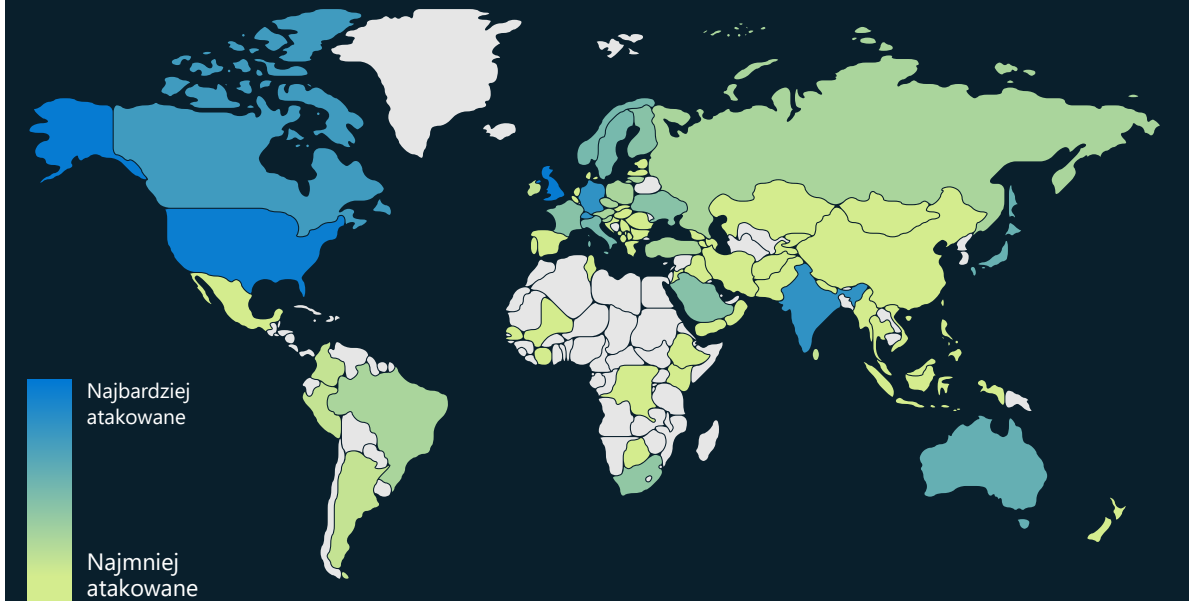


W ubiegłym roku wzrosła liczba ataków państw na infrastrukturę krytyczną[3]. Intruzi skupiali się na firmach z sektora IT, usług finansowych, transportu i infrastruktury komunikacyjnej.

„Przed inwazją na Ukrainę rządy uważały, że dane muszą pozostawać wewnątrz kraju, aby były bezpieczne. Obecnie, po inwazji, migracja danych do chmury i przeniesienie ich poza granice terytorialne jest częścią planowania odporności i dobrego zarządzania".

Cristin Flynn Goodwin,
Zastępca głównego radcy prawnego, bezpieczeństwo i zaufanie klientów

Cele atakujących państw



W ubiegłym roku cyberataki państw obejmowały cały świat, ze szczególnym uwzględnieniem przedsiębiorstw amerykańskich i brytyjskich. Z naszych danych NSN wynika, że częstymi celami ataków były również organizacje w Izraelu, Zjednoczonych Emiratach Arabskich, Kanadzie, Niemczech, Indiach, Szwajcarii i Japonii.

Praktyczne wskazówki

1. Zidentyfikuj i chroń potencjalne cele związane z danymi o dużej wartości, zagrożone technologie, informacje i operacje biznesowe, które mogą być zgodne ze strategicznymi priorytetami atakujących państw.
2. Włącz ochronę chmury, aby zapewnić identyfikowanie i likwidowanie na dużą skalę starszych i nowych zagrożeń dla Twojej sieci.

Łańcuch dostaw IT jako brama do ekosystemu cyfrowego

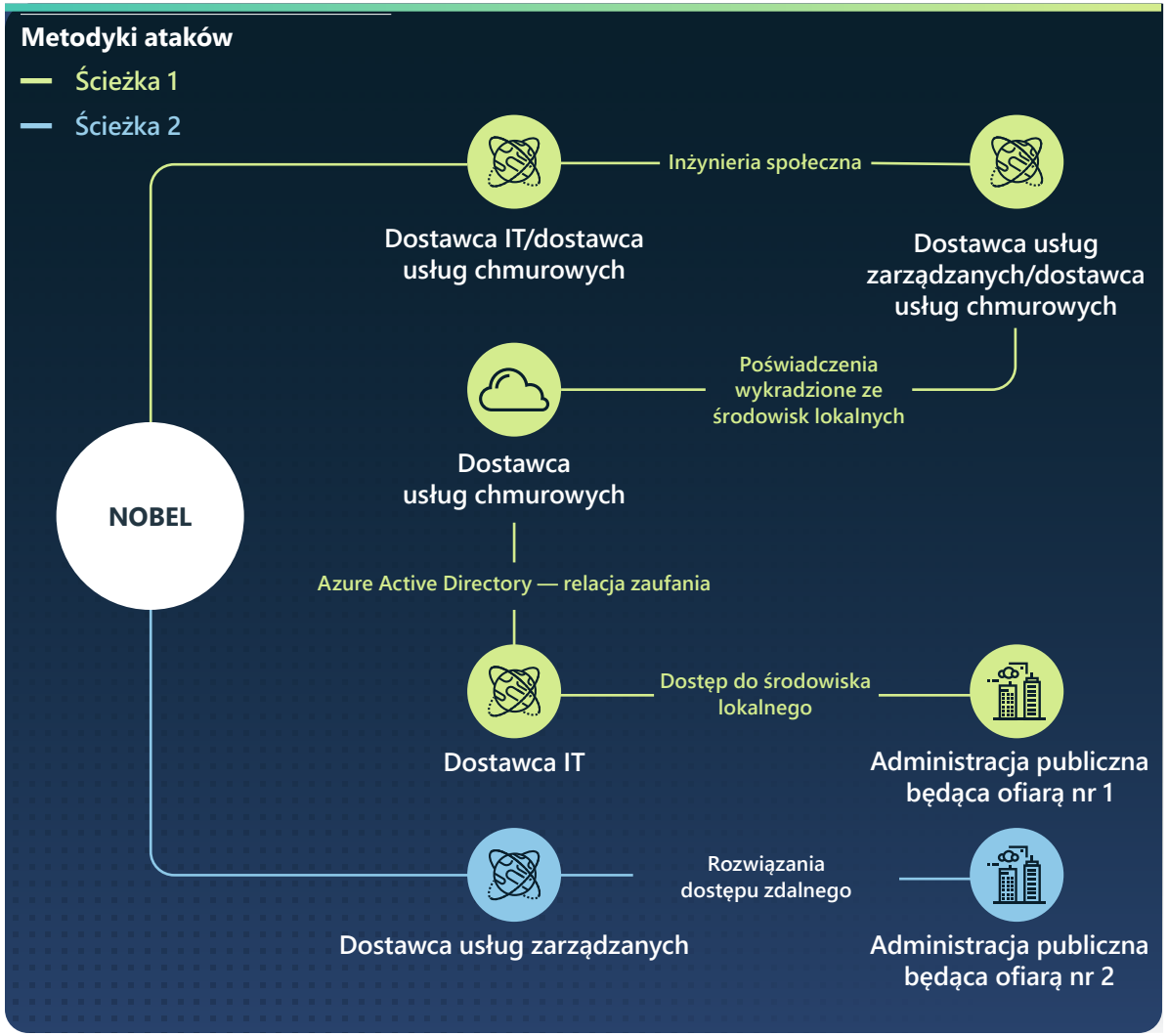
Ofensywne państwa, atakując dostawców usług IT, mogą wykorzystać zaufanie i prawa dostępu udzielone tym dostawcom przez różne organizacje w łańcuchu dostaw. W ubiegłym roku atakujące państwa obrały sobie za cel dostawców usług IT, aby zaatakować cele stron trzecich i uzyskać dostęp do klientów na dole łańcucha w administracji publicznej, gabinetach politycznych i infrastrukturze krytycznej.

Dostawcy usług IT stanowią atrakcyjne cele pośrednie, ponieważ obsługują setki bezpośrednich i tysiące pośrednich klientów, którymi zainteresowane są zagraniczne służby wywiadowcze. Rutynowe praktyki biznesowe i delegowane uprawnienia administratora stosowane w tych firmach mogą stanowić wektory ataku i pozwolić przestępcom na dostęp do sieci klientów dostawców usług IT oraz manipulowanie nimi bez natychmiastowego wywołania alarmów.

W zeszłym roku grupa NOBEL próbowała przejąć konta z wysokimi uprawnieniami u dostawców rozwiązań chmurowych i innych usług zarządzanych, aby uzyskać dostęp do klientów na dole łańcucha z sektora administracji publicznej i politycznego w Stanach Zjednoczonych i Europie.

Grupa NOBEL pokazała, jak podejście „włamanie do jednego systemu umożliwia włamanie do wielu" może być skierowane przeciwko przeciwnikowi geopolitycznemu. W minionym roku atakujący dokonywali włamań bezpośrednio do krytycznych organizacji w państwach członkowskich NATO, jak i do organizacji z nimi powiązanych. NATO jest postrzegane przez rząd rosyjski jako egzystencjalne zagrożenie. Między lipcem 2021 r. a początkiem czerwca 2022 r. 48% powiadomień przesyłanych klientom Microsoft o aktywności atakujących związanych z Rosją względem klientów usług online trafiło do firm z sektora IT w krajach członkowskich NATO. Ich infrastruktura miała się prawdopodobnie stać pośredniczącymi punktami dostępu. W sumie 90% powiadomień o atakujących powiązanych z Rosją w tym samym okresie trafiło do klientów z państw członkowskich NATO, głównie z sektora IT, think tanków, organizacji pozarządowych (NGO) oraz administracji publicznej. Sugeruje to strategię wykorzystywania wielu środków w celu uzyskania wstępnego dostępu do tych ofiar.

Nastąpiło przejście od wykorzystywania łańcucha dostaw oprogramowania do wykorzystania łańcucha dostaw usług IT. Celem ataków są rozwiązania chmurowe i dostawcy usług zarządzanych, których naruszenie pozwala następnie na dotarcie do klientów na dole łańcucha.



Ten diagram przedstawia wieloaspektowe podejście grupy NOBEL do atakowania celów i szkody uboczne innych ofiar po drodze. Oprócz działań podanych powyżej grupa NOBEL przeprowadziła ataki rozproszone na hasła (password spray) i wyłudzania informacji przeciwko zaangażowanym podmiotom, a także na osobiste konta co najmniej jednego pracownika administracji publicznej.

Łańcuch dostaw IT jako brama do ekosystemu cyfrowego

(c.d.)

W ciągu roku Microsoft Threat Intelligence Center (MSTIC) wykrył, że coraz więcej irańskich państwowych i powiązanych z państwem grup atakuje firmy IT. W wielu przypadkach wykradano poświadczenia logowania w celu uzyskania dostępu do klientów na dole łańcucha w różnych celach, od gromadzenia danych wywiadowczych po niszczycielskie ataki odwetowe.

- W lipcu i sierpniu 2021 r. DEV-0228 skutecznie zaatakował izraelskiego dostawcę oprogramowania biznesowego, a później włamał się do klientów na dole łańcucha w izraelskim sektorze obronnym, energetycznym i prawnym[4].
- Od sierpnia do września 2021 r. Microsoft wykrył gwałtowny wzrost liczby ataków Iranu na firmy z Indii. Brak pilnych kwestii geopolitycznych, które mogłyby skłonić do takiej zmiany, sugeruje, że to ukierunkowanie dotyczy pośredniego dostępu do spółek zależnych i klientów poza Indiami.
- W styczniu 2022 roku grupa DEV-0198, która według nas jest powiązana z rządem Iranu, skutecznie zaatakowała izraelskiego dostawcę rozwiązań chmurowych. Microsoft ocenia, że prawdopodobnie użyto wykradzionych od dostawcy poświadczeń do uwierzytelnienia w izraelskiej firmie logistycznej. MSTIC zaobserwował, że w tym samym miesiącu ten sam atakujący próbował przeprowadzić destrukcyjny cyberatak na firmę logistyczną.
- W kwietniu 2022 r. POLON, grupa z Libanu, która według naszej oceny współpracowała z grupami powiązanymi z Iranem w zakresie technik ataków na łańcuchy dostaw IT, skutecznie zaatakowała inną izraelską firmę IT, aby uzyskać dostęp do izraelskich organizacji w sektorze obronności i prawa[5].

W ostatnim roku grupy atakujących takie jak NOBEL czy DEV-0228 znały zaufane relacje organizacji lepiej niż one same. To zwiększone zagrożenie podkreśla potrzebę zrozumienia i wzmocnienia przez organizacje granic i punktów wejścia do ich zasobów cyfrowych. Również duże znaczenie ma dla dostawców usług IT rygorystyczne monitorowanie własnego stanu cyberbezpieczeństwa. Na przykład organizacje powinny wdrożyć uwierzytelnianie wieloskładnikowe i zasady dostępu warunkowego, które utrudniają atakującym przechwytywanie kont z wysokimi uprawnieniami czy penetrowanie sieci.

Przeprowadzenie dokładnego przeglądu i inspekcji relacji partnerskich pomaga zminimalizować wszelkie zbędne uprawnienia pomiędzy organizacją a dostawcami na górze łańcucha i natychmiast usunąć dostęp dla wszelkich relacji, które wyglądają na nieznane. Analiza dzienników aktywności i przegląd wszystkich działań pozwala na wykrycie anomalii.

> Atakowanie przez państwa stron trzecich umożliwia im wrogie wykorzystywanie wrażliwych organizacji przez nadużycie zaufania i uprawnień dostępu w łańcuchu dostaw.

Praktyczne wskazówki

1. Dokonaj przeglądu i kontroli relacji z dostawcami na górze i na dole łańcucha oraz delegowanych uprawnień dostępu w celu zminimalizowania uprawnień, które nie są niezbędne. Usuń dostęp wszelkim partnerom, z którymi relacje wyglądają na nieznane lub nie zostały jeszcze skontrolowane[6].
2. Włącz rejestrowanie i dokonaj przeglądu wszystkich poświadczeń dotyczących infrastruktury dostępu zdalnego i VPN, ze szczególnym uwzględnieniem kont z uwierzytelnianiem jednoskładnikowym, aby potwierdzić ich autentyczność i zbadać wszelkie anomalie.
3. Włącz uwierzytelnianie wieloskładnikowe dla wszystkich kont (w tym dla kont usług) i upewnij się, że uwierzytelnianie wieloskładnikowe jest wymuszone dla wszystkich połączeń zdalnych.
4. Stosuj rozwiązania bezhasłowe do zabezpieczania kont[7].

Linki do dalszych informacji

- Grupa NOBEL atakuje delegowane uprawnienia administracyjne w celu ułatwienia szerszych ataków | Microsoft Threat Intelligence Center (MSTIC)
- Wzrost ataków Iranu na sektor IT | Microsoft Thre at Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Ujawnienie działalności i infrastruktury POLON, którego celem są organizacje izraelskie | Microsoft Threat Intelligence Center (MSTIC)

Szybkie wykorzystywanie luk w zabezpieczeniach

W miarę jak organizacje wzmacniają swoje cyberzabezpieczenia, atakujące państwa reagują, stosując nowe i unikalne sposoby atakowania i unikania wykrycia. Kluczową taktyką w tych działaniach jest identyfikowanie i wykorzystywanie wcześniej nieznanych luk (zero-day).

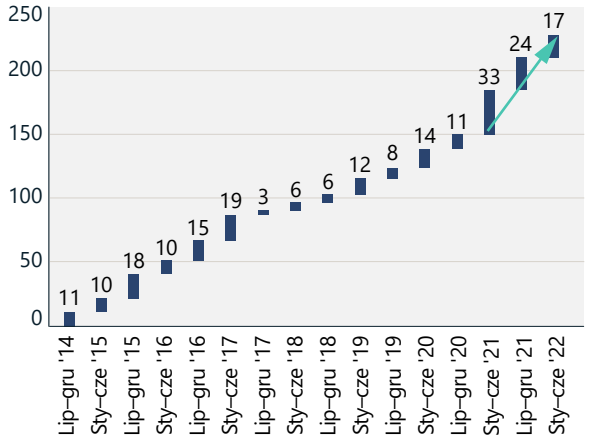
Luki zero-day są szczególnie skutecznym sposobem ataku wstępnego. Po ich publicznym ujawnieniu mogą być szybko wykorzystane przez inne grupy powiązane z państwami oraz innych przestępców. Liczba publicznie ujawnionych luk zero-day w ciągu ostatniego roku jest zbliżona do liczby luk z poprzedniego roku, który był rekordowy.

W miarę jak atakujący — zarówno państwa, jak i przestępcy — stają się coraz bardziej biegli w wykorzystywaniu tych luk, zaobserwowaliśmy skrócenie czasu pomiędzy ogłoszeniem luki a upowszechnieniem jej wykorzystania. To sprawia, że organizacje muszą natychmiast stosować poprawki usuwające luki. Podobnie bardzo ważne jest, aby organizacje lub osoby odkrywające nowe luki odpowiedzialnie ujawniały je lub zgłaszały zainteresowanym dostawcom tak szybko, jak to możliwe, zgodnie ze skoordynowanymi procedurami ujawniania luk.

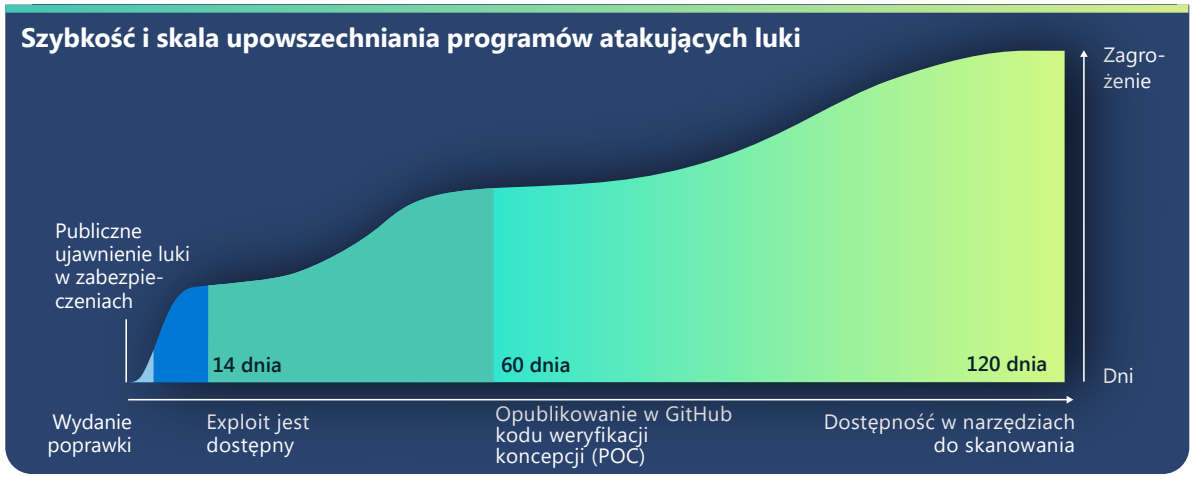
Dzięki temu podatności będą identyfikowane, a poprawki natychmiastowo opracowywane, aby chronić klientów przed nieznanymi wcześniej zagrożeniami.

Wiele organizacji zakłada, że są mniej narażone na ataki wykorzystujące luki zero-day, jeśli zarządzanie lukami jest integralną częścią ich bezpieczeństwa sieciowego. Jednak skomercjalizowanie programów atakujących luki prowadzi do upowszechnienia ich stosowania. Luki zero-day są często odnajdywane przez jednych atakujących, a wykorzystywane masowo w krótkim czasie przez innych, stwarzając ryzyko dla systemów bez zainstalowanych poprawek. Ataki na luki zero-day mogą być trudne do wykrycia, jednak będące ich konsekwencją działania przestępców są łatwiejsze do zaobserwowania.

Poprawki wydane na luki zero-day



Liczba publicznie ujawnionych luk zero-day z listy CVEs (Common Vulnerabilities and Disclosures).



Po publicznym ujawnieniu luki programy umożliwiające atak na nią są dostępne średnio po 14 dniach. Wykres ten pokazuje harmonogramy wykorzystania luk zero-day wraz z liczbą systemów podatnych i aktywnych w Internecie od momentu pierwszego publicznego ogłoszenia.

Chociaż ataki z wykorzystaniem luk zero-day są początkowo ukierunkowane na ograniczoną grupę organizacji, szybko zostają zaadoptowane szerzej przez przestępców. Rozpoczyna to wyścig atakujących w celu jak najszerszego wykorzystania luki, zanim potencjalne ofiary zainstalują poprawki.

Chociaż obserwujemy, że wiele atakujących państw opracowuje ataki na nieznane luki, to atakujący powiązani z Chinami są szczególnie biegli w odkrywaniu i opracowywaniu ataków na luki zero-day. Chińskie przepisy dotyczące zgłaszania luk weszły w życie we wrześniu 2021 r. Jest to pierwszy na świecie rząd, który wymaga zgłaszania luk organom administracji publicznej w celu dokonania analizy przed przekazaniem informacji właścicielowi produktu lub usługi. To nowe rozporządzenie może umożliwić ośrodkom w chińskiej administracji publicznej gromadzenie zgłoszonych luk w celu ich wykorzystywania. Zwiększone wykorzystanie luk zero-day w ciągu ostatniego roku przez atakujących powiązanych z Chinami prawdopodobnie odzwierciedla pierwszy pełny rok obowiązywania chińskich wymogów dotyczących ujawniania luk w zabezpieczeniach chińskiej społeczności bezpieczeństwa oraz duży krok w wykorzystaniu luk zero-day jako priorytetu państwowego. Opisane poniżej luki zostały najpierw opracowane i wykorzystane w atakach przez grupy powiązane z Chinami, a następnie odkryte i rozpowszechnione wśród innych atakujących w ekosystemie przestępczym.

Szybkie wykorzystywanie luk w zabezpieczeniach

(c.d.)

Nawet organizacje, które nie są celem atakujących państw, mają ograniczony czas na usunięcie luk zero-day w systemach, zanim zostaną one wykorzystane przez szerszy ekosystem przestępców.

Te przykłady nowo zidentyfikowanych luk pokazują, że organizacje mają średnio 60 dni od momentu usunięcia luki przez poprawkę i udostępnienia w sieci kodu weryfikacji koncepcji (POC, proof of concept), który często jest ponownie wykorzystywany przez innych atakujących. Luka zostanie też uwzględniona w automatycznych narzędziach do skanowania i analizowania luk, takich jak Metasploit, średnio dopiero po 120 dniach. Przez ten czas luka może być atakowana na masową skalę. Dlatego nawet organizacje, które nie są celem atakujących powiązanych z państwami, mają ograniczony czas na usunięcie luk zero-day w systemach, zanim zostaną one wykorzystane przez szeroki ekosystem przestępców.

CVE-2021-35211 SolarWinds Serv-U

W lipcu 2021 r. SolarWinds opublikował poradę dotyczącą bezpieczeństwa dla CVE-2021-35211, wspominając w niej Microsoft[8]. W tym czasie odkryliśmy, że grupa powiązana z państwem DEV-0322 aktywnie wykorzystuje lukę SolarWinds Serv-U. Nasz zespół RiskIQ od 15 czerwca do 9 lipca zaobserwował 12 646 adresów IP hostujących połączone z Internetem wersje podatnych urządzeń.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

We wrześniu 2021 r. nasi badacze zaobserwowali grupy powiązane z Chinami wykorzystujące Zoho ManageEngine w kilku organizacjach ze Stanów Zjednoczonych. Luka została publicznie zgłoszona 6 września jako CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, którego organizacje zazwyczaj używają do obsługi resetowania haseł[9]. DEV-0322 wykorzystał tę lukę później we wrześniu, używając jej jako wektora wejścia do zdobycia przyczółka w sieciach i wykonując dodatkowe działania, w tym zrzut poświadczeń, instalowanie niestandardowych plików binarnych czy porzucanie złośliwego oprogramowania w celu utrzymania się w naruszonym systemie. W momencie ujawnienia informacji RiskIQ zaobserwował 4011 instancji tych systemów aktywnych i działających w Internecie.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

Pod koniec października 2021 r. zaobserwowaliśmy, że DEV-0322 wykorzystuje lukę (CVE-2021-44077) w drugim produkcie Zoho ManageEngine, ServiceDesk Plus — oprogramowaniu typu help-desk IT z funkcjami zarządzania zasobami. DEV-0322 wykorzystał tę lukę do ataku na podmioty z sektora opieki zdrowotnej, IT, szkolnictwa wyższego i krytycznych sektorów produkcji. 2 grudnia FBI (Federalne Biuro Śledcze) i CISA (Agencja ds. cyberbezpieczeństwa i bezpieczeństwa infrastruktury) wydały wspólne ostrzeżenie dla opinii publicznej o wykorzystywaniu tej luki przez atakujące państwa. W momencie ujawnienia informacji RiskIQ zaobserwował 7956 instancji tych systemów aktywnych i działających w Internecie.

CVE-2021-42321 — Microsoft Exchange

Podczas międzynarodowego szczytu cyberbezpieczeństwa i zawodów hakerskich Tianfu Cup, które odbyły się 16–17 października 2021 r. w Chengdu w Chinach, odkryto lukę zero-day w Exchange (CVE-2021-42321). Badacze bezpieczeństwa Microsoft zaobserwowali wykorzystanie tej luki w Exchange w świecie rzeczywistym 21 października, zaledwie trzy dni po jej ujawnieniu. W momencie ujawnienia informacji RiskIQ zaobserwował 61 559 instancji tych systemów aktywnych i działających w Internecie. Obserwację wykorzystania luk kontynuowaliśmy do listopada 2021 r.

CVE-2022-26134 Confluence

Powiązana z Chinami grupa prawdopodobnie dysponowała programem atakującym lukę zero-day w Confluence (CVE-2022-26134) cztery dni przed jej publicznym ujawnieniem 2 czerwca i wykorzystała go przeciwko podmiotowi ze Stanów Zjednoczonych. W momencie ujawnienia informacji RiskIQ zaobserwował 53 621 instancji podatnych systemów Confluence w Internecie.

Luki w zabezpieczeniach są wykrywane i wykorzystywane na masową skalę w coraz krótszym czasie.

Praktyczne wskazówki

1. Priorytetowo traktuj usuwanie luk zero-day przez stosowanie poprawek zaraz po ich wydaniu. Nie czekaj ze stosowaniem poprawki na cykl wdrażania poprawek.
2. Dokumentuj i inwentaryzuj wszystkie zasoby sprzętowe i programowe firmy, aby szybko identyfikować zagrożenia i ustalać, kiedy zastosować poprawki.

Wojenna cybertaktyka atakujących powiązanych z Rosją zagraża nie tylko Ukrainie

Atakujący powiązani z Rosją rozpoczęli w tym roku cyberoperacje, niejako uzupełniając działania wojskowe związane z inwazją Rosji na Ukrainę, a często wykorzystując te same taktyki i techniki, które są stosowane przeciwko celom poza Ukrainą. Jest niezwykle ważne, aby organizacje na całym świecie podjęły działania zwiększające odporność przed cyberzagrożeniami pochodzącymi od atakujących powiązanych z Rosją.

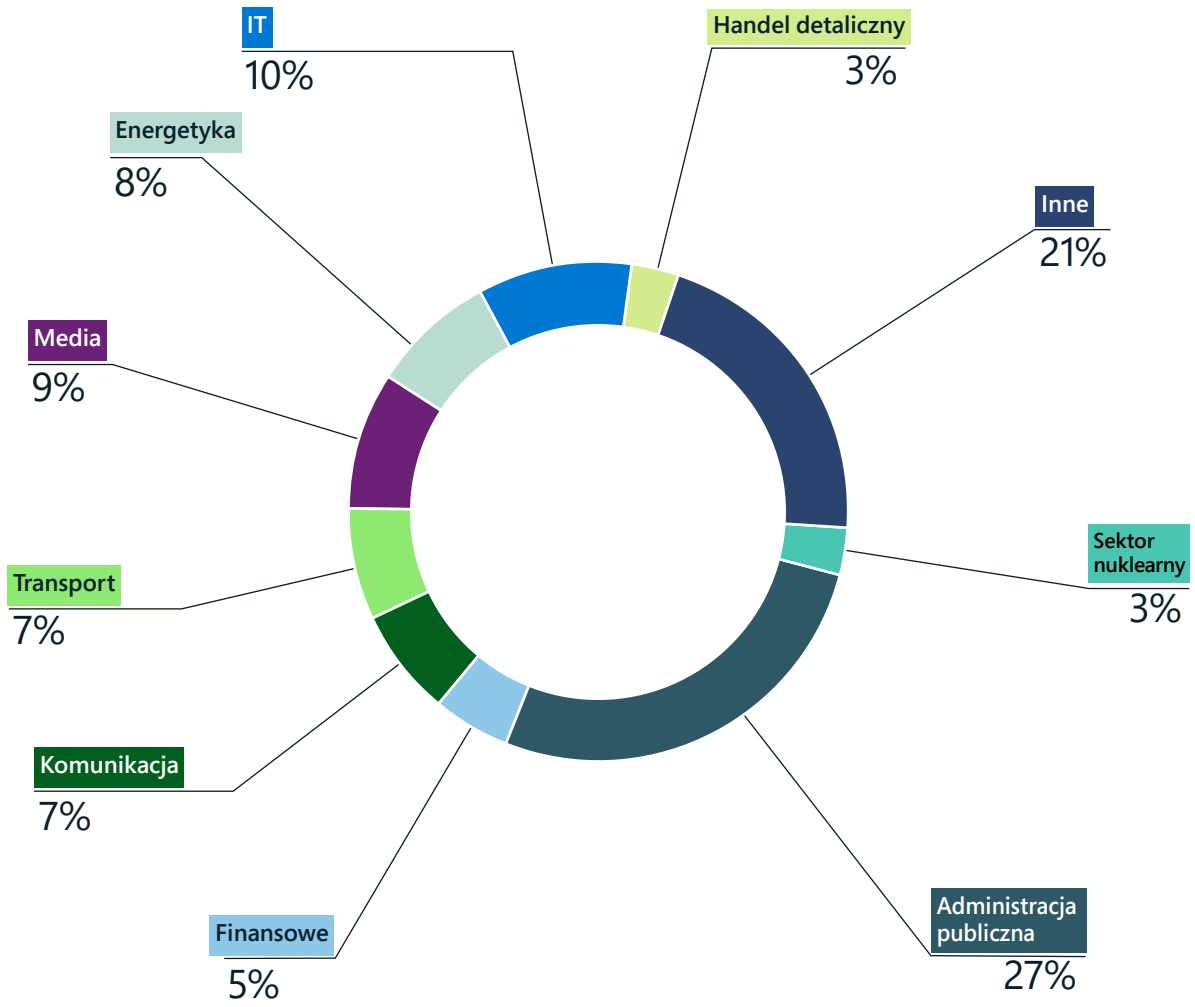
Sytuacja ulega zmianie wraz z toczeniem się konfliktu zbrojnego. Ukraina i jej sojusznicy powinni być przygotowani, że atakujący powiązani z Rosją mogą zwiększyć intensywność włamań, by wesprzeć cele wojskowe. W ciągu pierwszych czterech miesięcy wojny Microsoft zaobserwował, jak atakujący związani z rosyjską armią przeprowadzili wiele fal destrukcyjnych cyberataków na blisko 50 różnych ukraińskich instytucji i przedsiębiorstw oraz skoncentrowanych na szpiegostwie włamań na wiele innych. Z wyłączeniem operacji wymierzonych w klientów usług online 64% rosyjskich zagrożeń skierowanych przeciwko znanym celom od końca lutego do czerwca dotyczyło organizacji na Ukrainie.

W każdej operacji atakujący związani z Rosją stosowali wiele taktyk, technik i procedur, które zaobserwowaliśmy przed inwazją przeciwko celom zarówno na Ukrainie, jak i poza nią. Ich celem było zniszczenie danych i wytrącenie z równowagi ukraińskich instytucji administracji publicznej w początkowym okresie konfliktu. Od tego czasu celem jest zakłócenie transportu pomocy wojskowej i humanitarnej na Ukrainę oraz dostępu do usług użyteczności publicznej i innego typu, a także wykradzenie informacji o dużej wartości wywiadowczej lub gospodarczej dla Rosji.

Ataki na transport zagrażają obszarowi o krytycznym znaczeniu dla obywateli Ukrainy próbujących przetrwać konflikt. Według sondażu przeprowadzonego w maju przez UNICEF respondenci z obszarów miejskich dotkniętych konfliktem najbardziej martwili się o transport i paliwo, zakłócenia w dostawach, bezpieczeństwo oraz ograniczony dostęp do żywności, usług medycznych i finansowych[10]. W czerwcu koordynator ONZ ds. kryzysu na Ukrainie powiedział, że co najmniej 15,7 mln osób na Ukrainie pilnie potrzebuje pomocy humanitarnej, a liczba ta będzie rosła w miarę trwania wojny[11].

Poza Ukrainą Microsoft wykrył od końca lutego do czerwca rosyjskie próby włamania do sieci przeciwko 128 organizacjom w 42 krajach. Stany Zjednoczone były głównym celem Rosji. Polska, przez którą przechodzi znaczna część międzynarodowej pomocy wojskowej i humanitarnej dla Ukrainy, była w tym okresie również istotnym celem. Atakujący powiązani z Rosją w kwietniu i maju obrali za cel organizacje w krajach bałtyckich oraz sieci komputerowe w Danii, Norwegii, Finlandii i Szwecji.

Najbardziej atakowane sektory na Ukrainie od czasu inwazji



Federalne, państwowe i lokalne organizacje administracji publicznej na Ukrainie pozostały priorytetowymi celami dla rosyjskich państwowych i powiązanych z państwem atakujących w trakcie całego konfliktu. Skupienie się na organizacjach sektora transportowego, energetycznego, finansowego i medialnego podkreśla ryzyko, jakie te cyberoperacje stanowią dla usług, na których polegają obywatele Ukrainy.

Wojenna cybertaktyka atakujących powiązanych z Rosją zagraża nie tylko Ukrainie

(c.d.)

Obserwujemy wzrost podobnej aktywności, której celem są ministerstwa spraw zagranicznych państw NATO.

W minionym roku atakujący powiązani z Rosją byli nadal zainteresowani naruszeniem infrastruktury krytycznej zarówno na terenie Ukrainy, jak i poza nią. Grupa IRYD wdrożyła złośliwe oprogramowanie Industroyer2 w nieudanej próbie pozostawienia milionów ludzi na Ukrainie bez prądu. Poza Ukrainą na początku 2022 r. grupa BROM przeprowadziła włamania do organizacji zajmujących się produkcją oraz przemysłowych systemów sterowania.

Rosyjskie grupy państwowe i powiązane z państwem prowadziły w tym roku cyberoperacje przeciwko Ukrainie, jej sojusznikom i innym celom o wartości wywiadowczej, wykorzystując wiele z poniższych taktyk, technik i procedur:

Ukierunkowane wyłudzanie informacji z wykorzystaniem złośliwych załączników lub linków

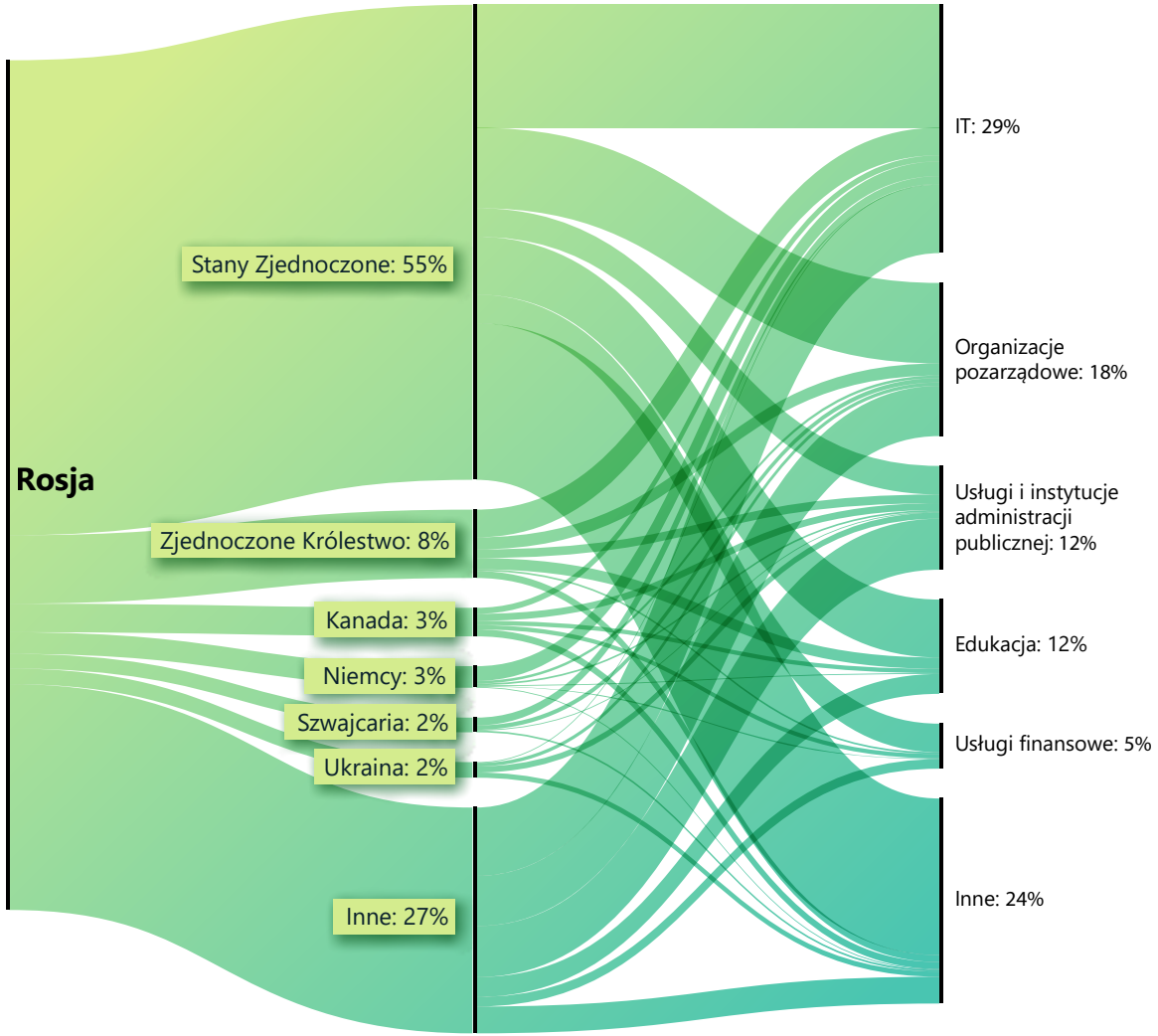
Rosyjskie grupy państwowe i powiązane z państwem, takie jak AKTYN, NOBEL, STRONT, DEV-0257, SEABORG i IRYD, wykorzystały kampanie wyłudzania informacji, aby uchwycić przyczółek dostępu do kont i sieci w organizacjach na terenie Ukrainy i poza nią. W wielu kampaniach, aby zwabić ofiary, użyto przejętych lub sfałszowanych kont w organizacjach-ofiarach lub w tej samej branży oraz przekonujących tematów. Grupa NOBEL wykorzystała przejęte konta dyplomatyczne do wysyłania wiadomości wyłudzających informacje, które były zamaskowane jako komunikaty dyplomatyczne do pracowników Ministerstw Spraw Zagranicznych na całym świecie. Grupa STRONT stworzyła fałszywe konta na podstawie publicznie dostępnych nazwisk posiadaczy kont w think tankach w Stanach Zjednoczonych i wysyłała wiadomości wyłudzające informacje w celu uzyskania dostępu do kont w tych think tankach. Grupa SEABORG przeprowadziła atak wyłudzający informacje wykorzystujący przynęty związane z relacjonowaniem konfliktu na Ukrainie w celu uchwycenia przyczółka dostępu do kont w think tankach zajmujących się sprawami międzynarodowymi w krajach nordyckich.

Wykorzystanie łańcucha dostaw usług IT w celu atakowania klientów na dole łańcucha

Pod koniec 2021 r. atakujący powiązani z Rosją skutecznie zaatakowali dostawców usług IT i wykorzystali dostęp do nich w celu uszkodzenia witryn internetowych oraz wdrożenia szkodliwego oprogramowania Whispergate przez DEV-0586 w styczniu[12]. DEV-0586 również skutecznie zaatakował sieć firmy informatycznej, która zbudowała systemy zarządzania zasobami dla MON Ukrainy oraz innych organizacji w sektorach komunikacji i transportu. Sugeruje to, że grupa badała możliwości ataku na strony trzecie również w tych sektorach.

Na całym świecie, ale przede wszystkim w Stanach Zjednoczonych i Europie Zachodniej, grupa NOBEL w latach 2021–2022 obrała za cel dostawców usług IT, aby uzyskać dostęp do sieci administracji publicznej i innych wrażliwych sieci (patrz omówienie luk w łańcuchach dostaw wcześniej w tym rozdziale).

Rosja: najbardziej atakowane kraje i sektory



Pomimo intensywnej koncentracji od początku 2022 r. na ukraińskich organizacjach przedsiębiorstwa z Ameryki Północnej i Europy Zachodniej nadal były najczęściej atakowanymi podmiotami przez grupy powiązane z Rosją. Kampania ataków NOBEL na firmy IT sprawiła, że w ubiegłym roku był to najbardziej atakowany sektor.

Wojenna cybertaktyka atakujących powiązanych z Rosją zagraża nie tylko Ukrainie

(c.d.)

Eksponowane w Internecie aplikacje przyczółkiem dostępu do sieci

Co najmniej od końca 2021 r. STRONT pracował nad udoskonalaniem możliwości w zakresie wykorzystywania usług publicznych, takich jak serwery Microsoft Exchange, w celu kradzieży informacji. STRONT wykorzystał serwery Exchange, w których nie stosowano poprawek, do uzyskania dostępu do ukraińskich kont administracji publicznej, a także organizacji związanych z wojskiem i sektorem obronności w Stanach Zjednoczonych, Libanie, Peru i Rumunii oraz innych instytucji administracji publicznej w Armenii, Bośni, Kosowie i Malezji. DEV-0586, również powiązany z rosyjską armią, wykorzystał luki w serwerze Confluence, aby uzyskać wstępny dostęp do organizacji administracji publicznej i sektora IT na Ukrainie i w innych krajach Europy Wschodniej.

Rosyjskie państwo i powiązane z nim grupy atakujących wykorzystują wiele z tych taktyk, technik i procedur do atakowania interesujących ich organizacji w czasie wojny i pokoju.

Wykorzystanie protokołów i kont administracyjnych oraz natywnych narzędzi do wykrywania sieci i jej penetracji

Microsoft zaobserwował, że po uzyskaniu wstępnego dostępu do sieci atakujący powiązani z Rosją wykorzystują legalne konta i oprogramowanie narzędziowe używane do wykonywania podstawowych zadań konserwacyjnych, aby jak najdłużej uniknąć wykrycia. Opierają się na wykradzionych tożsamościach z uprawnieniami administratora i ważnymi protokołami administracyjnymi, narzędziami i metodami, aby penetrować sieć bez natychmiastowego przyciągania uwagi automatycznych monitorów i obrońców sieci.

Podstawowa cyberhigiena oraz stosowanie narzędzi do wykrywania urządzeń klienckich i reagowania na nie może pomóc w reagowaniu na tego typu operacje zarówno w czasie pokoju, jak i wojny.

Nieprzewidywalność trwającego konfliktu wymaga od organizacji na całym świecie podjęcia działań mających na celu wzmocnienie cyberbezpieczeństwa przed cyfrowymi zagrożeniami pochodzącymi od rosyjskich grup państwowych i powiązanych z państwem.

Praktyczne wskazówki

1. Zminimalizuj ryzyko kradzieży poświadczeń i nadużywania uprawnień kont, chroniąc tożsamość użytkowników w kontach i systemach najbardziej wrażliwych i z wysokimi uprawnieniami przez wdrożenie ochrony tożsamości za pomocą uwierzytelniania wieloskładnikowego i przyznawania dostępu z minimalnymi uprawnieniami.
2. Stosuj aktualizacje tak szybko, jak to możliwe, aby wszystkie systemy miały najwyższy poziom ochrony i były aktualne.
3. Wdrażaj rozwiązania do ochrony przed złośliwym oprogramowaniem, wykrywania urządzeń klienckich i ochrony tożsamości w całej organizacji. Rozwiązania zabezpieczające „ochrony dogłębnej" w połączeniu z wyszkolonym personelem mogą umożliwić organizacji identyfikowanie i wykrywanie krytycznych włamań oraz zapobieganie im.
4. Umożliwiaj prowadzenie badań i odzyskiwanie danych w przypadku wykrycia zagrożenia lub otrzymania powiadomienia o nim — włącz tworzenie kopii zapasowych systemów krytycznych i rejestrowanie dzienników. Zdecydowanie zachęca się do stworzenia planu reagowania na incydenty.

Linki do dalszych informacji

- Obrona Ukrainy: pierwsze lekcje z cyberwojny | Microsoft On the Issues
- Wojna hybrydowa na Ukrainie | Microsoft On the Issues
- Cyberprzestępczość na Ukrainie: analizy i materiały | Microsoft Security Response Center (MSRC)
- Destrukcyjne cyberataki na Ukrainę | Microsoft On the Issues
- Ataki złośliwego oprogramowania na administrację publiczną Ukrainy | Microsoft On the Issues
- MagicWeb: Sztuczka NOBEL po udanym ataku — uwierzytelnianie się jako dowolny użytkownik | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

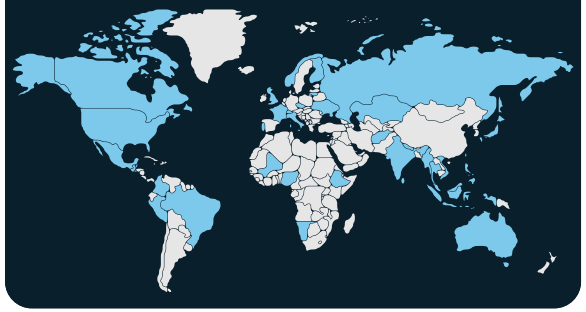
Chiny rozszerzają działania w celu zyskania przewagi konkurencyjnej

W dzisiejszym, złożonym klimacie geopolitycznym chińscy państwowi i powiązani z państwem atakujący prowadzący cyber-operacje często dążą do realizacji strategicznych celów wojskowych, gospodarczych i w zakresie stosunków zagranicznych w ramach dążenia Chin do osiągnięcia przewagi konkurencyjnej. W ostatnim roku Microsoft zaobserwował szeroko zakrojoną aktywność chińskich atakujących przeciwko krajom na całym świecie.

Od połowy 2021 r. Chiny chciały zapewnić stabilność gospodarczą i finansową w czasie najgorszego od dwóch lat skoku przypadków COVID-19[13]. Chiny nadal żonglowały swoim stanowiskiem w sprawie wydarzeń geopolitycznych, np. lawirowały między „bezgranicznym" partnerstwem z Rosją[14] a utrzymaniem swojej pozycji na scenie światowej[15]. Ponadto stanowisko Chin wobec Stanów Zjednoczonych i ich sojuszników w sprawie Tajwanu[16] i Morza Południowochińskiego nadal nadwyrężało stosunki zagraniczne z wieloma krajami[17].

Chińscy państwowi i powiązani z państwem atakujący zwiększyli liczbę ataków na mniejsze kraje na całym świecie, koncentrując się na Azji Południowo-Wschodniej, aby uzyskać przewagę konkurencyjną na wszystkich frontach.

Kraje będące celem ataków chińskich grup państwowych i powiązanych z państwem

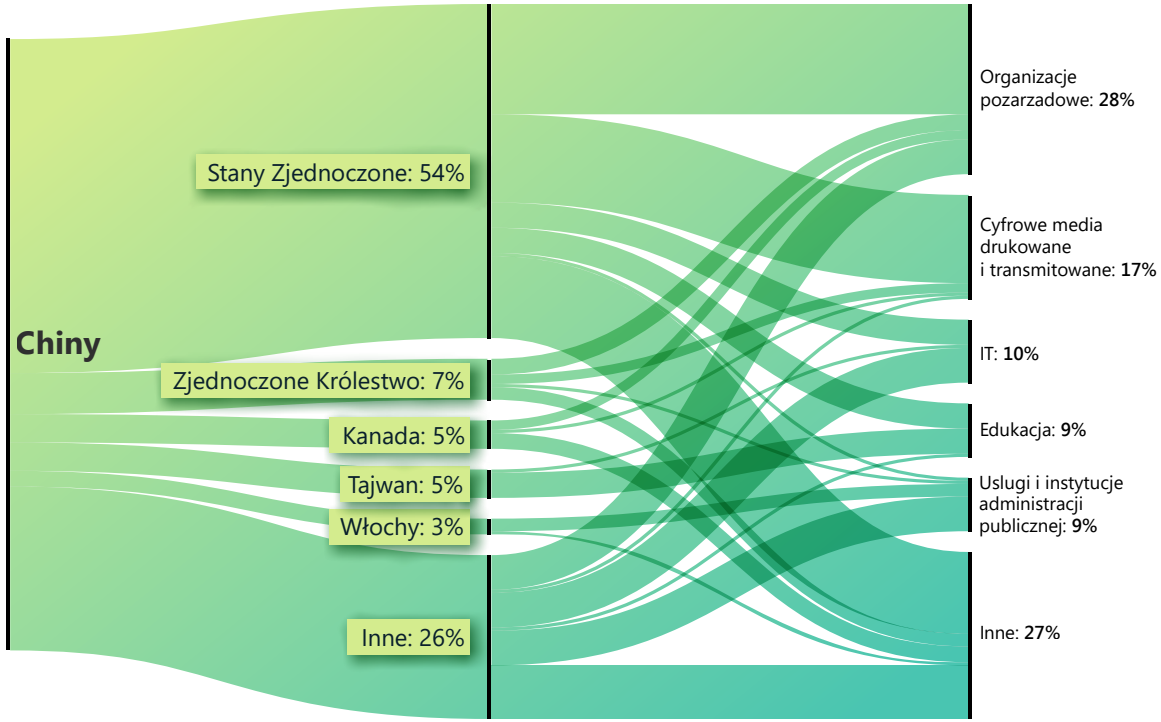


Chiny rozszerzały swoje wpływy gospodarcze na świecie na drodze wcześniej ustanowionej inicjatywy Pasa i Szlaku, próbując ożywić programy inwestycyjne z UE[18] i negocjując nową regionalną umowę handlową z 15 krajami Azji i Pacyfiku znaną jako Regional Comprehensive Economic Partnership (Regionalne Kompleksowe Partnerstwo Gospodarcze)[19]. Obserwując cyberoperacje i szeroką gamę atakowanych podmiotów, Microsoft ocenia, że Chiny nadal będą wykorzystywać zbieranie danych w cyberprzestrzeni jako narzędzie realizacji strategicznych celów politycznych, wojskowych i gospodarczych.

Cyberataki mogą prowadzić do rozwoju interesów gospodarczych i wojskowych.

Microsoft zaobserwował, że mniejsze kraje na całym świecie są powszechnie atakowane przez chińskie grupy państwowe i powiązane z państwem, co sugeruje, że Chiny prawdopodobnie wykorzystują cyberszpiegostwo jako element swoich globalnych wpływów gospodarczych i militarnych.

Chiny: najbardziej atakowane kraje i sektory



Think tanki/organizacje pozarządowe, media, IT, administracja publiczna i edukacja to sektory, które stanowiły najważniejszy cel dla atakujących powiązanych z Chinami, prawdopodobnie w celu ciągłego zbierania informacji wywiadowczych i prowadzenia rozpoznania.

Celami były m. in. kraje Afryki, Karaibów, Bliskiego Wschodu, Oceanii i Azji Południowej, ze szczególnym uwzględnieniem krajów Azji Południowo-Wschodniej i wysp Pacyfiku.

Zgodnie z chińską strategią Pasa i Szlaku atakujący powiązani z Chinami obrali za cel podmioty w Afganistanie, Kazachstanie, Mauritiusie, Namibii oraz Trynidadzie i Tobago[20]. Na przykład Trynidad i Tobago był pierwszym krajem karaibskim, który poparł chińską strategię BRI w 2018 r., a Chiny uważają go za ważnego partnera w regionie. Grupa NIKIEL od 2021 r. prowadziła ciągłe operacje sieciowe ukierunkowane na Trynidad i Tobago. Na przykład w marcu 2022 r. NIKIEL przeprowadził działania rozpoznawcze ukierunkowane na instytucje administracji publicznej, prawdopodobnie w celu gromadzenia danych wywiadowczych.

Chiny rozszerzają działania w celu zyskania przewagi konkurencyjnej

(c.d.)

Tymczasem Microsoft zaobserwował, że chińskie państwowe i powiązane z państwem grupy atakujących realizują operacje przeciwko podmiotom w Azji Południowo-Wschodniej i rozszerzają je na wyspiarskie kraje Pacyfiku. Chiny zmieniły swoje priorytety wojskowe i gospodarcze w odpowiedzi na ponowne zainteresowanie Stanów Zjednoczonych tym regionem. W styczniu 2022 r. Microsoft zaobserwował kampanię RAD, której celem była firma energetyczna i związana z energetyką instytucja administracji publicznej w Wietnamie oraz indonezyjska instytucja administracji publicznej. Działania RAD były zgodne ze strategicznymi celami Chin na Morzu Południowochińskim[21]. Pod koniec lutego i na początku marca kampania GAL naruszyła ponad 100 kont powiązanych z ważną organizacją międzyrządową (IGO) w regionie Azji Południowo-Wschodniej. Moment zaatakowania IGO w regionie w ramach GAL zbiegł się z zapowiedzią planowanego spotkania Stanów Zjednoczonych z regionalnymi przywódcami. Kampania GAL prawdopodobnie miała za zadanie monitorować komunikację i zbierać dane wywiadowcze przed tym wydarzeniem.

Działalność atakujących powiązanych z Chinami podążała za rozszerzaniem się wpływów Chin w krajach wyspiarskich Pacyfiku. W kwietniu Chiny i Wyspy Salomona podpisały umowę o bezpieczeństwie, której celem ma być „promowanie pokoju i bezpieczeństwa". Umowa pozwala Chinom na rozmieszczenie policji i uzbrojonego wojska na Wyspach Salomona[22]. W maju Chiny brały udział w drugim spotkaniu ministrów spraw zagranicznych Chin i krajów wyspiarskich Pacyfiku na Fidżi. Zaproponowały „wszechstronne partnerstwo strategiczne" w celu dalszego zacieśniania współpracy politycznej, kulturalnej, społecznej oraz w zakresie bezpieczeństwa i zmian klimatycznych, a także walki z pandemią[23]. Mniej więcej w tym samym czasie (w maju) Microsoft zidentyfikował złośliwe oprogramowanie GADOLIN w systemach administracji publicznej Wysp Salomona. RAD wprowadził także złośliwy kod w systemy firmy telekomunikacyjnej w Papui Nowej Gwinei. Oceniamy, że działania te prawdopodobnie służyły gromadzeniu danych wywiadowczych na potrzeby realizacji ogólnej strategii regionalnej Chin.

Microsoft przeciwdziała kampanii NIKIEL, ale atakujący nie poddają się.

W grudniu 2021 r. Microsoft Digital Crimes Unit (DCU) złożył pisma procesowe w Sądzie Okręgowym Stanów Zjednoczonych dla Wschodniego Dystryktu Wirginii, ubiegając się o konfiskatę 42 domen sterowania i kontroli grupy NIKIEL. Te domeny były wykorzystywane w operacjach przeciwko administracji publicznej, podmiotom dyplomatycznym i organizacjom pozarządowym w całej Ameryce Środkowej i Południowej, na Karaibach, w Europie i Ameryce Północnej od września 2019 r.[24] Poprzez te operacje NIKIEL uzyskał długoterminowy dostęp do kilku podmiotów i konsekwentnie eksfiltrował dane od końca 2019 r.

W miarę jak Chiny będą nawiązywać dwustronne relacje gospodarcze z kolejnymi krajami — często w ramach umów związanych z inicjatywą Pasa i Szlaku — globalne wpływy Chin będą rosły. Oceniamy, że chińskie państwowe i powiązane z państwem grupy atakujących będą atakować cele w administracji publicznej, dyplomacji i organizacjach pozarządowych w celu uzyskania nowych informacji, prawdopodobnie w ramach szpiegostwa gospodarczego lub tradycyjnych celów związanych z gromadzeniem danych wywiadowczych. Od czasu przeciwdziałania przez Microsoft grupa NIKIEL zaatakowała kilka instytucji administracji publicznej, prawdopodobnie próbując odzyskać utracony dostęp. Między końcem marca a majem 2022 r. NIKIEL ponownie skutecznie zaatakował co najmniej pięć instytucji administracji publicznej na całym świecie. Sugeruje to, że grupa miała dodatkowe punkty wejścia do tych podmiotów lub odzyskała dostęp poprzez nowe domeny sterowania i kontroli. Uporczywość NIKIEL w wielokrotnym naruszaniu tych samych instytucji administracji publicznej na całym świecie wskazuje na to, że jest to ważne zadanie postawione na wysokim szczeblu.

Chiny bardziej asertywnie podchodzą do polityki zagranicznej. Oceniamy, że cyberszpiegostwo gospodarcze i zbieranie informacji wywiadowczych będzie kontynuowane.

Praktyczne wskazówki

1. Wzmocnij cyberobronę, aby proaktywnie minimalizować cyberzagrożenia. Uporczywa działalność atakujących powiązanych z Chinami wymaga od organizacji szybkiego identyfikowania i wykrywania włamań, a także ochrony przed nimi i reagowania na nie.
2. Atakujący jako powszechną metodę utrzymywania się w naruszonych systemach i unikania działań obrony wykorzystują zaplanowane zadania[25]. Upewnij się, że Twoje środowisko stosuje dodatkowe wytyczne bezpieczeństwa w celu ochrony przed tą powszechnie stosowaną techniką[26].
3. Nadal obserwujemy wykorzystanie powłok sieciowych jako początkowego wektora umożliwiającego dostęp do sieci ofiar[27]. Organizacje powinny wzmocnić swoje systemy przed atakami na powłoki sieciowe, które mogą zapewnić napastnikom dostęp do uruchamiania zdalnych poleceń[28].

Linki do dalszych informacji

- NIKIEL atakuje instytucje administracji publicznej w Ameryce Łacińskiej i Europie | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Ochrona ludzi przed cyberatakami | Microsoft On the Issues

Iran jest coraz bardziej agresywny po zmianie władzy

Microsoft zaobserwował, że irańskie państwowe i powiązane z państwem grupy atakujących zwiększyły intensywność i zakres cyberataków na Izrael, rozszerzyły ataki ransomware z regionalnych przeciwników na ofiary w Stanach Zjednoczonych i UE, a także obrały za cel amerykańską infrastrukturę krytyczną, aby uchwycić przyczółek na potrzeby potencjalnych, niszczycielskich cyberataków.

Wzrost cyberagresji atakujących powiązanych z Iranem nastąpił po zmianie władzy prezydenckiej. Latem 2021 r. bezkompromisowy prezydent Ibrahim Raisi zastąpił umiarkowanego Hassana Rouhaniego. Raisi jest protegowanym Najwyższego Przywódcy i bliskim sojusznikiem Korpusu Strażników Rewolucji Islamskiej (IRGC). Preferowanie przez byłego prezydenta Rouhaniego dyplomacji przynosiło mu konflikty z Najwyższym Przywódcą i starszymi przywódcami IRGC[29]. Wydaje się, że pomimo wznowienia dyplomacji na rzecz porozumienia nuklearnego z Iranem jastrzębie poglądy administracji Raisiego skłoniły Iran do nasilania działań przeciwko Izraelowi i Zachodowi, zwłaszcza Stanom Zjednoczonym.

Zwiększone tempo i zakres irańskich cyberataków na Izrael

W ciągu kilku tygodni od zakończenia przez Raisiego formowania swojego zespołu ds. polityki zagranicznej[30] atakujący powiązani z Iranem wznowili destrukcyjne cyberataki na Izrael, zwiększając ich intensywność ponad poziom z zeszłego roku. Te ataki ransomware oraz hakowania i publikowania wykradzionych danych były przeprowadzane co kilka tygodni począwszy od września. Angażowały one co najmniej trzy grupy powiązane z Iranem. Sugeruje to, że mogły być one częścią ogólnokrajowej kampanii odwetu na Izraelu. W co najmniej jednym przypadku Microsoft ocenił, że atak ransomware na izraelską organizację pod koniec 2021 r. był jedynie przykrywką do ukrycia głównego ataku, którego celem było usunięcie danych. Analiza złośliwego oprogramowania przeprowadzona przez Microsoft pozwoliła ustalić, że ransomware dostarczone do ofiary miało po zaszyfrowaniu całkowicie usunąć dane.

W 2022 r. nastąpiła eskalacja irańskich cyberataków pod względem wyboru ich celów i formy. W lutym DEV-0198 próbował przeprowadzić destrukcyjny atak na izraelską infrastrukturę krytyczną. Microsoft ocenia również, że grupa powiązana z Iranem była najprawdopodobniej odpowiedzialna za wyrafinowany cyberatak, który w czerwcu uruchomił w Izraelu syreny awaryjne systemów rakietowych, prawdopodobnie przez wykorzystanie oprogramowania przesyłającego dźwięk przez sieci IP.

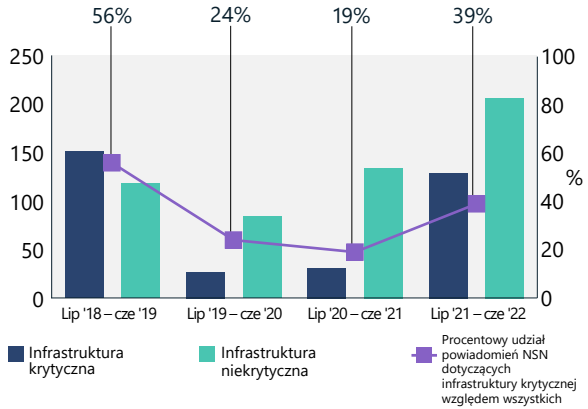
Irańskie zagrożenie dla amerykańskiej i izraelskiej infrastruktury krytycznej rosło przez cały rok

Atakujący powiązani z Iranem, którzy według oceny Microsoft są powiązani z IRGC (FOSFOR i DEV-0198), od końca 2021 do połowy 2022 r. atakowali amerykańską i izraelską infrastrukturę krytyczną. Prawdopodobnym celem było zapewnienie Teheranowi opcji odwetu na te same sektory, o których zakłócenie wyżsi urzędnicy IRGC w Iranie obwiniali Stany Zjednoczone i Izrael[31]. Oceniamy, że ta działalność jest powiązana z oświadczeniami z końca października 2021 r. generała IRGC Gholamrezy Jalaliego, szefa Irańskiej Organizacji Obrony Pasywnej, który powtórzył oskarżenia innych wpływowych postaci w reżimie, że Stany Zjednoczone i Izrael przeprowadziły cyberataki na irańskie porty, koleje i stacje paliw[32]. Jalali wygłosił to oskarżenie po raz drugi podczas zainscenizowanego przemówienia w czasie piątkowej modlitwy, której towarzyszył obraz pocisku uderzającego w słowo „USA". Sugeruje to, że jego przełożeni są tego samego zdania[33].

FOSFOR rozpoczął szerokie skanowanie amerykańskich organizacji w październiku 2021 r. pod kątem niezaktualizowanych luk Fortinet i ProxyShell. Te systemy z niezaktualizowanymi lukami, po skutecznym zaatakowaniu, zostały wykorzystane do przeprowadzenia ataków ransomware, w kilku przypadkach przeciwko infrastrukturze krytycznej w Stanach Zjednoczonych i innych krajach zachodnich. Były to pierwsze potwierdzone przypadki ataków ransomware dokonane przez grupy powiązane z Iranem przeprowadzone poza Bliskim Wschodem. Po cyberataku na irańskie stacje paliw pod koniec października Microsoft zaobserwował wzrost liczby irańskich ataków ransomware na firmy amerykańskie, co sugeruje możliwą korelację.

W tym samym czasie FOSFOR obrał sobie za cel, często za pomocą ukierunkowanego wyłudzania informacji, firmy obsługujące amerykańską infrastrukturę krytyczną, w tym główne porty morskie i lotniska, systemy tranzytowe, firmy użyteczności publicznej oraz firmy naftowe i gazowe. Takie ataki z precyzyjnie dobieranymi celami trwały do połowy 2022 r. — często były przeprowadzane metodami ukierunkowanego wyłudzania informacji. Cele ataków pokrywają się z sektorami, o których atakowanie Teheran oskarża Stany Zjednoczone i Izrael, i prawdopodobnie były odwetem ze strony Iranu. Atakowanie niemal identycznych celów może być próbą odwiedzenia od przyszłych ataków tego typu, a jednocześnie pozwala uniknąć eskalacji przez zasygnalizowanie przyczyny ataków bez przyznawania się do winy.

Ponowne irańskie ataki na infrastrukturę



Atakowanie przez Iran infrastruktury krytycznej wzrosło do najwyższych poziomów nienotowanych od końca 2018 r. do początku 2019 r. Wykorzystaliśmy US Presidential Policy Directive 21 (PPD-21), aby określić, czy dana firma pasuje do kryteriów infrastruktury krytycznej. (Lipiec 2021 r. – czerwiec 2022 r.).

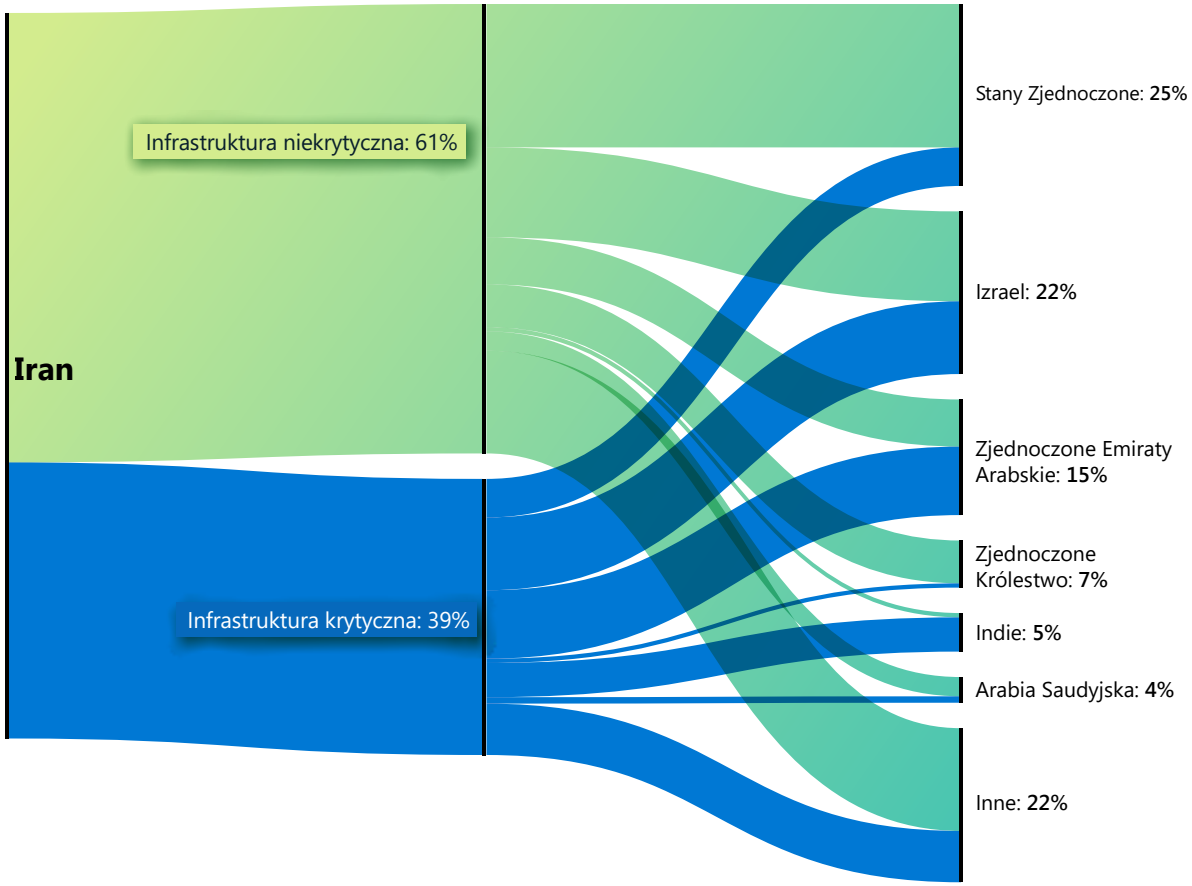
Iran jest coraz bardziej agresywny po zmianie władzy

(c.d.)

DEV-0198 koncentrował się na izraelskich kolejach, firmach logistycznych, dostawcach oprogramowania firm logistycznych i firmach paliwowych, ze szczególnym uwzględnieniem stacji paliw. Na początku 2022 r. grupa przeprowadziła destrukcyjny atak na sieć dużej izraelskiej firmy logistycznej, co zmusiło ją do wyłączenia systemów i wstrzymania części operacji w celu opanowania ataku. W innym przypadku zaobserwowaliśmy, że grupa próbowała uzyskać dostęp do sieci głównego izraelskiego dostawcy usług transportowych za pomocą skradzionych lub ponownie używanych poświadczeń. Tymczasem inna irańska grupa, DEV-0343, atakowała firmy zajmujące się obroną narodową, transportem morskim i obrazowaniem satelitarnym, co sugeruje jej powiązania z IRGC — na początku 2021 r. skutecznie zaatakowała konta izraelskich podmiotów związanych z transportem i portami.

Irańskie grupy prawdopodobnie pozostaną zagrożeniem dla amerykańskich i izraelskich firm transportowych i energetycznych, zwłaszcza że wysiłki dyplomatyczne zmierzające do odnowienia irańskiego porozumienia nuklearnego słabną, a Waszyngton, Tel Awiw i Teheran szukają alternatywnych środków przymusu, by wymusić ustępstwa.

Ataki Iranu na infrastrukturę krytyczną według kraju



Irańskie ataki na infrastrukturę krytyczną dotyczyły przede wszystkim organizacji izraelskich, emirackich i amerykańskich.

W nadchodzącym roku grupy irańskie prawdopodobnie pozostaną zagrożeniem dla amerykańskich i izraelskich firm transportowych i energetycznych.

Irańskie grupy rozszerzyły ataki ransomware z regionalnych przeciwników na amerykańską i izraelską infrastrukturę krytyczną.

Praktyczne wskazówki

1. Popraw ogólną cyberhigienę swojej organizacji, włączając rozwiązania bezhasłowe, takie jak uwierzytelnianie wieloskładnikowe, i egzekwując ich stosowanie dla wszystkich połączeń zdalnych, aby ograniczyć ryzyko wykorzystania wykradzionych poświadczeń.
2. Oceniaj autentyczność całego ruchu przychodzących e-maili, aby upewnić się, że adres nadawcy jest prawidłowy.
3. Stosuj poprawki bezpieczeństwa od razu i często[34].
4. Przeprowadź przegląd i kontrolę każdej z partnerskich relacji z dostawcami usług w celu zminimalizowania wszelkich zbędnych uprawnień pomiędzy Twoją organizacją a dostawcami na górze łańcucha. Microsoft zaleca natychmiastowe usunięcie dostępu wszelkim partnerom, z którymi relacje wyglądają na nieznane lub nie zostały jeszcze skontrolowane[35].

Linki do dalszych informacji

- Wzrost ataków Iranu na sektor IT | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Powiązany z Iranem DEV-0343 atakował sektor obronności, GIS i morski | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Libańska grupa powiązana z Iranem atakuje Izrael

Microsoft monitoruje cyberzagrożenia niezależnie od platformy, docelowej ofiary czy regionu geograficznego. Na bieżąco wyszukujemy zagrożenia na całym świecie, aby nasi klienci czuli się bezpiecznie.

Chociaż zagrożenia ze strony Rosji, Chin, Iranu i Korei Północnej stanowią większość obserwowanej przez nas aktywności państw, śledzimy i informujemy również o zagrożeniach ze strony państw członkowskich NATO i państw demokratycznych. W ubiegłym roku ujawniliśmy kampanię z Turcji (KRZEM) oraz z Wietnamu (BIZMUT). W tym roku uzupełniamy szczegóły dotyczące wcześniej ujawnionej grupy z Libanu[36].

Microsoft odkrył wcześniej nieudokumentowaną grupę z Libanu, która według naszej oceny (z umiarkowaną pewnością) działała w koordynacji z grupami powiązanymi z irańskim Ministerstwem Wywiadu i Bezpieczeństwa (MOIS). Takie współpracowanie z Teheranem lub kierowanie przez Teheran byłoby zgodne z ujawnianymi od końca 2020 r. informacjami, że Iran wykorzystuje strony trzecie do prowadzenia cyberoperacji, aby zapewnić sobie możliwość oficjalnego zaprzeczenia działaniom.

POLON w ramach operacji libańskich między lutym a majem 2022 r. zaatakował (w tym skutecznie) dziesiątki organizacji izraelskich i jedną międzynarodową, zanim Microsoft przerwał tę działalność i ujawnił ją publicznie. Prawie połowa izraelskich organizacji należała do izraelskiego sektora obronności lub miała z nim powiązania, co wskazuje na to, że ta grupa ma podobne interesy, co Iran, w zbieraniu informacji wywiadowczych na temat Izraela i bezpośredniego szkodzeniu temu krajowi[37].

Domniemane powiązania POLON z grupami MOIS opierają się na pokrywaniu się grup ofiar oraz jednolitości narzędzi i technik.

- Pokrywanie się ofiar: atakująca grupa powiązana z irańskim MOIS, którą Microsoft oznaczył jako RTĘĆ, wcześniej zaatakowała wiele ofiar kampanii POLON, co wskazuje na zbieżność wymagań misji lub „przekazywanie" ofiar między grupami.
- Wspólne narzędzia i techniki: MSTIC zaobserwował, że (podobnie jak POLON) DEV-0588 (znany również jako CopyKittens) wykorzystuje AirVPN, a DEV-0133 (znany również jako Lyceum[38]) wykorzystuje OneDrive do sterowania i kontroli oraz eksfiltracji. Podobnie jak grupy działające z inspiracji Iranu, POLON wykorzystał dostawcę usług chmurowych do zaatakowania izraelskiej firmy lotniczej i kancelarii prawnej[39].

POLON wdrożył serię niestandardowych implantów wykorzystujących usługi w chmurze na potrzeby sterowania i kontroli oraz ekfiltracji danych — zwłaszcza OneDrive i DropBox. POLON często tworzył unikalne aplikacje OneDrive dla ofiar, prawdopodobnie w celu uniknięcia wykrycia.

Od czerwca 2022 r. Microsoft zawiesił ponad 20 stworzonych przez POLON aplikacji OneDrive, powiadomił zaatakowane nimi organizacje i wdrożył serię aktualizacji w narzędziach zabezpieczających, aby poddać kwarantannie narzędzia stworzone przez POLON.

Microsoft skutecznie wykrył i uniemożliwił nadużywanie OneDrive przez POLON jako mechanizmu sterowania i kontroli.

Praktyczne wskazówki

1. Zaktualizuj narzędzia antywirusowe[40] i upewnij się, że ochrona w chmurze[41] jest włączona, aby móc wykrywać powiązane wskaźniki.
2. Jeśli masz relacje z dostawcami usług, przeprowadź przegląd i kontrolę wszystkich relacji partnerskich, aby zminimalizować niepotrzebne uprawnienia pomiędzy Twoją organizacją a dostawcami na górze łańcucha[42]. Natychmiast usuń dostęp wszelkim partnerom, z którymi relacje wyglądają na nieznane lub nie zostały jeszcze skontrolowane.

Linki do dalszych informacji

- Ujawnienie działalności i infrastruktury POLON, którego celem są organizacje izraelskie | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- RTĘĆ wykorzystuje luki w Log4j 2 w systemach bez zastosowanych poprawek do atakowania izraelskich organizacji | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

Północnokoreańskie cyberdziałania wspierają trzy główne cele reżimu

Priorytety Korei Północnej w cyberprzestrzeni w ubiegłym roku odzwierciedlały deklarowane przez rząd priorytety globalne. Kim Dzong Un w kilku kluczowych wystąpieniach podkreślił trzy priorytety: budowanie zdolności obronnych, wzmocnienie zmagającej się z problemami gospodarki kraju oraz zapewnienie stabilności wewnętrznej[43]. Ataki powiązane z Koreą Północną wyraźnie pokazują, że cyberprzestrzeń jest wykorzystywana do osiągnięcia tych trzech celów.

Atakujący powiązani z Koreą Północną stosowali różne taktyki, próbując przeniknąć do firm lotniczych na całym świecie.

Atakujący powiązani z Koreą Północną, głównie CER i CYNK, stosowali różne taktyki, aby przeniknąć do sieci firm z branży obronnej i lotniczej na całym świecie. Gdy w pierwszej połowie 2022 r. Korea Północna rozpoczęła najbardziej intensywny okres testów rakietowych w historii, dzięki cyberszpiegostwu chciała pomóc swoim naukowcom w opracowywaniu systemów obronnych w obliczu postępów przeciwników.

Zaobserwowaliśmy, że KOPERNIK atakuje na całym świecie firmy związane z kryptowalutami, często z powodzeniem, aby wspierać borykającą się z problemami gospodarkę Korei Północnej. Chociaż nie możemy potwierdzić, czy KOPERNIK wyprowadził pieniądze po skutecznym ataku, zaobserwowaliśmy, że zainfekował on dziesiątki urządzeń, wysyłając złośliwe dokumenty pod płaszczykiem propozycji od innych firm kryptowalutowych.

Wreszcie grupa, którą Microsoft oznaczył jako DEV-0215, pracowała nad utrzymaniem stabilności i lojalności społecznej w Korei Północnej, atakując organizacje informacyjne, które publikują wiadomości o sprawach północnokoreańskich. Te organizacje uzyskują informacje zarówno w Korei Północnej, jak i wśród uciekinierów, co Pjongjang postrzega jako zagrożenie egzystencjalne. Ponadto grupa pracowała nad uzyskaniem dostępu do sieci koreańskojęzycznych grup chrześcijańskich, które zwykle są otwarte na Koreę Północną i aktywnie współpracują z północnokoreańskimi uciekinierami.

Ukierunkowanie działań na firmy z sektora obronnego i lotniczego

Atakujący powiązani z Koreą Północną w ramach kampanii CER i CYNK włożyli wiele wysiłku w opracowanie taktyki mającej na celu penetrację przedsiębiorstw z sektora obronnego i lotniczego. CER wielokrotnie skanował południowokoreańskie sieci VPN, pobierając klientów i szukając słabych punktów. Pobierał również popularne aplikacje używane przez południowokoreańskich klientów wojskowych i administracji publicznej, prawdopodobnie w celu poszukiwania luk. Grupa uważnie śledziła bieżące wydarzenia i pisała nowe dokumenty wabiące, które jako przynęty wykorzystywały głośne tematy, aby zachęcić ofiary do kliknięcia złośliwych programów i linków.

Zarówno CYNK, jak i CER wykorzystywały w kampaniach media społecznościowe i inżynierię społeczną. CYNK był szczególnie sprawny w tworzeniu fałszywych profili na LinkedIn i innych profesjonalnych portalach społecznościowych, gdzie jego operatorzy podawali się za rekruterów głównych firm z sektora obronnego i lotniczego. Wykorzystując te profile, wysyłali oni linki lub załączniki ze złośliwymi plikami do potencjalnych ofiar za pomocą bezpośrednich wiadomości na mediach społecznościowych lub poczty elektronicznej.

Poza pracownikami korporacji CER atakował również szeroko członków południowokoreańskiej armii, wykazując szczególne zainteresowanie zarówno południowokoreańskimi akademiami wojskowymi, jak i wojskowymi pracującymi w środowisku akademickim.

Kradzież kryptowalut w celu pokrycia strat

Od czasu nałożenia sankcji ONZ w 2016 r. gospodarka Korei Północnej stale się kurczy, co jest spotęgowane przez klęski żywiołowe, takie jak powodzie[44] i susze[45], a także niemal całkowite zamknięcie granic dla importu od początku pandemii COVID-19 na początku 2020 r.[46] Chociaż Korea Północna na początku 2022 r. na krótko otworzyła swoje granice dla handlu z Chinami, wkrótce zostały one ponownie zamknięte[47]. W połowie maja Korea Północna zgłosiła pierwszy krajowy przypadek COVID-19[48]. Od tego czasu zastosowała strategię „zero-COVID" w stylu chińskim polegającą na masowych blokadach w celu zwalczania wirusa, co negatywnie wpłynęło na i tak już kruchą gospodarkę.

KOPERNIK, grupa powiązana z Koreą Północną, próbowała zrekompensować część utraconych przychodów, kradnąc pieniądze — zazwyczaj w formie kryptowalut — każdej firmie, której sieć udało się spenetrować. Zdołali oni skutecznie zaatakować dziesiątki urządzeń należących do firm związanych z kryptowalutami w Stanach Zjednoczonych, Kanadzie, Europie i całej Azji. KOPERNIK naruszył nawet urządzenia firm związanych z kryptowalutami w obrębie najsilniejszego sojusznika Korei Północnej, Chin, zarówno na kontynencie, jak i w Hongkongu. Grupa w dużej mierze polegała na mediach społecznościowych w zakresie wczesnego rozpoznania i wnikania do ofiar. Atakujący budowali profile udające programistów lub wyższych menedżerów w firmach związanych z kryptowalutami. Następnie nawiązywali relacje z osobami z branży, wysyłając złośliwe linki lub pliki po zyskaniu zaufania.

Północnokoreańskie cyberdziałania wspierają trzy główne cele reżimu

(c.d.)

Grupa powiązana z PLUTON opracowuje i wdraża oprogramowanie ransomware

Grupa atakujących powiązana z Koreą Północną, którą Microsoft oznaczył jako DEV-0530, zaczęła rozwijać i wykorzystywać ransomware w atakach w czerwcu 2021 r. Szajka ta, która nazwała siebie H0lyGh0st, wykorzystywała ładunek ransomware o tej samej nazwie i skutecznie atakowała małe firmy w wielu krajach już we wrześniu 2021 r.

Microsoft ocenił, że DEV-0530 ma powiązania z inną grupą związaną z Koreą Północną oznaczoną jako PLUTON (znaną również jako DarkSeoul lub Andariel). Wprawdzie wykorzystanie ransomware H0lyGh0st jest unikalne dla DEV-0530, MSTIC zaobserwował komunikację między tymi dwoma grupami oraz to, że DEV-0530 używa narzędzi stworzonych przez PLUTON.

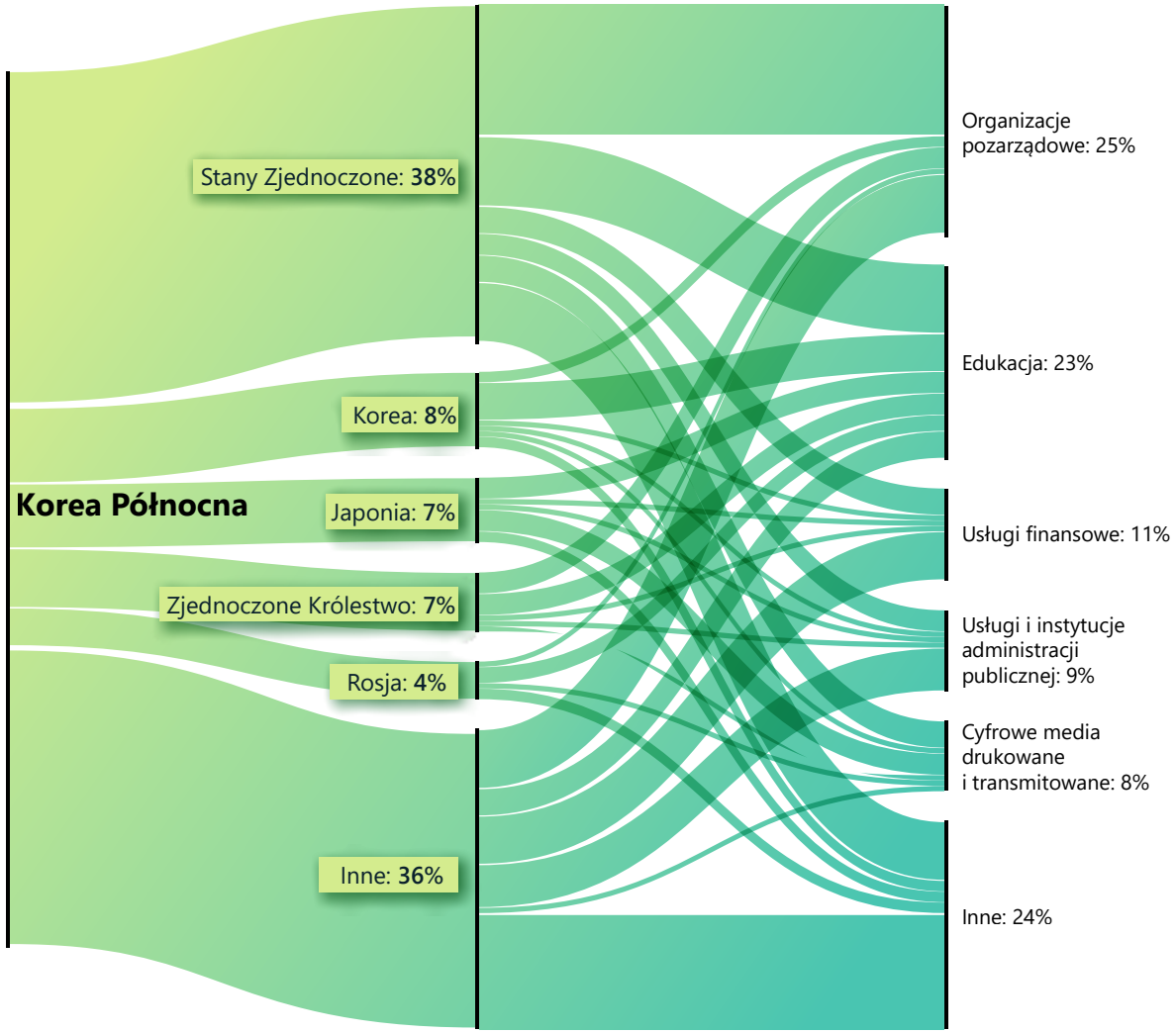
Nie jest pewne, czy działalność DEV-0530 była inspirowana przez rząd. Chociaż ataki ransomware mogły zostać zlecone przez rząd z tego samego powodu, dla którego sponsoruje on kradzieże z firm kryptowalutowych, możliwe jest również, że czynniki stojące za DEV-0530 działały niezależnie, aby zarobić dla siebie. Jeśli byli to północnokoreańscy hakerzy działający niezależnie, wyjaśniałoby to, dlaczego aktywność nie była szeroko rozpowszechniona w porównaniu do sponsorowanych przez rząd operacji kradzieży przeciwko firmom kryptowalutowym.

Atakowanie serwisów informacyjnych, uciekinierów, grup religijnych i organizacji pomocowych przez Korę Północną

W ubiegłym roku najwyższy przywódca Kim Dzong Un skupiał się publicznie bardziej na bezpieczeństwie wewnętrznym i lojalności niż na rakietach i broni jądrowej. Odzwierciedlając to zaabsorbowanie sprawami wewnętrznymi, przynajmniej dwie grupy powiązane z Koreą Północną skoncentrowały się na aspektach, które reżim postrzegałby jako zagrożenia wewnętrzne.

Pierwszą z nich była grupa, którą Microsoft nazwał DEV-0215, a która atakuje organizacje medialne ściśle śledzące wiadomości z Korei Północnej. Jednym z prawdopodobnych powodów takiego ataku jest fakt, że media te uzyskują informacje od uciekinierów z Korei Północnej, ściśle współpracujących z Koreą Północną obywateli Chin, a nawet mieszkańców Korei Północnej wykorzystujących różne metody komunikacji ze światem zewnętrznym. Rząd północnokoreański postrzega te grupy jako egzystencjalne zagrożenie dla swojego istnienia. Dotyczy to zwłaszcza mieszkańców Korei Północnej, którzy są postrzegani jako zdrajcy i szpiedzy. DEV-0215 prawdopodobnie starał się zidentyfikować źródła tych mediów, aby móc zneutralizować potencjalne wycieki informacji.

Korea Północna: najbardziej atakowane kraje i sektory



Korea Północna jako swoich głównych wrogów postrzega Stany Zjednoczone, Koreę Południową i Japonię. Chociaż Rosja jest długoletnim sojusznikiem, grupy atakujących powiązane z Koreą Północną obierają za cel rosyjskie think tanki, pracowników akademickich i urzędników dyplomatycznych, aby uzyskać informacje o rosyjskich poglądach na sprawy światowe.

Północnokoreańskie cyberdziałania wspierają trzy główne cele reżimu

(c.d.)

Microsoft ma również dowody na to, że DEV-0215 atakuje w koreańskojęzyczne społeczności chrześcijańskie. Ewangeliczne kościoły koreańskie są zazwyczaj krytyczne zarówno wobec Korei Północnej, jak i rządów południowokoreańskich, które sprzyjają współpracy z Koreą Północną. Kościoły te prowadzą działania na rzecz uchodźców i angażują się w pomoc humanitarną. Korea Północna postrzega je jako zagrożenie. Strumień uciekinierów z Korei Północnej niemal wysechł podczas pandemii[49]. Ci, którzy jednak uciekają, otrzymują kluczową pomoc od grup chrześcijańskich. DEV-0215 stworzył fałszywe dokumenty o chrześcijańskich konferencjach dla koreańskich mówców jako przynęty w celu rozpracowania grupy i odkrycia, kto pomaga w ucieczkach.

Wreszcie OSM, grupa atakujących powiązana z państwem, przez cały rok wykazywała stałe zainteresowanie międzynarodowymi organizacjami pomocowymi, w tym takimi, które w przeszłości pomagały Korei Północnej. Wprawdzie Korea Północna unikała ofert pomocy z zewnątrz, zwłaszcza od czasu wybuchu COVID-19[50], możliwe jest, że rozważa jej przyjęcie, ale obawia się konsekwencji w zakresie bezpieczeństwa związanych z wpuszczeniem do kraju zagranicznych pracowników pomocowych. Korea Północna może penetrować sieci organizacji pomocowych na całym świecie, aby ustalić, które z nich wpuścić do kraju.

Praktyczne wskazówki

1. Atakujący związani z Koreą Północną są wykwalifikowani, nieugięci i kreatywni, ale organizacje mogą się przed nimi bronić.
2. Większość naruszeń można powstrzymać dzięki podstawowej cyberhigienie, takiej jak uwierzytelnianie dwuskładnikowe czy nieotwieranie załączników od nieznanych osób w środowisku wirtualnym.

Linki do dalszych informacji

- Grupy powiązane z Koreą Północną atakują małe i średnie firmy, używając ransomware H0lyGh0st | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Wśród ekspertów zajmujących się Koreą Północną od dawna toczy się dyskusja, czy rząd północnokoreański jest szczery w swoich publicznych oświadczeniach, czy też blefuje. Zgodność cyberataków z głoszonymi przez Koreę Północną priorytetami oznacza, że komunikowane publicznie cele pokrywają się z czynami.

Cybernajemnicy zagrażają stabilności cyberprzestrzeni

Rośnie sektor prywatnych firm, które opracowują i sprzedają narzędzia, techniki i usługi umożliwiające klientom — często rządom — włamywanie się do sieci, komputerów, telefonów i urządzeń podłączonych do Internetu. Podmioty te są narzędziem w rękach ofensywnych państw. Często zagrażają dysydentom, obrońcom praw człowieka, dziennikarzom, obrońcom społeczeństwa obywatelskiego i innym obywatelom. Określamy ich cybernajemnikami lub podmiotami atakującymi z sektora prywatnego.

Świat, w którym firmy sektora prywatnego tworzą i sprzedają cyberbroń, jest bardziej niebezpieczny dla konsumentów, przedsiębiorstw każdej wielkości i rządów. Te ofensywne narzędzia mogą być wykorzystywane w sposób niezgodny z normami i wartościami dobrego rządzenia i demokracji. Microsoft uważa, że ochrona praw człowieka jest podstawowym obowiązkiem, który traktujemy poważnie, zwalczając „inwigilację jako usługę" na całym świecie.

Microsoft ocenił, że niektóre czynniki państwowe w demokracjach i reżimach autorytarnych zlecają na zewnątrz development lub wykorzystanie technologii „inwigilacji jako usługi". W ten sposób unikają odpowiedzialności i nadzoru, a także zdobywają zdolności, które trudno byłoby im stworzyć naturalnie.

> Te cyberbronie dają państwom możliwości inwigilacji, których nie byłyby w stanie same rozwinąć.

Rynek, na którym działają cybernajemnicy, jest nietransparentny. Niemniej nadal obserwujemy, jak te grupy stosują model „inwigilacji jako usługi", wykorzystując exploity „zero-day", a nawet „zero-click", w przypadku których ofiara nie musi nawet podjąć interakcji.

Microsoft ogłosił niedawno, że europejski podmiot atakujący z sektora prywatnego, którego określamy jako KNOTWEED, to austriacka firma DSIRF. Wiele doniesień łączy tę firmę z opracowaniem i próbą sprzedaży zestawu złośliwych narzędzi o nazwie Subzero[51]. Ofiarami są firmy prawnicze, banki i firmy doradztwa strategicznego w Austrii, Zjednoczonym Królestwie i Panamie[52].

Ponieważ te ofensywne systemy inwigilacji nie są już ściśle tajnymi narzędziami stworzonymi przez instytucje obronne i wywiadowcze, ale produktami komercyjnymi oferowanymi firmom i osobom prywatnym, wszelkie regulacje dotyczące cyberbroni muszą wykroczyć tylko poza kontrolę eksportu. Te cyberbronie mogą być niszczące.

Kiedy cybernajemnik wykorzystuje lukę w produkcie lub usłudze, naraża na niebezpieczeństwo cały ekosystem informatyczny. Po publicznym ujawnieniu luk firmy ścigają się z czasem, aby wprowadzić zabezpieczenia, zanim dojdzie do szerokich ataków (zobacz naszą wcześniejszą dyskusję na temat wykorzystywania luk). Jest to niebezpieczny i trudny cykl zarówno dla dostawców oprogramowania (którzy muszą szybko opracowywać poprawki), jak i konsumentów produktów (którzy muszą natychmiast wdrażać poprawki).

Jako członek-założyciel Cybersecurity Tech Accord[53] — wiodącego sojuszu skupiającego ponad 150 firm technologicznych — Microsoft zobowiązał się do nieangażowania się w operacje ofensywne online. Podtrzymujemy to zobowiązanie i nasze obowiązki w zakresie praw człowieka. Zaangażowaliśmy się w zwalczanie działań przestępców i pracę w obszarze prawnym. Podkreślamy negatywne skutki usług cybernajemników. Nadal będziemy chronić naszych klientów.

> Cybernajemnicy tworzą i dostarczają funkcje „inwigilacji jako usługi", które są technologicznie zaawansowane i szeroko dostępne, w tym zaawansowane złośliwe oprogramowanie oraz całą gamę technik.

Praktyczne wskazówki dla administracji publicznej

1. Wdrożyć zasady w zakresie transparentności i nadzoru względem „inwigilacji jako usługi", w szczególności w obszarze zamówień publicznych, w tym zakazać działalności atakujących podmiotów, jak to uczyniły Stany Zjednoczone, umieszczając odpowiednie firmy na liście Departamentu Handlu.
2. Ustanowić ograniczenia po zwolnieniu z pracy dla byłych pracowników tego sektora.
3. Dążyć do obowiązku KYC („Poznaj swojego klienta") i zachęć firmy do przestrzegania zobowiązań w zakresie praw człowieka.

Linki do dalszych informacji

- Analiza KNOTWEED: Europejski podmiot atakujący z sektora prywatnego wykorzystuje exploity na luki zero-day | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Kontynuacja walki z atakami podmiotów z sektora prywatnego | Microsoft On the Issues

Operacjonalizacja norm cyberbezpieczeństwa na rzecz pokoju i bezpieczeństwa w cyberprzestrzeni

Pilnie potrzebujemy spójnych, globalnych ram, które nadadzą priorytet prawom człowieka i będą chronić ludzi przed lekkomyślnym zachowaniem czynników państwowych w sieci. Nigdzie nie widać tego wyraźniej niż w trwającej wojnie na Ukrainie. Pomijając globalny wysiłek, rządy mogą zadziałać od razu, by poprawić sytuację.

Pięć lat temu Microsoft wezwał do stworzenia „cyfrowej konwencji genewskiej", która normowałaby odpowiedzialność i zobowiązania we wszystkich sektorach na rzecz obrony pokoju i bezpieczeństwa online. Cyberprzestrzeń stawała się odrębnym, niestabilnym obszarem konfliktów i rywalizacji między państwami. Ataki stawały się coraz częstsze, nawet w czasach pokoju.

Dziś nadal istnieje wyraźna potrzeba takich ram — czego dowodem są rosyjskie cyberataki na Ukrainę w ramach inwazji Rosji. Ta wojna stworzyła nową linię frontu, która znacznie różni się od znanych wcześniej.

Zapewnienie stabilności w cyberprzestrzeni będzie wymagało wzmocnienia i przeobrażenia globalnych instytucji, tak aby dostosować je do nowych realiów. Cyberprzestrzeń różni się zasadniczo od innych dziedzin — jest pozbawiona granic, syntetyczna i utrzymywana w dużej mierze przez przemysł prywatny. Oznacza to konieczność zwrócenia się do branży technologicznej o wzięcie większej odpowiedzialności zarówno za bezpieczeństwo produktów i usług, jak i za cały ekosystem cyfrowy. Choć na wszystkich frontach dokonano znaczących postępów, wyzwania dramatycznie wzrosły.

Musimy podwoić wspólne wysiłki na rzecz bezpieczeństwa w cyberprzestrzeni. Nie możemy uznawać za przyrodzone praw i wolności, których oczekiwaliśmy w Internecie. Podczas gdy my zmagamy się z tymi wyzwaniami, atakujący planują, jak i gdzie uderzyć w następnej kolejności, wykorzystując AI oraz dezinformację, a także znajdują sposoby na osłabienie raczkującego metaverse. Obrońcy praw człowieka, przemysł technologiczny i szanujące prawa rządy muszą współpracować na rzecz pozytywnej wizji bezpiecznego świata online. Droga jest długa. Jednak rządy mogą już teraz wykonać konkretne działania, aby natychmiast poprawić ekosystem cyberbezpieczeństwa:

- Podawać autorów ataków oraz przytaczać normy, prawa i konsekwencje. W ciągu ostatnich pięciu lat nastąpiła znaczna poprawa w zakresie szybkości i koordynacji podawania przez rządy autorów cyberataków. Poza nazwaniem i infamią oświadczenia te muszą podkreślać, jakie międzynarodowe prawa lub normy zostały naruszone i jakie konsekwencje zostaną wyciągnięte. Wzmocni to międzynarodowe dążenia do ścigania tych przestępstw.
- Podawać interpretację prawa międzynarodowego online. Chociaż rządy zgadzają się, że prawo międzynarodowe ma zastosowanie w Internecie, pozostają pytania dotyczące sposobu jego stosowania w konkretnych przypadkach. Jest to szczególnie istotne w następstwie inwazji na Ukrainę. Rządy mogą w znacznym stopniu przyczynić się do ustalenia oczekiwań, uniknięcia nieporozumień i zbudowania zaufania poprzez określenie, jak rozumieją swoje zobowiązania wynikające z prawa międzynarodowego.
- Konsultować z innymi zainteresowanymi stronami. Fora międzynarodowe powoli odkrywają, jak wspierać integrację multilateralną. Rządy mogą stymulować rzeczowy dialog poprzez konsultacje z różnorodnymi środowiskami, w szczególności z przemysłem technologicznym, w celu zapewnienia oparcia się na ludziach dysponujących odpowiednim doświadczeniem.
- Utworzyć stały organ wspierający odpowiedzialne zachowanie państw w cyberprzestrzeni. Praca międzynarodowych forów dyplomatycznych na rzecz odpowiedzialnego zachowania państw w sieci nigdy nie była tak ważna. Istnieje wyraźna potrzeba stworzenia stałego mechanizmu ONZ, który zajmowałby się cyberprzestrzenią jako domeną konfliktu.
- Określić nowe normy dla ewoluujących zagrożeń. Zagrożenia w cyberprzestrzeni stale ewoluują wraz z innowacjami technologicznymi. Chociaż normy międzynarodowe powinny być neutralne technologicznie, będą musiały być aktualizowane i łagodzone w oparciu o zmiany w krajobrazie zagrożeń i sposobie korzystania z technologii. Obserwujemy wykorzystywanie luk w obecnych regulacjach międzynarodowych. Państwa powinny zobowiązać się do zdecydowanego zabezpieczenia podstawowych procesów ekosystemu cyfrowego, które nie są obecnie chronione, takich jak proces aktualizacji oprogramowania. Ponadto wybrane obszary zasługują na dodatkową opiekę. Na przykład w czasie pandemii odkryliśmy, że niezbędne są normy dotyczące ochrony opieki zdrowotnej.

Ataki ze strony ofensywnych państw są coraz częstsze i coraz bardziej wyrafinowane. Ta sytuacja nie może być akceptowana.

Konieczne jest podjęcie natychmiastowych działań — rządy mogą już teraz podjąć działania mające na celu natychmiastową poprawę ekosystemu cyberbezpieczeństwa, w tym wdrożenie uzgodnionych norm i zasad dotyczących zachowania państw w cyberprzestrzeni oraz współpracy ze społecznością złożoną z wielu zainteresowanych stron w celu wyeliminowania pojawiających się luk.

Należy przeobrazić multilateralne instytucje tak, aby sprostać pilnemu wyzwaniu, jakim są cyberataki ze strony państw.

Linki do dalszych informacji

- Chwila zastanowienia: Potrzeba silnej i globalnej reakcji w zakresie cyberbezpieczeństwa | Microsoft On the Issues
- Cyberataki na opiekę zdrowotną muszą się skończyć | Microsoft On the Issues
- Kolejny rozdział cyberdyplomacji w ONZ | Microsoft On the Issues

Przypisy końcowe

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. Infrastruktura krytyczna w tym rozdziale jest zdefiniowana przez Presidential Policy Directive 21 (PPD-21), „Bezpieczeństwo i odporność infrastruktury krytycznej" (luty 2013 r.).
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

Przypisy końcowe — c.d.

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. W szczególności należy zaktualizować serwery Exchange pod kątem luk ProxyShell (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 oraz CVE-2021-27065, CVE-2021-34473). Należy również pamiętać o zaktualizowaniu luk w urządzeniach Fortinet FortiOS SSL VPN.
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. „In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin", Jan-Philipp Hein, FOCUS Online, (2022 r.), 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; „We unveil the «Subzero» state trojan from Austria", Sugar Mizzy, Europe-cities (2021 r.), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; „We unveil the state Trojan «Subzero» from Austria", Andre Meister, Netzpolitik.org (2022 r.), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.
52. Jak zauważyliśmy na naszym blogu technicznym, ustalenie ofiar w konkretnym kraju nie musi oznaczać, że klient DSIRF w nim rezyduje, ponieważ powszechne jest atakowanie celów z innych państw.
53. Strona główna | Cybersecurity Tech Accord (cybertechaccord.org)

Urządzenia i infrastruktura

Wraz z przyspieszeniem transformacji cyfrowej bezpieczeństwo infrastruktury cyfrowej jest ważniejsze niż kiedykolwiek.

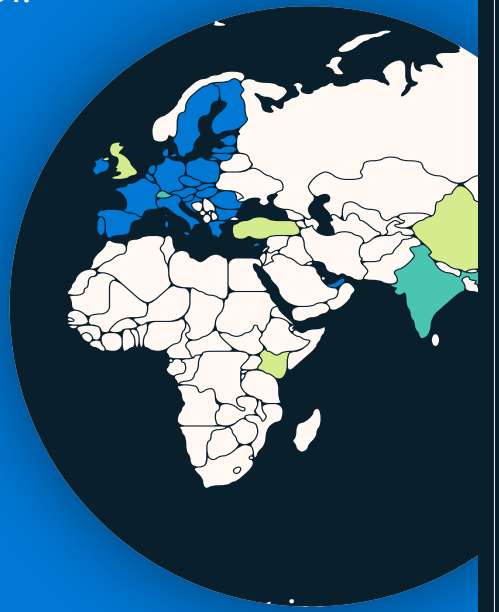
Przegląd

urządzeń i infrastruktury

Pandemia, w połączeniu z szybkim wdrożeniem wszelkiego rodzaju urządzeń z dostępem do Internetu w ramach przyspieszającej transformacji cyfrowej, znacznie zwiększyła obszar podatny na ataki naszego cyfrowego świata.

Cyberprzestępcy i atakujące państwa szybko to wykorzystują. Chociaż bezpieczeństwo sprzętu i oprogramowania IT w ostatnich latach się poprawiło, to urządzeń Internetu rzeczy (IoT) i technologii operacyjnej (OT) już nie. Atakujący wykorzystują te urządzenia do uzyskiwania dostępu do sieci i ich penetracji, zdobywania przyczółków w łańcuchach dostaw czy zakłócania operacji OT organizacji-ofiar.

Rządy na całym świecie dążą do ochrony infrastruktury krytycznej poprzez poprawę bezpieczeństwa IoT i OT.

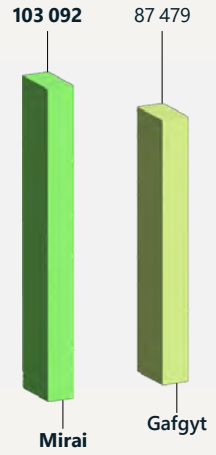


Więcej informacji na str. 59

Aby zapewnić szerokie wdrożenie, konieczne są globalnie spójne i interoperacyjne zasady bezpieczeństwa.

Więcej informacji na str. 59

Złośliwe oprogramowanie jako usługa zaczęło na dużą skalę atakować eksponowane w Internecie środowiska IoT i OT w infrastrukturze i zakładach użyteczności publicznej, a także w sieciach firmowych.



Więcej informacji na str. 63

Wzrasta liczba ataków na zdalnie zarządzane urządzenia, przy czym w maju 2022 r. zaobserwowano ponad 100 milionów ataków — pięciokrotny wzrost w ciągu ostatniego roku.

Więcej informacji na str. 62

Napastnicy coraz częściej wykorzystują luki w oprogramowaniu układowym urządzeń IoT do infiltracji sieci firmowych i niszczycielskich ataków.

Więcej informacji na str. 65

32% przeanalizowanych obrazów oprogramowania układowego zawierało co najmniej 10 znanych luk krytycznych.

Więcej informacji na str. 66

Wprowadzenie

Przyspieszająca transformacja cyfrowa zwiększyła cyberzagrożenia dla infrastruktury krytycznej i systemów cyberfizycznych.

Ostatnie kilka lat to bezprecedensowe zmiany w cyfrowym świecie. Organizacje ewoluują, aby wykorzystać postępy w zakresie możliwości obliczeniowych pochodzących zarówno z inteligentnej chmury, jak i inteligentnych urządzeń brzegowych. Wskutek pandemii, która zmusiła organizacje do digitalizacji, oraz tempa, w którym branże na całym świecie wdrażają urządzenia z dostępem do Internetu, powierzchnia obszaru podatnego na ataki w świecie cyfrowym rośnie wykładniczo.

Ta szybka migracja przerosła zdolność społeczności bezpieczeństwa do nadążania za nią. W ciągu ostatniego roku obserwowaliśmy skuteczne ataki na urządzenia w każdej części organizacji, od tradycyjnego sprzętu IT po kontrolery technologii operacyjnej (OT) czy proste czujniki Internetu rzeczy (IoT). Choć w ostatnich latach poprawiły się zabezpieczenia sprzętu IT, to bezpieczeństwo urządzeń IoT i OT pozostawia wiele do życzenia. Atakujący wykorzystują te urządzenia do uzyskiwania dostępu do sieci i umożliwienia penetracji sieci czy zakłócania operacji OT organizacji. Odnotowaliśmy ataki na sieci energetyczne, ataki ransomware zakłócające operacje OT, wykorzystywanie routerów IoT do utrzymywania się przestępców w naruszonych systemach oraz ataki na luki w oprogramowaniu układowym.

Chociaż powszechność luk w IoT i OT stanowi wyzwanie dla wszystkich organizacji, infrastruktura krytyczna jest narażona na zwiększone ryzyko, ponieważ atakujący wiedzą, że zakłócenie krytycznych usług ma ogromne konsekwencje. Atak ransomware z 2021 r. na Colonial Pipeline Company pokazał, jak przestępcy mogą zakłócić działanie krytycznej usługi, aby zwiększyć prawdopodobieństwo zapłacenia okupu. A cyberataki Rosji na Ukrainę pokazują, że niektóre państwa postrzegają cyberataki na infrastrukturę krytyczną jako dopuszczalny sabotaż dla osiągnięcia celów militarnych.

Na horyzoncie pojawia się jednak nadzieja. Decydenci polityczni i obrońcy sieci podejmują działania mające na celu poprawę cyberbezpieczeństwa infrastruktury krytycznej, w tym urządzeń IoT i OT, na których się opierają. Decydenci polityczni przyspieszają opracowywanie przepisów i regulacji mających na celu budowanie zaufania publicznego do cyberbezpieczeństwa infrastruktury i urządzeń krytycznych.

Microsoft współpracuje z rządami na całym świecie, aby wykorzystać tę okazję do poprawy cyberbezpieczeństwa. Z zadowoleniem przyjmujemy każde zaangażowanie. Obawiamy się jednak, że niespójne, niestandardowe lub złożone wymagania mogą mieć niezamierzone skutki, w tym w niektórych przypadkach obniżyć poziom bezpieczeństwa wskutek konieczności użycia ograniczonych zasobów bezpieczeństwa na zapewnianie zgodności z wieloma powielającymi się certyfikacjami.

Obrońcy sieci w organizacjach przyjmują wiele podejść do operacji bezpieczeństwa w celu poprawienia stanu zabezpieczeń IoT/OT. Jednym z podejść jest ciągłe monitorowanie urządzeń IoT i OT. Innym jest „przesunięcie w lewo” — co oznacza żądanie i wdrażanie lepszych praktyk cyberbezpieczeństwa dla samych urządzeń IoT i OT. Trzecim podejściem jest wdrażanie rozwiązań do monitorowania bezpieczeństwa, które obejmuje zarówno sieci IT, jak i OT. To holistyczne podejście daje znaczącą, dodatkową korzyść w postaci wkładu w krytyczne procesy organizacyjne, takie jak „burzenie silosów” pomiędzy OT i IT, co z kolei umożliwia organizacji osiągnięcie lepszego stanu zabezpieczeń przy jednoczesnym spełnieniu celów biznesowych.

Michal Braverman-Blumenstyk
Wiceprezes, dyrektor ds. technologii, bezpieczeństwo AI oraz chmury

Działalność administracji publicznej na rzecz poprawy bezpieczeństwa i odporności infrastruktury krytycznej

Administracja publiczna na całym świecie opracowuje i dostosowuje zasady w zakresie zwalczania cyberzagrożeń dla infrastruktury krytycznej. Wprowadzana jest również polityka mającą na celu poprawę bezpieczeństwa urządzeń IoT i OT. Rosnąca globalna fala inicjatyw politycznych stwarza ogromne możliwości zwiększenia cyberbezpieczeństwa, ale stawia również wyzwania przed interesariuszami w całym ekosystemie.

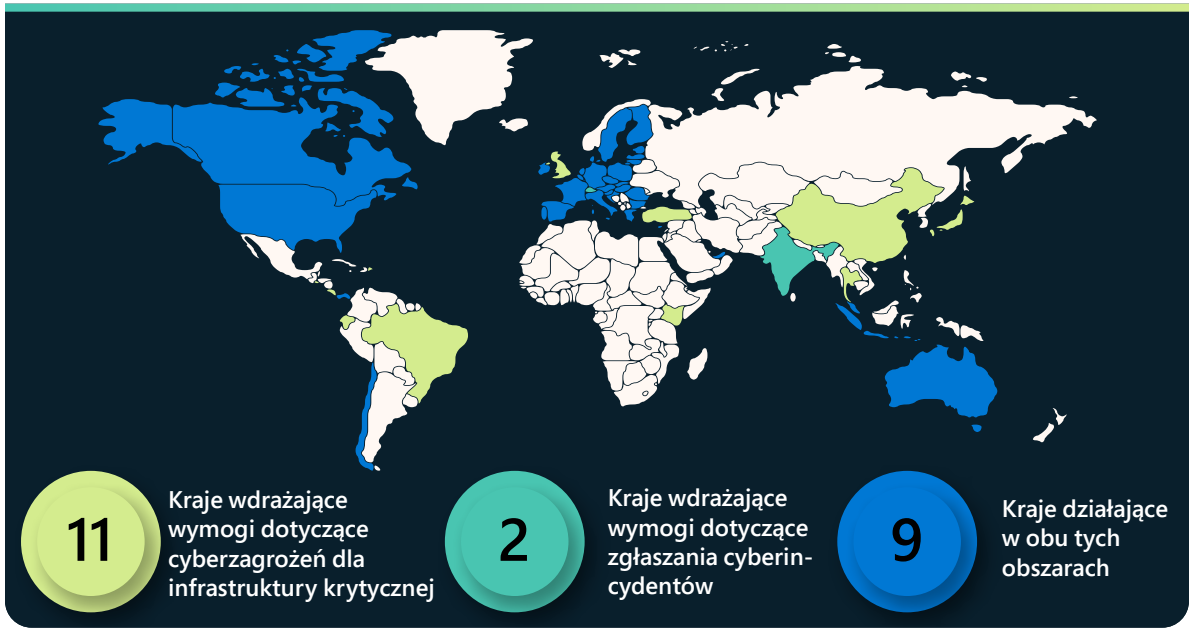
Opracowanie kompleksowej wizji zwalczania cyberzagrożeń dla infrastruktury krytycznej ma kluczowe znaczenie, ale jest złożone, zwłaszcza ze względu na stopień wzajemnych powiązań między technologiami i globalnymi dostawcami, zakres zastosowań technologii i związanych z nimi zagrożeń oraz konieczność inwestowania w strategie krótko- i długoterminowe. Efektywne polityki, które prowadzą do nieustannego podnoszenia kwalifikacji i stałych ulepszeń oraz wspierają globalną, międzysektorową interoperacyjność, mogą pomóc w zarządzaniu złożonością i umożliwić transformację cyfrową zapewniającą bezpieczeństwo. Jednakże fragmentaryczne podejście do prawodawstwa może prowadzić do nakładania się i niespójności wymogów regulacyjnych. To może wpłynąć negatywnie na zasoby i w efekcie zniweczyć cele w zakresie bezpieczeństwa. Na przykład organizacje mogą przekierować zasoby z promowania innowacji i bezpieczeństwa na formalistyczny wysiłek zapewniania zgodności z przepisami.

Microsoft współpracuje z administracją publiczną na całym świecie w zakresie wprowadzania skutecznych zasad cyberbezpieczeństwa infrastruktury krytycznej, zwiększania zrozumienia wyzwań i możliwości oraz wspierania wysiłków zwiększających zbiorową odporność wobec zagrożeń.

Zmiany zasad w zakresie zwalczania cyberzagrożeń dla infrastruktury krytycznej

W ciągu ostatniego roku wiele jurysdykcji, w tym Australia, Chile, Unia Europejska, Japonia, Singapur, Zjednoczone Królestwo czy Stany Zjednoczone, opracowało, zaktualizowało lub wdrożyło międzysektorowe lub sektorowe wymogi dotyczące cyberbezpieczeństwa[1]. Wiele z tych rządów — i inne, takie jak Indie[2] czy Szwajcaria[3] — już wydało lub opracowuje wymogi dotyczące zgłaszania incydentów związanych z cyberbezpieczeństwem dla dostawców infrastruktury krytycznej i usług podstawowych[4].

W ostatnim roku w Australii, UE, Indonezji i Stanach Zjednoczonych wprowadzono znaczące zmiany prawne. Australia przyjęła dwa akty prawne, które mają pomóc w zarządzaniu międzysektorowymi zagrożeniami dla cyberbezpieczeństwa infrastruktury krytycznej. Przepisy te, między innymi, wyznaczają nowe sektory infrastruktury krytycznej, wymagają opracowania planów zwalczania zagrożeń, nakazują zgłaszanie incydentów związanych z cyberbezpieczeństwem oraz upoważniają administrację publiczną do interwencji, jeśli operator infrastruktury krytycznej nie będzie chciał lub nie będzie w stanie odpowiednio zareagować na incydent.



UE pracowała nad zmianą swojej dyrektywy NIS z 2016 r., która zapewnia państwom członkowskim UE ramy dla usług i produktów technologicznych uznawanych za krytyczne dla gospodarek i funkcjonowania społeczeństw. Proponowany NIS 2 obejmuje zmiany, które stworzyłyby nową kategorię krytycznej infrastruktury cyfrowej, zwiększyłyby wymogi dotyczące zgłaszania cyberincydentów oraz nałożyłyby dodatkowe wymogi dotyczące zwalczania cyberzagrożeń. UE opracowała również proponowaną zmianę ustawy o cyfrowej odporności operacyjnej (Digital Operational Resilience Act, DORA), tworząc nowe wymogi dotyczące technologii informacyjno-komunikacyjnych stosowanych w sektorze usług finansowych.

W maju Indonezja wydała prezydenckie rozporządzenie w sprawie ochrony istotnej infrastruktury informacyjnej („IIV"), które wejdzie w życie w maju 2024 r. i obejmie m.in. sektory energii, transportu, finansów i zdrowia. Celem Indonezji jest ochrona ciągłości wdrażania IIV, zapobieganie cyberatakom i zwiększenie gotowości do radzenia sobie z cyberincydentami. Dostawcy IIV będą odpowiedzialni za zapewnienie pełnej i niezawodnej ochrony, wdrażanie programów zwalczania cyberzagrożeń oraz raportowanie stwierdzonego cyberryzyka do odpowiednich instytucji administracji publicznej. Rozporządzenie zawiera wymóg zgłaszania cyberincydentów w ciągu 24 godzin.

Działalność administracji publicznej na rzecz poprawy bezpieczeństwa i odporności infrastruktury krytycznej

(c.d.)

Kongres Stanów Zjednoczonych uchwalił akt prawny, który upoważniła Agencję ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA) do wydania przepisów wymagających od operatorów infrastruktury krytycznej raportowania o cyberincydentach, a amerykańska Administracja Bezpieczeństwa Transportu (TSA) opublikowała nowe wymagania dotyczące cyberbezpieczeństwa w sektorze transportu. W 2021 r. TSA wydała dwie dyrektywy dotyczące bezpieczeństwa dla operatorów rurociągów z niebezpiecznymi cieczami i gazem ziemnym w odpowiedzi na atak ransomware na Colonial Pipeline Company:

- Pierwsza dyrektywa wymagała od operatorów wyznaczenia koordynatora ds. cyberbezpieczeństwa, zgłaszania cyberincydentów w ciągu 12 godzin oraz przeprowadzenia oceny luk w systemach.
- Druga dyrektywa, którą TSA zmieniła w 2022 r., wymagała wdrożenia konkretnych środków zaradczych w celu ochrony przed atakami ransomware i innymi znanymi zagrożeniami dla systemów IT i OT, opracowania i wdrożenia w ciągu 30 dni planu awaryjnego i planu reagowania w zakresie cyberbezpieczeństwa oraz poddania się corocznemu przeglądowi architektury cyberbezpieczeństwa.

Opierając się na przepisach dotyczących rurociągów, TSA wydała w 2021 r. dwie dodatkowe dyrektywy w sprawie bezpieczeństwa, w których ogłosiła wymogi dotyczące cyberbezpieczeństwa dla kolei towarowych, pasażerskich przewoźników kolejowych lub systemów tranzytu kolejowego. Dyrektywy wymagały, aby objęci nimi operatorzy wyznaczyli koordynatora ds. cyberbezpieczeństwa, zgłaszali incydenty cyberbezpieczeństwa w ciągu 24 godzin, opracowali i wdrożyli plan reagowania na cyberincydenty oraz przeprowadzili ocenę luk w systemach. TSA ogłosiła jednocześnie, że zmieniła również swoje programy bezpieczeństwa w lotnictwie, zobowiązując operatorów lotnisk i linii lotniczych do wdrożenia dwóch pierwszych postanowień, wyznaczenia koordynatora i zgłaszania incydentów w ciągu 24 godzin.

Zmiany polityki w zakresie bezpieczeństwa urządzeń IoT i OT

W kilkudziesięciu krajach administracja publiczna aktywnie opracowuje wymogi mające na celu poprawę cyberbezpieczeństwa produktów i usług z zakresu ICT (technologii informacyjno-komunikacyjnych), w tym urządzeń IoT i OT. W kontekście produktów i usług ICT największe obawy budzi bezpieczeństwo łańcucha dostaw oprogramowania oraz bezpieczeństwo IoT.

- Komisja Europejska zaproponowała ustawę o odporności cybernetycznej (Cyber Resilience Act), która ustanowiłaby wymogi w zakresie cyberbezpieczeństwa dla samodzielnego oprogramowania i podłączonych urządzeń oraz usług pomocniczych[5]. Odpowiednie praktyki dla dostawców oprogramowania obejmują wykorzystanie bezpiecznego cyklu developmentu oprogramowania[6] oraz dostarczanie wykazu komponentów oprogramowania (SBOM)[7]. Nowe wymogi w zakresie bezpieczeństwa miałyby zastosowanie do podłączonych urządzeń, a wszyscy producenci mieliby za zadanie zarządzać skoordynowanymi procesami ujawniania luk w zabezpieczeniach[8] dla produktów wprowadzanych na rynek.

Decydenci polityczni skupili również uwagę na rozprzestrzenianiu się urządzeń IoT i połączonych do sieci urządzeń OT.

- W Zjednoczonym Królestwie projekt ustawy o bezpieczeństwie produktów i infrastrukturze telekomunikacyjnej zobowiąże producentów konsumenckich produktów podłączanych, takich jak inteligentne telewizory, do zaprzestania stosowania domyślnych haseł, które są łatwym celem dla cyberprzestępców, do ustanowienia zasady ujawniania luk w zabezpieczeniach (np. zapewnienia sposobu otrzymywania powiadomień o lukach w zabezpieczeniach) oraz do transparentności w zakresie minimalnego okresu, w którym będą dostarczane aktualizacje zabezpieczeń[9].
- W UE nowe standardy i wymogi bezpieczeństwa są wdrażane za pośrednictwem wielu instrumentów prawnych, w tym dyrektywy o sprzęcie radiowym (Radio Equipment Directive) dotyczącej urządzeń bezprzewodowych, która ma na celu poprawę odporności sieci, ochronę prywatności konsumentów oraz zmniejszenie ryzyka oszustw pieniężnych[10]. Ponadto wymagane może być stosowanie systemu certyfikacji chmury[11], który jest obecnie opracowywany w wyniku ustawy o cyberbezpieczeństwie UE z 2019 r. (2019 EU Cybersecurity Act)[12].

Potrzeba spójności

W wielu przypadkach działania w regionach, sektorach, technologiach i obszarach zarządzania ryzykiem operacyjnym są prowadzone jednocześnie, co powoduje nakładanie się lub niespójność zakresu, postanowień i złożoności przepisów dla organizacji starających się stosować wytyczne lub wykazać zgodność z przepisami. Bez powszechnie przyjętej definicji IoT szczególne wyzwanie dla przepisów dotyczących urządzeń IoT i OT stanowi ustalenie ich zakresu. Powyższe przykłady mogą potencjalnie dotyczyć „produktów połączonych i usług pomocniczych", „produktów podłączanych przez konsumentów" oraz „urządzeń bezprzewodowych". Jednocześnie wiele rządów dąży do wdrożenia efektywniejszych systemów oceny, aby lepiej zrozumieć, czy i jak organizacje i produkty spełniają obecne, pojawiające się i ewoluujące wymagania. W miarę jak te trendy będą się łączyć, wzrośnie złożoność. Co ciekawe, podczas konsultacji unijnego aktu w sprawie odporności na cyberzagrożenia (EU Cyber Resilience Act) badano, jak nowe przepisy będą pasować do dotychczasowej legislacji cyberbezpieczeństwa. Świadczy to o chęci uniknięcia sprzecznych przepisów dotyczących tego obszaru.

Podejścia stopniowe, które są oparte na ryzyku i zorientowane na wyniki lub procesy (a nie na wdrożenie), mogą sprzyjać zwiększeniu cyberbezpieczeństwa i ciągłym ulepszeniom. Podobnie skupienie się na umożliwieniu interoperacyjności w różnych sektorach, regionach i obszarach polityki mogłoby podnieść poziom cyberbezpieczeństwa w połączonych, globalnych łańcuchach dostaw.

Działalność administracji publicznej na rzecz poprawy bezpieczeństwa i odporności infrastruktury krytycznej

(c.d.)

W różnych regionach, sektorach i obszarach tematycznych opracowywane są coraz bardziej złożone strategie dotyczące cyberbezpieczeństwa infrastruktury krytycznej. Działalność ta niesie ze sobą wielkie możliwości i wyzwania. Sposób postępowania administracji publicznej będzie miał kluczowe znaczenie dla przyszłości transformacji cyfrowej i bezpieczeństwa w całym ekosystemie.

Przyspieszenie inwestycji w bezpieczeństwo łańcucha dostaw oprogramowania i architektury Zero Trust w całym ekosystemie

Zarządzenie wykonawcze Stanów Zjednoczonych (US Executive Order/ EO) 14028 w sprawie poprawy cyberbezpieczeństwa stało się katalizatorem bieżących inicjatyw Microsoft w zakresie poprawy bezpieczeństwa własnego łańcucha dostaw oraz całego ekosystemu, a także umożliwienia naszym klientom realizacji celów Zero Trust.

Od dawna uważamy, że usprawnienie łańcucha dostaw oprogramowania wymaga dzielenia się wiedzą i najlepszymi praktykami. Świadectwo temu daliśmy 15 lat temu, publikując Microsoft Security Development Lifecycle.

Ponadto ściśle współpracujemy z National Cybersecurity Center of Excellence, aby promować Zero Trust zarówno lokalnie, jak i w chmurze. Wprowadzamy także nowe możliwości do produktów, w tym uwierzytelnianie odporne na wyłudzanie informacji w środowiskach hybrydowych i wielochmurowych.

Dziś wykraczamy poza wymagania EO, aby wykazać, że nasze łańcuchy dostaw oprogramowania są zgodne z wymogami bezpieczeństwa, i dostarczyć wykaz komponentów oprogramowania (Software Bill of Materials/SBOM) — na dwa sposoby:

1. Po pierwsze, udostępniamy wersję open-source naszego narzędzia do generowania SBOM, które zbudowaliśmy tak, aby można je było łatwo zintegrować z potokami CI/CD obsługującymi kompilacje w Windows, Linux, Mac, iOS i Android[13].
2. Po drugie, przyczyniamy się do rozwoju standardów branżowych w zakresie uczciwości, transparentności i zaufania w łańcuchu dostaw (SCITT). Pozwoli to na zautomatyzowaną wymianę weryfikowalnych informacji o łańcuchu dostaw, w tym próbek udowadniających zgodność z wymaganiami, np. wytycznymi EO dotyczącymi łańcucha dostaw oprogramowania.

Praktyczne wskazówki

1. Należy przeobrazić multilateralne instytucje tak, aby sprostać pilnemu wyzwaniu, jakim są cyberataki ze strony państw.
2. Opracuj spójne i interoperacyjne zasady w zakresie cyberbezpieczeństwa we wszystkich regionach, sektorach i obszarach tematycznych.

Linki do dalszych informacji

- Dalsze inwestycje w bezpieczeństwo łańcucha dostaw w ramach wsparcia zarządzenia wykonawczego dotyczącego cyberbezpieczeństwa | Microsoft Tech Community
- Administracja publiczna Stanów Zjednoczonych określa strategię i wymagania architektury Zero Trust | Blog Microsoft Security
- CYBER EO | Microsoft Federal
- „Supply Chain Integrity, Transparency, and Trust" | github.com
- „Implementing a Zero Trust Architecture" | NCCoE (nist.gov)

Zagrożenia dla IoT i OT: trendy i ataki

Coraz bardziej połączony świat cyfrowy oznacza, że urządzenia szybko pojawiają się w sieci, komunikują się z większymi systemami, zbierają dane i ujawniają informacje, które wcześniej nie były dostępne. Stwarza to możliwości zarówno dla organizacji, jak i dla atakujących. Biznes cyberprzestępczy staje się zarówno wielomiliardową branżą, jak i ryzykiem.

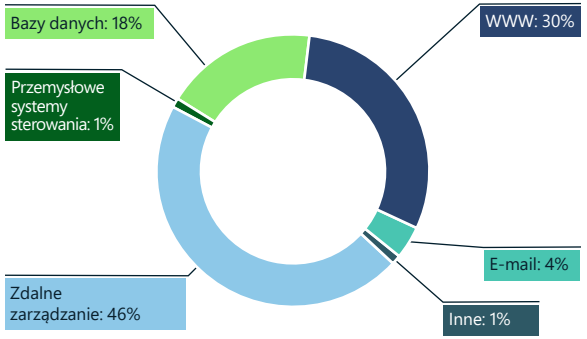
Urządzenia IoT — od drukarek po kamery internetowe, urządzenia do kontroli klimatyzacji i dostępu do budynków — stanowią wyjątkowe zagrożenie dla bezpieczeństwa osób, organizacji i sieci. Choć mają kluczowe znaczenie dla funkcjonowania wielu organizacji, mogą stać się obciążeniem i zagrożeniem bezpieczeństwa. Szybkie wdrożenie rozwiązań IoT w niemal każdej branży zwiększa liczbę wektorów ataku i zagrożeń dla organizacji.

Złośliwe oprogramowanie jako usługa przeszło do operacji na dużą skalę przeciwko infrastrukturze cywilnej i użyteczności publicznej (w tym szpitalom, branży ropy i gazu, sieciom elektrycznym, usługom transportowym i innej infrastrukturze krytycznej), a także sieciom firmowym. Odkrycie i zaatakowanie konfiguracji środowisk operacyjnych oraz osadzonych urządzeń IoT i OT wymaga poświęcenia przez atakujących znacznych wysiłków badawczych.

Urządzenia IoT stwarzają unikalne zagrożenia bezpieczeństwa jako punkty wejścia i punkty przeskoku w sieci. Miliony urządzeń IoT mają niezaktualizowane luki lub są eksponowane w Internecie.

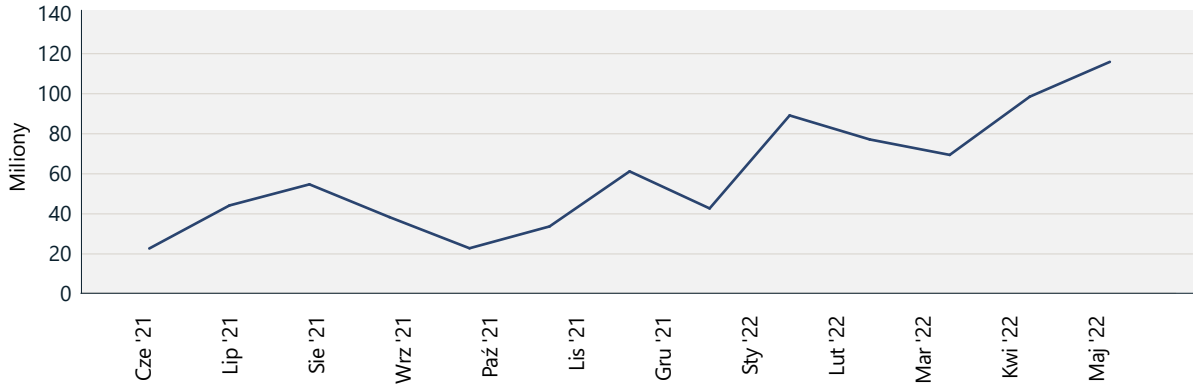
Eksponowane w Internecie urządzenia można wykryć za pomocą internetowych narzędzi wyszukiwania, identyfikując usługi nasłuchujące na otwartych portach sieciowych. Te porty są powszechnie wykorzystywane do zdalnego zarządzania urządzeniami. Eksponowane w Internecie urządzenie IoT, jeśli nie zostanie prawidłowo zabezpieczone, może zostać wykorzystane jako punkt przeskoku do innej warstwy sieci przedsiębiorstwa, gdy nieautoryzowani użytkownicy będą mogli zdalnie uzyskiwać dostęp do portów. Zaobserwowaliśmy, że różni atakujący próbują wykorzystać luki w urządzeniach eksponowanych w Internecie — od kamer, przez routery, po termostaty. Jednak, pomimo ryzyka, miliony urządzeń mają niezaktualizowane luki lub są eksponowane w Internecie.

Podsumowanie typów ataków na IoT/OT



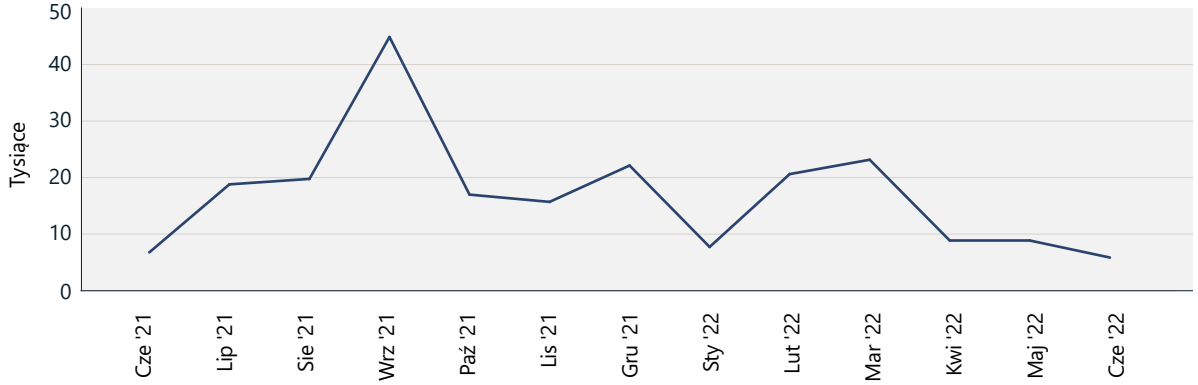
Rodzaje ataków zaobserwowane przez sieć czujników MSTIC. Najbardziej rozpowszechnione były ataki na zdalnie zarządzane urządzenia, ataki przez WWW oraz ataki na bazy danych (ataki siłowe/brute force lub programy wykorzystujące luki/exploits).

Ataki na zdalnie zarządzane urządzenia



Widoczne dzięki sieci czujników MSTIC nasilenie ataków na porty zdalnego zarządzania.

Ataki przez WWW na IoT i OT



Liczba ataków przez WWW w czasie, zarejestrowana przez sieć czujników MSTIC. Wraz ze spadkiem liczby urządzeń bezpośrednio podłączonych do sieci WWW atakujący mogą być mniej skłonni do ich skanowania.

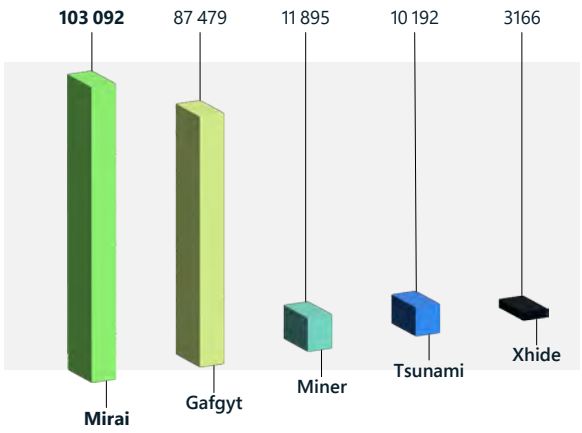
Zagrożenia dla IoT i OT: trendy i ataki

(c.d.)

Skuteczniejsze narzędzie złośliwego oprogramowania

Wraz z ewolucją grup cyberprzestępczych zmieniał się również sposób wdrażania przez nich złośliwego oprogramowania i wybór celów. W ciągu ostatniego roku zaobserwowaliśmy, że ataki na popularne protokoły IoT — takie jak Telnet — znacznie spadły, w niektórych przypadkach nawet o 60%. Jednocześnie grupy cyberprzestępcze i atakujące państwa zmieniły przeznaczenie botnetów. Uporczywość złośliwego oprogramowania, takiego jak Mirai, podkreśla modularność tych ataków i zdolność adaptacji istniejących zagrożeń.

Najczęściej wykrywane złośliwe oprogramowanie IoT



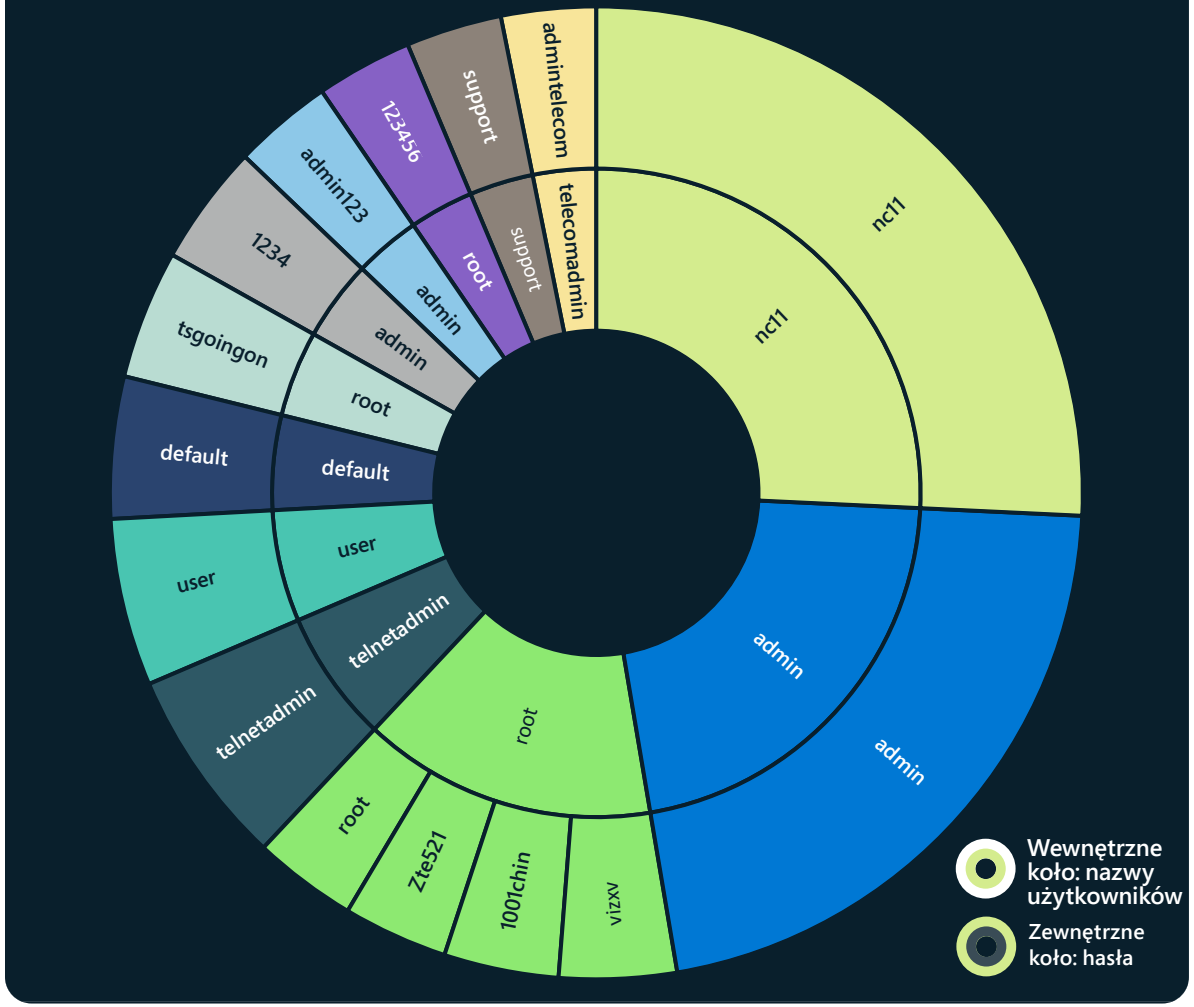
Mirai ewoluował, aby infekować szeroką gamę urządzeń IoT, w tym kamery z protokołem internetowym, cyfrowe rejestratory wideo kamer bezpieczeństwa i routery. Wektory ataku omijają dotychczasowe mechanizmy zabezpieczeń. Celem są urządzenia klienckie w sieci — wykorzystywane są kolejne luki, a po włamaniu następuje penetracja sieci. Mirai był wielokrotnie przeprojektowywany, a jego warianty dostosowują się do różnych architektur i wykorzystują zarówno znane luki, jak i luki zero-day w celu realizacji nowych wektorów ataku.

W ciągu ostatniego roku wykorzystanie Mirai wzrosło zarówno wśród 32-, jak i 64-bitowych architektur procesorów x86, a złośliwe oprogramowanie otrzymało nowe możliwości, które zostały szybko przyjęte przez atakujące państwa i grupy przestępcze. Atakujące państwa wykorzystują teraz nowe warianty istniejących botnetów w rozproszonych atakach DDoS („odmowa usługi") na zagranicznych przeciwników.

Wraz ze spadkiem ataków na urządzenia IoT w 2022 r. zaobserwowaliśmy kilka grup atakujących wykorzystujących luki — takie jak Log4j czy Spring4Shell — wdrażających złośliwe ładunki na urządzeniach takich jak serwery, infekując i włączając je do dużych botnetów przeprowadzających ataki DDoS. Nowe funkcje złośliwego oprogramowania zaprojektowane, by atakować luki urządzeń IoT, mają poważne implikacje zarówno dla organizacji, jak i państw, ponieważ spenetrowanie konkretnej sieci może umożliwić wdrożenie w niej backdoorów, które będą mogły być wykorzystywane przez kolejne ładunki i infekować kolejne urządzenia w sieci.

Wiele protokołów przemysłowych systemów sterowania jest niemonitorowanych i dlatego są one podatne na ataki specyficzne dla OT. Może to oznaczać zwiększone ryzyko dla infrastruktury krytycznej.

Względna częstość występowania par nazw użytkowników i haseł obserwowanych w urządzeniach IoT/OT w ciągu 45 dni od otrzymania sygnałów z czujników



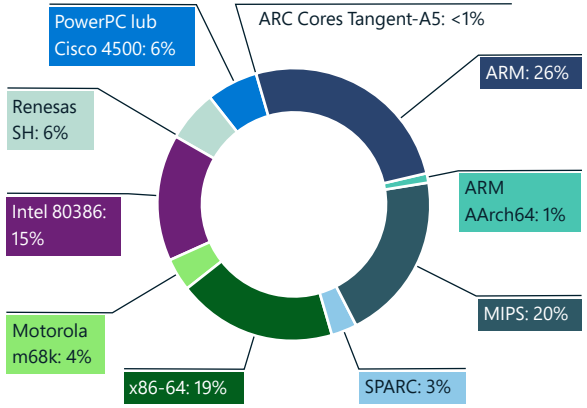
Używanie typowych par nazw użytkowników i haseł zwiększa ryzyko włamania. Na ponad 39 mln urządzeń IoT i OT przypadki identycznych nazw użytkowników i haseł stanowiły około 20%.

Zagrożenia dla IoT i OT: trendy i ataki

(c.d.)

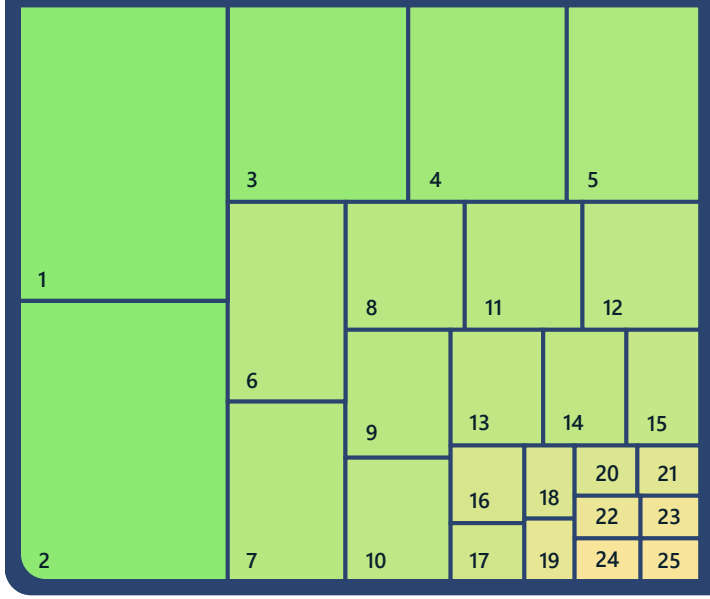
Słabe konfiguracje i domyślne poświadczenia nadal stanowią zagrożenia dla sieci. Microsoft zaobserwował też wiele programów atakujących luki WWW/HTTP. Wystąpił wzrost liczby ataków na usługi WWW z wykorzystaniem starszych botnetów. Tymczasem w Internecie odnotowano spadek liczby otwartych portów Telnet, co jest pozytywnym znakiem dla bezpieczeństwa sieci, ponieważ botnety, które do tej pory stanowiły zagrożenie dla urządzeń, tracą na znaczeniu. Pomimo tego spadku liczby otwartych portów Telnet nadal obserwowaliśmy uporczywe botnety w sieciach czujników.

Udział złośliwego oprogramowania IoT według architektury procesora



Microsoft zauważył, że najczęstszym celem złośliwego oprogramowania są urządzenia IoT działające na ARM, a następnie MIPS, X86-64 i Intel 80386 CPU.

Rozpowszechnienie poszczególnych protokołów przemysłowych systemów sterowania



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet Real-Time
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

Luki w protokołach przemysłowych systemów sterowania

Przeanalizowaliśmy dane OT z czujników podłączonych do chmury, ujawniając najczęstsze protokoły przemysłowych systemów sterowania (ICS). Protokoły te obrazują naturę tych urządzeń i ich obszar podatny na ataki. Ma to szczególne znaczenie dla bezpieczeństwa infrastruktury krytycznej. Oto kluczowe wnioski:

1. Większość protokołów jest autorska, więc standardowe narzędzia monitorowania IT nie zapewnią odpowiedniego wglądu w bezpieczeństwo tych protokołów i urządzeń. W efekcie sieci pozostają niemonitorowane, a przez to jeszcze bardziej narażone na ataki wymierzone w OT.
2. Istnieje duża różnorodność protokołów — są one specyficzne dla konkretnych producentów. Oznacza to, że rozwiązania bezpieczeństwa dostosowane do konkretnego producenta nie będą w stanie objąć całej sieci. Microsoft traktuje priorytetowo podejście agnostyczne wobec dostawców, aby zapewnić ochronę szerokiej gamy różnych urządzeń.
3. Organizacje powinny upewnić się, że te protokoły nie są eksponowane w Internecie z ich sieci. Taka ekspozycja może stanowić poważne zagrożenie bezpieczeństwa ze względu na luki w zabezpieczeniach i niebezpieczną naturę tych protokołów.

Złośliwe oprogramowanie takie jak Mirai jest w stanie utrzymać się w zaatakowanych systemach dzięki nowym funkcjom. Używają go grupy cyberprzestępcze, a także atakujące państwa, które wykorzystują nowe warianty istniejących botnetów w atakach DDoS na zagranicznych przeciwników.

Praktyczne wskazówki

1. Upewnij się, że urządzenia są odporne na ataki przez stosowanie poprawek oraz zmianę domyślnych haseł i portów SSH.
2. Zmniejsz obszar podatny na ataki, eliminując zbędne połączenia internetowe i otwarte porty, a także ograniczając zdalny dostęp przez blokowanie portów oraz odmawianie zdalnego dostępu i łączenia się przez VPN.
3. Używaj rozwiązania NDR (Wykrywanie w sieci i reagowanie) z obsługą IoT/OT oraz SIEM (Zarządzanie informacjami i zdarzeniami zabezpieczeń)/SOAR (Organizowanie zabezpieczeń i automatyzowanie reagowania) do monitorowania urządzeń pod kątem anomalnych lub nieautoryzowanych zachowań, takich jak komunikacja z nieznanymi hostami.
4. Segmentuj sieci, aby ograniczyć atakującym możliwość penetracji sieci po początkowym wtargnięciu i atakowania innych zasobów. Urządzenia IoT i sieci OT powinny być odizolowane od firmowych sieci IT za pomocą zapór.
5. Upewnij się, że protokoły ICS nie są eksponowane w Internecie.

Hakowanie łańcucha dostaw i oprogramowania układowego

Prawie każde urządzenie podłączone do Internetu ma oprogramowanie układowe (firmware), czyli oprogramowanie wbudowane w sprzęt lub płytkę obwodu drukowanego urządzenia. W ciągu ostatnich kilku lat obserwujemy wzrost ataków na oprogramowanie układowe. Ponieważ będzie to nadal atrakcyjny cel dla atakujących, organizacje muszą chronić się przed tym wektorem.

Oprogramowanie układowe odpowiada za podstawowe funkcje urządzenia, takie jak łączenie z siecią czy przechowywanie danych. Znajduje się ono w routerach, kamerach, telewizorach i innych urządzeniach używanych w przedsiębiorstwach (IoT) wraz z przemysłowymi systemami sterowania (OT) używanymi w infrastrukturze krytycznej. Do tej pory poziom zabezpieczeń oprogramowania układowego pozostawiał wiele do życzenia. Powodowało to znaczące luki umożliwiające przejęcie urządzenia lub wstrzykiwanie złośliwego kodu do tego oprogramowania.

To ryzyko potęguje się w łańcuchu dostaw. Większość urządzeń jest zbudowana z wykorzystaniem oprogramowania i komponentów sprzętowych wielu producentów, a także bibliotek open-source. W wielu przypadkach operatorzy urządzeń nie mają wglądu w wykaz komponentów sprzętu i oprogramowania (H/SBOM), aby ocenić ryzyko łańcucha dostaw urządzeń w swojej sieci. W czerwcu 2020 r. ujawniono luki w stosie sieciowym wykorzystywanym przez wielu producentów wpływające na setki milionów systemów IoT w urządzeniach konsumenckich i przemysłowych[14]. W niektórych przypadkach oznaczenie stosu sieciowego zostało przemianowane przez innych producentów, w związku z czym nie było żadnych przesłanek podatności urządzenia na atak. Widzimy rosnące zagrożenie ze strony przestępców, którzy atakują łańcuch dostaw oprogramowania i sprzętu urządzeń IoT/OT, aby włamać się do organizacji.

Proces aktualizacji oprogramowania układowego różni się znacznie w zależności od urządzenia. Złożoność i wyzwania logistyczne związane z tym procesem wpływają na częstotliwość aktualizacji. Nie zawsze można określić, czy urządzenie ma najnowsze oprogramowanie układowe, co utrudnia specjalistom ds. bezpieczeństwa monitorowanie i zapewnianie bezpieczeństwa urządzeń IoT i OT. Ponadto niektóre urządzenia mają oprogramowanie układowe, które nie jest podpisane kryptograficznie, co umożliwia jego aktualizację bez weryfikacji ze strony użytkownika. Te słabości dodatkowo zwiększają podatność urządzeń na ataki w całym łańcuchu produkcji i dystrybucji.

Aby przeciwdziałać tym zagrożeniom, Microsoft inwestuje znaczne środki w zapewnienie bezpieczeństwa i integralności oprogramowania układowego na różnych etapach łańcucha dostaw, a także w poświadczanie w każdym momencie, że nie zostało ono w żaden sposób naruszone, np. podczas przesyłania. Dzięki temu możemy zweryfikować zaufanie między każdym segmentem potoku oraz zapewnić certyfikowany i możliwy do udowodnienia, kompleksowy łańcuch nadzoru nad każdym komponentem, który dostarczamy klientom. Współpracujemy z partnerami, aby wprowadzić zabezpieczenie „od układu scalonego po chmurę" do wszystkich urządzeń w sieci przedsiębiorstw i OT.

„Dostawcy infrastruktury teleinformatycznej są coraz częściej celem ataku, ponieważ umożliwiają szerokie powielanie pojedynczego ataku. Jednocześnie rozrastają się globalne przepisy, regulacje i wymagania klientów dotyczące bezpieczeństwa i odporności łańcucha dostaw. Ich wymagania są często rozbieżne.

Rozwiązaniem jest partnerstwo. Wraz z dostawcami i rządami na całym świecie Microsoft dokłada wszelkich starań, aby rozwiązać problem bezpieczeństwa w ekosystemie łańcucha dostaw, przekraczając wymagania zarówno klientów, jak i organów regulacyjnych. Aby to osiągnąć, stosujemy kompleksowe podejście do bezpieczeństwa i odporności operacyjnej, które jest elastycznie wdrażane w całym łańcuchu dostaw.

Kluczem do naszego kompleksowego podejścia jest dbałość o integralność oprogramowania układowego, od projektu po eksploatację urządzenia. Zapewnienie procesów SDL u dostawców i wdrożenie sprzętowego mechanizmu weryfikacji (root of trust) to przykłady tego, jak możemy zapewnić „wbudowaną" integralność łańcucha dostaw.

Nasza społeczność wykorzystuje wspólne badania obejmujące nowe techniki przeciwdziałania manipulacjom i mechanizmy kryptograficzne w połączeniu z ciągłym monitorowaniem i wykrywaniem anomalii. Minimalizujemy atrakcyjność łańcucha dostaw jako obszaru podatnego na ataki".

Edna Conway
Wiceprezes ds. bezpieczeństwa i zagrożeń, infrastruktura chmury

Luki w oprogramowaniu układowym

Atakujący coraz częściej wykorzystują luki w oprogramowaniu układowym urządzeń IoT do infiltracji sieci firmowych. W przeciwieństwie do tradycyjnych urządzeń klienckich IT, które do identyfikacji podatności wykorzystują agentów XDR, identyfikacja luk w urządzeniach IoT/OT jest znacznie trudniejsza.

Ostatnie badanie przeprowadzone przez Microsoft i Ponemon Institute podkreśla zarówno możliwości, jak i wyzwania związane z bezpieczeństwem urządzeń IoT/OT w przedsiębiorstwie[15]. 68% respondentów uważa, że przyjęcie IoT/OT jest krytyczne dla ich strategicznej transformacji cyfrowej, jednak 60% uznaje, że zabezpieczenia IoT/OT są niedostateczne.

Przykładem ataku na luki w oprogramowaniu układowym urządzeń IoT w celu infiltracji sieci jest trojan Trickbot, który wykorzystuje domyślne hasła i luki w routerach Mikrotik[16] do obejścia firmowych systemów bezpieczeństwa. Podstawowym wyzwaniem związanym z oprogramowaniem układowym urządzeń IoT jest brak wglądu w stan zabezpieczeń i luki urządzeń.

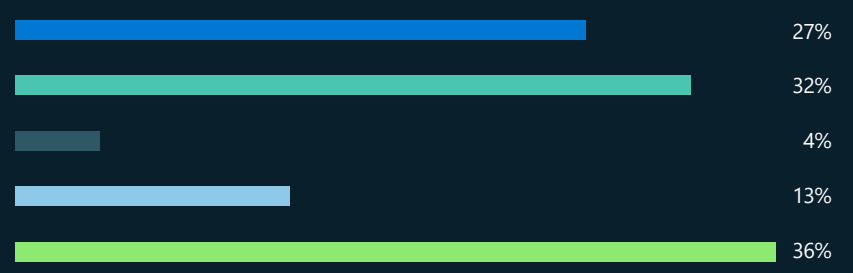
Choć dostępne są rozwiązania pozwalające na budowę bezpiecznych urządzeń, to na rynku są już miliardy urządzeń wdrożonych w przedsiębiorstwach. Są to tak zwane urządzenia brownfield. W 2021 r. Microsoft nabył firmę ReFirm Labs, aby rzucić światło na bezpieczeństwo urządzeń brownfield i umożliwić producentów urządzeń poprawę bezpieczeństwa ich produktów. ReFirm Labs analizuje binarny obraz oprogramowania układowego urządzenia i tworzy szczegółowy raport na temat potencjalnych podatności[17]. Technologia ta zostanie włączona do przyszłego wydania Microsoft Defender dla IoT.

W ciągu ostatniego roku przeanalizowaliśmy zbiorcze wyniki skanowania przez naszych klientów oprogramowania układowego. Chociaż nie każda odkryta luka może zostać zaatakowana, podkreślają one fundamentalne wyzwanie, jakim jest bezpieczeństwo oprogramowania układowego urządzeń.

Dodajmy, że luki występujące w urządzeniach IoT/OT nigdy nie byłyby akceptowalne w tradycyjnych urządzeniach klienckich z Windows lub Linux.

- Słabe hasła: 27% zeskanowanych obrazów oprogramowania układowego zawierało konta z hasłami zakodowanymi przy użyciu słabych algorytmów (MD5/DES), które są łatwe do złamania.

Odkryte podatności w obrazach oprogramowania układowego



- Znane luki w zabezpieczeniach: Tak jak inne systemy, oprogramowanie układowe urządzeń IoT/OT szeroko wykorzystuje biblioteki open-source. Jednak urządzenia są często dostarczane z nieaktualnymi wersjami tych składników. W naszej analizie 32% obrazów zawierało co najmniej 10 znanych podatności (CVE) ocenionych jako krytyczne (9,0 lub więcej). 4% zawierało co najmniej 10 krytycznych luk, które miały ponad 6 lat.
- Wygasłe certyfikaty: Certyfikaty są używane do uwierzytelniania połączeń i tożsamości, a także ochrony danych wrażliwych, ale 13% analizowanych obrazów zawierało co najmniej 10 certyfikatów, które wygasły ponad 3 lata temu.
- Składniki oprogramowania: 36% obrazów zawiera składniki oprogramowania, których Microsoft nie zaleca stosować w urządzeniach IoT, takie jak narzędzia do przechwytywania pakietów (tcpdump, libpcap). Mogą one służyć do rozpoznawania sieci w ramach łańcucha ataku.

Ataki na oprogramowanie układowe

Viasat: Wykorzystanie luki w oprogramowaniu układowym do ataku na komunikację satelitarną

W lutym 2022 r. incydent w sieci satelitarnej spowodował odłączenie strategicznej sieci komunikacyjnej, czego skutki odczuwalne były w całej Europie. System KA-SAT firmy Viasat został zaatakowany dużym ruchem przychodzącym (DDoS/odmowy usługi). Spowodowało to odłączenie wielu modemów. W związku z przerwaniem stałego łącza szerokopasmowego tysiące turbin wiatrowych przestało być zdalnie dostępnych dla operatorów, a do modemów zostało wdrożone złośliwe oprogramowanie „wiper". Zakłócenia dotknęły ponad 30 000 terminali satelitarnych wykorzystywanych przez firmy i organizacje do komunikacji.

Cyclops Blink: Wykorzystanie łańcucha dostaw oprogramowania układowego do ataku na bramy zapór

Dla atakujących rozwój i ekspansja infrastruktury sterowania i kontroli (C2) oraz ataku jest kluczowym elementem sukcesu. Wraz ze wzrostem zapotrzebowania na stabilną infrastrukturę C2 routery stały się pożądanym wektorem ataku ze względu na rzadkie stosowanie względem nich poprawek i brak kompleksowych rozwiązań bezpieczeństwa.

Microsoft współpracuje z rządami i branżą, aby stworzyć technologię analizy oprogramowania układowego pozwalającą na dogłębniejszą analizę luk w urządzeniach, która zapewni bezpieczeństwo w całym cyklu ich życia dla ich producentów i operatorów.

Od czerwca 2019 r. powiązana z państwem grupa APT (advanced persistent threat) wykorzystywała modularne, złośliwe oprogramowanie Cyclops Blink, aby atakować podatne zapory sprzętowe WatchGuard i routery ASUS, wykonując złośliwe aktualizacje oprogramowania układowego i włączając je do dużego botnetu. Złośliwe oprogramowanie skutecznie infekuje urządzenia poprzez wykorzystanie znanej luki, która pozwala na zwiększenie uprawnień, umożliwiając atakującym zarządzanie urządzeniem. Po zainfekowaniu złośliwe oprogramowanie pozwala na instalację kolejnych modułów i uniemożliwia aktualizację oprogramowania układowego. Zaobserwowano, że zhakowane urządzenia łączą się z serwerami C2 hostowanymi na innych urządzeniach WatchGuard. Wystawiając wiele certyfikatów SSL dla swoich C2 na różnych portach TCP, operatorzy Cyclops Blink uzyskali zdalny dostęp do sieci z wysokimi uprawnieniami, co umożliwiło im wykonywanie złośliwych aktualizacji oprogramowania układowego oraz omijanie tradycyjnych metod zabezpieczeń takich jak skanowanie.

Jak Microsoft poprawia bezpieczeństwo łańcucha dostaw

Microsoft współpracuje z rządami i branżą w celu pokonania wyzwań związanych z bezpieczeństwem urządzeń IoT i OT (patrz omówienie na stronie 66). Nasz wkład obejmuje wykorzystanie technologii analizy oprogramowania układowego w celu zapewnienia operatorom urządzeń wglądu w stan zabezpieczeń urządzeń w ich sieci. Umożliwi to klientom identyfikowanie i ustalanie priorytetów dla urządzeń wymagających dodatkowej ochrony, uaktualniania lub wymiany, a także wymusi zwiększenie nacisku producentów urządzeń na bezpieczeństwo. Jednocześnie wspieramy producentów za pomocą kompleksowych rozwiązań w zakresie projektowania bezpiecznych urządzeń i wdrażania bezpiecznych cykli developmentu.

Kolejną kluczową sprawą jest zapewnienie producentom i operatorom solidnej infrastruktury umożliwiającej aktualizację oprogramowania układowego urządzeń w miarę odkrywania i rozwiązywania problemów bezpieczeństwa. Microsoft łączy analizę oprogramowania układowego i Defender dla IoT z Device Update for IoT Hub, aby zapewnić rozwiązanie obejmujące pełny cykl życia urządzeń IoT i OT. Są to ważne składniki naszej wizji zabezpieczania infrastruktury klientów: promujemy urządzenia obsługujące model Zero Trust w rozwiązaniach IoT i OT[18].

Atakujący coraz częściej wykorzystują luki w oprogramowaniu układowym urządzeń IoT do infiltracji sieci firmowych.

Praktyczne wskazówki

1. Uzyskaj dogłębniejszy wgląd w urządzenia IoT/OT w sieci. Ustal, naruszenie których z nich stanowiłoby największe ryzyko dla firmy.
2. Użyj narzędzi do skanowania oprogramowania układowego, aby poznać słabe punkty zabezpieczeń oraz ustalić we współpracy z dostawcami działania względem urządzeń wysokiego ryzyka.
3. Pozytywnie wpływaj na bezpieczeństwo urządzeń IoT/OT, wymagając od dostawców przyjęcia najlepszych praktyk bezpiecznego cyklu developmentu.

Linki do dalszych informacji

- „Assessment of the Critical Supply Chains Supporting the US Information and Communications Technology Industry"

Ataki na OT poprzedzone rozpoznaniem

Do planowania złożonych łańcuchów dostaw są wykorzystywane określone informacje projektowe. W niezliczonych zasobach, które składają się na informacje dotyczące projektu, najbardziej wrażliwy jest plik projektu, który definiuje środowisko i jego zasoby. Ten plik jest kluczowym celem dla atakujących, którzy chcą uzyskać dostęp i przeprowadzić skuteczny atak w pełni dostosowany do środowiska.

Atakowanie systemów przemysłowych w celu zakłócenia procesów operacyjnych obejmuje dwa etapy.

1. Po pierwsze, atakujący musi uzyskać dostęp do sieci OT. Może to zrobić, wnikając do sieci przez urządzenia IoT po stronie przedsiębiorstwa (Purdue Model Level 4) i przekraczając granicę IT-OT, tradycyjnie oddzieloną zaporami i urządzeniami sieciowymi, przeskakując na poziom operacji i kontroli.
2. Po drugie, musi zidentyfikować urządzenia sieciowe. Systemy przemysłowe wykorzystują standardowe urządzenia i składniki w niestandardowych architekturach zaprojektowanych specjalnie dla tych środowisk. Jednym z takich standardowych urządzeń są PLC (programowalne sterowniki logiczne). Sterowniki PLC są kluczowym elementem systemów przemysłowych. Każdy producent opracowuje unikalne interfejsy i funkcje dla swoich PLC, a następnie są one konfigurowane z użyciem niestandardowych schematów specjalnie zaprojektowanych pod kątem środowiska konkretnego klienta.

Unikalna konfiguracja każdego sterownika PLC jest opisana w pliku projektu, który zawiera definicję środowiska i jego zasobów, logikę drabinkową i inne elementy.

W większości środowisk, w których widoczne są dowody ataku, analiza pokazuje, że działania poprzedzające atak są znacznie dłuższe od długości samego ataku. Atakujący często inwestują miesiące w zdalne symulowanie środowiska i jego zasobów, podejmując wiele prób skonstruowania modelu i przygotowania finalnego ataku. Ponieważ środowiska stale się zmieniają i integrują nowe urządzenia, luki w zabezpieczeniach powstają właśnie wokół danych w plikach projektu i konfiguracji. Kradzież pliku projektu może przyspieszyć atak o tygodnie czy miesiące i umożliwić atakującym szybkie i dokładne zmodelowanie środowiska docelowego, co zwiększy trudność wykrycia złośliwych działań.

Industroyer i Incontroller

Zaobserwowaliśmy wzmożone ataki na organizacje, infrastrukturę krytyczną i administrację publiczną przez grupy powiązane z państwami wykorzystujące modułowe złośliwe oprogramowanie i frameworki ataku. Nowe próby zakłócenia krytycznych operacji na Ukrainie podkreślają rosnące zagrożenie atakami na OT poprzedzonymi rozpoznaniem, które są wysoce dostosowane do środowisk docelowych. Rozbudowane fazy rozpoznawania i badania prowadzone przez atakujące państwa poprzedzają zdalny paraliż infrastruktury. Cyberwojna obejmuje realizację celów strategicznych lub operacyjnych w ramach mieszanych operacji cybernetycznych i kinetycznych podporządkowanych strategii politycznej.

Obserwujemy wzrost liczby ataków na OT, które są wysoce dostosowane do środowisk docelowych, gdyż są poprzedzone rozpoznaniem.

Ataki na OT poprzedzone rozpoznaniem

(c.d.)

Na początku 2022 r. zidentyfikowano dwa adaptacyjne ataki krytyczne na OT. Cyberfizyczny atak na podstacje elektryczne i przekaźniki ochronne na Ukrainie został przeprowadzony przy użyciu niestandardowego złośliwego oprogramowania, w tym wariantu Industroyer — złośliwego oprogramowania, o którym wiadomo, że spowodowało przerwy w dostawach energii na Ukrainie w 2016 r.

Industroyer2 to pierwszy znany ponowny atak złośliwego oprogramowania na nowy cel OT. Wykorzystuje on wtyczkę w ramach protokołu IEC104 (standardowy protokół monitorowania i kontroli systemu energetycznego) opracowany dla Industroyer i atakujący głównie zdalne terminale PLC o numerze modelu ABB RTU540/560. Twórca tego złośliwego oprogramowania wykorzystał wiedzę o środowisku ofiary, aby wielokrotnie wydawać polecenia na z góry określone wyjścia, przez co urządzeń nie można było włączyć ręcznie. Efektem były długie przerwy w dostawach prądu i znaczące szkody.

Incontroller, modułowy framework ataku zidentyfikowany w tym samym okresie, jest modułowym zestawem narzędzi, który znacznie skraca czas realizacji penetracji i ataku na urządzenia OT, omijając starsze rozwiązania zabezpieczające. Ten zestaw narzędzi ogólnego przeznaczenia ma możliwość gromadzenia danych oraz przeprowadzania rozpoznania i ataku. Dostosowuje się do różnych środowisk i ułatwia ich symulowanie dzięki możliwości wydobywania informacji o urządzeniach i ich konfiguracji. Pozwala to skrócić fazę analiz i rozpoznania przed atakiem na OT.

Framework Incontroller obsługuje protokoły dla sterowników PLC Schneider Electric i Omron. Zbiera informacje takie jak wersja oprogramowania układowego, typ modelu i podłączone urządzenia. Zestaw narzędzi może wydawać polecenia zmiany konfiguracji oraz włączania i wyłączania wyjść. Po uzyskaniu dostępu do środowiska framework umożliwia instalowanie backdoorów w urządzeniach, co pozwala na wdrożenie większej liczby ładunków, wprowadzanie luk w celu zwiększenia liczby punktów dostępu, przesyłanie logiki drabinkowej oraz inicjowanie ataków DoS. Ogólny charakter zestawu narzędzi umożliwia szybki atak na środowisko bez konieczności oprogramowywania nowych ataków dla każdego sterownika PLC lub każdej lokalizacji. Pozwala to atakującemu na łatwą interakcję z różnymi typami maszyn, potencjalnie w wielu branżach.

Praktyczne wskazówki

1. Unikaj przesyłania plików zawierających definicje systemu przez niezabezpieczone kanały lub do nieistotnego personelu.
2. Jeśli przesyłanie takich plików jest nieuniknione, należy monitorować aktywność w sieci i upewnić się, że zasoby są bezpieczne.
3. Chroń stacje inżynierskie przez monitorowanie za pomocą rozwiązań EDR.
4. Proaktywnie reaguj na incydenty w sieciach OT.
5. Wdrażaj systemy ciągłego monitorowania takie jak Defender dla IoT.

Przypisy końcowe

1. Patrz np. „Revised Directive on Security of Network and Information Systems (NIS2)" | Shaping Europe's digital future (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; „Security Legislation Amendment (Critical Infrastructure Protection) Act 2022" (homeaffairs.gov.au); „Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate" | News post | DataGuidance; „Japan passes economic security bill to guard sensitive technology" | The Japan Times; „Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs" (csa.gov.sg); „Proposal for legislation to improve the UK's cyber resilience" — GOV.UK (www.gov.uk); „Telecommunications (Security) Act 2021" (legislation.gov.uk); „Updating the NIST Cybersecurity Framework — Journey To CSF 2.0" | NIST
2. Cert-In — Strona główna
3. „Initiation of consultation on introduction of cyberattack reporting obligation" (admin.ch)
4. Patrz np. Bez tytułu (house.gov)
5. Cyber Resilience Act | „Shaping Europe's digital future" (europa.eu)
6. Patrz np. Microsoft Security Development Lifecycle
7. Patrz np. „Tworzenie wykazu komponentów oprogramowania (SBOM) z użyciem SPDX w Microsoft" — Engineering@Microsoft, „The Minimum Elements For a Software Bill of Materials (SBOM)" | National Telecommunications and Information Administration (ntia.gov)
8. Patrz np. https://www.microsoft.com/en-us/msrc/cvd
9. „The Product Security and Telecommunications Infrastructure (PSTI) Bill—product security factsheet" — GOV.UK (www.gov.uk)
10. „Commission strengthens cybersecurity of wireless devices and products" (europa.eu)
11. „Cloud Certification Scheme: Building Trusted Cloud Services Across Europe" — ENISA (europa.eu)
12. „Certification" — ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool „GitHub - microsoft/sbom-tool: The SBOM tool is a highly scalable and enterprise ready tool to create SPDX 2.2 compatible SBOMs for any variety of artifacts".
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. „Innowacje w zakresie IoT/OT mają kluczowe znaczenie, ale wiążą się ze znacznymi zagrożeniami" (grudzień 2021 r.): 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. „Odkrycie wykorzystania przez Trickbot urządzeń IoT w infrastrukturze sterowania i kontroli" (marzec 2022 r.): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. IoT Show na Channel 9 — „Skanowanie oprogramowania układowego" (maj 2022 r.): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. „Jak zastosować podejście Zero Trust do rozwiązań IoT" (maj 2021 r.): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Operacje wpływu

Operacje wpływu zagranicznego mające na celu osłabienie zaufania społecznego wykorzystują nowe metody i technologie, aby zwiększyć efektywność.

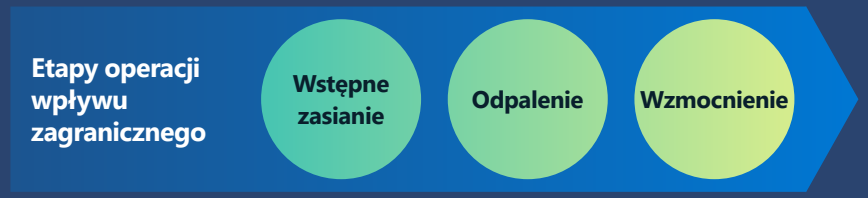
Przegląd

operacji wpływu

Operacje wpływu zagranicznego mające na celu osłabienie zaufania społecznego wykorzystują nowe metody i technologie, aby zwiększyć efektywność.

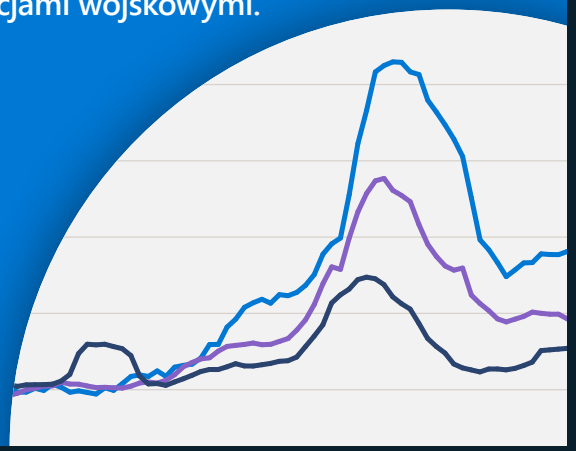
Państwa coraz częściej stosują wyrafinowane operacje wpływu w celu rozpowszechniania propagandy i kształtowania opinii publicznej zarówno wewnętrznie, jak i za granicą. Kampanie te podkopują zaufanie, zwiększają polaryzację społeczną i zagrażają demokracji. Zaawansowani i zdeterminowani manipulatorzy wykorzystują tradycyjne media oraz Internet i media społecznościowe, aby znacznie zwiększyć zakres, skalę i skuteczność swoich kampanii oraz i tak już ogromny wpływ, jaki wywierają na globalny ekosystem informacyjny. W zeszłym roku tego typu operacje były realizowane w ramach rosyjskiej wojny hybrydowej na Ukrainie. Rosja i inne kraje, w tym Chiny i Iran, coraz częściej stosują operacje propagandowe przez media społecznościowe, aby rozszerzyć swoje globalne wpływy.

Operacje wpływu stają się bardziej wyrafinowane. Coraz więcej rządów i państw wykorzystuje je do kształtowania opinii, dyskredytowania przeciwników i zasiewania niezgody.



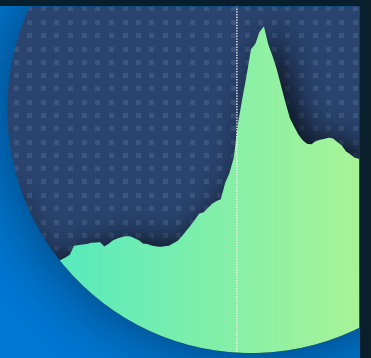
Więcej informacji na str. 74

Inwazja Rosji na Ukrainę pokazuje, że operacje wpływu są połączone z tradycyjnymi cyberatakami i kinetycznymi operacjami wojskowymi.



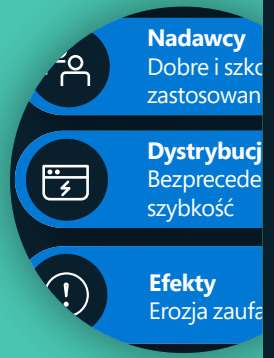
Więcej informacji na str. 76

Rosja, Iran i Chiny stosowały propagandę i kampanie wpływu podczas pandemii COVID-19 często jako strategiczne narzędzie do osiągania szerszych celów politycznych.



Więcej informacji na str. 76

Media syntetyczne stają się coraz bardziej powszechne ze względu na rozpowszechnienie narzędzi, które łatwo tworzą i rozpowszechniają wysoce realistyczne, sztuczne obrazy, wideo i audio. Technologia cyfrowego dowodu pochodzenia, która poświadcza pochodzenie zasobów medialnych, może pomóc w walce z nadużyciami.



Więcej informacji na str. 80

Kompleksowe podejście do ochrony przed operacjami wpływu

Microsoft wykorzystuje swoją zaawansowaną infrastrukturę analityki cyberzagrożeń, aby zwalczać operacje wpływu. Naszą strategię względem kampanii propagandowych prowadzonych przez zagranicznych agresorów można streścić do czterech punktów: wykrywanie, przeciwdziałanie, obrona, odstraszanie.

Więcej informacji na str. 83

Wprowadzenie

Aby demokracja mogła się rozwijać, potrzebuje wiarygodnych informacji. Kluczowym obszarem zainteresowania Microsoft są operacje wpływu realizowane przez państwa. Kampanie te podkopują zaufanie, zwiększają polaryzację społeczną i zagrażają demokracji.

Operacje wpływu zagranicznego zawsze stanowiły zagrożenie dla ekosystemu informacyjnego. Jednak w erze Internetu i mediów społecznościowych mamy do czynienia ze zwiększeniem zakresu, skali i skuteczności kampanii oraz ogromnym wpływem, jaki mogą one mieć na kondycję globalnego ekosystemu informacyjnego.

Powiedzenie „kłamstwo przemierzy pół świata, zanim prawda zdąży założyć buty" jest obecnie potwierdzane danymi. Badanie Massachusetts Institute of Technology (MIT)[1] wykazało, że kłamstwa mają o 70% większe szanse na retweet niż prawda i sześciokrotnie szybciej docierają do pierwszych 1500 osób. Ekosystem informacyjny staje się coraz bardziej mroczny, ponieważ w Internecie i mediach społecznościowych kwitną kampanie propagandowe, które podważają zaufanie do tradycyjnych wiadomości. W badaniu z 2021 r.[2] tylko 7% dorosłych Amerykanów stwierdziło, że ma „duże zaufanie" do wiadomości prasowych, telewizyjnych i radiowych, a 34% „wcale".

Microsoft identyfikuje główne grupy, zagrożenia i stosowane taktyki w ramach operacji wpływu zagranicznego oraz publicznie informuje o odkryciach. W czerwcu tego roku opublikowaliśmy obszerny raport na temat wniosków wyciągniętych z wojny na Ukrainie, który zawierał szczegółowe spojrzenie na operacje wpływu prowadzone przez Rosję[3].

Badamy również, jak zaawansowane technologie, takie jak „deep fake", mogą być wykorzystane jako broń i podważać wiarygodność dziennikarzy. Współpracujemy z branżą, administracją publiczną i ośrodkami akademickimi, aby opracować lepsze sposoby wykrywania mediów syntetycznych i przywrócić zaufanie — np. użycie AI do wykrywania fałszerstw.

Szybko zmieniający się charakter ekosystemu informacyjnego i propagandy internetowej prowadzonej przez państwa, w tym łączenie tradycyjnych cyberataków z operacjami wpływu i ingerencją w demokratyczne wybory, wymaga podejścia obejmującego całe społeczeństwo w celu przeciwdziałania zagrożeniom dla demokracji zarówno w Internecie, jak i poza nim.

Microsoft jest zaangażowany we wspieranie zdrowego ekosystemu informacyjnego, w którym promowane są wiarygodne wiadomości i informacje. Opracowujemy narzędzia i możliwości wykrywania zagrożeń, aby zwalczać rosnące ryzyko operacji wpływu prowadzonych przez państwa. Aby umożliwić tę pracę, niedawno nabyliśmy firmę Miburo Solutions, współpracujemy z zewnętrznymi podmiotami zajmującymi się weryfikacją, takimi jak Global Disinformation Index czy NewsGuard, a także uczestniczymy w wielostronnych partnerstwach (a czasem im przewodzimy), w tym Coalition for Content Provenance and Authenticity (C2PA). Tylko dzięki wspólnej pracy możemy odnieść sukces w walce z tymi, którzy dążą do osłabienia procesów i instytucji demokratycznych.

Teresa Hutson

Wiceprezes ds. technologii i odpowiedzialności przedsiębiorstwa

Trendy w operacjach wpływu

W miarę ewolucji technologii operacje wpływu stają się coraz bardziej zaawansowane. Obserwujemy nakładanie się i rozszerzanie narzędzi stosowanych w tradycyjnych cyberatakach na operacje wpływu. Ponadto zwiększa się skoordynowanie między państwami i wzajemne wzmacnianie przekazów.

Microsoft zainwestował w tym roku w zwalczanie operacji wpływu zagranicznego przez nabycie firmy Miburo Solutions specjalizującej się w analizie tego obszaru. Połączyliśmy specjalistów tej firmy i analityków zagrożeń Microsoft, tworząc Digital Threat Analysis Center (DTAC). DTAC analizuje i raportuje zagrożenia ze strony państw, w tym zarówno cyberataki, jak i operacje wpływu, łącząc informacje o zagrożeniach i ich analitykę z analizą geopolityczną, aby zapewnić szczegółowe informacje umożliwiające skuteczne reagowanie i chronienie.

Ponad trzy czwarte ludzi na całym świecie stwierdziło, że martwi się o wykorzystywanie informacji jako broni[4]. Nasze dane potwierdzają te obawy. Microsoft i partnerzy śledzą, jak atakujący powiązani z państwami realizują operacje wpływu, by osiągać strategiczne cele, w tym polityczne. Oprócz niszczycielskich cyberataków i cyberszpiegostwa reżimy autorytarne w coraz większym stopniu wykorzystują operacje wpływu do kształtowania opinii, dyskredytowania przeciwników, wzniecania strachu, zasiewania niezgody i zniekształcania rzeczywistości.

Te operacje wpływu zagranicznego mają zazwyczaj trzy etapy:

Wstępne zasianie

Tak jak hakerzy wstępnie zasiewają złośliwe oprogramowanie w sieci komputerowej organizacji-ofiary, tak w ramach operacji wpływu zagranicznego następuje wstępne zasiewanie fałszywych narracji w Internecie. Taktyka wstępnego zasiewania była od dawna stosowana w tradycyjnych cyberdziałaniach, zwłaszcza jeśli administratorzy IT skanują aktywność w swojej sieci. Jeśli złośliwe oprogramowanie w sieci przez dłuższy czas pozostaje uśpione, może to zwiększyć skuteczność jego późniejszego wykorzystania. Fałszywe narracje, które pozostają niezauważone w Internecie, mogą sprawić, że kolejne wzmianki wydadzą się bardziej wiarygodne.

Odpalenie

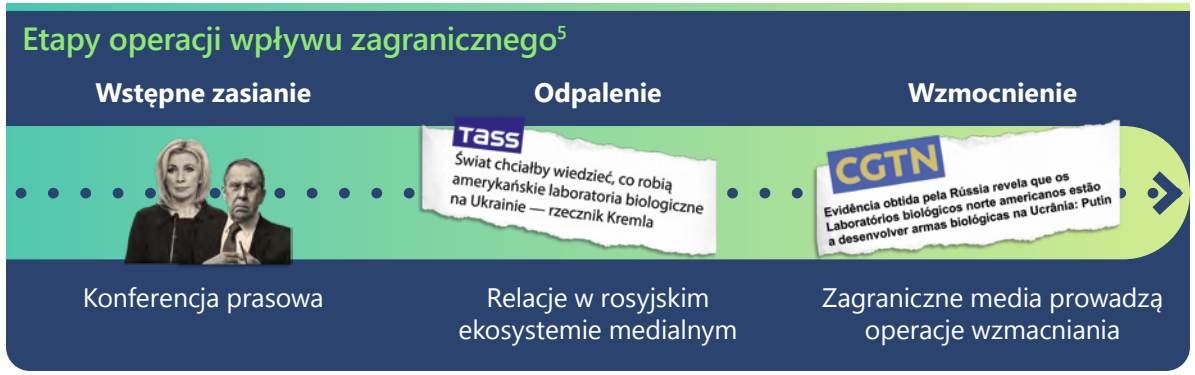
Często w czasie najbardziej korzystnym dla osiągnięcia celów atakujących zostaje rozpoczęta skoordynowana kampania propagowania narracji za pośrednictwem wspieranych przez rząd i pozostających pod jego wpływem mediów oraz kanałów mediów społecznościowych.

Wzmocnienie

Wreszcie, kontrolowane przez państwo media i ośrodki pośredniczące wzmacniają narracje wśród docelowych odbiorców. Często nieświadome ośrodki technologiczne poszerzają zasięg narracji. Na przykład reklama online może pomóc w finansowaniu działalności, a skoordynowane systemy dostarczania treści mogą zalać wyszukiwarki.

To trzyetapowe podejście zostało zastosowane pod koniec 2021 r. w ramach rosyjskiej, fałszywej narracji wokół rzekomej broni biologicznej i laboratoriów biologicznych na Ukrainie. Przekaz ten został po raz pierwszy zasiany na YouTube 29 listopada 2021 r. w regularnym, anglojęzycznym programie amerykańskiego emigranta mieszkającego w Moskwie, który stwierdził, że finansowane przez Stany Zjednoczone laboratoria biologiczne na Ukrainie zajmowały się bronią biologiczną. Historia ta przez wiele miesięcy przeszła w dużej mierze niezauważona. 24 lutego 2022 r., akurat gdy rosyjskie czołgi przekraczały granicę, narracja ta została „odpalona". Zespół analityków danych Microsoft zidentyfikował 10 kontrolowanych przez Rosjan lub będących pod ich wpływem serwisów informacyjnych, które 24 lutego jednocześnie opublikowały doniesienia wskazujące na „zeszłoroczny raport" i starały się mu nadać wiarygodność. Ponadto urzędnicy rosyjskiego MSZ zorganizowali konferencje prasowe, które ugruntowały w środowisku informacyjnym fałszywe twierdzenia o amerykańskich laboratoriach biologicznych. Sponsorowane przez Rosję zespoły pracowały następnie nad wzmocnieniem tej narracji w mediach społecznościowych i na stronach internetowych.

Obserwujemy, że autorytarne reżimy na całym świecie współpracują ze sobą w celu zanieczyszczania ekosystemu informacyjnego na swoją korzyść. Na przykład w trakcie pandemii COVID-19 Rosja, Iran i Chiny stosowały propagandę i operacje wpływu, wykorzystując mieszankę jawnych, półjawnych i niejawnych metod rozpowszechniania informacji, aby zaatakować demokracje i realizować cele geopolityczne (patrz str. 76). Trzy reżimy wykorzystywały nawzajem swoją komunikację i ekosystemy informacyjne, aby promować preferowane narracje. Duża część tych relacji składała się z krytyki lub teorii spiskowych na temat Stanów Zjednoczonych i ich sojuszników, które były rozpowszechniane przez przedstawicieli rządu w oficjalnych oświadczeniach. Jednocześnie promowano własne szczepionki i reakcje na COVID-19 jako lepsze od Stanów Zjednoczonych i innych demokracji. Wspierając się nawzajem, państwowe media stworzyły ekosystem, w którym negatywne relacje o demokracjach i pozytywne o Rosji, Iranie i Chinach produkowane przez jedne państwowe publikatory były wzmacniane przez inne.



Ilustracja pokazująca, jak narracje o amerykańskich laboratoriach biologicznych i broni biologicznej rozprzestrzeniają się w trzech szerokich fazach wielu operacji wpływu zagranicznego — „wstępne zasianie", „odpalenie" i „wzmocnienie".

Trendy w operacjach wpływu

(c.d.)

Na domiar złego firmy technologiczne z sektora prywatnego mogą nieświadomie umożliwiać takie kampanie. „Podmiotami umożliwiającymi" mogą być firmy, które rejestrują domeny internetowe, hostują strony internetowe, promują materiały w mediach społecznościowych i wyszukiwarkach, przekierowują ruch w Internecie i płacą za te działania reklamą cyfrową. Organizacje muszą być świadome narzędzi i metod stosowanych przez reżimy autorytarne do operacji wpływu, aby mogły wykrywać kampanie, a następnie zapobiegać ich rozprzestrzenianiu się. Rośnie również potrzeba edukowania konsumentów w umiejętności rozpoznawania operacji wpływu zagranicznego, by ograniczyć skuteczność tego typu narracji oraz treści.

Operacje wpływu, w tym autorytarna propaganda, stanowią zagrożenie dla demokracji na całym świecie, ponieważ podważają zaufanie, zwiększają polaryzację i zagrażają procesom demokratycznym.

Niezbędna jest większa koordynacja i wymiana informacji między administracją publiczną, sektorem prywatnym a społeczeństwem, aby zwiększyć transparentność oraz umożliwić ujawnianie tych kampanii wpływu i przeciwdziałanie im.

Ponad trzy czwarte ludzi na świecie martwi się tym, że informacje są wykorzystywane jako broń.

Operacje wpływu podczas pandemii COVID-19 i inwazji Rosji na Ukrainę

Próby wpływania przez państwa na środowisko informacyjne w czasie pandemii i rosyjskiej inwazji na Ukrainę stanowią jaskrawe przykłady tego, jak reżimy autorytarne łączą operacje cybernetyczne i informacyjne.

Propaganda dotycząca COVID-19

Rosja, Iran i Chiny stosowały kampanie propagandowe i wywierania wpływu w trakcie pandemii COVID-19. Obecność COVID-19 w tych kampaniach można podzielić na dwa aspekty:

1. Sposoby przedstawiania samej pandemii.
2. Kampanie wykorzystujące COVID-19 jako sposób osiągania szerszych celów politycznych.

Ogólny cel tego typu kampanii jest dwojaki: po pierwsze, osłabić demokracje, instytucje demokratyczne oraz wizerunek Stanów Zjednoczonych i ich sojuszników na arenie międzynarodowej. Po drugie, wzmocnić własną pozycję w kraju i na arenie międzynarodowej.

Przykładem tego mogą być komunikaty znanych rosyjskich kont i organizacji medialnych skierowane do czytelników anglojęzycznych w porównaniu z tym, co rząd rosyjski komunikował własnym obywatelom w sprawie szczepionki i doniosłości COVID-19.

Tematy 10 najczęściej oglądanych historii na temat koronawirusa na RT.com
(październik 2021 r. – kwiecień 2022 r.)

Antyszczepionkowa propaganda skierowana do nierosyjskich czytelników

Do odbiorców rosyjskich (przetłumaczono z rosyjskiego)	Do odbiorców angielskojęzycznych
„Lockdowny i wielokrotne szczepienia uniemożliwiają transmisję wirusa”	„Szczepienia nie ograniczają transmisji i są nieskuteczne wobec nowych szczepów”
„Rosyjskie osoby publiczne mają koronawirusa”	„Szczepionka Pfizer ma niebezpieczne skutki uboczne”
„W Rosji rośnie liczba przypadków i zgonów”	„Masowe szczepienia są motywowane politycznie”
„Szczepionka Sputnik V jest bardzo skuteczna”	„Firmy Pfizer i Moderna prowadzą nieuregulowane testy”
„Dowód szczepienia wymagany w transporcie publicznym”	

Rosyjskie komunikaty dotyczące COVID-19 różnią się w zależności od języka.

Innym przykładem są kampanie mające na celu ukrycie pochodzenia wirusa COVID-19. Od początku pandemii rosyjska, irańska i chińska propaganda na temat COVID-19 wzmacniała narracje pozostałych stron, aby promować główne przekazy. Znaczna część tych relacji dotyczyła promowania krytyki lub teorii spiskowych dotyczących Stanów Zjednoczonych. Wspierając się nawzajem, państwowe media stworzyły ekosystem, w którym negatywne relacje o demokracjach i pozytywne o Rosji, Iranie i Chinach produkowane przez jedne państwowe media były wzmacniane przez inne.

Jednym z takich przykładów jest wcześniejsza sugestia rosyjskich i irańskich mediów państwowych, że COVID-19 może być bronią biologiczną stworzoną przez Stany Zjednoczone. Twierdzenie to krążyło na marginalnych stronach internetowych promujących teorie spiskowe na początku pandemii po wywiadzie z profesorem prawa, który uważał, że COVID-19 został stworzony jako broń[6]. Po opublikowaniu wywiadu na kilku stronach internetowych o ograniczonym zasięgu historia została podchwycona przez państwowe media. PressTV, irański angielsko- i francuskojęzyczny serwis informacyjny sponsorowany przez rząd Iranu[7], opublikował w lutym 2020 r. artykuł po angielsku zatytułowany „Czy koronawirus jest amerykańską bronią biologiczną, jak uważa Francis Boyle?”. Artykuł sugerował, że Stany Zjednoczone stoją za epidemią COVID-19: „we wszystkich amerykańskich wojnach używa się broni radiologicznej, chemicznej, biologicznej i innych zakazanych środków, co powoduje wiele ofiar”[8]. Rosyjskie media państwowe i chińskie konta rządowe powtórzyły tę narrację. Państwowe medium Russia Today (RT) znane ze swojej roli w rozpowszechnianiu kremlowskiej propagandy[9] opublikowało co najmniej jedną historię, która promowała oświadczenia irańskich urzędników twierdzących, że COVID-19 może być „produktem amerykańskiego «ataku biologicznego» wymierzonego w Iran i Chiny”[10] i rozpowszechniła sugerujące to posty w mediach społecznościowych. Oto przykładowy tweet RT z 27 lutego 2020 r.: „Kto nie będzie zaskoczony, jeśli okaże się, że #koronawirus to broń biologiczna?”[11].

Wojna na Ukrainie — propaganda jako broń na wojnie

Inwazja Rosji na Ukrainę stanowi wyraźny przykład tego, jak operacje wpływu mogą być łączone z tradycyjnymi cyberatakami i naziemnymi operacjami wojskowymi, aby zmaksymalizować skuteczność.

W okresie poprzedzającym inwazję na Ukrainę analitycy ds. zagrożeń Microsoft zauważyli, że co najmniej sześć odrębnych grup związanych z Rosją przeprowadziło ponad 237 cyberataków na Ukrainę. Kampanie te miały na celu upośledzenie usług i instytucji, zakłócenie dostępu Ukraińców do rzetelnej informacji oraz zasianie wątpliwości co do przywództwa ich kraju.

Operacje wpływu podczas pandemii COVID-19 i inwazji Rosji na Ukrainę

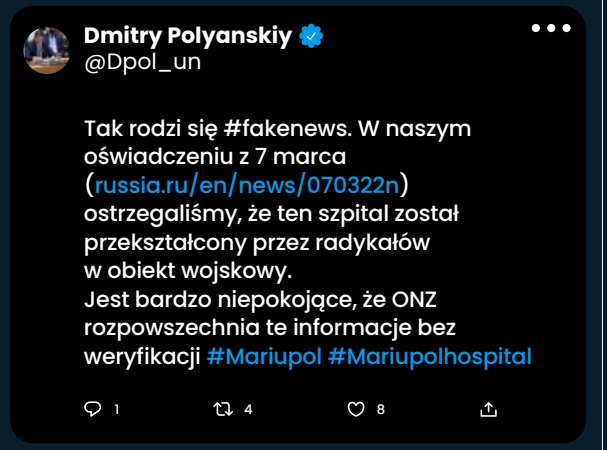
(c.d.)

W raporcie Microsoft opublikowanym w kwietniu 2022 r. pokazaliśmy, jak w oczywistej próbie kontrolowania ukraińskiego środowiska informacyjnego Rosja przeprowadziła atak rakietowy na wieżę telewizyjną w Kijowie w tym samym dniu, w którym wdrożyła destrukcyjne, złośliwe oprogramowanie przeciwko dużej, ukraińskiej firmie medialnej[12].

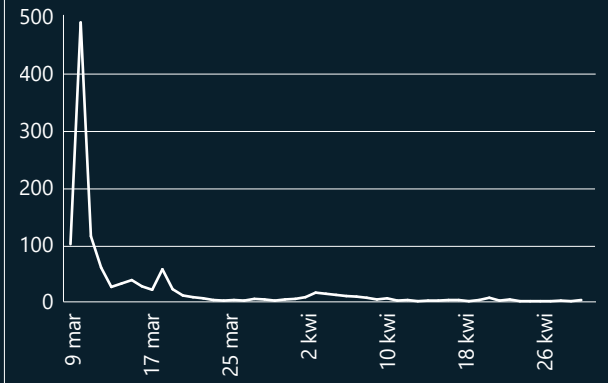
Innym przykładem zbieżności cyberataków i operacji wpływu jest grupa powiązana z Rosją, która wysłała do obywateli Ukrainy e-maile podszywające się pod mieszkańców Mariupola, obwiniając ukraiński rząd za eskalację wojny i wzywając swoich rodaków do przeciwstawienia się własnemu rządowi. Te wiadomości e-mail były specjalnie adresowane (z imienia i nazwiska) do konkretnych osób. Oznacza to, że dane tych osób mogły zostać wykradzione podczas wcześniejszego cyberataku. Nie dodano żadnych złośliwych linków, co sugeruje, że intencją była sama operacja wpływu.

Wykorzystywanie materiałów, które wyciekły lub zostały zhakowane albo są wrażliwe jest powszechną taktyką stosowaną w operacjach wpływu przez atakujących powiązanych z Rosją. Przez cały okres wojny na Ukrainie prorosyjskie kanały w mediach społecznościowych promowały to, co według nich jest wyciekiem lub innymi informacjami wrażliwymi ze źródeł ukraińskich. Wyciekające lub wrażliwe materiały są wykorzystywane przez prorosyjskie kanały i media społecznościowe w ramach szerszej strategii wywierania wpływu w celu zmniejszenia zaufania do instytucji i podważenia głównych narracji. Informacje te mogą być zmanipulowane w celu stworzenia propagandy skierowanej przeciwko Ukrainie i Zachodowi, zmniejszenia zaufania do bezpieczeństwa cyfrowego i osłabienia poparcia dla zachodniej pomocy Ukrainie.

Po konkretnych wydarzeniach Rosja stosowała innego typu ataki informacyjne, aby zaciemnić lub podważyć fakty i odpowiednio uformować opinię publiczną. Na przykład 7 marca Rosja, poprzez złożenie wniosku do ONZ, wstępnie zasiała informację, że szpital położniczy w Mariupolu na Ukrainie został opuszczony i był wykorzystywany jako obiekt wojskowy. 9 marca Rosja zbombardowała ten szpital. Po pojawieniu się informacji o bombardowaniu przedstawiciel Rosji w ONZ Dmitrij Polianskij napisał na Twitterze, że relacja o zamachu to „fake news" i przytoczył wcześniejsze twierdzenia Rosji o rzekomym wykorzystywaniu tego miejsca jako obiektu wojskowego. Przez dwa tygodnie po ataku na szpital Rosja szeroko rozpowszechniała tę narrację na kontrolowanych przez siebie stronach internetowych.



Domeny z ruchem
(9 marca 2022 r. – 30 kwietnia 2022 r.)



Propagandowe witryny internetowe publikowały historie o szpitalu położniczym przez około dwa tygodnie, z krótkim ożywieniem rozpoczynającym się 1 kwietnia 2022 r. Źródło: Microsoft AI for Good Lab.

Zdjęcia satelitarne szpitala położniczego w Mariupolu w lutym i marcu 2022 r.

Analiza zdjęć satelitarnych przez Microsoft wykazała, że szpital położniczy został zbombardowany. Pierwsze zdjęcie pochodzi z 24 lutego 2022 r., a drugie z 24 marca 2022 r. Źródło zdjęcia: Planet Labs.

Wybielanie przez Rosję okrucieństw trwało w miarę postępu wojny. Na przykład bombardowanie centrum handlowego pod koniec czerwca 2022 r. zostało przedstawione przez rosyjskie media i rosyjskich influencerów jako uzasadnione i konieczne. Fałszywie twierdzono, że nie było ono używane jako centrum handlowe, ale jako zbrojownia sił obrony terytorialnej Ukrainy[13]. Kilku prokremlowskich blogerów na Telegramie zamieściło i wzmocniło treści promujące narrację „fałszywej flagi", przy czym blogerzy wskazali na rzekome wskaźniki sfabrykowania, w tym obecność ludzi w mundurach wojskowych na nagraniach z miejsca zdarzenia[14] i brak kobiet na zdjęciach[15]. Rosja przeprowadziła kampanię, opierając się na zbudowanym systemie propagandowych posłańców i mediów. Wzmocnienie tych historii w Internecie daje Rosji możliwość zrzucenia z siebie winy na scenie międzynarodowej i uniknięcia odpowiedzialności.

Państwa takie jak Rosja rozumieją wartość wykorzystywania informacji pochodzących z zamkniętych źródeł do wpływania na opinię publiczną. Prowadzą one kampanie „hakowania i publikowania" w celu szerzenia kontrnarracji i siania nieufności.

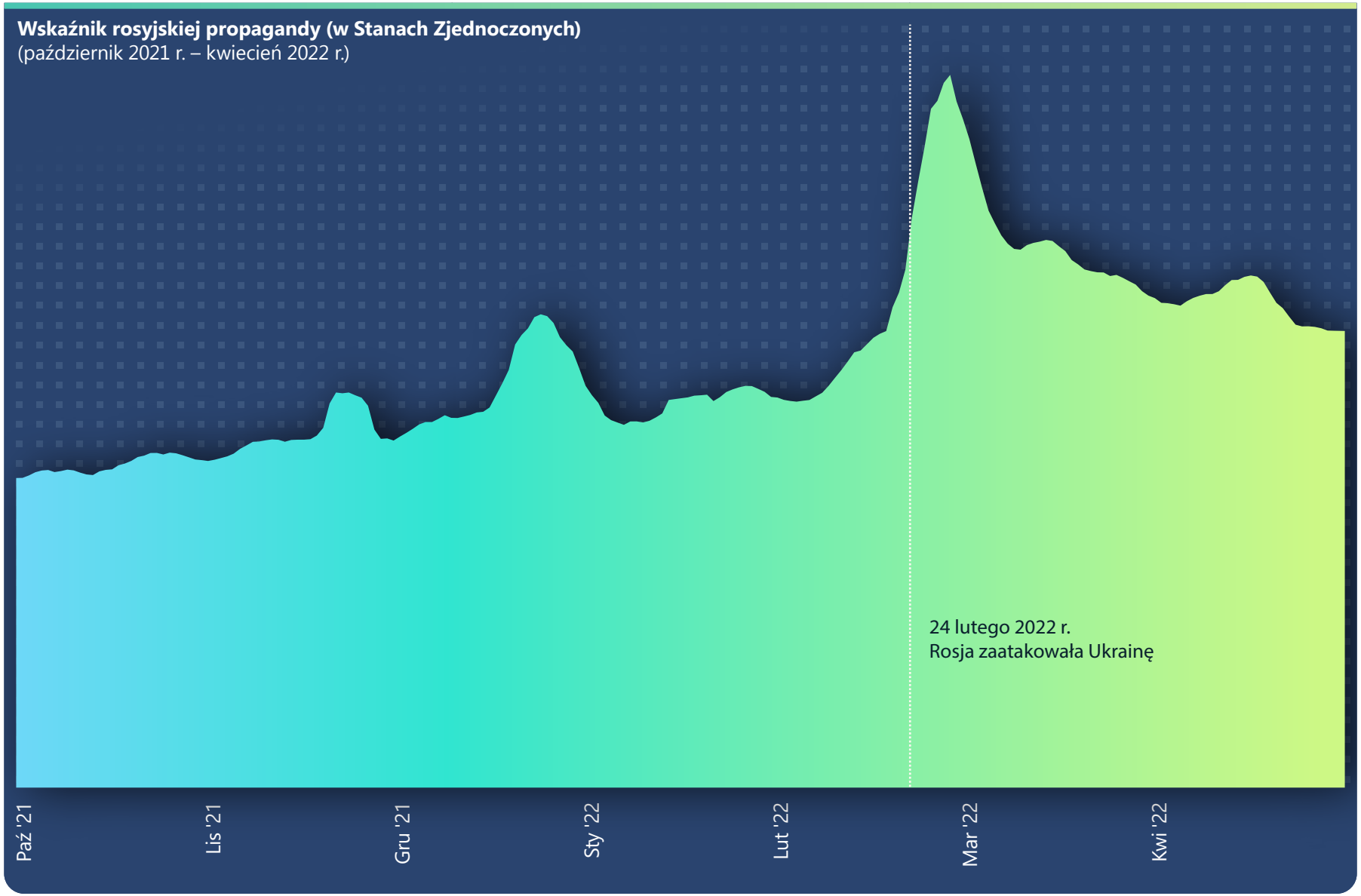
Linki do dalszych informacji

- Obrona Ukrainy: pierwsze lekcje z cyberwojny | Microsoft On the Issues
- Przegląd aktywności Rosji w zakresie cyberataków na Ukrainie | Microsoft Special Report
- Destrukcyjne cyberataki na Ukrainę | Microsoft On the Issues

Trendy w rosyjskiej propagandzie

W styczniu 2022 r. blisko tysiąc amerykańskich witryn internetowych przekierowywało ruch na rosyjskie strony propagandowe. Najczęstszymi tematami rosyjskich witryn propagandowych kierowanych do odbiorców amerykańskich była wojna na Ukrainie, polityka wewnętrzna Stanów Zjednoczonych (pro-Trump lub pro-Biden) oraz narracje związane z COVID-19 i szczepionkami.

Wskaźnik rosyjskiej propagandy (RPI, Russian Propaganda Index) obrazuje przepływ newsów z kontrolowanych przez Rosję lub sponsorowanych przez nią serwisów informacyjnych i ośrodków wzmacniania narracji względem całości przepływu newsów w Internecie. RPI pozwala na stworzenie wykresu w czasie konsumpcji rosyjskiej propagandy w całym Internecie i w różnych regionach geograficznych. Microsoft zaznacza jednak, że widzimy jedynie rosyjską propagandę publikowaną w witrynach, które zostały wcześniej zidentyfikowane. Nie mamy wglądu w propagandę na innych typach witryn internetowych, w tym na autorytatywnych witrynach informacyjnych, witrynach niezidentyfikowanych i w grupach społecznościowych.



Trendy w rosyjskiej propagandzie

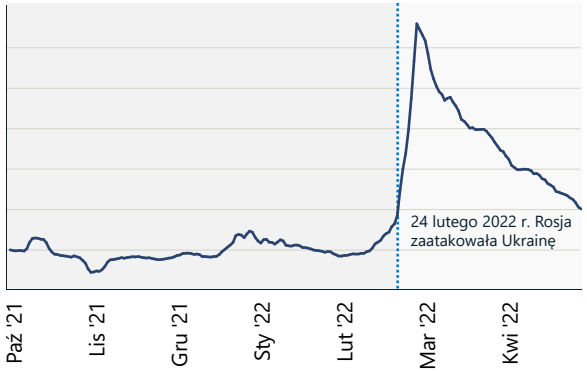
(c.d.)

Wskaźnik rosyjskiej propagandy: Ukraina

Po rozpoczęciu wojny na Ukrainie odnotowaliśmy wzrost rosyjskiej propagandy o 216%. Osiągnęła ona szczyt 2 marca. Poniższy wykres pokazuje, że ten nagły wzrost zbiegł się z inwazją. Te dwa wykresy pokazują gwałtowny wzrost rosyjskiej propagandy wkrótce po rozpoczęciu inwazji.

RPI: Ukraina

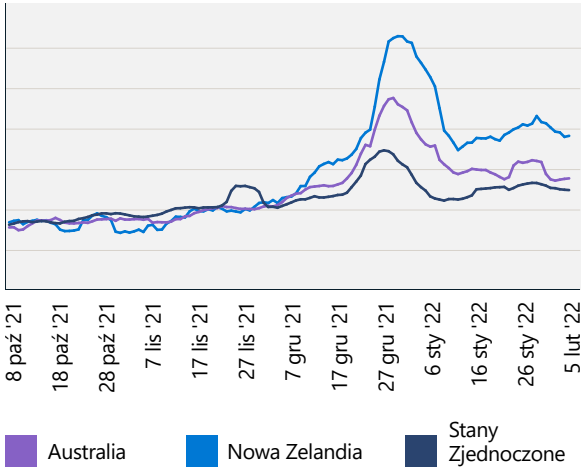
(7 października 2021 r. – 30 kwietnia 2022 r.)



„Wskaźnik rosyjskiej propagandy: Nowa Zelandia" względem Australii i Stanów Zjednoczonych

Ocena RPI w Nowej Zelandii wykazała gwałtowny wzrost pod koniec 2021 r. — był on związany z propagandą COVID-19. Ten skok konsumpcji rosyjskiej propagandy w Nowej Zelandii poprzedził wzrost publicznych protestów na początku 2022 r. w Wellington. Drugi szczyt był wyraźnie związany z inwazją Rosji na Ukrainę i przekroczył RPI Australii i Stanów Zjednoczonych.

„RPI: Nowa Zelandia" w porównaniu do Australii i Stanów Zjednoczonych



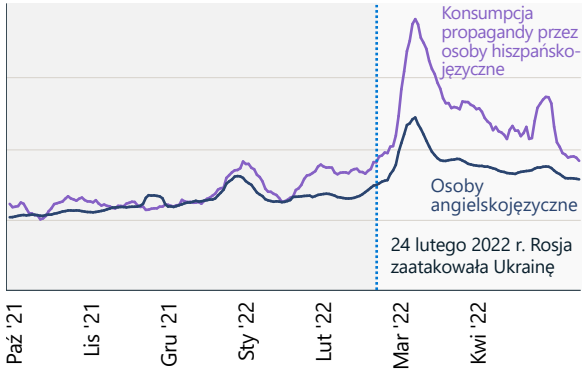
Do pierwszego tygodnia grudnia 2021 r. konsumpcja rosyjskiej propagandy w Nowej Zelandii była na podobnym poziomie, co w Australii. Po grudniu konsumpcja rosyjskiej propagandy w Nowej Zelandii wzrosła o ponad 30% w stosunku do Australii i Stanów Zjednoczonych.

Wskaźnik rosyjskiej propagandy w Stanach Zjednoczonych: angielski i hiszpański

RPI śledzi również propagandę w różnych językach. Wiele mediów, w tym RT i Sputnik News, jest dostępnych w ponad 20 językach. Są to: angielski, hiszpański, niemiecki, francuski, grecki, włoski, czeski, polski, serbski, łotewski, litewski, mołdawski, białoruski, ormiański, osetyjski, gruziński, azerski, arabski, turecki, perski i dari.

Poniższy wykres pokazuje, że wskaźnik RPI dla wiadomości w języku hiszpańskim w Stanach Zjednoczonych jest znacznie wyższy niż dla wiadomości w języku angielskim.

Konsumpcja rosyjskiej propagandy jest 2 razy większa wśród osób hiszpańskojęzycznych



Konsumpcja rosyjskiej propagandy w Stanach Zjednoczonych jest dwukrotnie wyższa wśród osób hiszpańskojęzycznych.

Rosyjska propaganda jest na fali w Ameryce Łacińskiej

RT po hiszpańsku to międzynarodowy serwis informacyjny z największą liczbą odsłon i obserwujących na Facebooku.

Źródło: Microsoft AI for Good Research Lab

Media syntetyczne

Wchodzimy w złotą erę tworzenia i manipulowania mediami przez AI. Analitycy Microsoft zauważają, że wynika to z dwóch kluczowych trendów: rozpowszechnienia łatwych w użyciu narzędzi i usług do sztucznego tworzenia wysoce realistycznych, syntetycznych obrazów, filmów, dźwięków i tekstów oraz możliwości szybkiego rozpowszechniania treści zoptymalizowanych pod kątem konkretnych odbiorców.

Żadna z tych nowości nie jest sama w sobie problematyczna. Technologia oparta na AI może tworzyć zabawne i ekscytujące treści cyfrowe. Mogą być one wykreowane czysto syntetyczne albo stanowić modyfikację istniejących materiałów. Narzędzia te są szeroko wykorzystywane przez przedsiębiorstwa do reklamy i komunikacji oraz przez osoby prywatne do tworzenia angażujących treści dla obserwujących. Jednak media syntetyczne, jeśli są tworzone i rozpowszechniane ze złymi zamiarami, mogą poważnie zaszkodzić osobom, firmom, instytucjom i społeczeństwu. Microsoft był i jest motorem opracowywania technologii i praktyk ograniczających te szkody — zarówno wewnętrznie, jak i w szerszym ekosystemie mediów.

W tej części przedstawiono spostrzeżenia Microsoft na temat obecnego stanu technologii tworzenia szkodliwych treści syntetycznych, szkód, które mogą powstać w przypadku ich rozpowszechnienia, oraz technicznych środków zaradczych, które mogą chronić przed cyberzagrożeniami związanymi z mediami syntetycznymi.

Tworzenie mediów syntetycznych

Dziedzina syntetycznego tekstu i mediów rozwija się niezwykle szybko, ponieważ techniki, które kiedyś były możliwe tylko dzięki ogromnym zasobom obliczeniowym wielkich studiów filmowych, są obecnie dostępne w aplikacjach na telefony. Jednocześnie narzędzia stają się łatwiejsze w użyciu i mogą generować treści o poziomie realizmu, który może oszukać nawet specjalistów kryminalistycznych. Jesteśmy bardzo blisko osiągnięcia punktu, w którym każdy będzie mógł stworzyć syntetyczne wideo, na którym dowolna osoba mówi lub robi cokolwiek. Wchodzimy w erę, w której znaczna część treści w sieci będzie w pełni lub częściowo tworzona syntetycznie przy użyciu AI.

Wraz z dostępnością wyrafinowanych, łatwych w użyciu i szeroko dostępnych narzędzi tworzenie treści syntetycznych jest coraz powszechniejsze. Wkrótce nie będzie można ich odróżnić od rzeczywistości.

Istnieje wiele wysokiej jakości, bezpłatnych i komercyjnych narzędzi do edycji obrazów, wideo i audio. Dzięki tym narzędziom można wprowadzać proste, ale potencjalnie szkodliwe zmiany w treściach cyfrowych, takie jak dodanie wprowadzającego w błąd tekstu, zamiana twarzy czy usunięcie lub zmiana kontekstu. Takie „tanie podróbki" są szeroko wykorzystywane do rozpowszechniania szkodliwych treści, promowania ideologii politycznych i niszczenia reputacji. Znanym przykładem jest wideo z 2019 r.[16] przedstawiające Przewodniczącą Izby Reprezentantów USA, Nancy Pelosi, która mówi niewyraźnie i wygląda na nietrzeźwą. Chociaż szybko ustalono, że wideo zostało spowolnione, aby stworzyć taki efekt, „tania podróbka" rozprzestrzeniła się, zanim oryginalne wideo i kontekst wypłynęły na powierzchnię.

Bardziej wyrafinowane podejścia do zmiany treści medialnych to m.in. zastosowanie zaawansowanych technik AI do (a) tworzenia czysto syntetycznych mediów oraz (b) dokonywania wyrafinowanych edycji istniejących mediów. Termin „deepfake" (głębokie fałszerstwo) jest często używany w odniesieniu do syntetycznych mediów, które zostały stworzone przy użyciu najnowocześniejszych technik AI (nazwa pochodzi od głębokich sieci neuronowych). Technologie te są opracowywane jako samodzielne aplikacje, narzędzia i usługi oraz integrowane z uznanymi narzędziami do edycji, komercyjnymi i open-source.

Takie technologie są wykorzystywane jako broń przez atakujących, którzy chcą zaszkodzić osobom i instytucjom. Przykładami technik deepfake są:

- **Zamiana twarzy (wideo, obrazy) —** zastąpienie twarzy w filmie inną twarzą. Technikę tę można wykorzystać do próby szantażu osoby, firmy lub instytucji albo do umieszczenia osób w kłopotliwych miejscach lub sytuacjach.
- **Puppeteering (wideo, obrazy) —** użycie jednego filmu do zaanimowania nieruchomego obrazu lub innego filmu. W efekcie można otrzymać film, w którym osoba „mówi" coś zawstydzającego lub wprowadzającego w błąd.
- **Generatywne sieci przeciwstawne (Generative Adversarial Network/ GAN — wideo, obrazy) —** rodzina technik generowania fotorealistycznych obrazów.
- **Modele typu transformer (wideo, obrazy, tekst) —** tworzenie bogatych obrazów na podstawie opisów tekstowych.

Tak zaawansowane techniki oparte na AI nie są jeszcze dziś powszechnie wykorzystywane w kampaniach wpływu, ale spodziewamy się, że problem będzie narastał w miarę, jak te narzędzia staną się łatwiejsze w użyciu i szerzej dostępne.

Konsekwencje syntetycznych manipulacji medialnych

Wykorzystanie operacji informacyjnych do wyrządzania szkód lub rozszerzania wpływów nie jest niczym nowym. Jednak szybkość, z jaką informacje mogą się rozprzestrzeniać, oraz nasza niezdolność do szybkiego oddzielania faktów od fikcji oznaczają, że wpływ i szkody spowodowane przez fałszywe i inne syntetycznie wygenerowane złośliwe media mogą być znacznie większe, jak pokazał przykład Pelosi.

Istnieje kilka kategorii szkód, które bierzemy pod uwagę: manipulacje rynkiem, oszustwa płatnicze, vishing (wyłudzanie danych w wersji głosowej), podszywanie się, szkody dla marki, szkody dla reputacji czy botnety. Wiele z tych kategorii ma szeroko opisywane przykłady, które mogą podważać naszą zdolność do oddzielania faktów od fikcji.

Sytuacja, w której nie będziemy już mogli ufać temu, co widzimy i słyszymy, i nie będziemy mogli w niektórych kontekstach odróżnić prawdy od fikcji, wydaje się istotnym zagrożeniem. Z tego powodu każdy kompromitujący obraz, dźwięk lub film osoby publicznej lub prywatnej może zostać uznany za fałszywy (ten efekt znany jest „dywidendą kłamcy")[17]. Najnowsze badania[18] pokazują, że to nadużycie technologii jest już wykorzystywane do atakowania systemów finansowych. Można sobie wyobrazić też wiele innych nadużyć.

Media syntetyczne

(c.d.)

Wykrywanie mediów syntetycznych

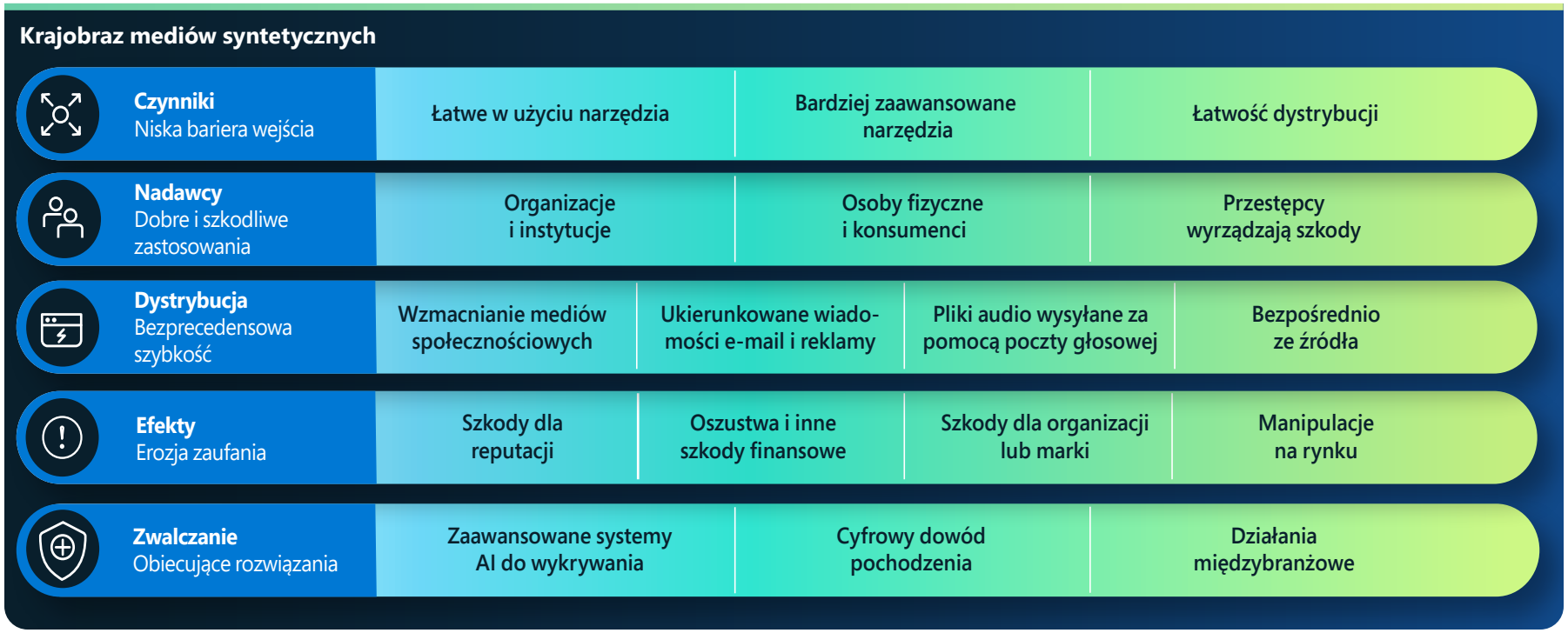
W branży, rządach i środowisku akademickim podejmowane są wysiłki w celu opracowania lepszych sposobów wykrywania mediów syntetycznych i rozwiązywania wynikłych z nich problemów w celu przywrócenia zaufania. Istnieje kilka obiecujących dróg rozwoju, jak również barier, które należy rozważyć.

Jednym z podejść jest budowanie systemów AI wykrywających fałszerstwa czy podróbki („obronne" systemy AI przeciwdziałające „atakującym" systemom AI). Obecne systemy tworzenia syntetycznego audio i wideo pozostawiają wyraźne artefakty, które mogą być wykrywane przez wyszkolonych analityków kryminalistycznych i zautomatyzowane narzędzia. Prowadzi się w tym obszarze badania.

Niestety, wprawdzie fałszerstwa mają charakterystyczne niedoskonałości, jednak konkretne artefakty są specyficzne dla danego narzędzia czy algorytmu. Oznacza to, że wyszkolenie modeli na znanych fałszywkach zwykle nie pozwala na generalizację na inne algorytmy (wykazano to w otwartym konkursie na budowę detektorów obrazów deepfake w 2020 r.)[19]. Można inwestować w tworzenie bardziej zaawansowanych detektorów, jednak Microsoft jest wysoce sceptyczny, czy na pewno spowoduje to znaczącą poprawę — z dwóch powodów:

Po pierwsze, mamy doskonałe modele fizyczne, które odzwierciedlają świat rzeczywisty. Obecni twórcy fałszywek idą na skróty, co skutkuje wykrywalnymi artefaktami, ale nowsze modele będą coraz bardziej realistyczne. Nie ma niczego immanentnie szczególnego w realnej scenie sfilmowanej kamerą, czego nie mógłby wygenerować komputer.

Po drugie, zaawansowane algorytmy tworzenia fałszywek wykorzystują w procesie tworzenia technikę zwaną generatywnymi sieciami przeciwstawnymi (Generative Adversarial Network/GAN). GAN rozgrywa dwa systemy AI przeciwko sobie, używając generatora do tworzenia fałszywek i dyskryminatora do wykrywania fałszywych obrazów i uczenia generatora. Wszelkie inwestycje w opracowanie lepszego wykrywacza pozwolą jedynie generatorowi poprawić jakość podróbek.



Media syntetyczne

(c.d.)

Dowód pochodzenia zasobów cyfrowych

Skoro wykrywanie fałszerstw jest zawodne, to co można zrobić, aby uchronić się przed szkodliwymi zastosowaniami mediów syntetycznych? Jedną z ważnych nowych technologii jest cyfrowy dowód pochodzenia — mechanizm, który umożliwia twórcom mediów cyfrowych na certyfikację zasobów i pomaga konsumentom identyfikować, czy zasoby cyfrowe nie zostały zmodyfikowane. Cyfrowy dowód pochodzenia jest szczególnie ważny w kontekście dzisiejszych sieci mediów społecznościowych, biorąc pod uwagę szybkość, z jaką treści mogą przemieszczać się w Internecie, oraz możliwość łatwego manipulowania nimi przez przestępców.

900%

wzrostu użycia deepfake rok do roku od 2019 r.[20]

Technologia cyfrowego dowodu pochodzenia to nowoczesna wersja kryptograficznego podpisywania dokumentów zaprojektowana do rejestrowania źródła, historii edycji i metadanych obiektów przepływających przez sieć. Zespół badaczy i naukowców Microsoft opracował wizję i metody techniczne umożliwiające tego rodzaju kompleksową certyfikację mediów pod kątem braku manipulacji. Współpracujemy w ramach międzybranżowego partnerstwa mającego na celu wprowadzenie w życie technologii dowodów pochodzenia mediów w ramach projektu Origin (rozpoczętego przez Microsoft, BBC, CBC/Radio-Canada i New York Times) oraz angażujemy się w inicjatywę Content Authenticity Initiative (rozpoczętą przez Adobe). Microsoft współpracował również z partnerami z branży technologicznej i usług medialnych w celu utworzenia Coalition for Content Provenance and Authenticity (C2PA). C2PA to organizacja zajmująca się standardami, która niedawno opublikowała najbardziej zaawansowaną specyfikację cyfrowego dowodu pochodzenia, która jest przeznaczona do wykorzystania z zasobami medialnymi takimi jak obrazy, filmy, audio i tekst.

Obiekt z obsługą C2PA zawiera manifest, który chroni obiekt i metadane przed manipulacją, a towarzyszący mu certyfikat identyfikuje wydawcę.

Media syntetyczne nie zostały pierwotnie zaprojektowane, aby wyrządzać szkody, ale są wykorzystywane przez przestępców do podważania zaufania do osób i instytucji.

Cyfrowy dowód pochodzenia jest obiecującą, nową technologią, która może pomóc przywrócić zaufanie ludzi do treści medialnych online przez poświadczanie pochodzenia treści multimedialnych.

Publicznie dostępne rozwiązania oparte na specyfikacji C2PA pojawiają się jako nowe funkcje w istniejących produktach lub nowe samodzielne aplikacje i usługi. Oczekujemy, że w ciągu kilku lat większość powszechnie używanych narzędzi do przechwytywania, edytowania i tworzenia będzie obsługiwać standard C2PA. To okazja dla przedsiębiorstw, aby już dziś określić potrzeby w zakresie cyfrowego dowodu pochodzenia i zastosować tę technologię u siebie, a także, aby wymagać tego typu dodatkowej warstwy ochrony w narzędziach używanych obecnie do obsługi przepływów pracy.

Praktyczne wskazówki

1. Podejmij proaktywne kroki, aby chronić swoją organizację przed zagrożeniami związanymi z dezinformacją przez proaktywne reagowanie PR i proaktywną komunikację.
2. Użyj technologii dowodu pochodzenia do ochrony oficjalnej komunikacji.

Linki do dalszych informacji

- Obiecujący krok naprzód w sprawie dezinformacji | Microsoft On the Issues
- „Osiągnięty kamień milowy", 31 stycznia 2022 r.
- Projekt Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Poznaj szczegóły techniczne projektu Origin używanego do uwierzytelniania mediów | Microsoft ALT Innovation

Kompleksowe podejście do ochrony przed operacjami wpływu

Microsoft dzięki swojej zaawansowanej infrastrukturze analityki cyberzagrożeń może zapewnić szerszy, bardziej kompleksowy wgląd w operacje wpływu.

Naszą strategię reagowania w walce z tymi operacjami można podzielić na cztery kluczowe filary: wykrywanie, przeciwdziałanie, obronę, odstraszanie.

Ponadto Microsoft przyjął cztery zasady, które stanowią podstawę naszej pracy w tym obszarze. Pierwszą z nich jest zobowiązanie do poszanowania wolności słowa i utrzymania zdolności naszych klientów do tworzenia, publikowania i wyszukiwania informacji za pośrednictwem naszych platform, produktów i usług. Po drugie, aktywnie pracujemy nad tym, aby nasze platformy i produkty nie były wykorzystywane na potrzeby witryn i treści służących do operacji wpływu zagranicznego. Po trzecie, nie będziemy świadomie czerpać korzyści z treści ani podmiotów realizujących operacje wpływu zagranicznego. Wreszcie, priorytetem jest dla nas identyfikowanie treści w celu przeciwdziałania operacjom wpływu zagranicznego przez wykorzystanie w naszych produktach danych własnych i zaufanych podmiotów trzecich.

Wykrywanie

Podobnie jak w przypadku cyberobrony pierwszym krokiem w przeciwdziałaniu operacjom wpływu zagranicznego jest rozwijanie zdolności do ich wykrywania. Żadna pojedyncza firma czy organizacja nie może samodzielnie dokonać niezbędnego postępu. Nowa, szersza współpraca w całym sektorze technologicznym będzie miała kluczowe znaczenie, a postęp w analizowaniu i raportowaniu operacji wpływu zależy w dużej mierze od siły społeczeństwa obywatelskiego, w tym instytucji akademickich i organizacji non-profit.

Uznając tę rolę, badacze Jake Shapiro i Alicia Wanless (z odpowiednio Uniwersytetu Princeton i Carnegie Endowment for International Peace) opracowali plany utworzenia nowego Instytutu Badań nad Środowiskiem Informacyjnym (IRIE). Dzięki wsparciu Microsoft, Knight Foundation i Craig Newmark Philanthropies, IRIE stworzy instytucję badawczą, w której uczestniczyć będą wszystkie zainteresowane strony, wzorowaną na Europejskiej Organizacji Badań Jądrowych (CERN). Połączy on wiedzę z zakresu przetwarzania i analizy danych w celu przyspieszenia i zwiększenia skali nowych odkryć w tej dziedzinie. Wyniki będą udostępniane, aby korzystali z nich decydenci, firmy technologiczne i konsumenci.

Obrona

Drugim filarem strategicznym jest wzmocnienie mechanizmów obrony demokracji. Ten obszar od dawna stanowi priorytet wymagający inwestycji i innowacji. Powinna ona uwzględniać wyzwania, jakie technologia stawia demokracji, oraz możliwości, jakie technologia stworzyła, w celu skuteczniejszej obrony demokratycznych społeczeństw.

Ramy strategii Microsoft proponowane interesariuszom w różnych sektorach wobec propagandy zagranicznych agresorów obejmują cztery filary: wykrywanie, przeciwdziałanie, obronę, odstraszanie.

Warto zacząć od jednego z wielkich wyzwań technologicznych naszego wieku — wpływu Internetu i reklamy cyfrowej na tradycyjne dziennikarstwo. Od 1700 r. wolna i niezależna prasa odgrywała szczególną rolę we wspieraniu każdej demokracji na świecie — ujawniając korupcję, dokumentując wojny i przedstawiając największe wyzwania społeczne epoki. Jednak Internet unicestwił lokalne wiadomości, pochłaniając przychody z reklam i zabierając płatnych subskrybentów. Wiele lokalnych gazet upadło. Jednym z wielu wniosków płynących z naszej ostatniej pracy jest to, że miasta, w których brakuje gazet, są nieświadomie i nieuchronnie narażone na większą niż przeciętna ilość obcej propagandy. Z tych powodów jednym z najważniejszych elementów obronnych demokracji musi być wzmocnienie tradycyjnego dziennikarstwa i wolnej prasy, zwłaszcza na szczeblu lokalnym. Wymaga to ciągłych inwestycji i innowacji, które muszą odzwierciedlać lokalne potrzeby różnych krajów i kontynentów. Te kwestie nie są łatwe i wymagają podejścia obejmującego wiele zainteresowanych stron, które Microsoft i inne firmy technologiczne coraz częściej stosują.

Potrzebujemy również innowacji w polityce publicznej opartych na konsensusie społecznym. Chodzi m.in. o przepisy umożliwiające wydawcom zbiorowe negocjowanie przychodów z reklam z firmami technologicznymi czy przepisy zapewniające ulgi podatkowe zwalniające lokalne redakcje z części podatków od wynagrodzeń dla zatrudnianych przez nie dziennikarzy. Dziennikarze potrzebują wielu innych narzędzi do swojej pracy, w tym umiejętności oddzielania treści pochodzących z legalnych i fałszywych źródeł.

Jest również pilna potrzeba zapewnienia konsumentom zdolności do rozpoznawania operacji wpływu inicjowanych przez państwa. To wszystko może wydawać się trudne, jednak tak naprawdę przypomina pracę, którą sektor technologiczny od dawna wykonuje, zwalczając inne cyberzagrożenia. Należy nauczyć konsumentów analizowania adresów e-mail w celu wykrywania spamu i innych nieuczciwych wiadomości. Inicjatywy w Stanach Zjednoczonych — takie jak News Literacy Project i Trusted Journalism

Sytuacja, w której nie będziemy już mogli ufać temu, co widzimy i słyszymy, i nie będziemy mogli w niektórych kontekstach odróżnić prawdy od fikcji, wydaje się istotnym zagrożeniem.

Kompleksowe podejście do ochrony przed operacjami wpływu

(c.d.)

Program — rozwijają świadomość odbiorców wiadomości i informacji. W skali globalnej nowe technologie, takie jak wtyczka do przeglądarki NewsGuard, może pomóc w przyspieszeniu tych działań.

Pamiętajmy, że fundamentem demokracji jest edukacja obywatelska. Jak zawsze, wysiłek ten należy rozpocząć w szkołach. Żyjemy jednak w świecie, który wymaga od nas ciągłej edukacji obywatelskiej przez całe życie. Nowe zobowiązanie Civics at Work, prowadzone przez Center for Strategic and International Studies, którego Microsoft był inauguracyjnym sygnatariuszem i partnerem, ma na celu ożywienie umiejętności obywatelskich w społecznościach przedsiębiorstw. Jest to dobry przykład na to, jak szerokie są możliwości wzmocnienia naszej obrony w ramach demokracji.

Przeciwdziałanie

W ostatnich latach Digital Crimes Unit (DCU) Microsoft udoskonalił taktykę i opracował narzędzia do przeciwdziałania cyberzagrożeniom, od ransomware po botnety i ataki organizowane przez państwa. Wyciągnęliśmy wiele ważnych wniosków, począwszy od roli aktywnego przeciwdziałania szerokiej gamie cyberataków.

Przeciwdziałanie operacjom wpływu może odgrywać jeszcze ważniejszą rolę. Najbardziej skutecznym antidotum na masowe oszustwo jest transparentność. Dlatego Microsoft zwiększył swoje możliwości wykrywania operacji wpływu realizowanych przez państwa oraz przeciwdziałania im dzięki nabyciu Miburo Solutions, wiodącej firmy zajmującej się analizą i badaniem cyberzagrożeń, specjalizującej się w wykrywaniu operacji wpływu zagranicznego i reagowaniu na nie.

Nasze doświadczenie pokazuje, że rządy, firmy technologiczne i organizacje pozarządowe powinny ogłaszać autorów cyberataków ostrożnie i mając dużo dowodów. Zrozumienie skutków tego typu działań jest kluczowe i może zwiększyć skuteczność walki z operacjami wpływu. Przykładem może być praktyczne zastosowanie transparentności przez administrację Stanów Zjednoczonych przed inwazją Rosji na Ukrainę przez udostępnianie publicznie informacji, np. ujawnienie rosyjskich planów dotyczących konkretnych kampanii, w tym wykorzystania pewnego fałszywego, drastycznego filmu.

Jak pokazuje publikacja wydana latem ubiegłego roku przez CyberPeace Institute w Genewie na temat trwających cyberataków na Ukrainie i poza nią, jest teraz okazja, aby szerokie spektrum organizacji społeczeństwa obywatelskiego i z sektora prywatnego zwiększyło transparentność związaną z cyberoperacjami wpływu. Rzetelne raporty o nowo odkrytych i dobrze udokumentowanych operacjach mogą pomóc społeczeństwu lepiej oceniać to, co czyta, widzi i słyszy — zwłaszcza w Internecie. Microsoft będzie uzupełniać swoje raporty dotyczące cyberprzestrzeni, a także publikować nowe raporty, dane i aktualizacje związane z odkryciami dotyczącymi operacji wpływu, a w stosownych przypadkach ogłaszać autorów ataków. Będziemy publikować coroczny raport, opierając się na danych, analizując całą firmę pod kątem występowania operacji wpływu zagranicznego i podejmować kolejne kroki w celu zapewnienia stopniowej poprawy. Rozważymy również inne działania, opierając się na podobnej transparentności.

Rola reklamy cyfrowej jest szczególnie ważna — reklama może finansować operacje zagraniczne, a jednocześnie stwarza pozory legalności witryn propagandowych sponsorowanych przez państwa. Konieczne będą nowe działania w celu zakłócenia tych przepływów finansowych.

Odstraszanie

Wreszcie, nie możemy oczekiwać od państw zmiany zachowań, jeśli nie będzie odpowiedzialności za łamanie zasad międzynarodowych. Odpowiedzialność za egzekwowanie takiej odpowiedzialności spoczywa na rządach. Jednak coraz częściej to działania multilateralne odgrywają ważną rolę we wzmacnianiu i rozszerzaniu norm międzynarodowych. Ponad 30 platform internetowych, reklamodawców i wydawców — w tym Microsoft — podpisało się pod niedawno zaktualizowanym Kodeksem postępowania Komisji Europejskiej w zakresie dezinformacji, zgadzając się na wzmocnienie zobowiązań w zakresie walki z tym rosnącym wyzwaniem. Podobnie jak niedawne Wezwanie z Paryża, Wezwanie z Christchurch i Deklaracja w sprawie przyszłości Internetu, działania multilateralne, obejmujące wielu interesariuszy, mogą zjednoczyć rządy i społeczeństwa demokratycznych krajów. Rządy mogą następnie opierać się na tych normach i prawach, aby rozwijać odpowiedzialność, której potrzebują i na którą zasługują światowe demokracje.

Dzięki radykalnej transparentności demokratyczne rządy i społeczeństwa mogą skutecznie przeciwdziałać kampaniom wpływu, ujawniając sprawców ataków organizowanych przez państwa, informując opinię publiczną i budując zaufanie do instytucji.

Zwiększyliśmy możliwości techniczne w zakresie wykrywania i zakłócania operacji wpływu zagranicznego. Zobowiązaliśmy się do transparentnego o nich informowania oraz do publikowania raportów o cyberatakach.

Praktyczne wskazówki

1. Wdróż silne praktyki higieny cyfrowej w swojej organizacji.
2. Rozważ sposoby ograniczenia niezamierzonego umożliwiania kampanii wpływu przez Twoich pracowników lub Twoje praktyki biznesowe. Obejmuje to ograniczenie dostępu do znanych witryn propagandy zagranicznej.
3. Wspieraj umiejętność korzystania z informacji i obywatelskie kampanie obywatelskie jako kluczowy element pomocy społeczeństwu w obronie przed propagandą i wpływami zagranicznymi.
4. Nawiąż bezpośrednią współpracę z grupami związanymi z Twoją branżą, które pracują nad rozwiązaniem problemu operacji wpływu.

Przypisy końcowe

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. Obrona Ukrainy: pierwsze lekcje z cyberwojny (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. Rzecznik prasowy rosyjskiego MSZ, Maria Zacharowa: https://tass.com/politics/1401777; Ławrow: 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. „Russia's Kremenchuk Claims Versus the Evidence" — 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 oraz Kristjan Peterson, październik 2020 r.

Cyberodporność

Zrozumienie ryzyka i korzyści wynikających z modernizacji staje się kluczowe dla holistycznego podejścia do odporności.

Omówienie

cyberodporności

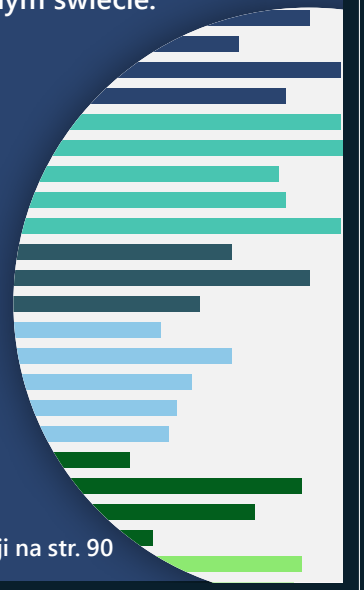
Cyberbezpieczeństwo jest kluczowym czynnikiem sukcesu technologicznego. Innowacyjność i wysoką produktywność można osiągnąć jedynie poprzez wprowadzenie zabezpieczeń, które zwiększą odporność organizacji na nowoczesne ataki.

Wskutek pandemii musieliśmy zmienić praktyki i technologie bezpieczeństwa Microsoft, aby chronić naszych pracowników niezależnie od tego, gdzie pracują. W minionym roku atakujący nadal wykorzystywali luki ujawnione w okresie pandemii i przechodzenia na pracę hybrydową. Od tego czasu naszą główną troską jest masowość i złożoność ataków oraz zwiększona aktywność atakujących państw.

Efektywna cyberodporność wymaga holistycznego, adaptacyjnego podejścia, aby stawić czoła zmieniającym się zagrożeniom dla podstawowych usług i składników infrastruktury.

Więcej informacji na str. 89

Zmodernizowanie systemów i architektur jest ważne, by radzić sobie z zagrożeniami w hiperpołączonym świecie.

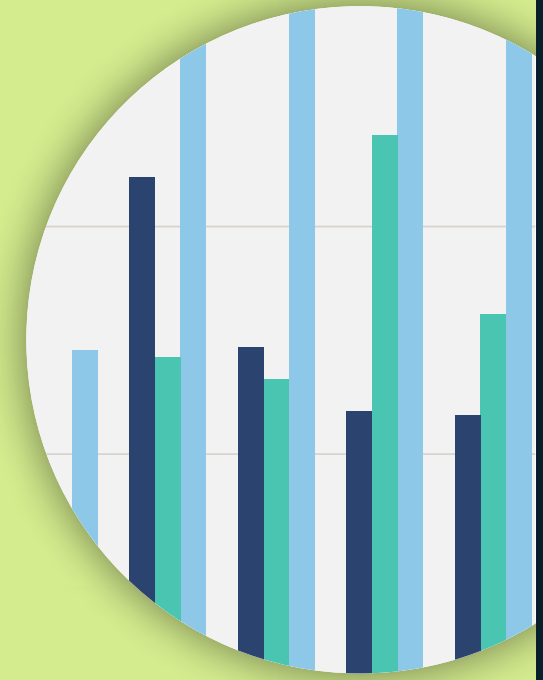


Więcej informacji na str. 90

Ogólny stan zabezpieczeń decyduje o skuteczności zaawansowanych rozwiązań.

Więcej informacji na str. 92

Chociaż ataki oparte na hasłach pozostają głównym źródłem naruszania tożsamości, pojawiają się też inne ich rodzaje.



Więcej informacji na str. 93

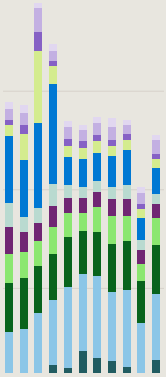
Ludzkim wymiarem odporności na operacje wpływu jest nasza zdolność do współpracy.

Więcej informacji na str. 102

Zdecydowanej większości udanych cyberataków można zapobiec, stosując podstawowe zasady bezpieczeństwa.

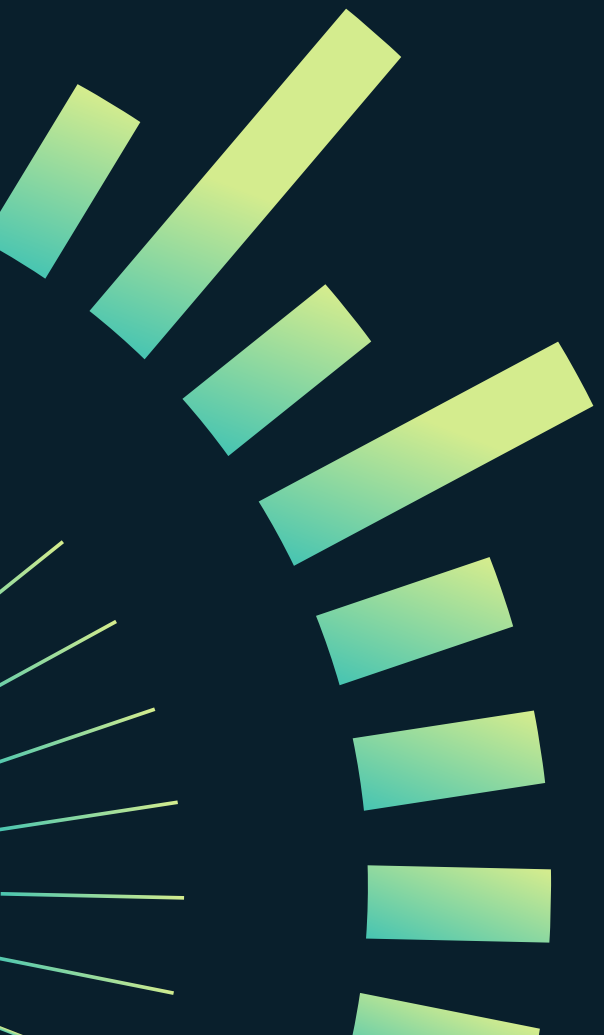
Więcej informacji na str. 108

W ciągu ostatniego roku świat doświadczył ataków DDoS o niespotykanej dotąd skali, złożoności i częstotliwości.



Więcej informacji na str. 98

Wprowadzenie



Wskutek pandemii musieliśmy zmienić praktyki i technologie bezpieczeństwa Microsoft, aby chronić naszych pracowników niezależnie od tego, gdzie pracują. W minionym roku atakujący nadal wykorzystywali luki ujawnione w okresie pandemii i przechodzenia na pracę hybrydową. Od tego czasu naszą główną troską jest masowość i złożoność ataków oraz zwiększona aktywność atakujących państw.

Aktywność w zakresie zagrożeń cyfrowych i poziom wyrafinowania cyberataków rośnie każdego dnia. Wiele współczesnych, złożonych ataków koncentruje się na naruszaniu architektur tożsamości, łańcuchów dostaw i podmiotów trzecich, z których część ma słabe zabezpieczenia. W szczególności znaczącym obecnie zagrożeniem są ataki wyłudzania informacji dotyczące tożsamości. Jednak tego typu ataki będą zazwyczaj nieskuteczne w przypadku zastosowania dobrych praktyk zarządzania tożsamością, kontroli wyłudzania informacji i zarządzania urządzeniami klienckimi. Dlatego należy pamiętać o podstawach: 98% ataków można powstrzymać, stosując podstawowe zasady bezpieczeństwa. W Microsoft zarządzamy tożsamościami i urządzeniami w ramach podejścia Zero Trust, które obejmuje przyznawanie dostępu z minimalnymi uprawnieniami i poświadczenia odporne na ataki wyłudzania informacji, aby skutecznie powstrzymać przestępców i zapewnić ochronę danych.

Obecnie nawet atakujący, którym brakuje zaawansowanych umiejętności technicznych, mogą przeprowadzać destrukcyjne ataki — dostęp do zaawansowanych taktyk, technik i procedur stał się szeroko dostępny w gospodarce cyberprzestępczej. Wojna na Ukrainie pokazała, że atakujące państwa eskalowały ofensywne cyberoperacje, m.in. zwiększono użycie ransomware. Ransomware to obecnie rozwinięty segment, w którym atakujący stosują podwójne lub potrójne wymuszenia w celu uzyskania zapłaty, a programiści ransomware oferują model RaaS (ransomware jako usługa). W modelu RaaS organizatorzy ataków do ich przeprowadzania wykorzystują sieć „wspólników" (affiliates). Obniża to barierę wejścia dla mniej wykwalifikowanych cyberprzestępców i w efekcie powiększa liczbę atakujących.

W obliczu tych okoliczności Microsoft zaprojektował program eliminacji ransomware. Jego celem jest usunięcie luk w mechanizmach kontroli i pokryciu, przyczynienie się do ulepszenia funkcji usług oraz opracowanie podręczników odzyskiwania po atakach ransomware dla naszego centrum operacji bezpieczeństwa i zespołów inżynierskich.

Niedawne ataki na łańcuch dostaw i dostawców zewnętrznych wskazują na główny punkt zwrotny w branży. Zakłócenia powodowane przez te ataki u naszych klientów i partnerów oraz w administracji publicznej i samym Microsoft wciąż rosną. Ważne jest więc skupienie uwagi na cyberodporności i współpraca w dziedzinie bezpieczeństwa między zainteresowanymi stronami. Przestępcy atakują również systemy lokalne. Zwiększa to potrzebę zarządzania w ramach organizacji lukami w zabezpieczeniach starszych systemów przez modernizację i przenoszenie infrastruktury do chmury, w której zabezpieczenia są bardziej niezawodne.

Żyjemy w czasach, w których bezpieczeństwo jest kluczowym czynnikiem warunkującym sukces technologiczny. Innowacyjność i wysoką produktywność można osiągnąć jedynie poprzez wprowadzenie zabezpieczeń, które zwiększą odporność organizacji na nowoczesne ataki. W miarę wzrostu i ewolucji zagrożeń cyfrowych kluczowe znaczenie ma wbudowanie cyberodporności w tkankę każdej organizacji.

Bret Arsenault
Dyrektor ds. bezpieczeństwa IT

Cyberodporność: kluczowy fundament połączonego społeczeństwa

Rewolucja w technologii cyfrowej sprawiła, że organizacje są coraz bardziej połączone zarówno w sposobie działania, jak i w oferowanych usługach. W obliczu wzrostu cyberzagrożeń wbudowanie cyberodporności w tkankę organizacji jest tak samo ważne, jak odporność finansowa i operacyjna.

Transformacja cyfrowa na zawsze zmieniła sposób, w jaki organizacje wchodzą w interakcje z klientami, partnerami, pracownikami i innymi interesariuszami. Nowe technologie dają ogromne możliwości angażowania ludzi, przekształcania produktów i optymalizowania operacji. Pandemia przyspieszyła transformację cyfrową, napędzając innowacyjne technologie, które pozwalają ludziom współpracować na nowe sposoby i z dowolnego miejsca.

Cyberzagrożenia stają się „endemiczne". Zapobieganie szkodom dla organizacji staje się coraz trudniejsze w „zawsze połączonym" świecie. Cyberodporność reprezentuje zdolność organizacji do kontynuowania operacji i utrzymania przyspieszenia wzrostu pomimo obciążenia atakami. Zapobieganie musi być zrównoważone ze zdolnością przetrwania i odzyskiwania. Rządy i przedsiębiorstwa opracowują kompleksowe modele, które wykraczają poza bezpieczeństwo i prywatność, aby chronić aktywa, dane i inne zasoby w ramach cyberodporności.

Opracowanie holistycznego podejścia do cyberodporności

Cyberodporność wymaga holistycznego, adaptacyjnego i globalnego podejścia, które stawi czoła zmieniającym się zagrożeniom dla podstawowych usług i składników infrastruktury, w tym:

- Podstawowej cyberhigieny opisanej naszą krzywą dzwonową cyberodporności.
- Zrozumienia kompromisu między ryzykiem a efektywnością w transformacji cyfrowej i zarządzania nim.
- Możliwości reagowania w czasie rzeczywistym, by proaktywnie wykrywać zagrożenia i luki w zabezpieczeniach.
- Ochrony przed znanymi atakami oraz działań zapobiegawczych przed nowymi i przewidywanymi wektorami ataków, w tym możliwości automatycznego przeciwdziałania im.
- Zmniejszonej konsekwencji ataków i katastrof dzięki izolacji i segmentacji błędów.
- Automatycznego odzyskiwania i zapewniania redundancji w przypadku zakłóceń.
- Nadania priorytetu testom operacyjnym w celu znajdowania luk oraz zrozumienia wspólnych obowiązków i zależności od zasobów zewnętrznych, takich jak rozwiązania bezpieczeństwa oparte na chmurze.

Skuteczny program cyberodporności zaczyna się od zasobów — np. zrozumienia dostępnych usług czy zapewnienia niezawodnych zasobów, z których można skorzystać w przypadku zakłóceń. Opierając się na tym fundamencie, program musi być w stanie ocenić własną skuteczność, zmierzyć wydajność usług krytycznych i ich zależności, przetestować i zweryfikować możliwości w ramach usług lokalnych i chmurowych oraz zapewnić ciągłe doskonalenie w całym cyfrowym cyklu życia organizacji.

Współpracujemy z organizacjami kompleksowo — identyfikujemy ich najbardziej krytyczne usługi lokalne i online, procesy biznesowe, zależności, personel, sprzedawców i dostawców. Poszukujemy również możliwości identyfikacji aktywów i zasobów związanych z oczekiwaniami klientów i rynku, zobowiązaniami regulacyjnymi i umownymi oraz operacjami wewnętrznymi. Po zidentyfikowaniu tych krytycznych zasobów równolegle należy wykrywać i monitorować zagrożenia, zakłócenia, potencjalne wektory ataku oraz podatności systemów i procesów. Zdolność do tego w warunkach obecnego niedoboru umiejętności wymaga rygorystycznego ustalania priorytetów w oparciu o ogólne ryzyko stwarzane dla organizacji.

Tego rodzaju holistyczne podejście musi być adaptacyjne na tle stale zmieniającego się krajobrazu zagrożeń, a jego celem jest wymierne zwiększenie wydajności, skrócenie czasu wykrywania, reagowania i odzyskiwania danych oraz zmniejszenie konsekwencji zakłóceń. Podejście to musi również uwzględniać rosnące powiązania zagrożeń. Na przykład incydent bezpieczeństwa może skutkować naruszeniem danych z implikacjami dotyczącymi prywatności, co wymaga współpracy wielu zespołów wewnętrznych i zewnętrznych w celu szybkiego reagowania i minimalizacji skutków.

Cyberodporność to zdolność przedsiębiorstwa do kontynuowania działalności i wzrostu pomimo zakłóceń, w tym cyberataków.

Praktyczne wskazówki

1. Zapewnij systemy technologiczne, które będą ograniczać wpływ naruszeń, umożliwiając im dalsze bezpieczne i efektywne działanie, nawet jeśli atak się powiedzie. Skup się na zasobach krytycznych, promuj zwinność, projektuj architekturę tak, by zapewnić adaptacyjność (na przykład środowiska hybrydowe, wielochmurowe i wieloplatformowe), ograniczaj obszar podatny na ataki (na przykład usuwaj nieużywane aplikacje i nadmiernie prawa dostępu), zakładaj, że naruszenie już wystąpiło, i przygotuj się na ewolucję atakujących.
2. Podczas planowania projektów cyfrowych należy rozważyć potencjalne zagrożenia wraz z możliwościami, a także wspólną odpowiedzialność za odporność w całym łańcuchu dostaw technologii cyfrowych, w tym rozwiązania bezpieczeństwa oparte na chmurze.
3. Tworząc systemy, myśl o bezpieczeństwie już w fazie projektowania. Podejmuj kroki w celu przewidywania i wykrywania przyszłych zagrożeń, a także opierania się im, dostosowywania się do nich i reagowania na nie.
4. Upewnij się, że liderzy biznesowi konsultują się z zespołami ds. bezpieczeństwa, aby zrozumieć ryzyko związane postępem atakujących. Podobnie, zespoły ds. bezpieczeństwa powinny uwzględniać cele biznesowe i doradzać liderom, jak bezpiecznie je realizować.
5. W odpowiedzi na cyberincydenty przygotuj klarowne praktyki operacyjne i procedury odporności organizacyjnej.

Znaczenie modernizacji systemów i architektury

Tworząc nowe możliwości hiperpołączonego świata, musimy usuwać zagrożenia stwarzane przez starsze systemy i oprogramowanie.

Starsze systemy (opracowane zanim nowoczesne narzędzia łączności, takie jak smartfony, tablety i usługi w chmurze stały się normą) stanowią zagrożenie dla organizacji, które nadal z nich korzystają. Microsoft Security Services for Incident Response, zespół specjalistów ds. bezpieczeństwa, który pomaga klientom reagować na ataki i likwidować ich skutki, odkrył nowe ryzyko w tym obszarze.

W ostatnim roku problemy wykryte wśród skutecznie zaatakowanych klientów były związane z sześcioma kategoriami (patrz diagram na tej stronie). Na następnej stronie przedstawiono kroki, które można podjąć w celu zwiększenia odporności.

Ponad 80% incydentów związanych z bezpieczeństwem przypisuje się kilku brakującym elementom, które można wprowadzić, wdrażając nowoczesne modele zabezpieczeń.

Kluczowe problemy wpływające na cyberodporność

Ten wykres pokazuje odsetek skutecznie zaatakowanych klientów, którym brakowało krytycznych, podstawowych mechanizmów bezpieczeństwa. Wyniki są oparte na ustaleniach Microsoft w ciągu ostatniego roku.

„Liderzy powinni myśleć o cyberodporności jako o kluczowym aspekcie odporności biznesowej. Powinni planować reakcje na cyberzakłócenia tak samo, jak w przypadku klęsk żywiołowych czy innych nieprzewidzianych zdarzeń. Należy wypracowywać strategie, łącząc wewnętrznych interesariuszy (działy operacji, komunikacji, prawne i inne). Pomoże to w szybkim przywróceniu krytycznych systemów biznesowych i wznowieniu normalnej działalności.

Ale na tym nie koniec. Ponieważ wiele organizacji polega na dostawcach i usługodawcach zewnętrznych, liderzy powinni rozszerzyć planowanie cyberodporności na swój kompleksowy łańcuch wartości, aby zapewnić ciągłość i odporność biznesową”.

Ann Johnson
Wiceprezes ds. bezpieczeństwa, zgodności z przepisami, tożsamości i zarządzania rozwojem biznesu

Znaczenie modernizacji systemów i architektury

(c.d.)

Istnieją konkretne obszary, którymi organizacje mogą się zająć, aby zmodernizować swoje podejście i chronić się przed zagrożeniami:

Problem	Kroki do wykonania
Niebezpieczna konfiguracja dostawcy tożsamości Błędna konfiguracja oraz ekspozycja w Internecie platform tożsamości i ich składników to powszechne wektory uzyskiwania nieautoryzowanego dostępu z wysokimi uprawnieniami.	Podczas wdrażania i konserwowania systemów tożsamości, takich jak infrastruktura AD czy Azure AD, przestrzegaj zasad konfiguracji zabezpieczeń i najlepszych rozwiązań. Implementuj ograniczenia dostępu, wymuszając segregację uprawnień, przyznając dostęp z minimalnymi uprawnieniami i wykorzystując stacje robocze z dostępem uprzywilejowanym (PAW) do zarządzania systemami tożsamości.
Niewystarczająca kontrola dostępu z wysokimi uprawnieniami i penetracji sieci Administratorzy mają nadmierne uprawnienia w całym środowisku cyfrowym, co często prowadzi do ryzyka ekspozycji w Internecie poświadczeń administratorów ze stacji roboczych i ograniczenia produktywności.	Zabezpiecz i ogranicz dostęp administracyjny, aby uczynić środowisko bardziej odpornym i ograniczyć zakres ataku. Zastosuj mechanizmy zarządzania dostępem z wysokimi uprawnieniami, takie jak dostęp just-in-time i just-enough-administration (minimalny poziom uprawnień administracyjnych).
Brak uwierzytelniania wieloskładnikowego (MFA) Współcześni atakujący nie włamują się. Oni po prostu się logują.	MFA to krytyczny, fundamentalny mechanizm dostępu użytkowników, który powinny wdrożyć wszystkie organizacje. MFA, w połączeniu z dostępem warunkowym, może być nieocenione w walce z cyberzagrożeniami.
Operacje bezpieczeństwa o niskiej dojrzałości Większość skutecznie zaatakowanych organizacji korzystała z tradycyjnych narzędzi do wykrywania zagrożeń i nie dysponowała odpowiednimi danymi umożliwiającymi szybkie reagowanie i przeciwdziałanie.	Kompleksowa strategia wykrywania zagrożeń wymaga inwestycji w systemy XDR (Rozszerzone możliwości wykrywania zagrożeń i reagowania na nie) oraz nowoczesne narzędzia natywne dla chmury wykorzystujące uczenie maszynowe do oddzielania szumu od sygnałów. Zmodernizuj narzędzia do operacji bezpieczeństwa przez wdrożenie XDR, dzięki któremu zapewnisz analizy bezpieczeństwa z całego środowiska cyfrowego.
Brak mechanizmów ochrony informacji Organizacje nadal borykają się z zapewnieniem kompleksowych mechanizmów ochrony informacji, które obejmowałaby wszystkie lokalizacje danych, pozostawałaby skuteczne przez cały cykl życia informacji oraz byłyby dostosowane do krytyczności danych biznesowych.	Zidentyfikuj krytyczne dane biznesowe i ich lokalizację. Przeanalizuj procesy cyklu życia informacji i egzekwuj ochronę danych przy jednoczesnym zapewnieniu ciągłości działania.
Ograniczone wdrożenie nowoczesnego modelu zabezpieczeń Tożsamość to nowa granica bezpieczeństwa umożliwiająca dostęp do zróżnicowanych usług cyfrowych i środowisk obliczeniowych. Zintegrowanie zasad Zero Trust, bezpieczeństwa aplikacji i innych nowoczesnych ram cybernetycznych umożliwia organizacjom proaktywne zarządzanie ryzykiem, które w innym przypadku mogłoby być trudne do przewidzenia.	Ramy Zero Trust wymuszają koncepcje przyznawania dostępu z minimalnymi uprawnieniami, wyraźnej weryfikacji wszystkich dostępów i zakładania zawsze, że naruszenie już wystąpiło. Organizacje powinny również wdrożyć mechanizmy kontroli i praktyki bezpieczeństwa w procesach DevOps i cyklu życia aplikacji, aby uzyskać wyższy poziom pewności w swoich systemach biznesowych.

Ogólny stan zabezpieczeń decyduje o skuteczności zaawansowanych rozwiązań

Dzięki naszej analizie odkryliśmy przewagę typowych luk w mechanizmach ochrony organizacji, które umożliwiają atakującym uzyskanie wstępnego dostępu, uchwycenie przyczółka i przeprowadzenie ataku — nawet w przypadku zaawansowanych rozwiązań bezpieczeństwa.

W wielu przypadkach wynik cyberataku jest przesądzony na długo przed jego rozpoczęciem. Atakujący wykorzystują podatne środowiska do uzyskania wstępnego dostępu, prowadzenia obserwacji i siania spustoszenia przez penetrację sieci, szyfrowanie lub eksfiltrację. Powstrzymanie atakującego na wczesnym etapie znacznie zwiększa szansę na ograniczenie ogólnych skutków.

Microsoft przeanalizował konkretne konfiguracje zabezpieczeń, aby zidentyfikować najczęstsze niedociągnięcia w tych środowiskach — w praktyce. Umożliwiło nam to zaobserwowanie najczęstszych luk w zabezpieczeniach wykorzystywanych podczas ataków ransomware obsługiwanych przez człowieka, które pozwalały atakującym na uzyskanie dostępu i penetrację sieci w niezauważony sposób.

Podstawowe konfiguracje zabezpieczeń muszą być włączone

Urządzenia organizacji, które nie są włączone do systemu lub są przestarzałe (zarówno w odniesieniu do luk w zabezpieczeniach, jak i stanu agentów zabezpieczeń), służą jako potencjalne punkty wejścia i drogi dostępu dla atakujących. Stwierdziliśmy, że wprawdzie wyposażenie urządzeń organizacji w najnowsze rozwiązanie EDR[1] (Wykrywanie zagrożeń dla urządzeń klienckich i reagowanie na nie) i EPP[2] (Platforma ochrony urządzeń klienckich) jest ważnym krokiem, to nie gwarantuje powstrzymania ransomware.

Zaawansowane rozwiązania, takie jak EDR i EPP, mają kluczowe znaczenie w wykrywaniu ataków na wczesnych etapach oraz umożliwiają automatyczne przeciwdziałanie i chronienie. Jednak ponieważ te zaawansowane rozwiązania opierają się na podstawowej zdolności wykrywania ataku, wymagają włączenia podstawowych konfiguracji zabezpieczeń. W praktyce zaobserwowaliśmy przypadki używania zaawansowanych rozwiązań, które zostały upośledzone przez brak podstawowej konfiguracji zabezpieczeń.

Właściwa konfiguracja zabezpieczeń jest lepszym predyktorem odporności niż czas reakcji analityków z centrum operacji bezpieczeństwa (SOC)

W okresie 6 miesięcy u naszych klientów i partnerów zaobserwowaliśmy 70% skrócenie czasu potrzebnego analitykowi SOC na przejrzenie alertu i podjęcie działań w związku z nim. Ta zwiększona świadomość to dobry znak. Jednak chociaż widoczność konfiguracji zabezpieczeń poprawia wydajność analityków SOC, umożliwienie wglądu w urządzenia organizacji dzięki ich wdrożeniu i modernizacji jest lepszym predyktorem skutecznego zapobiegania.

Ryzyko stwarzane przez nieznane urządzenia

W przeciwieństwie do sieci w chmurze, w przypadku których klienci wiedzą, które zasoby działają na których systemach operacyjnych, sieci lokalne mogą zawierać szeroką gamę urządzeń, takich jak IoT, komputery desktop, serwery i urządzenia sieciowe, które nie są monitorowane ani zarządzane przez organizację.

W przeciętnej sieci przedsiębiorstwa jest ponad 3500 podłączonych urządzeń, które nie są chronione przez agenta EDR, a mogą mieć dostęp do zasobów przedsiębiorstwa lub nawet do zasobów o dużej wartości. Ochrona punktu końcowego w usłudze Microsoft Defender (MDE) używa inspekcji sieci do wykrywania urządzeń podłączonych do sieci i dostarczania o nich informacji takich jak nazwa i typ czy dystrybucja systemu operacyjnego.

3500

— średnia liczba połączonych urządzeń w przedsiębiorstwie, które nie są chronione przez agenta wykrywania zagrożeń dla urządzeń klienckich i reagowania na nie.

W przypadku urządzeń nieobsługiwanych przez agenta EDR należy przynajmniej pamiętać o ich istnieniu i podjąć działania w celu ich ochrony przez ocenę podatności, a także ograniczenie ich dostępu do sieci.

Praktyczne wskazówki

1. Brak podstawowych konfiguracji zabezpieczeń może zagrozić nawet zaawansowanym rozwiązaniom.
2. Zainwestuj w najlepsze praktyki dotyczące konfiguracji zabezpieczeń, aby chronić się przed przyszłymi atakami. Te podstawowe ustawienia dają ogromne korzyści w zakresie zdolności organizacji do obrony przed atakami.
3. Zaimplementuj wszystkie odpowiednie urządzenia w rozwiązaniu EDR.
4. Należy zaktualizować agentów zabezpieczeń i zapewnić ochronę przed ingerencją osób niepowołanych, aby zagwarantować lepszą widoczność i pełniejszą ochronę produktów.

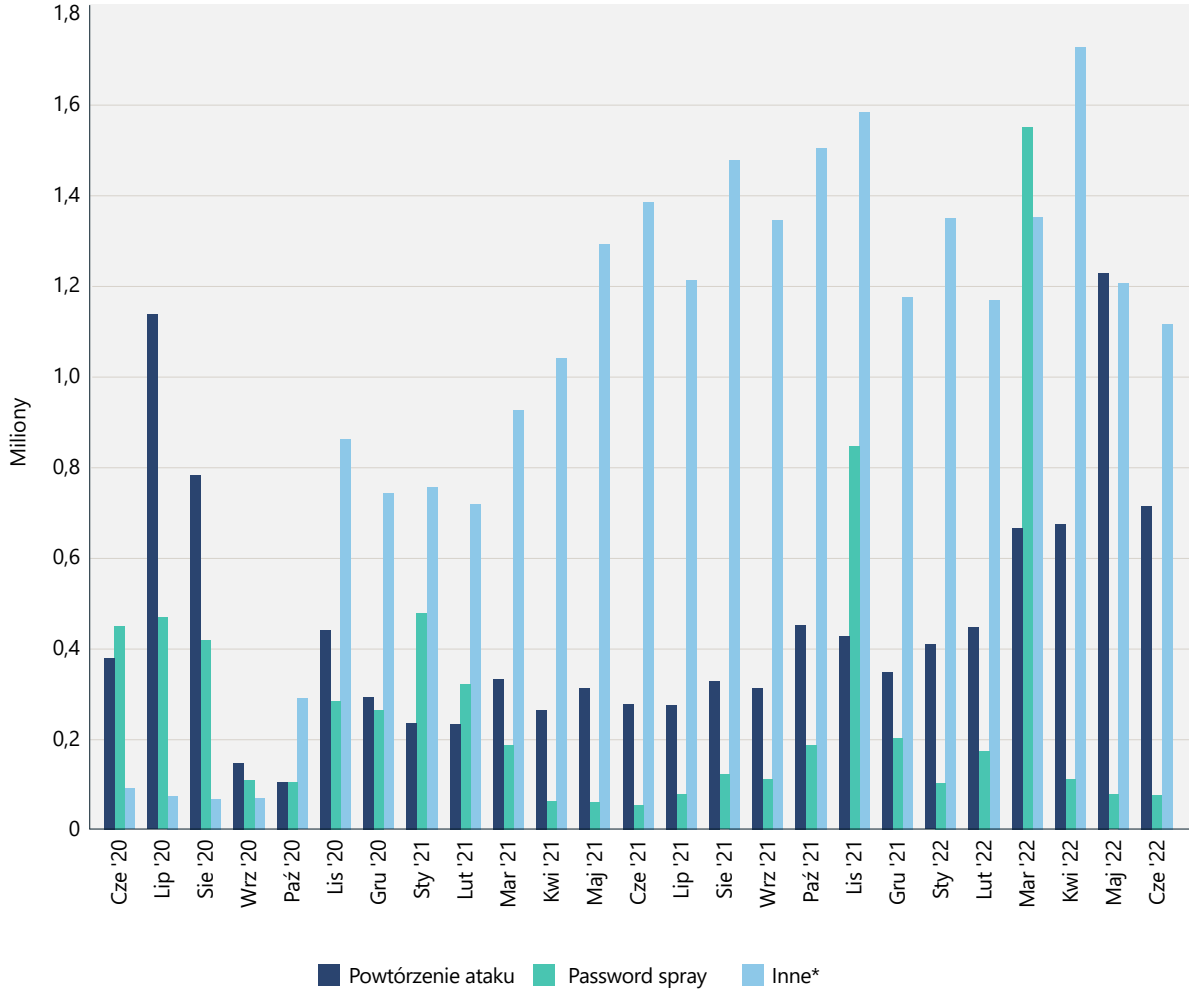
Ochrona tożsamości podstawą dobrego funkcjonowania organizacji

Ochrona tożsamości jeszcze nigdy nie była tak ważna. Chociaż ataki oparte na hasłach pozostają głównym źródłem naruszania tożsamości, pojawiają się też inne ich rodzaje. Liczba wyrafinowanych ataków wciąż rośnie w stosunku do poprzedniej „normy", jaką były ataki rozproszone na hasła (password spray) i metodą powtórzenia ataku.

Ataki oparte na hasłach są nadal powszechne. Ponad 90% kont zaatakowanych przy użyciu tych metod nie jest chronionych za pomocą silnego uwierzytelniania. Silne uwierzytelnianie wykorzystuje więcej niż jeden składnik uwierzytelniania, na przykład hasło + SMS czy klucze zabezpieczeń FIDO2.

Zauważyliśmy wzrost ukierunkowanych ataków password spray, z bardzo dużymi skokami natężenia rozproszonymi na tysiące adresów IP.

Użytkownicy skutecznie zaatakowani według kategorii ataku



Użytkownicy skutecznie zaatakowani miesięcznie według kategorii ataku. Wolumeny ataków password spray były bardzo niestabilne, co widać w skokach z listopada 2021 r. i marca 2022 r. Skoki te reprezentują tysiące użytkowników i tysiące dotkniętych adresów IP.

* „Inne" oznacza ataki inne niż password spray i metodą powtórzenia ataku, w tym wyłudzanie informacji, złośliwe oprogramowanie, man-in-the-middle, naruszenie lokalnego wydawcy tokenów i inne. Źródło: Azure AD Identity Protection.

4500

W czasie potrzebnym do odczytania tego oświadczenia broniliśmy się przed 4500 atakami opartymi na hasłach.

Ochrona tożsamości podstawą dobrego funkcjonowania organizacji

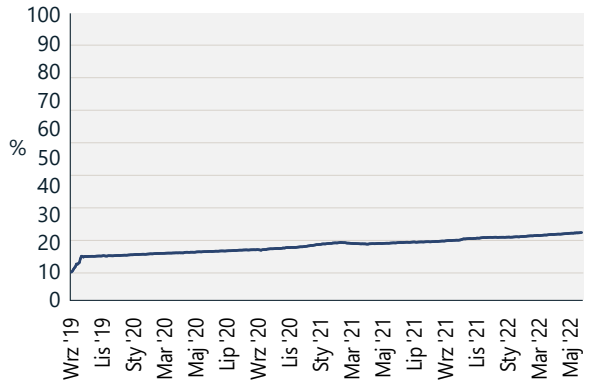
(c.d.)

Wdrażanie silnego uwierzytelnienia

Pozytywne jest to, że obserwujemy stały wzrost adopcji silnego uwierzytelniania wśród bazy klientów korporacyjnych Azure Active Directory (Azure AD). W przypadku Azure AD miesięczna liczba aktywnych użytkowników (MAU) korzystających z silnego uwierzytelniania wzrosła w ostatnim roku z 19% do 26%, natomiast dla kont administracyjnych z 30% do około 33%.

Tendencja ta jest pozytywna, ale nadal potrzebny jest znaczny wzrost, aby osiągnąć większościowy zasięg silnego uwierzytelniania. Klienci, którzy nie używają silnego uwierzytelniania w swoich środowiskach, powinni rozpocząć planowanie i wdrażanie tego środka w celu ochrony swoich użytkowników[3]. Podczas planowania wdrażania silnego uwierzytelniania należy rozważyć uwierzytelnianie bezhasłowe, ponieważ oferuje ono najbezpieczniejsze środowisko użytkownika, eliminując ryzyko ataków opartych na hasłach.

Użycie silnego uwierzytelniania
(wrzesień 2019 r. – maj 2022 r.)

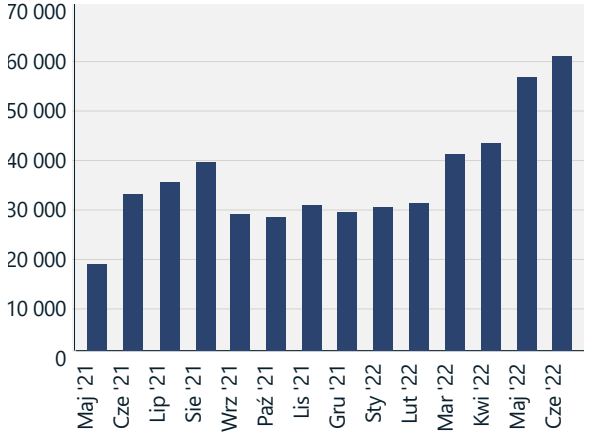


Chociaż poziom silnego uwierzytelniania podwoił się od 2019 r., tylko 26% użytkowników i 33% administratorów używa silnego uwierzytelniania. Źródło: Azure Active Directory.

Stały wzrost liczby ataków powtórnego wykorzystywania tokenów

Odsetek innych form ataków w 2022 r. zwiększył się. Zauważyliśmy wzrost liczby ataków ukierunkowanych, które unikają uwierzytelniania za pomocą haseł, aby zmniejszyć ryzyko wykrycia. Ataki te wykorzystują pliki cookie jednokrotnego logowania (SSO/single sign-on) w przeglądarce lub tokeny odświeżania uzyskane za pomocą złośliwego oprogramowania, wyłudzania informacji i innych metod. W niektórych przypadkach atakujący wybierają infrastrukturę w lokalizacjach zbliżonych do położenia geograficznego docelowego użytkownika, aby jeszcze zmniejszyć szanse na wykrycie. Zauważyliśmy stały wzrost liczby ataków powtórnego wykorzystywania tokenów — w Azure AD Identity Protection dochodzi do ponad 40 000 wykryć miesięcznie. Powtórne wykorzystywanie tokenów (token replay) to użycie tokenu, który został wydany prawowitemu użytkownikowi, przez atakującego, który wszedł w jego posiadanie. Tokeny są powszechnie pozyskiwane za pomocą złośliwego oprogramowania, na przykład przez eksfiltrację plików cookie z przeglądarki użytkownika lub zaawansowane metody wyłudzania informacji.

Liczba wykrytych ataków powtórnego wykorzystywania tokenów



Miesięczna liczba wykrytych ataków powtórnego wykorzystywania tokenów. Źródło: Azure AD Identity Protection, unikalne sesje, w których wykryto anomalne tokeny.

Ochrona tożsamości podstawą dobrego funkcjonowania organizacji

(c.d.)

Pozyskiwanie tokenów

Atakujący, aby osiągnąć swoje cele, bardziej niż złośliwego oprogramowania potrzebują poświadczeń. W rzeczywistości 100% wszystkich ataków ransomware obsługiwanych przez człowieka wykorzystuje wykradzione poświadczenia. Wiele wyrafinowanych włamań wykorzystuje poświadczenia kupione w dark web, które były pierwotnie wykradzione z użyciem niewyszukanego i szeroko rozpowszechnionego złośliwego oprogramowania do kradzieży poświadczeń. Ta klasa złośliwego oprogramowania ewoluowała w kierunku kradzieży tokenów, w tym informacji o sesji i żądań MFA. Oznacza to, że infekcje na systemach domowych, na których użytkownicy logują się do zasobów firmowych, mogą prowadzić do poważnych incydentów w sieciach korporacyjnych.

Atakujący mogą również pozyskiwać tokeny z urządzeń ofiar w atakach man-in-the-middle, w których ofiara klika złośliwe łącze w e-mailu lub wiadomości błyskawicznej (będących częścią kampanii wyłudzania informacji) i zostaje przekierowana na stronę internetową, która wygląda jak normalna strona logowania. W rzeczywistości jest to usługa sieciowa prowadzona przez atakujących, która przechwytuje i przekazuje cały ruch między użytkownikiem a dostawcą tożsamości. Atakujący jest w stanie przechwycić nazwę użytkownika i hasło, a także przekazywać żądania MFA. Wynikowe tokeny wystawione przez dostawcę tożsamości i przechwycone przez atakującego mogą zawierać żądania MFA, których atakujący może użyć do pomyślnego przejścia testu MFA.

Microsoft Defender for Cloud Apps wykrył średnio 895 takich ataków miesięcznie od początku 2022 r. Tej formie ataków można zapobiec, stosując odporne na wyłudzanie informacji składniki MFA, takie jak uwierzytelnianie oparte na certyfikatach, Windows Hello dla firm czy klucze zabezpieczające FIDO2.

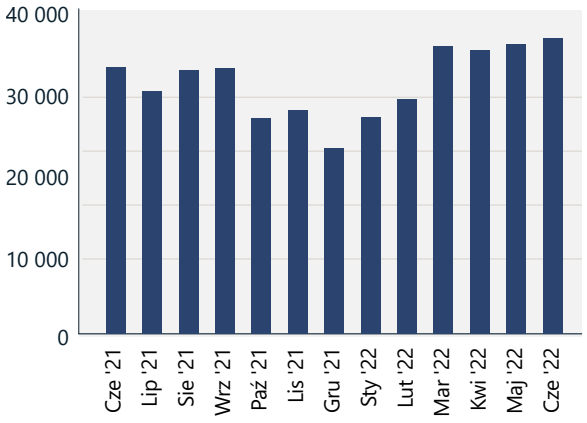
Ataki oparte na hasłach są podstawową metodą przejmowania kont.

Zmęczenie MFA

Wykorzystując koncepcję „zmęczenia MFA", atakujący generują wiele żądań MFA do urządzenia ofiary, mając nadzieję, że ofiara w końcu zaakceptuje żądanie nieumyślnie lub w wyniku zmęczenia. Temu atakowi można zapobiec, korzystając z nowoczesnych aplikacji uwierzytelniających, takich jak Microsoft Authenticator, w połączeniu z funkcjami takimi jak dopasowanie liczb[4] czy włączenie dodatkowego kontekstu[5]. Azure AD Identity Protection wykrywa miesięcznie 30 000 ataków opierających się na zmęczeniu MFA.

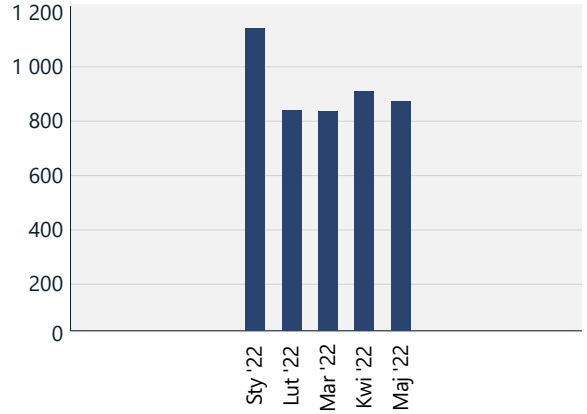
Udział wyrafinowanych ataków stale rośnie, co podkreśla potrzebę stosowania uwierzytelniania wieloskładnikowego obejmującego składniki, które są odporne na wyłudzanie informacji.

Szacowane przypadki ataków opierających się na zmęczeniu MFA



Źródło: Azure AD Identity Protection.

Wykryte przypadki wyłudzania informacji, po których następowały ataki man-in-the-middle



Źródło: Microsoft Defender for Cloud Apps.

Praktyczne wskazówki

1. Upewnij się, że wszystkie konta w Twojej organizacji są chronione za pomocą silnych środków uwierzytelniania.
2. Uwierzytelnianie bezhasłowe zapewnia najbardziej bezpieczne i przyjazne dla użytkownika środowisko, eliminując ryzyko ataków opartych na hasłach.
3. Wyłącz starsze typy uwierzytelniania w całej organizacji.
4. Chroń konta o wysokiej wartości i administracyjne za pomocą odpornych na wyłudzanie informacji form silnego uwierzytelniania.
5. Przeprowadź modernizację z lokalnego dostawcy tożsamości do dostawcy tożsamości w chmurze i połącz wszystkie swoje aplikacje z dostawcą tożsamości w chmurze, aby zapewnić spójne środowisko użytkownika i bezpieczeństwo.

Linki do dalszych informacji

› Podczas Światowego Dnia Haseł rozważmy całkowite ich porzucenie | Microsoft Security

Domyślne ustawienia zabezpieczeń systemu operacyjnego

Wraz ze stale ewoluującym krajobrazem zagrożeń widzimy dążenie, aby zabezpieczenia były od razu skonfigurowane pod kątem zapewniania cyberodporności. Bezpieczeństwo systemów operacyjnych jest sprawą bardziej pilną, złożoną i krytyczną dla biznesu niż kiedykolwiek wcześniej. Jednak jego właściwa realizacja może być trudna.

W przeszłości zabezpieczenia komputerów i urządzeń obejmowały wbudowane funkcje zabezpieczeń, które klient lub informatyk konfigurował według własnego uznania. Takie podejście nie jest już wystarczające, ponieważ atakujący wykorzystują bardziej zaawansowane narzędzia w zakresie automatyzacji, infrastruktury chmury i technologii zdalnego dostępu. Kluczowe stało się, aby wszystkie warstwy zabezpieczeń, od układu scalonego po chmurę, były skonfigurowane fabrycznie. Microsoft dostosował się: zabezpieczenia Windows są skonfigurowane domyślnie[6].

Klienci, którzy stosują dogłębną ochronę, obejmującą wielowarstwowe zabezpieczenia, nowe funkcje zabezpieczeń, regularne i konsekwentne stosowanie poprawek i aktualizacji, a także szkolenia w zakresie bezpieczeństwa i świadomość zgłaszania wyłudzania informacji i innych oszustw — mogą spodziewać się mniejszych problemów ze złośliwym oprogramowaniem.

Aby uprościć dogłębną ochronę, Windows 11 ma domyślnie włączone, ściśle zintegrowane zabezpieczenia sprzętowe i programowe, w tym funkcję integralności pamięci, Secure Boot i Trusted Platform Module 2.0. Użytkownicy Windows 10 na odpowiednim sprzęcie mogą również te funkcje włączyć w aplikacji Ustawienia Windows lub w menu BIOS.

Starsze urządzenia często w ogóle nie mają tak silnej integracji zabezpieczeń sprzętu i oprogramowania. W przypadku urządzeń, w których zabezpieczenia nie są domyślnie włączone, w miarę możliwości skonfiguruj je ręcznie[7].

W przypadku urządzeń, w których zabezpieczenia nie są domyślnie włączone, Microsoft zaleca (w miarę możliwości) skonfigurowanie ich ręcznie.

Należy aktywnie, stale stosować aktualizacje systemu operacyjnego i poprawki zabezpieczeń, aby zapewnić ochronę w całym cyklu życia sprzętu i oprogramowania.

Praktyczne wskazówki

1. Użyj rozwiązania bezhasłowego, które wiąże poświadczenia logowania w Trusted Platform Module — w szczególności poszukaj rozwiązania bezhasłowego, które spełnia standard FIDO (Faster Identity Online)[8].
2. Regularnie usuwaj wszystkie nieużywane i nieaktualne pliki wykonywalne na urządzeniach organizacji.
3. Chroń przed zaawansowanymi atakami na oprogramowanie układowe, włączając funkcje integralności pamięci, Secure Boot i Trusted Platform Module 2.0 (jeśli nie są włączone domyślnie). Zwiększy to ochronę rozruchu dzięki funkcjom wbudowanym w nowoczesne procesory.
4. Włącz szyfrowanie danych i ochronę poświadczeń.
5. Włącz mechanizmy kontroli aplikacji i przeglądarki, aby zapewnić lepszą ochronę przed niezaufanymi aplikacjami oraz inne wbudowane zabezpieczenia przed exploitami.
6. Włącz ochronę dostępu do pamięci, aby chronić się przed atakami fizycznymi takimi jak podłączenie przez kogoś złośliwego urządzenia do zewnętrznie dostępnych portów.

Linki do dalszych informacji

- Książka o zabezpieczeniach Windows
- Nowe funkcje zabezpieczeń w Windows 11 pomogą chronić pracowników hybrydowych | Blog Microsoft Security

Łańcuch dostaw oprogramowania jest w centrum

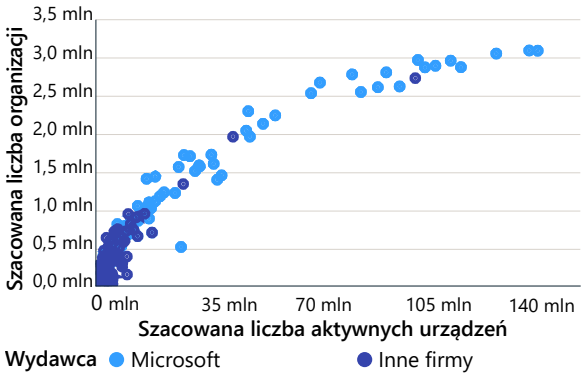
Ataki na aplikacje, wtyczki i rozszerzenia innych firm mogą podważyć zaufanie klientów do dostawców, którzy odgrywają centralną rolę w ekosystemie dostaw. Wykorzystanie teorii sieci do przyjrzenia się centralności oprogramowania pomaga wyjaśnić krytyczność stosowania poprawek, zwłaszcza w przypadku aplikacji centralnych.

Windows App Network obejmuje 18 milionów plików wykonywalnych aplikacji zainstalowanych i używanych w pięciu milionach organizacji. Zapewnia więc dobrą reprezentację naszego ekosystemu oprogramowania. 97% ze 100 000 najczęściej używanych aplikacji jest produkowanych przez inne organizacje. To one zajmują się aktualizacjami i poprawkami bezpieczeństwa. Ten fakt ilustruje dwie ważne cechy naszego ekosystemu aplikacji komercyjnych.

Po pierwsze, w ekosystemie aplikacji komercyjnych Windows występuje centralizacja. Tylko 100 000 najpopularniejszych aplikacji (z 18 milionów) jest używanych na 1000 lub większej liczbie urządzeń. Innymi słowy, jedynie nieco ponad 0,5% tych aplikacji jest szeroko używanych w ekosystemie urządzeń.

Po drugie, zarządzanie tymi aplikacjami jest zróżnicowane: aktualizacjami i poprawkami zabezpieczeń tych najczęściej używanych aplikacji komercyjnych zarządza 10 000 największych dostawców aplikacji. To pokazuje, jak firmy są uzależnione od różnorodnego zestawu mechanizmów zabezpieczeń, zgodności z przepisami i zarządzania dostawców oprogramowania.

Zasięg rynkowy najczęściej używanych aplikacji



Najpopularniejsze aplikacje są używane przez miliony organizacji na dziesiątkach milionów urządzeń. Ponieważ są one niemal wszechobecne, atakujący nieustannie poszukują w tych najpopularniejszych aplikacjach możliwości wykorzystania luk — w przypadku powodzenia skutki mogą obejmować miliony urządzeń.

Na milionach urządzeń nadal są używane podatne na ataki wersje aplikacji — wiele miesięcy po wydaniu poprawki, a nawet lata po zakończeniu wsparcia technicznego produktu. Przykładowo na ponad milionie aktywnych urządzeń z Windows działa wersja czytnika PDF, która nie jest wspierana od 2017 roku.

Stare wersje aplikacji, które nie są wspierane, nadal są aktywnie używane na milionach urządzeń. W rezultacie organizacje są narażone na występowanie luk, które nie zostaną już usunięte poprawkami.

W przypadku aplikacji w wersjach wciąż objętych wsparciem technicznym obserwujemy stagnację szybkości stosowania poprawek krytycznych — nie sprzyja to bezpieczeństwu. Aby osiągnąć wymaganą odporność, krzywa stosowania poprawek powinna, z miesiąca na miesiąc, iść wykładniczo w górę.

Szybkość wdrażania krytycznych poprawek

Po zbadaniu krytycznej luki, która dotyczyła 134 wersji różnych przeglądarek, odkryliśmy, że dziewięć miesięcy po wydaniu poprawki 78% urządzeń (czyli miliony) nadal korzystało z jednej z podatnych wersji.

Wykorzystaliśmy zestaw narzędzi InterpretML[9] do zidentyfikowania cech skorelowanych z organizacjami, w których istnieje większe ryzyko występowania urządzeń ze starszymi wersjami aplikacji. Najważniejsze z tych predyktorów obejmowały: rzadkie używanie urządzeń, obszary geograficzne, takie jak Azja i Pacyfik oraz Ameryka Łacińska, a także branże takie jak motoryzacja, chemia, telekomunikacja, transport i logistyka, płatnicy świadczeń zdrowotnych (obsługa roszczeń) i ubezpieczenia.

Należy regularnie wyłączać lub odinstalowywać nieużywane aplikacje.

Bezpieczeństwo organizacji i jej zgodność z przepisami zależy od jej własnych wysiłków oraz od wysiłków jej dostawców oprogramowania.

Praktyczne wskazówki

1. Regularnie aktualizuj wszystkie aplikacje i urządzenia klienckie w swojej organizacji.
2. Regularnie usuwaj wszystkie nieużywane i nieaktualne pliki wykonywalne na urządzeniach organizacji.

Linki do dalszych informacji

- Dokumentacja Microsoft Intune | Microsoft Docs
- Zarządzanie aplikacjami | Microsoft Docs
- Ochrona punktu końcowego w usłudze Microsoft Defender | Microsoft Security
- Ramy bezpiecznego łańcucha dostaw OSS | Microsoft Security Engineering
- „Microsoft Open Source Software Secure Supply Chain Framework” | GitHub

Zapewnianie odporności na ataki DDoS oraz wymierzone w sieci i w aplikacje internetowe

Przyspieszona transformacja cyfrowa położyła kres tradycyjnemu modelowi sieci i granic bezpieczeństwa. Przejście do chmury oznacza, że w celu ochrony zasobów cyfrowych przedsiębiorstwa muszą przyjąć zabezpieczenia sieciowe natywne dla chmury.

Złożoność, częstość i liczba ataków stale rośnie. Nie są już one ograniczone do okresów świątecznych — trwają cały rok. To pokazuje, jak ważna jest ciągła ochrona wykraczająca poza tradycyjne szczyty ruchu.

Ataki DDoS

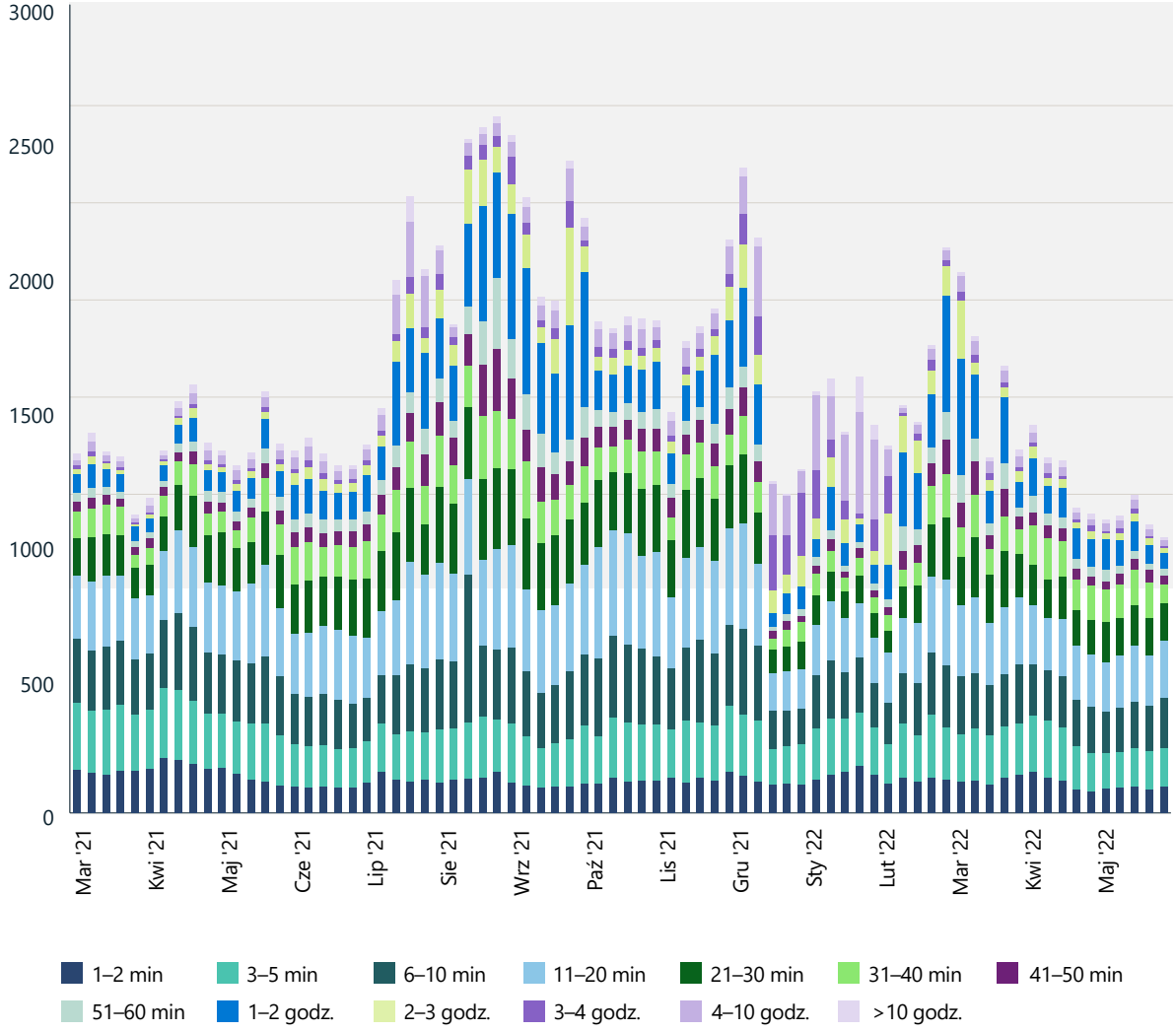
W ciągu ostatniego roku świat doświadczył ataków DDoS o niespotykanej dotąd skali, złożoności i częstotliwości. Eksplozja DDoS (Distributed Denial Of Service, Rozproszona odmowa usługi) była spowodowana znacznym wzrostem liczby ataków organizowanych przez państwa i ciągłą proliferacją tanich, dostępnych na rynku przestępczym usług DDoS. Microsoft zwalczał średnio 1955 ataków dziennie, co stanowi wzrost o 40% w porównaniu z rokiem poprzednim. Wcześniej szczytowa liczba ataków miała miejsce zwykle w okresie świątecznym pod koniec roku. W tym roku jednak najwięcej odnotowano w ciągu jednego dnia — 10 sierpnia 2021 r. Wskazuje to na zmianę w kierunku całorocznych ataków i podkreśla znaczenie bieżącej ochrony, poza tradycyjnymi okresami największego ruchu.

W listopadzie 2021 r. Microsoft udaremnił duży atak DDoS z przepływnością 3,4 terabita na sekundę (Tbps) pochodzący z około 10 000 źródeł w wielu krajach. Podobne ataki powyżej 2 Tb/s zostały odparte w 2022 r. Podkreśla to, że rośnie nie tylko złożoność i częstotliwość ataków, ale także ich intensywność (przepustowość).

Czas trwania ataku

Większość ataków zaobserwowanych w ciągu ostatniego roku miała charakter krótkotrwały. Około 28% ataków trwało krócej niż 10 minut, 26% — 10–30 minut, a 14% — 31–60 minut. 32% ataków trwało ponad godzinę.

Liczba ataków DDoS i rozkład ich czasu trwania
(od marca 2021 r. do maja 2022 r.)



Większość ataków w ubiegłym roku miała charakter krótkotrwały. Około 28% ataków trwało krócej niż 10 minut.

Zapewnianie odporności na ataki DDoS oraz wymierzone w sieci i w aplikacje internetowe

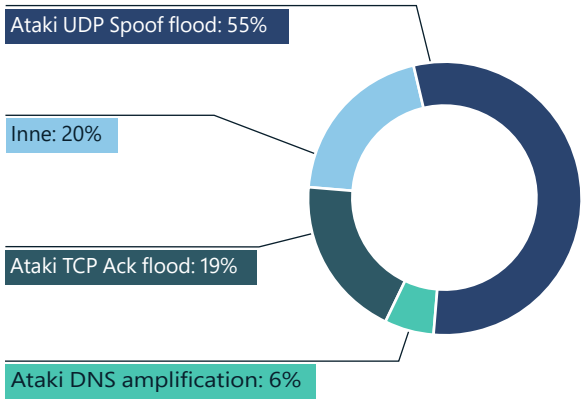
c.d.)

Wektory ataku DDoS

W minionym roku powszechnie stosowanymi wektorami ataków były ataki typu UDP (User Datagram Protocol) reflection na porcie 80 z wykorzystaniem SSDP (Simple Service Discovery Protocol), CLDAP (Connectionless Lightweight Directory Access Protocol), DNS (Domain Name System) i NTP (Network Time Protocol) (pojedynczy szczyt). Zauważyliśmy również wzrost liczby ataków DDoS w warstwie aplikacji na witryny internetowe — szczytem było 16,3 miliona żądań na sekundę i ruch 9,89 Tbps.

W 2022 r. Microsoft przeciwdziałał prawie 2000 atakom DDoS dziennie i udaremnił największy w historii atak DDoS.

Wektory ataku DDoS



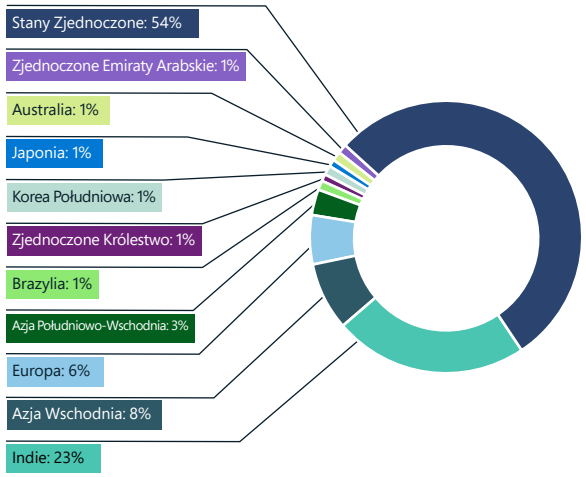
Ataki UDP Spoof flood stały się głównym wektorem w pierwszej połowie 2022 r., rosnąc z 16% do 55%. Ataki TCP Ack flood spadły z 54% do 19%.

Branża gier komputerowych nadal jest głównym celem ataków DDoS, głównie z powodu mutacji botnetu Mirai i ataków o niskiej intensywności z użyciem protokołu UDP. Ponieważ UDP jest powszechnie używany w grach i aplikacjach do strumieniowego przesyłania, przytłaczającą większość wektorów ataku stanowiły ataki typu UDP spoof flood, natomiast niewielką część stanowiły ataki typu UDP reflection i amplification.

Regiony geograficzne ataków

Spośród ataków DDoS wykrytych w ciągu ostatniego roku 54% przeprowadzono przeciwko celom w Stanach Zjednoczonych — trend ten można częściowo wyjaśnić tym, że większość klientów Azure i Microsoft znajduje się w Stanach Zjednoczonych. Zauważyliśmy również gwałtowny wzrost liczby ataków na Indie — z zaledwie 2% wszystkich ataków w drugiej połowie 2021 r. do 23% w pierwszej połowie 2022 r. Azja Wschodnia, w szczególności Hongkong, pozostaje popularnym celem (8%). W Europie obserwowaliśmy koncentrację ataków na regiony Amsterdamu, Wiednia, Paryża i Frankfurtu.

Cele ataków DDoS

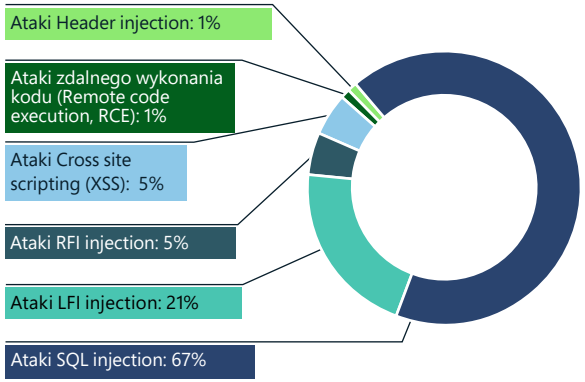


Intensywność ataków w Azji przypisujemy ogromnej liczbie graczy w tym regionie, zwłaszcza w Chinach, Japonii, Korei Południowej i Indiach. Ich liczba będzie wciąż rosła, ponieważ rosnąca popularność smartfonów napędza popularność gier mobilnych. Dlatego udział tego regionu geograficznego jako celu będzie się nadal zwiększał.

Exploity aplikacji internetowych

Zapora aplikacji internetowej (WAF) w połączeniu z ochroną przed atakami DDoS stanowi integralną część strategii dogłębnej ochrony zasobów internetowych i interfejsów API. Microsoft zaobserwował ponad 300 miliardów reguł WAF uruchamianych miesięcznie przez Azure WAF.

Rozkład najbardziej rozpowszechnionych typów ataków



Azure WAF wykrywa dziennie miliardy ataków z listy „Top 10"[10] projektu OWASP (Open Web Application Security Project). Z naszych sygnałów wynika, że atakujący najczęściej próbowali ataków typu SQL injection, a także ataków typu local file injection oraz remote file injection. Jest to zgodne z listą „Top 10" OWASP, w której ataki z wykorzystaniem wstrzykiwania kodu (injection) stanowią trzeci pod względem popularności typ ataków internetowych.

Odnotowano również wzrost ataków botów na aplikacje internetowe Azure — średnio 1,7 mld żądań botów miesięcznie, a 4,6% tego ruchu stanowią boty atakujących.

Zapewnianie odporności na ataki DDoS oraz wymierzone w sieci i w aplikacje internetowe

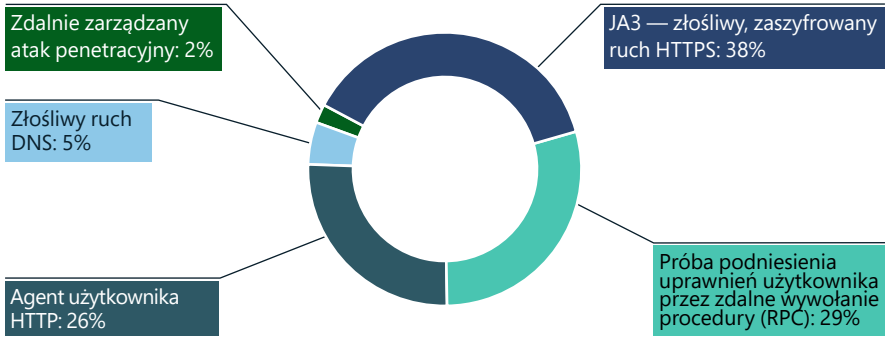
(c.d.)

Ze względu na rosnącą liczbę botów realizujących ataki credential stuffing, oszustwa z użyciem kart kredytowych, kampanie wpływu oraz ataki na łańcuch dostaw, spodziewamy się stałego wzrostu ataków botów na aplikacje internetowe.

Włamania do sieci: wykrywanie i zapobieganie

W 2022 r. zaobserwowaliśmy znaczny wzrost liczby exploitów w warstwie sieciowej, w szczególności złośliwego oprogramowania. System wykrywania i zapobiegania włamaniom (IDPS) Azure Firewall tylko w czerwcu zablokował ponad 150 mln połączeń.

IDPS: powód odmowy dotyczącej ruchu w sieci



IDPS: powody alertów o ruchu w sieci

Analiza alertów IDPS zezwoleń i odmów dotyczących ruchu w sieci wskazuje na następujące podejścia stosowane przez atakujących. W przypadku odmowy ruchu w sieci widzimy atakujących używających protokołu SSL do ukrywania swoich działań oraz że ataki typu remote execution stają się coraz bardziej powszechne. W przypadku alertów widzimy, że protokoły SMB/SMB2 są wykorzystywane do przeprowadzania ataków typu remote execution.

Praktyczne wskazówki

1. Prowadź inspekcję całego ruchu pomiędzy systemami w ramach centrum danych lub usługi w chmurze oraz ruchu próbującego uzyskać dostęp do tych zasobów.
2. Opracuj efektywną, całoroczną strategię reagowania na zagrożenia bezpieczeństwa sieci.
3. Skorzystaj z usług zabezpieczeń natywnych dla chmury, aby zaimplementować odporną sieć w modelu Zero Trust.

Linki do dalszych informacji

- Usprawnij zabezpieczenia przed atakami ransomware dzięki Azure Firewall | Azure Blog and Updates | Microsoft Azure
- Anatomia ataku DDoS amplification | Microsoft Security Blog
- Inteligentna ochrona aplikacji od środowisk brzegowych do chmury dzięki Azure Web Application Firewall | Azure Blog and Updates | Microsoft Azure

Opracowanie zrównoważonego podejścia do bezpieczeństwa danych i cyberodporności

Transformacja cyfrowa spowodowała ogromną ekspansję zasobów danych oraz wzrost zagrożeń bezpieczeństwa, zgodności z przepisami i prywatności. Cyberodporne organizacje muszą zapewnić jednocześnie ochronę danych, zgodność z przepisami i odzyskiwanie, a także zintegrować te funkcje ze specjalistycznymi procesami reagowania na zmiany w przepisach w celu eliminowania różnych rodzajów naruszeń.

Naruszenia bezpieczeństwa danych to nie kwestia czy, ale kiedy. Badanie IBM i Ponemon Institute „Cost of a Data Breach" z 2021 r. podaje, że globalny średni koszt naruszenia danych to 4,24 mln USD (wzrost o 10% w stosunku do roku poprzedniego), a 9,05 mln USD w Stanach Zjednoczonych. Stwierdzono, że głównym czynnikiem zwiększającym koszty okazały się być zaniedbania w zakresie zgodności z przepisami. Z kolei obniżenie kosztów naruszeń wiązało się ze stosowaniem najlepszych praktyk takich jak planowanie reakcji na zdarzenia (IR), Zero Trust, AI oraz automatyzacja w zabezpieczeniach oraz szyfrowanie.

Naruszenia danych są nieuniknione. Organizacje, które stosują zrównoważone podejście do odporności, zmniejszają częstotliwość, konsekwencje i koszty naruszeń.

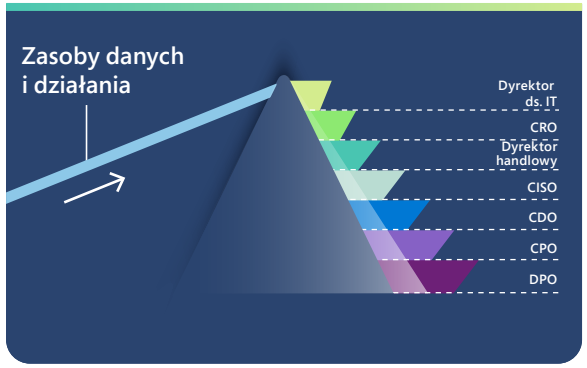
Zarządzanie danymi, bezpieczeństwo, zgodność z przepisami i prywatność są od siebie zależne

W ostatnich latach obserwujemy, jak dane zyskują na znaczeniu jako kluczowy motor dla organizacji. Jednocześnie wzrost liczby przepisów dotyczących prywatności, które wymagają zarówno zarządzania danymi, jak i ich zabezpieczania, spowodował zatarcie granic między stanowiskami zajmującymi się ryzykiem. Wprawdzie obowiązki nowych stanowisk kierowniczych najwyższego szczebla takich jak dyrektor ds. danych (Chief Data Officer/CDO) czy dyrektor ds. ochrony prywatności (Chief Privacy Officers/CPO) obejmują bezpieczeństwo i zgodność z przepisami, to wdrażanie i operacjonalizacja ochrony danych często zależy od zespołów kierowanych przez dyrektorów ds. IT (Chief Information Officer/CIO) i/lub dyrektorów ds. bezpieczeństwa IT (Chief Information Security Officer/CISO). Ta kwestia nie jest jednowymiarowa, gdyż na przykład inicjatywy w zakresie zarządzania danymi prowadzone przez CDO dają również korzyści w zakresie bezpieczeństwa. W wyniku tych wzajemnych powiązań zespoły IT, zarządzania danymi, bezpieczeństwa, zgodności z przepisami i prywatności muszą współpracować coraz ściślej, aby zapewnić efektywność.

Przyszłością są zunifikowane platformy zarządzania ryzykiem obejmujące wszystkie zasoby danych organizacji

Skuteczne koordynowanie działań w zakresie IT, zarządzania danymi, bezpieczeństwa, zgodności z przepisami i zarządzania prywatnością jest trudne w środowisku, w którym występuje wiele niestandardowych aplikacji i nie jest zapewnione spójne pokrycie rozległych danych w środowiskach hybrydowych i wielochmurowych. Uważamy, że organizacje potrzebują scentralizowanego środowiska zarządzania, aby lokalizować i poznawać swoje dane, chronić je, zarządzać dostępem do nich oraz ich wykorzystaniem i cyklem życia, a także zapobiegać ich utracie.

Dzięki ujednoliconym zasobom danych i informacjom o działaniach procesy między zespołami są efektywniejsze, obraz ryzyka jest bardziej kompleksowy, a organizacje mogą lepiej się przygotować na naruszenia i usprawnić na nie reakcje.



Scentralizowane środowisko zarządzania powinno działać jak pryzmat. Zespoły, które są zainteresowane bezpieczeństwem danych, zgodnością z przepisami i prywatnością, potrzebują różnych, ale spójnych widoków zasobów danych i działań, aby koordynować pracę. Działania na danych obejmują dostęp do nich oraz ich modyfikowanie i przesyłanie. Wszystkie je trzeba objąć mechanizmami zabezpieczeń.

Skuteczne zarządzanie danymi, bezpieczeństwo, zgodność z przepisami i prywatność są współzależne i wymagają współpracy między zespołami.

Praktyczne wskazówki

1. Zapewnij jednocześnie ochronę, odzyskiwanie oraz minimalizację konsekwencji naruszeń danych przez inwestowanie w zgodność z przepisami, ochronę danych i funkcje reagowania.
2. Stwórz i wdróż procesy i narzędzia obejmujące różne silosy danych i wszystkie zasoby danych.

Linki do dalszych informacji

- Microsoft Purview — rozwiązania do ochrony danych | Microsoft Security
- Przyszłość zapewniania zgodności z przepisami i zarządzania danymi jest już dziś: przedstawiamy Microsoft Purview | Microsoft Security Blog

Odporność na operacje wpływu: wymiar ludzki

W ciągu ostatnich pięciu lat postępy w dziedzinie grafiki i uczenia maszynowego wprowadziły łatwe w użyciu narzędzia zdolne do szybkiego generowania wysokiej jakości, realistycznych treści, które mogą błyskawicznie i masowo rozprzestrzenić się w Internecie.

W przypadku wydarzeń relacjonowanych za pomocą tekstu, dźwięku i obrazu doszliśmy do punktu, w którym ani ludzie, ani algorytmy nie są w stanie skutecznie odróżnić faktów od fikcji. Rozprzestrzenianie się tych narzędzi i tworzonych przez nie treści poddaje w wątpliwość wiarygodność wszystkich mediów cyfrowych, zakłócając nasze rozumienie wydarzeń lokalnych i światowych. Nowe formy operacji wpływu, które są możliwe dzięki postępom technologicznym, mają poważne konsekwencje dla procesów demokratycznych[11].

Pojawiają się pytania, co można zrobić, aby przeciwdziałać w przyszłości tym operacjom wpływu. Jednak technologia to tylko jedna część układanki. Będzie to wymagało wielu wysiłków, w tym edukacji ukierunkowanej na umiejętność korzystania z mediów, świadomości, czujności, inwestycji w wysokiej jakości dziennikarstwo (z zaufanymi dziennikarzami lokalnymi, krajowymi i zagranicznymi), sieci wymiany informacji i ostrzegania o operacjach wpływu oraz nowych rodzajów regulacji karających tych, którzy tworzą lub manipulują mediami cyfrowymi w celu oszustw.

Zdajemy sobie również sprawę, że przywrócenie zaufania do treści cyfrowych jest ambitnym celem, który będzie wymagał zróżnicowanych perspektyw i szerokiego udziału. Nie ma jednej firmy, instytucji ani rządu mogących samodzielnie przeciwstawić się tym zagrożeniom. Naszą supermocą jako ludzi jest zdolność do współpracy i współdziałania. Jest to szczególnie ważne teraz, ponieważ będzie to wymagało współpracy wszystkich, na całym świecie — rządów, przemysłu, środowisk akademickich, a zwłaszcza organizacji informacyjnych, społecznych i medialnych — dla poprawy kondycji naszego społeczeństwa.

Linki do dalszych informacji

- Zastosowania AI w cybermisjach Departamentu Obrony | Microsoft On the Issues
- AI oraz cyberbezpieczeństwo: rosnące wyzwania i obiecujące kierunki. Przesłuchanie na temat zastosowań AI w cyberoperacjach przed Podkomitetem ds. Cyberbezpieczeństwa Senackiej Komisji ds. Sił Zbrojnych, posiedzenie 117 (3 maja 2022 r., zeznanie Erica Horvitza)

Zwiększanie efektywności ludzi dzięki szkoleniom

Uwzględnienie czynnika ludzkiego jest kluczowe w każdej strategii szkoleń w zakresie cyberbezpieczeństwa. Według badania „Human Factor in IT Security" przeprowadzonego przez Kaspersky[12] 46% incydentów związanych z cyberbezpieczeństwem dotyczy nieostrożnego lub niewyszkolonego personelu, który nieumyślnie ułatwia atak.

Zespół ds. edukacji i świadomości Microsoft w organizacji Digital Security and Resilience odpowiada za wzmocnienie czynnika ludzkiego w cyberbezpieczeństwie przez umożliwienie pracownikom zabezpieczenia systemów i danych własnych oraz klientów. Nasze cele to:

- Zmniejszenie ryzyka dla Microsoft i naszych klientów przez wprowadzenie scentralizowanego, ogólnofirmowego zestawu podstawowych umiejętności wszystkich pracowników w zakresie bezpieczeństwa.
- Ugruntowanie wiedzy pracowników na temat bezpieczeństwa dzięki wieloetapowym szkoleniom, aby wspierać pożądane zachowania.
- Wspieranie zmian kulturowych przez uczynienie myślenia o bezpieczeństwie nieodłączną częścią kultury Microsoft dzięki wymaganym, corocznym szkoleniom i wydarzeniom związanym z bezpieczeństwem.
- Promowanie scentralizowanego, kompleksowego zasobu internetowego udostępniającego najlepsze praktyki, informacje o zasadach firmowych i możliwość zgłaszania incydentów dotyczących cyberbezpieczeństwa.

Ukierunkowany, scentralizowany program szkoleń z zakresu cyberbezpieczeństwa dociera do każdego pracownika Microsoft co najmniej raz w roku. Oferta szkoleniowa jest zoptymalizowana pod kątem wspierania bieżących inicjatyw związanych z cyberbezpieczeństwem i przynosi wymierne efekty w postaci zmiany zachowań. Rada ds. zarządzania ryzykiem informacyjnym (IRMC) Microsoft odgrywa kluczową rolę w określaniu ważnych efektów zmiany zachowań w zakresie cyberbezpieczeństwa, które należy uwzględnić w szkoleniach.

We wszystkich naszych programach szkoleniowych z zakresu cyberbezpieczeństwa mierzymy efektywność, skuteczność i wyniki rozwiązania tam, gdzie jest to możliwe. Na przykład w naszych szkoleniach z zakresu zagrożeń wewnętrznych osiągamy poziom 95% stosowania się uczestników do zaleceń i wyjątkowy poziom ich zadowolenia. Zaowocowało to znacznym wzrostem liczby menedżerów zgłaszających potencjalne przypadki zagrożeń wewnętrznych za pośrednictwem firmowego narzędzia Report It Now. Program obejmuje:

Podstawy bezpieczeństwa: Seria szkoleń o zgodności z przepisami i scentralizowanej, obejmującej całą firmę świadomości w zakresie cyberbezpieczeństwa dotyczy podstawowych praktyk bezpieczeństwa i ochrony prywatności. Wykorzystano tu model edutainment, aby uczynić naukę o cyberbezpieczeństwie wciągającą i interesującą.

STRIKE: Wymagane przez Microsoft szkolenie techniczne dla inżynierów, którzy tworzą i utrzymują rozwiązania biznesowe. Szkolenie dostępne tylko na zaproszenie dotyczy aktualnych i kluczowych obszarów najlepszych praktyk w zakresie cyberhigieny i wykorzystuje hybrydowy model prezentacji na żywo dostosowany do potrzeb odbiorców.

Programy ukierunkowane: Ukierunkowane programy szkoleniowe dotyczą konkretnych inicjatyw w zakresie cyberbezpieczeństwa, w tym Shadow IT, Insider Threat czy Microsoft Federal. Oferty są ściśle powiązane z konkretnymi inicjatywami cyberbezpieczeństwa oraz zapewniają opiekę kierownictwa i raportowanie w formie kart wyników, aby zapobiec podejściu edukacyjnemu opartemu na „odhaczaniu wykonanych zadań".

MSProtect: Scentralizowany zasób internetowy Microsoft udostępniający najlepsze praktyki, informacje o zasadach firmowych i możliwość zgłaszania incydentów dotyczących cyberbezpieczeństwa. Ten zasób na żądanie jest przeznaczony dla pracowników poza ofertą formalnych szkoleń.

Szkolenia w zakresie bezpieczeństwa nie mogą być postrzegane jako działania narzucane przez przepisy, gdzie wystarczy jedynie odhaczyć wykonanie zadania. Zamiast tego należy skupić się na zmianie zachowań oraz monitorować tę zmianę w celu określenia efektu szkoleń.

Praktyczne wskazówki

1. Zapewnij pracownikom szkolenia i zasoby dotyczące bezpieczeństwa, kiedy i gdzie będą ich potrzebować.
2. Opracuj scentralizowaną strategię zdobywania umiejętności opartą na informacjach od interesariuszy z całego przedsiębiorstwa.
3. Upewnij się, że efekty szkoleń są śledzone i analizowane pod kątem wydajności (ilościowo), skuteczności (jakościowo) i wyników (wpływu na biznes).

Linki do dalszych informacji

- Microsoft rozpoczyna kolejny etap inicjatywy na rzecz podnoszenia umiejętności po udzieleniu pomocy 30 mln osób

Wnioski z naszego programu eliminacji oprogramowania wymuszającego okup

Microsoft w ciągu ostatnich pięciu lat prowadził własny program Zero Trust[13]. Celem było zapewnienie efektywnego zarządzania tożsamościami i urządzeniami oraz ich dobrego stanu. Wraz z rosnącymi zagrożeniami ransomware opracowaliśmy dogłębne metody ochrony naszej organizacji i klientów.

Po przeprowadzeniu dogłębnej oceny wewnętrznej stworzyliśmy program eliminacji ransomware, który polega na usuwaniu luk w pokryciu i mechanizmach kontroli, ulepszaniu usług, takich jak Ochrona punktu końcowego w usłudze Microsoft Defender, Azure czy M365, oraz opracowywaniu podręczników dla naszych zespołów SOC i inżynierskich dotyczących sposobu przywracania po ataku ransomware.

Pierwszym krokiem było zrozumienie zakresu naszej ochrony przed atakami ransomware wymierzonymi w Microsoft. Wdrażanie Ochrony punktu końcowego w usłudze Microsoft Defender było już zaawansowane. Chcieliśmy też zapewnić, że wszystkie urządzenia są zarządzane i zgodne z zasadami Zero Trust. Ale musieliśmy też poznać odpowiedź na najważniejsze pytanie — czy możemy realizować skutecznie przywracanie po ataku. W tym celu przeanalizowaliśmy dokument „Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile" (NIST 8374),[14] który jest zgodny z naszymi ogólnymi zasadami w przedsiębiorstwie. Ta analiza pozwoliła szybko zidentyfikować luki w pokryciu.

Następnie ustaliliśmy istotność poszczególnych luk w funkcjach składających się na ramy cyberbezpieczeństwa CSF (identyfikowanie, wykrywanie, ochrona, reagowanie i odzyskiwanie). Odkryliśmy strategiczną zgodność z Zero Trust i innymi programami, ale także luki, w których brakowało przypisanych procedur. Po oszacowaniu ilości pracy i wysiłku potrzebnego do usunięcia tych luk, podzieliliśmy je na dwie grupy:

- **Ochrona przedsiębiorstwa (PtE):** Zdefiniowanie pozycji roboczych, które musimy wykonać jako przedsiębiorstwo, aby zapewnić sobie ochronę i możliwość przywracania po ataku.
- **Ochrona klienta (PtC):** Dodawanie funkcji do naszej oferty, aby chronić naszych klientów i naszą firmę.

Wdrażanie wniosków w naszej firmie

Aby wyeliminować największe zagrożenia i chronić nasze krytyczne usługi przed atakami ransomware, w ciągu najbliższych 6–12 miesięcy planujemy skupić inwestycje na realizacji pięciu poniższych scenariuszy w ramach dedykowanego programu zwalczania ransomware. Gdy uda nam się zrealizować każdy ze scenariuszy, będziemy stopniowo rozszerzać zakres programu, aby objąć nim wszystkie części przedsiębiorstwa.

Scenariusz 1: Członkowie zespołu ds. bezpieczeństwa rozumieją ogólne ryzyko związane z atakami ransomware i opracowali proces informowania kadry kierowniczej o lukach w zabezpieczeniach i aktualnym ryzyku.

Scenariusz 2: Członkowie zespołu ds. bezpieczeństwa mają dostęp do podręczników, które pomagają im i innym zespołom w Microsoft reagować na problemy w krytycznych usługach i przywracać je do pracy po ataku ransomware.

Scenariusz 3: Członkowie zespołu ds. odporności przedsiębiorstwa mają ustalony standard postępowania przy tworzeniu kopii zapasowych systemów krytycznych. Istnieją podręczniki i przeprowadzane są regularne ćwiczenia tworzenia kopii zapasowych i odzyskiwania, aby zapewnić możliwość odzyskania danych w przypadku ataku ransomware.

Scenariusz 4: Właściciele usług rozumieją i wdrażają wymagane zabezpieczenia, mechanizmy kontroli oraz zasady, aby chronić swoje usługi, dane klientów, urządzenia klienckie i zasoby sieciowe przed atakami ransomware, ze szczególnym uwzględnieniem usług krytycznych Microsoft.

Scenariusz 5: Wszyscy pracownicy mają dostęp do zasobów edukacyjnych i szkoleniowych, które opisują, jak rozpoznać atak ransomware oraz jak powiadomić zespół ds. bezpieczeństwa i zainicjować odpowiedź.

Praktyczne wskazówki

1. Dokumentuj i weryfikuj kompleksowo działania związane z przywracaniem po atakach ransomware na krytyczne usługi i przeciwdziałaniem im.
2. Zaangażuj interesariuszy w aktualizację podręczników zarządzania kryzysowego w przedsiębiorstwie, aby uwzględnić działania specyficzne dla ransomware oraz proces decyzyjny i wskazówki dotyczące określenia, czy i kiedy należy zapłacić okup.
3. Zwiększ zasięg wykrywania i ochrony przez włączenie możliwości dostępnych we wdrożonych produktach bezpieczeństwa (np. reguły ograniczania obszaru podatnego na ataki w Ochronie punktu końcowego w usłudze Microsoft Defender).
4. Współpracuj z zespołem ds. standardów bezpieczeństwa w celu zdefiniowania podstawowego poziomu ochrony przed atakami ransomware oraz zapewnij szkolenia i dokumentację zespołom inżynierskim w tym obszarze.
5. Wprowadź automatyzację, aby ułatwić zespołom DevOps wdrażanie zasad dotyczących bezpieczeństwa i operacji oraz zapewnianie, że jeśli system będzie odchodzić od zgodności z przepisami, będzie to szybko sygnalizowane i naprawiane.

Linki do dalszych informacji

- Sposób ochrony Microsoft przed oprogramowaniem wymuszającym okup | Microsoft Inside Track

Działaj już teraz w obszarze bezpieczeństwa kwantowego

Coraz częściej mówi się o konieczności opanowania zagrożenia, jakie obliczenia kwantowe stanowią dla współczesnej kryptografii i wszystkich chronionych przez nią zasobów. Memorandum w sprawie poprawy cyberbezpieczeństwa wydane niedawno przez National Security Department of Defense and Intelligence Community Systems[15] opiera się na zarządzeniu wykonawczym Stanów Zjednoczonych (Executive Order – EO) nr 10428[16] w sprawie poprawy cyberbezpieczeństwa kraju. Podkreśla ono, że bezpieczeństwo łańcucha dostaw oprogramowania ma kluczowe znaczenie dla przeciwdziałania przyszłym atakom ze strony państw.

Czym są komputery kwantowe?

Komputery kwantowe to maszyny wykorzystujące właściwości fizyki kwantowej do przechowywania danych i wykonywania obliczeń. W przypadku niektórych zadań mogą one znacznie przewyższyć najlepsze superkomputery. Obliczenia kwantowe już teraz otwierają nowe horyzonty w zakresie szyfrowania i przetwarzania danych. Badania przewidują, że obliczenia kwantowe już w 2030 r. staną się branżą o wartości wielu miliardów dolarów17. Obliczenia kwantowe i komunikacja kwantowa mają szansę znacząco wpłynąć na wiele branż, od opieki zdrowotnej i energetyki po finanse i bezpieczeństwo.

Obliczenia kwantowe stanowią zagrożenie dla współczesnej kryptografii i wszystkiego, co ona chroni.

Zagrożenie dla współczesnej kryptografii

Dzięki algorytmowi Shora z 1994 roku i komputerowi kwantowemu o dużej skali (składającemu się z co najmniej milionów fizycznych kubitów) wszystkie nasze obecnie szeroko stosowane algorytmy kryptograficzne oparte na kluczu publicznym mogłyby zostać złamane. Dlatego kluczowe znaczenie ma rozważenie, ocena i standaryzacja kryptosystemów „bezpiecznych pod względem kwantowym", które byłyby wydajne, elastyczne i odporne na ataki kwantowe. Migracja oprogramowania do „kryptografii postkwantowej", czyli do już istniejących algorytmów i protokołów odpornych na ataki kwantowe, zajmie lata, a może dekady[18].

Oznacza to konieczność opanowania zagrożenia dla współczesnej kryptografii i wszystkich chronionych przez nią zasobów. Atakujący mogą rejestrować zaszyfrowane dane teraz i wykorzystać je później, gdy komputery kwantowe będą już dostępne. Jeśli wszyscy będziemy bezczynnie czekać na nadejście obliczeń kwantowych, a nie przygotujemy wcześniej się na ich konsekwencje dla kryptografii, spóźnimy się.

Ponieważ kryptografia jest używana w całej cyberprzestrzeni, wszystkie usługi bezpieczeństwa oparte na kryptografii mogą być zagrożone. Na przykład usługi komunikacyjne (TLS, IPSec), przesyłanie wiadomości (e-mail, konferencje internetowe), zarządzanie tożsamością i dostępem, przeglądanie stron internetowych, podpisywanie kodu, transakcje płatnicze i inne usługi, których ochrona opiera się na kryptografii.

Ponieważ komputery kwantowe stają się rzeczywistością, składniki oprogramowania innych firm zawierające implementacje algorytmów i funkcje kryptograficzne będą również wymagać dodatkowej analizy. Wymaga to, aby wszystkie organizacje w łańcuchu wartości zajęły się zapewnieniem jego bezpieczeństwa. Organy branżowe i rządy zwiększają wysiłki w celu zdefiniowania wymagań dotyczących bezpieczeństwa łańcucha dostaw oprogramowania, a w niektórych przypadkach wprowadzają nowe wymagania dotyczące jego zabezpieczenia. Memorandum w sprawie bezpieczeństwa narodowego NSM-8[19] ustanawia wymagania i harmonogramy wdrażania kryptografii postkwantowej w krajowych systemach bezpieczeństwa (NSS). Na jego mocy w ciągu 180 dni oczekiwane jest „zaplanowanie modernizacji, zajęcie się użyciem nieobsługiwanego szyfrowania, specyficznych dla rozwiązań protokołów oraz protokołów odpornych na obliczenia kwantowe, a także zaplanowanie użycia w razie potrzeby kryptografii odpornej na obliczenia kwantowe".

Standaryzacja to działanie, które wymaga długiego czasu realizacji w przejściu na kryptografię bezpieczną kwantowo. Organy regulacyjne, które pracują nad standardami wykorzystującymi kryptografię opartą na kluczach publicznych, muszą już teraz eksperymentować z algorytmami postkwantowymi i dostosowywać się do nich.

Algorytmy kryptografii postkwantowej (PQC) — istniejące już algorytmy uważane za odporne na ataki kwantowe — są obecnie poddawane analizie w ramach projektu ustalania norm dla ery postkwantowej NIST[20]. Ta praca wpłynie na działania organów regulacyjnych na całym świecie. Fakt, że różne organy krajowe i regulacyjne mogą wybrać odmienne algorytmy, może stworzyć wyzwanie na skalę międzynarodową. To rozdrobnienie skomplikuje z kolei inżynierię produktów i usług.

Algorytmy kryptografii postkwantowej (PQC) są obecnie poddawane analizie w ramach projektu ustalania norm dla ery postkwantowej NIST. Ta praca wpłynie na działania organów regulacyjnych na całym świecie.

Praktyczne wskazówki

Wraz z SAFECode i członkami partnerskimi branża powinna podjąć natychmiastowe, szybkie działania w celu przygotowania się do przejścia na algorytmy PQC[21]:

1. Przeprowadź inwentaryzację produktów/baz kodowych, które wykorzystują kryptografię.
2. Wdróż strategię elastyczności kryptograficznej w całej organizacji, m.in. zminimalizuj ilość kodu, którego zmiana będzie konieczna w momencie fundamentalnej transformacji kryptografii.
3. Pilotuj wykorzystanie bezpiecznych kwantowo algorytmów-kandydatów w swoich produktach i usługach wykorzystujących kryptografię.
4. Przygotuj się na używanie różnych algorytmów opartych na kluczach publicznych do szyfrowania, wymiany kluczy i podpisów.
5. Przetestuj swoje aplikacje pod kątem wpływu bardzo dużych rozmiarów kluczy, szyfrów i podpisów.

Linki do dalszych informacji

- Microsoft przedstawił uzasadnienie fizyczne nowych rodzajów kubitów | Microsoft Research

Integracja działów biznesowego, bezpieczeństwa i IT w celu zwiększenia odporności

Poziom cyberodporności zależy od efektywności współpracy liderów biznesowych z zespołami ds. bezpieczeństwa w obszarze wdrażania zabezpieczeń. Z doświadczenia Microsoft wynika, że skuteczna realizacja wizji bezpieczeństwa to wymagający projekt, w którym konieczne jest wsparcie liderów organizacji.

Liderzy działów bezpieczeństwa mierzą się z całą gamą dynamicznych wyzwań obejmujących ryzyko, technologię, ekonomię, procesy organizacyjne, modele biznesowe, transformację kulturową, interesy geopolityczne, szpiegostwo i przestrzeganie sankcji międzynarodowych. Każda z tych dziedzin zawiera niuanse, które należy zrozumieć i wobec których należy właściwie postępować.

Zadaniem liderów działów bezpieczeństwa jest również przeciwdziałanie zarówno inteligentnym, dobrze finansowanym i wysoce zmotywowanym atakującym, jak i tym nisko wykwalifikowanym, ale również skutecznym. Ich zespoły muszą bronić złożonych zasobów technicznych, często budowanych stopniowo przez 30 lub więcej lat, kiedy to bezpieczeństwo stanowiło niski lub żaden priorytet. Decyzje podjęte przed laty mogą stwarzać zagrożenia dzisiaj, dopóki nie spłacimy długu technicznego i nie zajmiemy się lukami w zabezpieczeniach.

Decydenci i liderzy organizacji mogą mieć znaczący, pozytywny wpływ na bezpieczeństwo, aktywnie wspierając liderów działów bezpieczeństwa i pomagając w budowaniu pomostu między zintegrowanymi zabezpieczeniami a resztą organizacji. Kiedy Microsoft współpracuje z klientami, którzy mają takie podejście, widzimy, jak budują bardziej odporną organizację, a także poprawiają swoją elastyczność w dostosowywaniu się i wprowadzaniu innowacji.

Kierownictwo organizacji może wspierać liderów działów bezpieczeństwa przez skupienie się na trzech kluczowych obszarach:

1. Bezpieczeństwo wbudowane już na etapie projektu

Bezpieczeństwo jest niekiedy postrzegane jako przeszkoda w procesach biznesowych lub obszar, którym się należy zajmować po fakcie. Często bierze się je pod uwagę przy podejmowaniu decyzji, gdy jest już za późno, aby uniknąć ryzyka lub rozwiązać problemy tanio i szybko.

Decydenci i liderzy organizacji powinni:

Zapewnić włączenie kwestii bezpieczeństwa już na wczesnych etapach nowych inicjatyw. Nowe inicjatywy cyfrowe i wdrożenie chmury powinny priorytetyzować bezpieczeństwo, aby zapewnić, że ryzyko organizacyjne nie będzie wzrastać wraz z każdą nową aplikacją lub funkcją cyfrową. Te same procesy można wykorzystać do modernizacji starszych systemów, aby uzyskać jednocześnie korzyści w zakresie bezpieczeństwa, jak i wydajności.

Normalizować konserwację prewencyjną w obszarze zabezpieczeń. Podstawowe działania związane z konserwacją zabezpieczeń (stosowanie aktualizacji i poprawek oraz utrzymywanie bezpiecznych konfiguracji) powinny mieć pełne wsparcie organizacji (w tym budżety, zaplanowane przestoje, wymagania dotyczące pozyskiwania wsparcia dla produktów dostawcy).

Niestety, wiele organizacji opóźnia wprowadzenie tych zaleceń lub stosuje je tylko częściowo. Stwarza to szerokie możliwości dla atakujących. Potrzebę normalizacji zabezpieczeń ujęto w US NIST 800-40[22].

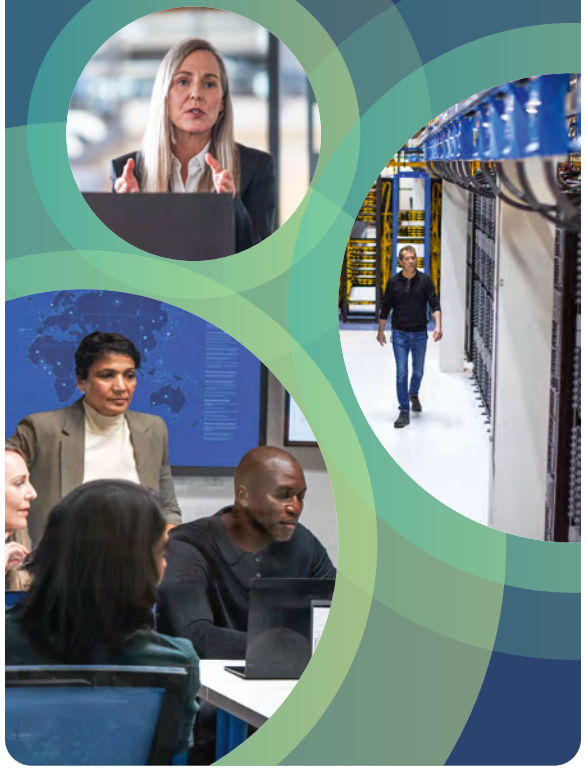
2. Zaangażuj się w bezpieczeństwo

Kierownictwo powinno aktywnie uczestniczyć w kluczowych procesach bezpieczeństwa oraz sponsorować je, aby zasoby były odpowiednio kierowane, a organizacja była gotowa na problemy. Obejmuje to angażowanie się w:

Identyfikację krytycznych zasobów biznesowych. Zespoły ds. bezpieczeństwa i ich liderzy muszą wiedzieć, które zasoby są krytyczne dla biznesu, aby skoncentrować się na tym, co najważniejsze. Często jest to dla nich nowy obszar, w którym analizuje się nieporuszane wcześniej pytania i odpowiedzi.

Ćwiczenia zapewniania ciągłości działania i odzyskiwania. Cyberataki mogą stać się poważnymi problemami, które zakłócają lub zatrzymują większość operacji biznesowych lub wszystkie z nich. Zapewnienie, że zespoły w całej organizacji są przygotowane do radzenia sobie w takich sytuacjach, skróci czas przywracania operacji biznesowych, ograniczy szkody w organizacji i pomoże utrzymać zaufanie klientów, obywateli i wyborców. Te działania powinny być zintegrowane z istniejącymi procesami zapewniania ciągłości działania i odzyskiwania.

Decyzje dotyczące ryzyka związanego z bezpieczeństwem najlepiej podejmują właściciele firm lub misji, którzy mają pełną widoczność wszystkich zagrożeń i możliwości.



Integracja działów biznesowego, bezpieczeństwa i IT w celu zwiększenia odporności

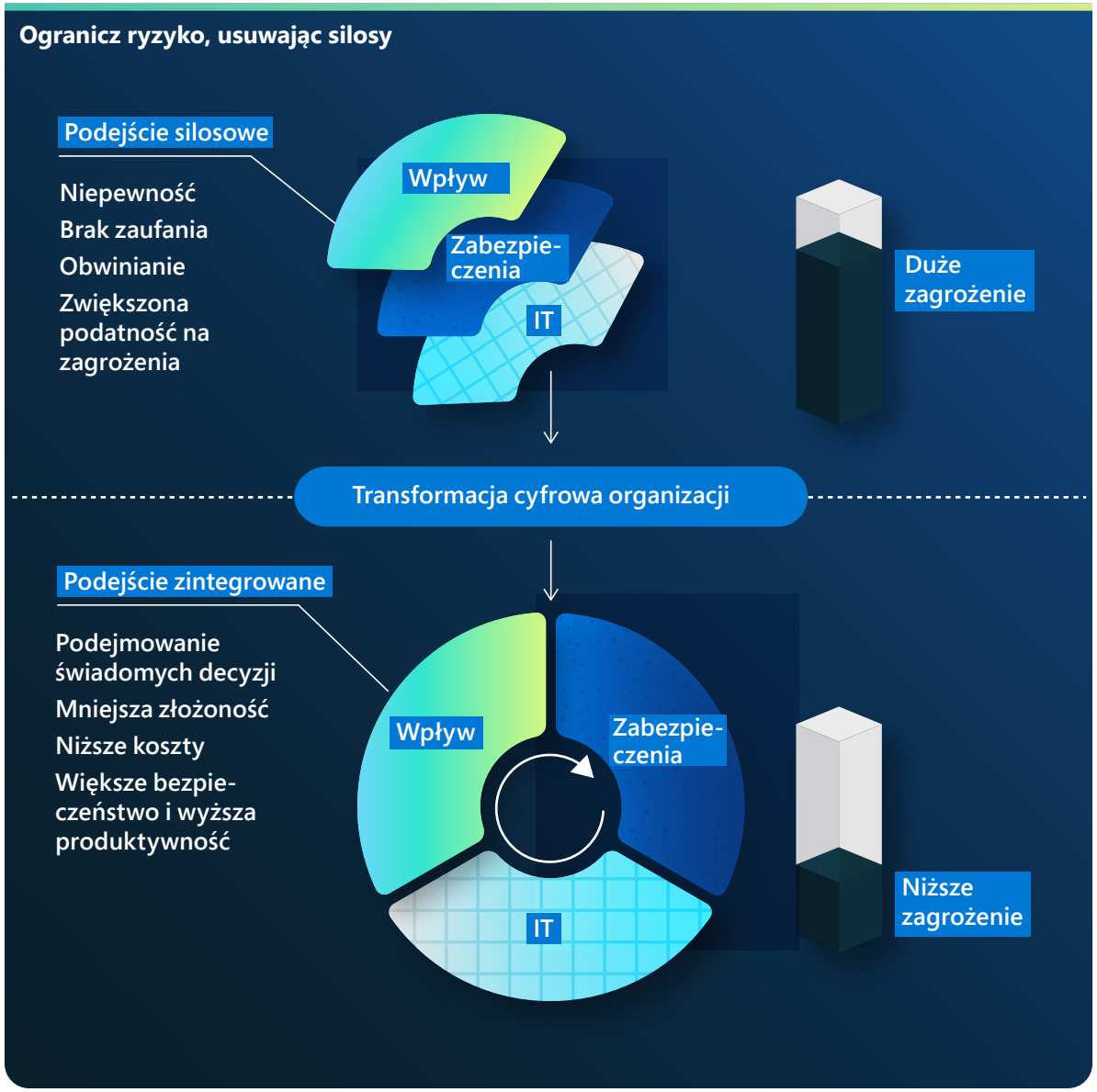
(c.d.)

3. Poprawnie pozycjonuj bezpieczeństwo

Istniejąca w organizacjach struktura odpowiedzialności za ryzyko związane z bezpieczeństwem niestety często powoduje, że podejmują one niewłaściwe w tym obszarze. Decyzje dotyczące ryzyka powinni podejmować właściciele biznesowi lub misji, którzy mają pełny wgląd we wszystkie ryzyka i szanse. Jednak organizacje często (domyślnie lub jawnie) przypisują odpowiedzialność za ryzyko bezpieczeństwa ekspertom w danej dziedzinie w zespole ds. bezpieczeństwa. Niekorzystnie obciąża to zespoły ds. bezpieczeństwa, a jednocześnie pozbawia właścicieli firm widoczności i kontroli nad kluczowymi zagrożeniami. Organizacje mogą to poprawić przez:

Przygotowanie właścicieli firm: Należy informować właścicieli firm o ogólnym zagrożeniu bezpieczeństwa oraz o tym, jak te zagrożenia mogą wpłynąć na ich działalność. Bezpośrednie zaangażowanie w te wysiłki zespołów ds. bezpieczeństwa poprawia również współpracę w obszarze bezpieczeństwa i ogólną elastyczność biznesową.

Przenoszenie odpowiedzialności za zagrożenia bezpieczeństwa na właścicieli firm: Kiedy właściciele firm otrzymują wystarczające informacje, aby zrozumieć i zaakceptować zagrożenia dla bezpieczeństwa, organizacja powinna jawnie przenieść na nich odpowiedzialność za to ryzyko, jednocześnie utrzymując odpowiedzialność zespołów ds. bezpieczeństwa w zakresie zarządzania nim oraz zapewniania właścicielowi fachowej wiedzy i wskazówek.



„Cyberodporność to całe spektrum: od klasycznej ciągłości działania i odzyskiwania (efektywne tworzenie kopii zapasowych), przez możliwości przywracania procesów, technologii i ich zależności (w tym ludzi i zasobów innych firm), po zawsze włączone, samonaprawiające się usługi, odporność krytycznych ról i przełączanie awaryjne (failover) zasobów krytycznych innych firm. Najbardziej odporne organizacje promują integrację między specjalistami IT, menedżerami biznesowymi a specjalistami ds. bezpieczeństwa. Wysoka odporność obejmuje projektowanie odporności już na wczesnych etapach, bezpieczne zarządzanie zmianami i precyzyjną izolację błędów. Cyberodporność to tylko jeden z wielu scenariuszy w dobrym programie planowania wszystkich zagrożeń. W miarę wzrostu cyberzagrożeń i znaczenia wzajemnych powiązań między cyberbezpieczeństwem a odpornością związek dyrektora ds. bezpieczeństwa informacji (CISO) z programem odporności przedsiębiorstwa staje się coraz silniejszy. Każdego roku coraz więcej CISO przejmuje odpowiedzialność za odporność w całej firmie”.

Lisa Reshaur
Dyrektor generalny ds. zwalczania zagrożeń, Microsoft

Linki do dalszych informacji

- Od odporności do wytrwałości cyfrowej: jak organizacje dzięki technologii cyfrowej wychodzą na prostą w trudnych czasach | Official Microsoft Blog
- Jak zespoły IT i zespoły ds. bezpieczeństwa mogą współpracować w celu poprawy bezpieczeństwa urządzeń klienckich | Microsoft Security

Krzywa dzwonowa cyberodporności

Czynniki odporności powinny zostać przyjęte przez każdą organizację

Jak widzieliśmy, wiele cyberataków kończy się sukcesem tylko dlatego, że nie przestrzegano podstawowych praktyk bezpieczeństwa. Minimalne standardy, które powinna przyjąć każda organizacja to:

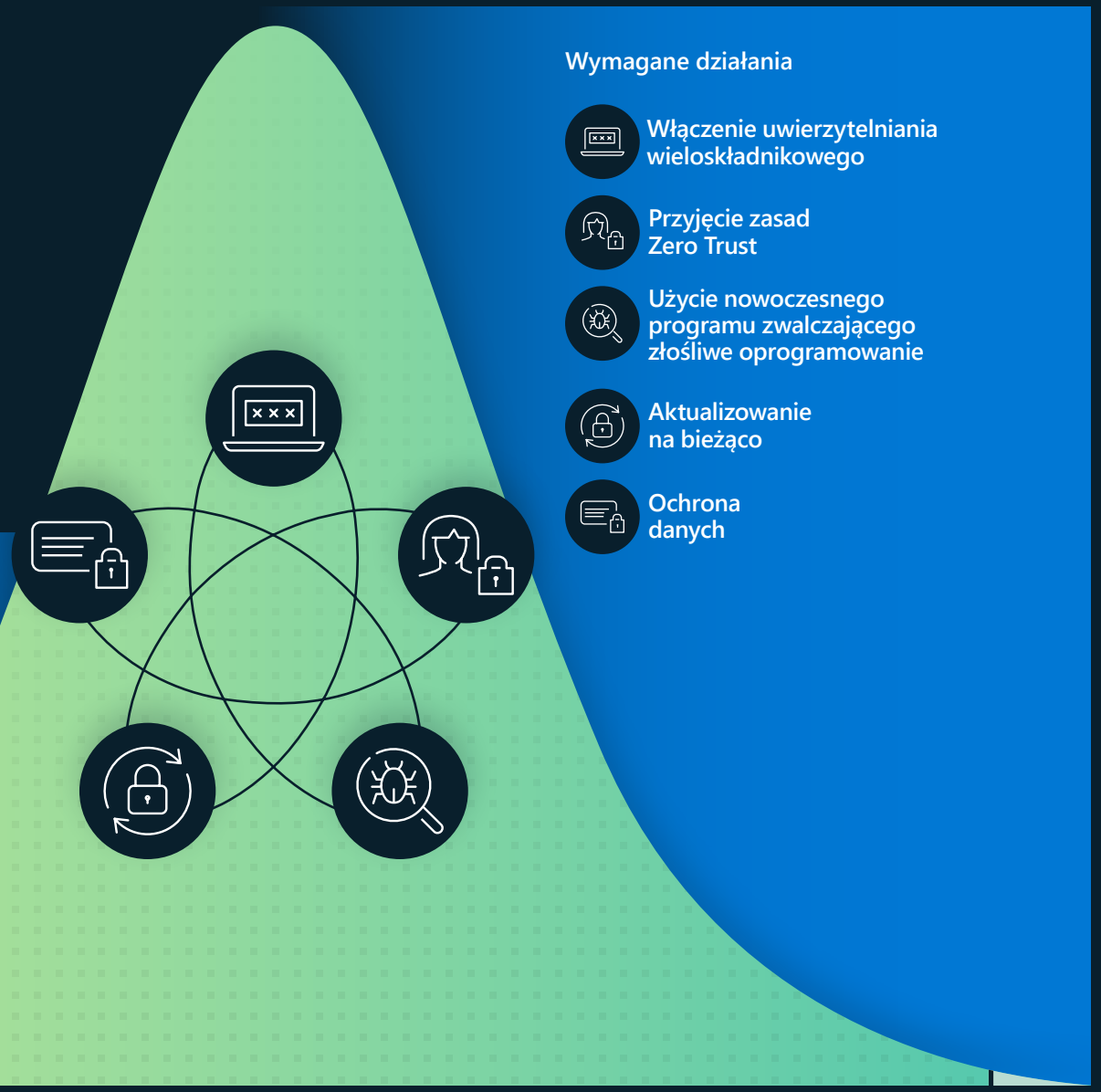
- **Włączenie uwierzytelniania wieloskładnikowego (MFA):** ochrona przed naruszeniem haseł użytkowników i zapewnienie dodatkowej odporności dla tożsamości.
- **Przyjęcie zasad Zero Trust:** podstawa każdego planu odporności ograniczającego ryzyko dla organizacji. Te zasady to:

1. — Weryfikuj jawnie — przed umożliwieniem dostępu do zasobów upewnij się, że użytkownicy i urządzenia są w dobrej kondycji.
2. — Przydzielaj dostęp z minimalnymi uprawnieniami — zezwalaj tylko na uprawnienia potrzebne do uzyskania dostępu do zasobu, ale nie większe.
3. — Zakładaj wystąpienie naruszenia — przyjmuj, że już doszło do naruszenia zabezpieczeń systemu i że mógł on zostać przejęty. Oznacza to ciągłe monitorowanie środowiska pod kątem ewentualnego ataku.

- **Wykorzystaj XDR (Rozszerzone możliwości wykrywania zagrożeń i reagowania na nie):** Wdróż oprogramowanie do wykrywania i automatycznego blokowania ataków oraz dostarczania analiz operacji bezpieczeństwa. Monitorowanie analiz z systemów wykrywania zagrożeń jest niezbędne, aby móc szybko reagować na zagrożenia.
- **Aktualizuj na bieżąco:** Wiele organizacji padnie ofiarą ataku tylko z jednego powodu — ich systemy są przestarzałe lub bez zastosowanych poprawek. Zapewnij, że wszystkie systemy są aktualizowane (w tym oprogramowanie układowe, systemy operacyjne i aplikacje).
- **Chroń dane:** Znajomość ważnych danych, ich lokalizacji i tego, czy zostały wdrożone właściwe systemy, ma kluczowe znaczenie dla odpowiedniej ochrony.

98%

podstawowych praktyk bezpieczeństwa chroni przed 98% ataków



Przypisy końcowe

1. EDR (Wykrywanie zagrożeń dla urządzeń klienckich i reagowania na nie) to platforma klasy korporacyjnej zapewniająca bezpieczeństwo urządzeń klienckich, którą zaprojektowano tak, aby pomagała sieciom w przedsiębiorstwach w zapobieganiu zaawansowanym zagrożeniom, ich wykrywaniu i badaniu oraz reagowaniu na nie. Funkcje wykrywania zagrożeń dla urządzeń klienckich i reagowania na nie zapewniają zaawansowane wykrywanie ataków w czasie zbliżonym do rzeczywistego. Analitycy bezpieczeństwa mogą efektywnie nadawać priorytety alertom, uzyskiwać kompleksowy wgląd w stan naruszeń i reagować w celu przeciwdziałania zagrożeniom.
2. Platformy ochrony punktów końcowych (EPP) to rozwiązanie wdrażane na urządzeniach klienckich w celu zapobiegania złośliwemu oprogramowaniu opartemu na plikach, wykrywania i blokowania złośliwej aktywności z zaufanych i niezaufanych aplikacji oraz badania i przeciwdziałania, które są niezbędne do dynamicznego reagowania na incydenty i alarmy dotyczące bezpieczeństwa.
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. Książka o zabezpieczeniach Windows
7. Nowe funkcje zabezpieczeń w Windows 11 pomogą chronić pracowników hybrydowych | Blog Microsoft Security
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

Współpracujące zespoły

Współpracujące zespoły

Dane i spostrzeżenia zawarte w tym raporcie zostały dostarczone przez zróżnicowaną grupę specjalistów ds. bezpieczeństwa pracujących w wielu różnych zespołach Microsoft. Celem ich wszystkich jest ochrona Microsoft, klientów Microsoft i całego świata przed cyberatakami. Z dumą dzielimy się tymi spostrzeżeniami w duchu transparentności. Naszym wspólnym celem jest uczynienie świata bezpieczniejszym dla wszystkich.

AI for Good Research Lab: Mottem zespołu jest wykorzystywanie potencjału danych oraz AI w celu sprostania globalnym wyzwaniom. Laboratorium współpracuje z organizacjami spoza Microsoft, stosując AI do poprawy warunków życia i środowiska. Obszarami zainteresowania są bezpieczeństwo w sieci (dezinformacja, cyberbezpieczeństwo, bezpieczeństwo dzieci), reagowanie na incydenty, zrównoważony rozwój oraz AI w obszarze opieki zdrowotnej.

Azure Edge & Platform, Enterprise & OS Security: Odpowiada za bezpieczeństwo podstawowych systemów operacyjnych i platform w Windows, Azure i innych produktach Microsoft. Zespół ten wbudowuje w platformy Microsoft wiodące w branży rozwiązania w zakresie bezpieczeństwa i sprzętu, aby ograniczyć zagrożenia związane z exploitami, tożsamością i złośliwym oprogramowaniem — od układu scalonego po chmurę. Są to m.in. twórcy platformy Secured-core Microsoft na komputery PC, środowiska brzegowe i serwery czy procesora bezpieczeństwa Microsoft Pluton Security Processor.

Azure Networking, Core: Zespół ds. sieci w chmurze skoncentrowany na sieci Microsoft WAN, sieciach centrów danych oraz infrastrukturze sieciowej zdefiniowanej programowo Azure, w tym platformie DDoS, platformie brzegowej sieci oraz produktach bezpieczeństwa sieciowego takich jak Azure WAF, Azure Firewall czy Azure DDoS Protection Standard.

Zespół Cloud Security Research: Dzięki zabezpieczeniu chmury Microsoft, tworzeniu innowacyjnych produktów i funkcji bezpieczeństwa oraz przeprowadzaniu badań zespół ten chroni klientów Microsoft i umożliwia im bezpieczne przekształcanie organizacji.

Customer Security and Trust (CST): Interdyscyplinarny zespół zapewniający ciągłą poprawę bezpieczeństwa klientów w produktach Microsoft i usługach online. CST współpracuje z zespołami inżynierskimi i ds. zabezpieczeń w całej firmie. Jego misją jest zapewnianie zgodności z przepisami oraz zwiększanie bezpieczeństwa i transparentności w celu ochrony naszych klientów i promowania globalnego zaufania do Microsoft.

Customer Success: Zespoły ds. bezpieczeństwa w grupie Customer Success współpracują bezpośrednio z klientami w celu wymiany najlepszych praktyk, wniosków i wskazówek, aby przyspieszyć transformację i modernizację zabezpieczeń. Zespół ten gromadzi i porządkuje najlepsze praktyki i wnioski z doświadczeń Microsoft i klientów, tworząc strategie referencyjne, architektury referencyjne, plany referencyjne i inne.

Cyber Defense Operations Center (CDOC): Centrum cyberbezpieczeństwa i ochrony Microsoft to połączone centrum zrzeszające specjalistów ds. bezpieczeństwa z całej firmy w celu ochrony infrastruktury naszego przedsiębiorstwa i infrastruktury w chmurze, do której mają dostęp klienci. Osoby reagujące na incydenty wspierają specjalistów ds. danych i inżynierów bezpieczeństwa pracujących nad usługami, produktami i grupami urządzeń Microsoft, aby pomagać im w ochronie oraz wykrywaniu zagrożeń i reagowaniu na nie 24 godziny na dobę, 7 dni w tygodniu.

Democracy Forward Initiative: Zespół Microsoft działający na rzecz zachowania, ochrony i rozwoju podstaw demokracji przez promowanie zdrowego ekosystemu informacyjnego i społecznej odpowiedzialności biznesu oraz ochronę otwartych i bezpiecznych procesów demokratycznych.

Digital Crimes Unit (DCU): Zespół prawników, śledczych, analityków danych, inżynierów, analityków i specjalistów biznesowych, którzy zwalczają cyberprzestępczość na całym świecie dzięki innowacyjnemu zastosowaniu technologii, kryminalistyki, powództw cywilnych, przekazań karnych oraz partnerstw publicznych i prywatnych.

Digital Diplomacy: Międzynarodowy zespół byłych dyplomatów, decydentów i ekspertów prawnych pracujących na rzecz pokojowej, stabilnej i bezpiecznej cyberprzestrzeni w obliczu narastających konfliktów między państwami.

Digital Security & Resilience (DSR): Grupa, której celem jest umożliwienie Microsoft tworzenia najbardziej zaufanych urządzeń i usług przy jednoczesnym zapewnieniu bezpieczeństwa naszej firmie, a także ochrony danych naszych i klientów.

Digital Security Unit (DSU): Zespół prawników i analityków ds. cyberbezpieczeństwa, którzy zapewniają wiedzę prawną, geopolityczną i techniczną w celu ochrony firmy Microsoft i jej klientów. DSU buduje zaufanie do zabezpieczeń przedsiębiorstw Microsoft przed zaawansowanymi cyberatakami na całym świecie.

Digital Threat Analysis Center (DTAC): Zespół ekspertów, którzy analizują i zgłaszają zagrożenia ze strony państw, w tym cyberataki i operacje wpływu. Zespół ten łączy dane z analityki cyberzagrożeń z analizą geopolityczną, aby zapewnić naszym klientom i Microsoft możliwość skutecznego reagowania.

Enterprise and Security: Zespół zajmujący się zapewnianiem nowoczesnej, bezpiecznej i łatwej do zarządzania platformy dla inteligentnej chmury i inteligentnych środowisk brzegowych.

Enterprise Mobility: Zespół, który pomaga zapewnić nowoczesne miejsce pracy i nowoczesne zarządzanie w celu utrzymania bezpieczeństwa danych — w chmurze i w środowiskach lokalnych. Endpoint Manager obejmuje usługi i narzędzia, których Microsoft i klienci używają do nadzorowania i monitorowania urządzeń mobilnych, komputerów stacjonarnych, maszyn wirtualnych, urządzeń wbudowanych i serwerów.

Współpracujące zespoły

(c.d.)

Enterprise Risk Management: Zespół pracujący w różnych jednostkach biznesowych, wspierający omawianie zagrożeń z wyższym kierownictwem Microsoft. Zrzesza on wiele grup zajmujących się ryzykiem operacyjnym, zarządza ramami ryzyka korporacyjnego Microsoft i ułatwia ocenę bezpieczeństwa wewnętrznego firmy, opierając się na NIST Cybersecurity Framework.

Global Cybersecurity Policy: Zespół współpracujący z rządami, organizacjami pozarządowymi i partnerami branżowymi w ramach promowania polityki publicznej w zakresie cyberbezpieczeństwa, która umożliwia klientom zwiększanie bezpieczeństwa i odporności dzięki wdrażaniu technologii Microsoft.

Identity and Network Access (IDNA) Security: Zespół pracujący nad ochroną wszystkich klientów Microsoft przed nieautoryzowanym dostępem i oszustwami. To interdyscyplinarny zespół inżynierów, menadżerów produktów, badaczy danych oraz analityków bezpieczeństwa.

M365 Security: Grupa, która opracowuje rozwiązania zabezpieczające, w tym Ochronę punktu końcowego w usłudze Microsoft Defender (MDE), Microsoft Defender for Identity (MDI) i inne, w celu zabezpieczenia klientów korporacyjnych.

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): Rada doradcza w Microsoft, której zadaniem jest zapewnienie, że nowe technologie są opracowywane i wprowadzane na rynek w sposób odpowiedzialny.

Microsoft Bing Search and Distribution: Zespół zajmujący się najwyższej klasy wyszukiwarką internetową umożliwiającą użytkownikom na całym świecie szybkie znajdowanie trafnych wyników wyszukiwania i informacji, w tym śledzenie dopasowanych do nich tematów i trendów, jednocześnie zapewniając kontrolę nad prywatnością.

Microsoft Customer and Partner Solutions: Zespół Microsoft zajmujący się wprowadzaniem rozwiązań na rynek, odpowiedzialny za role takie jak sprzedawcy-specjaliści i sprzedawcy-doradcy w obszarze bezpieczeństwa czy technicznym.

Microsoft Defender Experts: Microsoft to największa na świecie organizacja zorientowana na badania bezpieczeństwa produktów, badania stosowane i analitykę zagrożeń. Grupa Defender Experts zapewnia innowacyjne możliwości wykrywania i reagowania w produktach zabezpieczających Microsoft 365 i usługach zarządzanych przez ekspertów Microsoft Defender.

Microsoft Defender for IoT: Zespół ekspertów dziedzinowych specjalizujących się w inżynierii wstecznej złośliwego oprogramowania, protokołów i oprogramowania układowego IoT/OT. Zespół wyszukuje zagrożenia dla IoT/OT, aby ustalić trendy i kampanie atakujących.

Microsoft Defender Threat Intelligence (RiskIQ): Zespół zapewniający analitykę taktyczną przez analizę obszernych zasobów Microsoft telemetrii zewnętrznej, budowanie krajobrazu zagrożeń w miarę ich ewolucji, w tym wykrywanie nieznanej wcześniej infrastruktury przestępców, i nadający kontekst atakującym i ich kampaniom. Zespół regularnie publikuje aktualne i specyficzne badania, aby dostarczyć obrońcom kluczową analitykę taktyczną.

Microsoft Security Business Development Team: Zespół, który kieruje strategią rozwoju cyberbezpieczeństwa, partnerstwami i strategicznymi inwestycjami Microsoft.

Microsoft Security Response Center (MSRC): Zespół współpracujący z analitykami bezpieczeństwa, zajmujący się ochroną klientów i ekosystemu partnerów Microsoft. Jest on integralną częścią Cyber Defense Operations Center (CDOC) Microsoft. Zrzesza ekspertów ds. reagowania na zdarzenia związane z bezpieczeństwem, którzy wykrywają zagrożenia i reagują na nie w czasie rzeczywistym.

Microsoft Security Services for Incident Response: Grupa ekspertów ds. cyberbezpieczeństwa pomagająca klientom w całym łańcuchu cyberataku — od dochodzenia po skuteczne działania związane z powstrzymywaniem i odzyskiwaniem. Usługi oferowane są przez dwa ściśle współpracujące zespoły: Detection and Response Team (DART), który koncentruje się na badaniach i przygotowywaniu odzyskiwania danych, oraz Compromise Recovery Security Practice (CRSP), który koncentruje się na aspektach związanych z usuwaniem skutków i odzyskiwaniem danych.

Microsoft Threat Intelligence Center (MSTIC): Zespół skupiony na identyfikowaniu i śledzeniu najbardziej wyrafinowanych zagrożeń dla klientów Microsoft oraz gromadzeniu na ich temat danych, w tym grup powiązanych z państwami, złośliwego oprogramowania i ataków wyłudzania informacji.

One Engineering System (1ES): Zespół, którego misją jest dostarczanie światowej klasy narzędzi, które pomagają programistom Microsoft być tak produktywnymi i bezpiecznymi, jak to tylko możliwe. Kieruje on centralną strategią zabezpieczania całego łańcucha dostaw oprogramowania Microsoft.

Operational Threat Intelligence Center (OpTIC): Zespół odpowiedzialny za zarządzanie informacjami o cyberzagrożeniach i rozpowszechnianie ich. Wspiera on misję Microsoft Cyber Defense Operation Center (CDOC) w zakresie ochrony Microsoft i naszych klientów.

Microsoft

Omówienie krajobrazu zagrożeń i wzmocnienie cyfrowej obrony.

- Dowiedz się więcej: **https://microsoft.com/mddr**
- Zyskaj dogłębniejsze informacje: **https://blogs.microsoft.com/on-the-issues/**
- Pozostań w kontakcie: **@msftissues oraz @msftsecurity**