Numer 2/2021 (37)
ISSN 2720-0604

DLP expert

Data Leak Prevention

www.dlp-expert.pl

Jak chronić małe firmy przed zaawansowanymi atakami

Od cyberbezpieczeństwa do cyberodporności

Cyberprzestępcy spędzają w firmowej sieci średnio 11 dni, zanim zostaną wykryci

Ransomware ma już ponad 30 lat

Rynek pracy w cyberbezpieczeństwie

Palantir Technologies (Taki sobie StartUp)

Państwa zachodnie (wedle tradycyjnej, zimnowojennej nomenklatury) z lubością, rzeczy znajomością i bez pardonu szpiegują wszystkich wokół, nie szczędząc nawet swych sojuszników. Poliszynel, który w artykule o figlarnym tytule „A beery European spy club is revealed" (https://www.economist.com/europe/2020/05/28/a-beery-european-spy-club-is-revealed) odkrył kolejny monachijski spisek, tym razem Duńczyków, Szwedów, Niemców i Holendrów, wymierzony w Europę i, w porywach, samego hegemona zza wielkiej wody. Rzecz wyartykułował profesor Bart Jacobs (holenderski profesor informatyki, Uniwersytet im. Radbouda w Nijmegen, Holandia) na łamach owego publikatora.

Od czasu „puczu piwnego" pod auspicjami pewnego malarza pokojowego, poprzez geszeft, dyktatem monachijskim zwany, Monachium stało się miejscem fatalnym. Bürgerbräukeller, który onegdaj gościł ekipę Austriaka, zostało zburzone w 1979 r., ale podobny wyszynk (Alkoholausschank), zwany Maximator, przygarnął w tymże 1979 roku ową czwórkę kolejnych spiskowców, tym razem fachowców.

Czwórka owa zawarła sojusz zwany nomen omen Maximator. Pracę myślową wykonali też potem Francuzi i do Maximatora doszlusowali w 1985 r. Ferajna owa egzystuje do dziś. Obok Maximatora funkcjonują jeszcze Seniors Europe (obsługuje Hiszpanię, Norwegię, Belgię i Italię), Five Eyes (Stany Zjednoczone, Wielka Brytania, Kanada, Australia i Nowa Zelandia) itp., ale Maximator jest najmniej znany z nich.

Szwedzka firma Crypto AG, ówczesny monopolista, dostarczała urządzenia szyfrujące wszystkim zainteresowanym. Nieliczni tylko wiedzieli, że właścicielem owego przedsięwzięcia jest CIA oraz BND (https://en.wikipedia.org/wiki/Crypto_AG), więc korespondencja via maszyny Crypto AG tajemnic wobec Maximatora nie miała i nie ma. O ile Maximator był prekursorem, to Echelon, Carnivore (późniejszy Omnivore) są już systemami o zasięgu globalnym. Słyszą i analizują wszystko.

Palantir zaś jest kompanią i zarazem technologią (wedle nowomowy), która sprzedaje oprogramowanie do pracy z masywami danych (Big Data) sensu stricto. Dane o działaniach militarnych w Afganistanie poprzez status szefów kompanii energetycznych (OPEC czy Gazprom...) są żerem decydentów na poziomie strategicznym (Blinken and Co., dajmy na to). Im są potrzebne dane przetworzone do postaci przydatnej w procederze decyzyjnym. Tym bardziej, że w przestrzeni informacyjnej świata dominują dane klasy Big Data.

A tu działa Palantir. Filozofię tej firmy określił prof. Jürgen Habermas (https://en.wikipedia.org/wiki/Jürgen_Habermas), którego sentencję „Nikt nie wie na pewno, kto jest jego wrogiem" cytuje „The Economist". Komu to i po co? Ano komuś, kto zainwestował w ową kompanię ~$3x10^9 za ok. 17 lat jej egzystencji.

Wedle tygodnika The Economist (https://www.economist.com/business/2020/08/27/palantirs-stockmarket-prospectus-reveals-both-losses-and-promise) zapotrzebowanie na jej usługi ma się dobrze, a nawet lepiej.

Nic dziwnego: w tym powodzeniu bowiem twór Alexa Karpa, stwórcy i szefa Palantir Technologies (obronił dysertację o agresji w polityce we frankfurckim Uniwersytecie im Goethego) opracowuje, za pomocą projektów Gotham i Metropolis, masywy danych dostarczanych przez PRISM (https://pl.wikipedia.org/wiki/Prism_(program_szpiegowski)).

A jak to się ma do naszego DLP? Ano ma się wprost. Twoje, dyrektorze, dane wędrują do chmury (taki trynd, wicie, rozumicie), która to chmura obsługiwana jest przez ów Palantir, a koszyk, w którym umieściłeś swe dane (jaja, znaczy), jest gdzieś... hen, hen. Zaszyfrowałeś dane? No problem. Algorytmy stworzyliśmy i tworzymy MY! Przesłałeś via routery Cisco? To też MY! Nie dziw się więc, że kontrakt przeszedł Ci koło nosa.

Bo supermonopol informacyjny Stanów Zjednoczonych (Oracle, Hewlett-Packard, Xerox, Yahoo!, Intel, eBay, Cisco, Adobe, AMD, Alphabet, Facebook, Twitter, Instagram czy M$) istnieje, a Twoja, dyrektorze, firma i Ty sam jesteście więźniami cyfrowego obozu koncentracyjnego.

„It's Not Personal, It's Just Business" - The Godfather
Redakcja DLP

DLP Expert
kwartalnik
numer 2/2021 (37)
lipiec 2021

ISSN
2720-0604

Wydawca
DLP Expert Sp. z o.o.
ul. Leszczyńskiego 4 lok. 25
50-078 Wrocław
tel. 71 722 76 15
fax: 71 735 18 82
e-mail: redakcja@dlp-expert.pl
www.dlp-expert.pl

Przygotowanie DTP
Batorski Poligrafia
www.batorski.pl
firma@batorski.pl

Redaktor naczelny
Piotr Domagała

Redaktor techniczny
Grzegorz Grodzki

Spis treści

Dane 533 milionów użytkowników Facebooka wyciekły

3.04.2021 r. - W kwietniu w serwisie Niebezpiecznik można było przeczytać, że na jednym z forum dla hakerów ktoś udostępnił bazę zawierającą dane ponad 533 milionów użytkowników Facebooka, z czego ponad 2,5 miliona należało do Polaków. Plik nie zawierał haseł (ani ich hashów) ani wiadomości prywatnych.

Przedstawiciel Facebooka potwierdził, że zbiór powstał w wyniku wykorzystania błędu, który Facebook załatał w 2019 roku. Redaktorzy Niebezpiecznika ustalili, że część z osób znajdujących się w ujawnionym pliku nigdy publicznie nie prezentowało swojego adresu e-mail ani numeru telefonu. Błąd musiał więc pozwalać na pozyskanie danych co najmniej z poziomu „dla znajomych".

Plik zawierał poniższe dane:

- imię i nazwisko,
- numer telefonu komórkowego,
- adres e-mail (nie zawsze),
- płeć,
- stan cywilny,
- zawód,
- miasto.

Plik ważył ponad 400 MB i zawierał 2 669 381 rekordów. Nie wiadomo, dlaczego wyciek nie objął większej liczby Polaków — być może przyczyniły się do tego jakieś specyficzne ustawienia

prywatności. Zawartość pliku z danymi jest posortowana po numerach telefonów, więc możliwe, że ktoś zwyczajnie sprawdzał, czy kolejne numery telefonów zwracają w Facebooku jakiekolwiek dane użytkowników. W 2019 trafiono[1] nawet na bazę, która miała być w ten sposób „zebrana" — niewykluczone, że to jest właśnie ta baza.

Chociaż w pliku nie ma ani haseł, ani wiadomości prywatnych, redakcja serwisu niebezpiecznik.pl podpowiada, że warto ten incydent potraktować jako impuls do pokasowania takich danych z konta w serwisie Facebook, które po upublicznieniu mogłyby wywołać u nas jakąś formę dyskomfortu.

[1] *https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/*

Cring, oprogramowanie wymuszające okup, infekuje obiekty przemysłowe

7.04.2021 r. - Na początku 2021 r. cyberprzestępcy przeprowadzili serię ataków przy użyciu oprogramowania wymuszającego okup, o nazwie Cring. Poinformował o tym zespół CSIRT szwajcarskiego dostawcy usług telekomunikacyjnych, Swisscom, jednak sposób, w jaki oprogramowanie ransomware infekowało sieć organizacji, pozostawał nieznany. Badanie incydentu, który wystąpił w jednym z zaatakowanych przedsiębiorstw, przeprowadzone przez ekspertów z zespołu ICS CERT firmy Kaspersky, wykazało, że ataki przy użyciu oprogramowania Cring wykorzystują lukę w zabezpieczeniach serwerów VPN. Wśród ofiar znajdują się przedsiębiorstwa przemysłowe w państwach europejskich. W co najmniej jednym przypadku atak z wykorzystaniem ransomware spowodował tymczasowe zamknięcie zakładu produkcyjnego.

W 2019 roku ujawniono lukę CVE-2018-13379[2] w serwerach VPN Fortigate. Mimo pojawienia się łaty[3] nie wszystkie urządzenia zostały zaktualizowane – i od jesieni 2020 r. na forach darkwebu zaczęły pojawiać się oferty zakupu gotowej listy zawierającej adresy IP urządzeń podatnych na ataki. Dzięki nim nieuwierzytelniony atakujący może połączyć się z urządzeniem za pośrednictwem internetu i uzyskać zdalny dostęp do pliku sesji, który zawiera nazwę użytkownika i hasło przechowywane w postaci niezaszyfrowanego tekstu.

Badanie incydentu przeprowadzone przez ekspertów z zespołu ICS CERT firmy Kaspersky wykazało, że w serii ataków z użyciem oprogramowania Cring ugrupowanie cyberprzestępcze uzyskało dostęp do sieci przedsiębiorstwa z wykorzystaniem luki CVE-2018-13379. Dochodzenie wykazało, że na jakiś czas przed główną fazą operacji przestępcy wykonali połączenia testowe z bramą sieci VPN, najwyraźniej w celu upewnienia się, że skradzione dane uwierzytelniające użytkowników do sieci VPN są nadal ważne.

W dniu ataku, po uzyskaniu dostępu do pierwszego systemu w sieci przedsiębiorstwa, atakujący wykorzystali narzędzie Mimikatz w celu kradzieży poświadczeń kont użytkowników systemu Windows, którzy wcześniej logowali się do zhakowanego systemu. Przestępcom udało się następnie włamać do konta administratora domeny, po czym zaczęli przenikać do innych systemów w sieci organizacji dzięki temu, że administrator posiadał prawa dostępu do wszystkich systemów z jednego konta użytkownika.

Po przeprowadzeniu rekonesansu i przejęciu kontroli nad systemami, które były istotne dla operacji przedsiębiorstwa przemysłowego, cyberprzestępcy pobrali i uruchomili oprogramowa-

nie wymuszające okup — Cring.

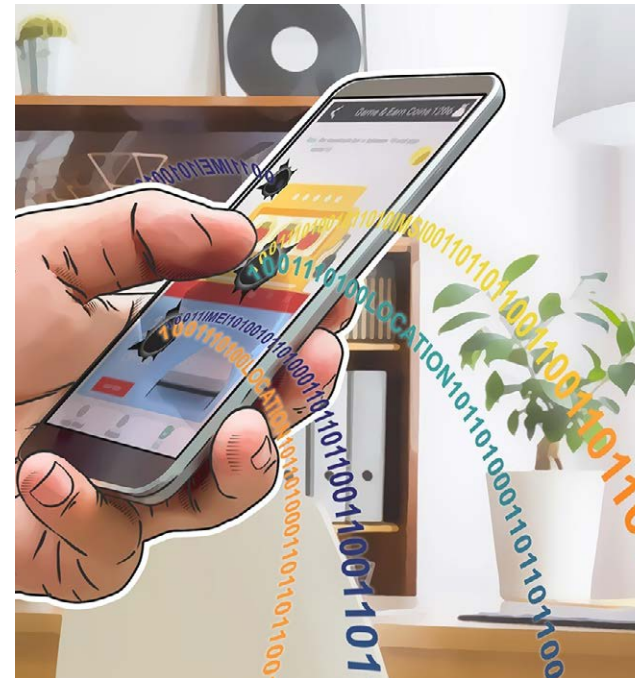
Według badaczy z firmy Kaspersky kluczową rolę odegrało również to, że nie uaktualniono na czas bazy danych rozwiązania bezpieczeństwa wykorzystywanego w atakowanych systemach, przez co ochrona nie była w stanie wykryć ani zablokować zagrożenia. Ponadto wyłączone zostały niektóre komponenty rozwiązania antywirusowego, co jeszcze bardziej obniżyło jakość zabezpieczeń.

[2] *https://nvd.nist.gov/vuln/detail/CVE-2018-13379*

[3] *https://www.fortinet.com/blog/psirt-blogs/update-regarding-cve-2018-13379*

Połowa klientów trzymałaby się z daleka od dostawcy usług online, u którego doszło do incydentu naruszenia bezpieczeństwa danych

8.04.2021 r. – Jeden na dwóch klientów (50%) nie chciałby mieć dłużej do czynienia z dostawcą usług online, który padł ofiarą jakiegokolwiek incydentu naruszenia bezpieczeństwa danych – wynika z badania obejmującego 15 000 klientów na całym świecie przeprowadzonego przez firmę Kaspersky. Respondenci byliby jeszcze bardziej rozgoryczeni, gdyby okazało się, że można było uniknąć takiego incydentu – 63% ankietowanych zrezygnowałoby z korzystania z usług takiego dostawcy z obawy, że ich dane mogłyby zostać sprzedane osobom trzecim. Ponieważ klienci mają coraz większą świadomość spoczywających na firmach obowiązków dotyczących zapewnienia prywatności danych, firmy muszą być bardziej transparentne w zakresie postępowania z danymi użytkowników.



Konieczność dokonywania zakupów, korzystania z rozrywki, komunikowania się czy prowadzenia biznesu online sprawiła, że jesteśmy bardziej świadomi, jak wiele danych udostępniamy i jakie to może mieć konsekwencje. Niemal dwie trzecie (62%) respondentów obawia się, że ich aktywność online jest nieustannie śledzona przez odwiedzane przez nich strony internetowe lub serwisy.

50% konsumentów zrezygnowałoby z dostawcy usług online, gdyby zostało naruszone bezpieczeństwo ich danych. Co więcej, ogromna część już teraz domaga się większej ochrony swoich danych zarówno od przedsiębiorstw, jak i rządów. Około połowa (51%) chce przejrzystości odnośnie przetwarzania danych przez firmy, podczas gdy 48% uważa, że firmy powinny być jednakowo otwarte, jeśli chodzi o sposób działania ich technologii. Podobnie 50% domaga się od rządów transparentności w zakresie procesów gromadzenia danych i zarządzania nimi.

Nie oznacza to, że klienci są przeciwni przetwarzaniu danych w ogóle. 68% przyznaje, że aplikacje oraz usługi cyfrowe, z jakich korzystają, znacznie ułatwiają im życie. Jednak dodatkowa ostrożność wydaje się zrozumiała, zważywszy na to, że więcej niż jedna na dziesięć osób (12%) doświadczyła sytuacji, w której jej dane osobowe wyciekły lub zostały udostępnione osobie trzeciej, w wyniku czego doszło do ujawnienia poufnych informacji (64%) lub utraty pieniędzy (62%).

Pełny raport wykorzystany w tek informacji prasowej jest dostępny na stronie http://r.kaspersky.pl/aJxas.

Nowy atak na mandat karny

9.04.2021 r - Serwis niebezpiecznik.pl poinformował o nowym ataku. Polacy otrzymują SMS-y informujące ich o niezapłaconym mandacie karnym w wysokości 10 PLN i skierowaniu sprawy do sądu w przypadku jego nieuregulowania.

SMS od MandatKarny

Kliknięcie łącza znajdującego się w SMS-ie przenosi ofiarę na fałszywą stronę podszywającą się pod bramkę płatności PayU.

Jeśli ofiara nie zorientuje się, że jest na złej stronie, wybierze bank oraz poda login i hasło do swojego konta, zostanie poproszona o kod SMS.

Podanie kodu SMS umożliwia atakującym kradzież środków z naszego konta, dlatego jeśli ktoś otrzymał taką wiadomość, kliknął łącze i podał swoje dane logowania, powinien jak najszybciej zadzwonić na infolinię swojego banku i poinformować o tej sytuacji.

Kaspersky zabezpieczył ponad 9 000 klientów przed atakami z zainfekowanego sklepu z aplikacjami mobilnymi

12.04.2021 r. - Eksperci z firmy Kaspersky wykryli szkodliwy kod w wersji 3.17.18 oficjalnego klienta sklepu z aplikacjami APKPure dla systemu Android. Do chwili obecnej zagrożenie zostało wykryte i zablokowane na urządzeniach mobilnych niemal 9 400 użytkowników produktów firmy Kaspersky.

Według badaczy szkodliwy kod został wykryty w module odpowiedzialnym za wyświetlanie reklam w aplikacji. Pojawił się tam najprawdopodobniej w wyniku współpracy producenta z nieetyczną organizacją reklamową. Podobny przypadek miał miejsce w ramach incydentu z aplikacją CamScanner, gdy zastosowano nowy pakiet reklamowy od niezweryfikowanego dostawcy.

Szkodliwy kod osadzony w aplikacji APKPure działa następująco: po uruchomieniu programu dochodzi do deszyfrowania i aktywacji modułu cyberprzestępczego, który następnie gromadzi informacje o urządzeniu i wysyła je do serwera kontrolowanego przez atakujących. Następnie ładowany jest trojan, który cechuje się szeregiem możliwości – od wyświetlania i automatycznego klikania reklam po rejestrowanie użytkownika w płatnych usługach subskrypcyjnych i pobieranie innych szkodliwych programów.

Następnie, w zależności od odpowiedzi serwera kontrolowanego przez cyberprzestępców, trojan może:

- wyświetlać reklamy po każdym odblokowaniu urządzenia,
- otwierać seryjnie reklamy na kolejnych zakładkach przeglądarki,
- ładować dodatkowe moduły wykonywalne.

8 kwietnia badacze z firmy Kaspersky zgłosili incydent sklepowi z aplikacjami. Następnego dnia sklep poinformował, że problem zostanie usunięty w nowej wersji. Stało się tak wraz z publikacją wersji 3.17.19, która jest już dostępna do pobrania.

Produkty firmy Kaspersky wykrywają omawiane zagrożenie jako HEUR:Trojan-Dropper.AndroidOS.Triada.ap.

Kaspersky wykrywa lukę dnia zerowego w systemowym procesie Desktop Window Manager

13.04.2021 r. - Na początku 2021 r. badacze z firmy Kaspersky, po wnikliwej analizie szkodliwego modułu cybergangu BITTER wykorzystującego znaną już podatność CVE-2021-1732[4], zidentyfikowali kolejną lukę dnia zerowego. Eksperci nie są obecnie w stanie powiązać aktywności cyberprzestępców stojących za narzędziem wykorzystującym tę lukę w procesie Desktop Windows Manager systemu Windows z żadnym znanym cybergangiem.

Luki dnia zerowego to nieznane błędy w oprogramowaniu. Zanim zostaną zidentyfikowane, mogą służyć cyberprzestępcom do prowadzenia wielu szkodliwych działań, które mogą mieć nieprzewidywalne i destrukcyjne konsekwencje. Zidentyfikowana przez badaczy z firmy Kaspersky podatność występuje w procesie Desktop Windows Manager systemu Windows i została zgłoszona firmie Microsoft w lutym 2021 r. Po potwierdzeniu luce nadano sygnaturę CVE-2021-28310.

Według badaczy z firmy Kaspersky luka ta jest wykorzystywana do przeprowadzania ataków przez kilka różnych cybergangów. Podatność umożliwia atakującym podniesienie uprawnień w systemie ofiary i wykonanie w nim dowolnego kodu. Wstępne wyniki dochodzenia firmy Kaspersky nie umożliwiają zidentyfikowania pełnego łańcucha infekcji, dlatego na chwilę obecną nie wiadomo, czy szkodliwy moduł wykorzystujący nową lukę jest stosowany wraz z innymi narzędziami.

Łata usuwająca podatność CVE-2021-28310 została opublikowana[5] 13 kwietnia 2021 r.

Produkty firmy Kaspersky wykrywają szkodliwy kod wykorzystujący nową lukę z następującymi werdyktami: HEUR:Exploit.Win32.Generic, HEUR:Trojan.Win32.Generic, PDM:Exploit.Win32.Generic.

Dalsze szczegóły dotyczące szkodliwych narzędzi wykorzystujących nową podatność są dostępne na stronie https://r.kaspersky.pl/wdNYl.

[4] *https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/*

[5] *https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28310*

CSIRT NASK w 2020 roku: coraz więcej wyłudzeń danych i oszustw w sieci

14.04.2021 r. - Nasze dane logowania do poczty, banku, portalu społecznościowego czy innej usługi online – głównie na takich informacjach zależy w tej chwili internetowym przestępcom. Według obserwacji specjalistów CSIRT NASK, w porównaniu z rokiem 2019 liczba odnotowanych ataków phishingowych w Polsce wzrosła w 2020 roku o 117%.

Zjawisko phishingu to podszywanie się pod inną osobę lub instytucję w celu wyłudzenia loginu i hasła do jakiejś ważnej usługi, np. konta bankowego, poczty elektronicznej lub portalu społecznościowego i właśnie takich incydentów CSIRT

NASK zarejestrował w minionym roku najwięcej – ponad 7,6 tys. Korzystając z możliwości, jakie daje internet, należy zachować podwyższoną czujność i przestrzegać reguł bezpieczeństwa, żeby nie stwarzać cyberprzestępcom okazji do nadużyć. Jest to istotne szczególnie w okresie pandemii, kiedy większość naszej aktywności dzieje się w sieci: praca, nauka, rozrywka, zakupy itp.

Prawie 35 tys. zgłoszeń o naruszeniach w sieci

W 2020 roku eksperci CSIRT NASK zarejestrowali ponad 34,5 tys. zgłoszeń o potencjalnych zagrożeniach cyberbezpieczeństwa, w tym przeanalizowali ponad 10,4 tys. incydentów bezpieczeństwa. Uwagę przestępców zwróciły coraz popularniejsze urządzenia związane z Internetem Rzeczy (IoT). W tym samym czasie odnotowano niemal 6 tys. powiadomień o infekcjach tego typu urządzeń. Jednocześnie przestępcy wykorzystywali ataki przy użyciu szkodliwego oprogramowania – w ubiegłym roku było 746 takich przypadków.

W 2020 roku przy pomocy systemu wymiany informacji o zagrożeniach n6 przetworzono 212 mln zdarzeń bezpieczeństwa, z czego ponad połowa dotyczyła polskich sieci. Na koniec 2020 roku z platformy n6 korzystało 920 organizacji. W tym samym czasie system MWDB umożliwił przeanalizowanie 492 tys. próbek szkodliwego oprogramowania, w tym 22 tys. unikalnych konfiguracji malware.

Coraz więcej materiałów CSAM

Widoczny jest ponadto wzrost liczby incydentów związanych z seksualnym wykorzystywaniem dzieci, na które reaguje Zespół Dyżurnet.pl, działający w strukturach NASK. Na koniec 2020 roku liczba zgłoszeń potencjalnie nielegalnych treści wyniosła 13,4 tys., a liczba zarejestrowanych incydentów CSAM (materiałów prezentujących seksualne wykorzystywanie dzieci) przekroczyła 2,5 tys. 183 sprawy zgłoszono policji, a zdecydowaną większość (91%) treści CSAM usunięto w ciągu 48 godzin.

Już blisko 70 podmiotów w PdC

Coraz więcej podmiotów uczestniczy w koordynowanym przez NASK programie *Partnerstwo dla Cyberbezpieczeństwa*. Na koniec 2020 roku program wspierało blisko 70 partnerów reprezentujących różne sektory gospodarki. Ułatwia on m.in. wymianę informacji (przesyłanie ostrzeżeń, rekomendacji) oraz podejmowanie wspólnych inicjatyw i działań, takich jak organizacja konferencji, szkoleń, warsztatów oraz wystąpień ekspertów. W minionym roku w ramach 9 bezpłatnych szkoleń z cyberbezpieczeństwa przeszkolono 806 pracowników jednostek samorządu terytorialnego z różnych województw.

Zgłoś fałszywą stronę lub incydent zagrażający bezpieczeństwu w sieci

Aby ostrzegać użytkowników przed nadużyciami w sieci, CERT Polska w NASK z inicjatywy Ministerstwa Cyfryzacji pod koniec marca ubiegłego roku uruchomił specjalną podstronę z listą ostrzeżeń przed fałszywymi i przestępczymi stronami. Lista ostrzeżeń jest efektem porozumienia Ministerstwa Cyfryzacji, NASK i UKE z największymi polskimi operatorami komórkowymi. Z informacji o przestępczych stronach mogą korzystać bezpłatnie również wszyscy inni administratorzy, którzy chcą chronić swoich użytkowników przed atakami poprzez strony podszywające się pod znane podmioty czy oferowane usługi. Każdy może tam zgłosić naruszenia oraz zapoznać się z ostrzeżeniami https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/.

Jak oszuści przejmują kosztowne paczki?

15.04.2021 r. - Czytelnik serwisu Niebezpiecznik zamówił w sklepie X-kom kilka laptopów i jako opcję dostawy wybrał kuriera Pocztex. Niestety paczka z zawartością nigdy do niego nie dotarła, bo ktoś odebrał ją przed nim. O tym, że paczka została odebrana, mężczyzna dowiedział się w Urzędzie Pocztowym, i podczas rozmowy z naczelniczką ustalił, co się stało.

Paczkę przejął ktoś, kto zadzwonił do urzędu pocztowego i przedstawił się jako Łukasz – tak właśnie ma na imię ofiara, której historię opisał Niebezpiecznik. Co ważne, oszust zadzwonił z numeru innego niż podany na etykiecie paczki, ale wytłumaczył to faktem, że w celu odbioru paczki podał numer teściowej. Następnie:

1. Oszust powiedział, że chciałby odebrać paczkę na mieście, bo nie będzie go w domu.
2. Zgodnie z ustaleniami kurier spotkał się z oszustem na mieście. Poprosił o dowód, jednak oszust powiedział, że go zapomniał.
3. Kurier „zweryfikował" tożsamość odbierającego paczkę, dzwoniąc na numer telefonu odbiorcy — ale na ten, z którego oszust dzwonił wcześniej, by poinformować, że chciałby umówić się na mieście.

Pan Łukasz usłyszał od naczelniczki UP, że podobny przypadek miał już miejsce w Grodzisku Mazowieckim. Redaktorzy Niebezpiecznika ustalili, że takie kradzieże już się zdarzały i dotyczyły głównie paczek z jednego sklepu. Nie wiadomo, na ile te przypadki są powiązane, ale rysuje się pewien trend. Wygląda na to, że oszuści działają w okolicach Warszawy i mają:

- informację o wartościowych paczkach,
- dane prawowitych odbiorców,
- informacje o sposobie wysyłki.

Dzięki temu mogą dzwonić do kurierów i przejmować cudze paczki. Dostęp do tych informacji ma sprzedawca, firma kurierska, ale potencjalnie również osoby bliskie odbiorcy. Poza tym taki dostęp mają także systemy komputerowe, z których czasami wyciekają informacje o przesyłkach.

Rodzi się pytanie, czy w dzisiejszych czasach weryfikacja przez telefon jest wystarczająca. Przecież zdarza się, że oszuści podszywają się pod cudze numery telefonów, i w tym celu nie muszą nawet klonować karty SIM ofiary.

Problematyczna może też być weryfikacja poprzez dowód osobisty. Pracownik PP nie zawsze będzie w stanie ocenić autentyczność dokumentu, co pokazywały przypadki wyłudzeń Profili Zaufanych przez Envelo. Co istotne, w opisanym przypadku oszust w ogóle nie musiał posiadać dowodu.

Poniżej zamieszczamy komentarz Poczty Polskiej:

(...) o ile dopuszczalne jest doręczenie przesyłki kurierskiej poza miejscem zamieszkania adresata, o tyle – zgodnie z procedurami Poczty Polskiej – musi to nastąpić po uzgodnieniu z adresatem i na jego prośbę, a dodatkowo po uprzednim – nie budzącym wątpliwości – ustaleniu, że osoba zgłaszająca się po odbiór przesyłki jest jej adresatem.

Oczywiście, w przypadku, gdy zostanie stwierdzone niedopełnienie tego obowiązku przez naszego pracownika – w wyniku reklamacji – nadawca lub adresat może liczyć na odszkodowanie. Z uwagi na obowiązujące przepisy, że to nadawca może złożyć reklamację, adresat powinien powiadomić nadawcę o zaistniałych nieprawidłowościach, aby to nadawca tę reklamację złożył. Istnieje też druga droga, zgodnie z którą nadawca może zrzec się na rzecz adresata prawa do dochodzenia roszczeń. (...).

I podpowiedź od rzecznika sklepu X-kom, co w takiej sytuacji może zrobić klient:

Klient może otrzymać zwrot od firmy kurierskiej albo od nas – to jego decyzja. Ja sugerowałbym załatwienie tej sprawy w X-komie. Zależy nam na tym, żeby w takich nieprzyjemnych sytuacjach osoby, które robią u nas zakupy miały jak najmniej dodatkowych obowiązków i straconego czasu. Dlatego też zwykle to my zwracamy pieniądze, a później sami już rozliczamy się z firmą kurierską.

A jeśli ktoś zamawia wartościowy sprzęt i nie chce ryzykować podobnej sytuacji, może wybrać odbiór osobisty.

Nie wiadomo, co dokładnie jest źródłem wiedzy dla oszusta (lub oszustów), ani czy niepokojące sygnały, które dotyczyły znanych przypadków wyłudzeń przesyłek z ostatnich dni, są ze sobą powiązane. Być można kilka osób w okolicy Warszawy niezależnie od siebie wpadło na podobny pomysł i zhakowało jakiś system komputerowy zawierający dane o przesyłkach lub zatrudniło się w sklepach z elektroniką albo na poczcie.

Nowe zagrożenie dla użytkowników WhatsApp. Jakie mogą być konsekwencje?

DAGMA BEZPIECZEŃSTWO IT

16.04.2021 r. – Użytkownicy popularnego komunikatora WhatsApp muszą być czujni wobec perspektywy nowych ataków. Tym razem hakerzy mogą zawiesić dowolne konto, używając wyłącznie numeru powiązanego z nim telefonu. – To zagrożenie, którego nie należy lekceważyć. W czasie, gdy coraz więcej osób komunikuje się i pracuje zdalnie, możliwość blokady konta dowolnego użytkownika to spore zagrożenie – przestrzegają specjaliści ds. cyberbezpieczeństwa ESET.

Mechanizm nowego, potencjalnego ataku jest dość prosty. Zdaniem przedstawicieli WhatsApp można się przed nim chronić, podając adres e-mail w ustawieniach dwustopniowej weryfikacji. Pojawiają się jednak głosy, że aby zapewnić użytkownikom pełne bezpieczeństwo, luka w domyślnym procesie weryfikacji powinna zostać usunięta.

Jak działa mechanizm ataku? Kiedy po raz pierwszy następuje proces konfigurowania konta WhatsApp, na urządzeniu pojawia się prośba o podanie swojego numeru telefonu, na który wysyłany jest kod weryfikacyjny. Jeśli jakaś osoba będzie chciała użyć dowolnego, nienależącego do niej numeru telefonu w procesie weryfikacji, może to zrobić. Gdy go poda, pełnoprawny właściciel telefonu otrzyma wiadomości od WhatsApp z kodem weryfikacyjnym, wraz z zastrzeżeniem, aby nie przekazywać go nikomu. Przestępca jest w stanie aktywować ten mechanizm wielokrotnie, podczas gdy nieświadomy użytkownik może traktować ciągłe monity jako błąd aplikacji. Żądania spowodują ograniczenie przez WhatsApp liczby wysyłanych kodów poprzez zablokowanie kodów po kilku błędnych próbach na okres 12 godzin. Blokada wpłynie również na użytkownika, chociaż może on tego nie zauważyć, chyba że wyloguje się w międzyczasie z aplikacji.

W następnym kroku, atakujący tworzy nowy adres e-mail i wysyła wiadomość mailową do zespołu pomocy WhatsApp w temacie rzekomo „zgubionego" lub „skradzionego telefonu", prosząc o dezaktywację numeru prawowitego właściciela konta. Platforma weryfikuje „tożsamość" atakującego tylko poprzez wysłanie automatycznej wiadomości e-mail z żądaniem ponownego podania numeru. Jeśli atakujący to zrobi, WhatsApp zawiesi wówczas konto właściciela telefonu. A ponieważ został osiągnięty limit prób weryfikacji, użytkownik nie będzie mógł się zalogować, dopóki nie upłynie 12 godzin. Niestety, jeśli osoba atakująca użyje 12-godzinnego cyklu trzy razy z rzędu, WhatsApp zamiast informować użytkownika powiadomieniem „spróbuj ponownie po 12 godzinach", ulegnie awarii i wyświetli komunikat „spróbuj ponownie po -1 sekundach". Jeśli cyberprzestępca dotrze do tego momentu, nie będzie możliwości odzyskania konta bez pomocy konsultantów WhatsApp.

Specjaliści ds. cyberbezpieczeństwa ESET już w ubiegłymroku wskazywali, jak ktoś może przejąć kontrolę nad kontem WhatsApp, znając tylko numer telefonu użytkownika. Teraz podkreślają, że luki w procesie weryfikacji nie należy lekceważyć, zwłaszcza że może mieć wpływ na miliony użytkowników.

Pięć przełomowych zmian we współczesnych atakach ransomware

19.04.2021 r. - W ciągu kilku ubiegłych lat metody wykorzystywane przez cyberprzestępców w atakach z użyciem ransomware uległy znacznej zmianie. Podczas gdy dawniej atakujący dążyli do zaszyfrowania danych jak największej liczby użytkowników, obecnie ich działania są znacznie bardziej precyzyjne – przestępcy szczegółowo badają każdy cel, szukając słabych punktów. Zaawansowane cybergangi działają niemal jak dostawcy usług online, stosując tradycyjne mechanizmy marketingowe. Na bazie działań grupy przestępczej Darkside badacze z firmy Kaspersky zidentyfikowali pięć przykładów tej transformacji.

1. Członkowie cybergangu Darkside aktywnie nawiązują kontakty z mediami. Na swojej stronie zamieścili stosowną sekcję, w której dziennikarze mogą zadawać pytania i otrzymywać informacje z pierwszej ręki, a także sprawdzać na bieżąco, które z danych skradzionych w ramach ataków będą w najbliższym czasie ujawniane. Wyraźnie widać, że cyberprzestępcy chcą uzyskać jak najwięcej rozgłosu w internecie.
2. Grupy wykorzystujące narzędzia ransomware współpracują z firmami oferującymi usługi deszyfrowania danych. Dzieje się tak dlatego, że wiele firm z sektora publicznego ma zakaz negocjowania z cyberprzestępcami. Z tego powodu powstało zapotrzebowanie na swego rodzaju pośredników, którzy działają legalnie i oferują usługi odzyskania danych po ataku, a w rzeczywistości po prostu płacą przestępcom okup w imieniu ofiary.
3. Członkowie cybergangu Darkside utrzymują, że przekazują część swoich zysków na cele charytatywne. W ten sposób pokazują ofiarom ataków, które nie chcą finansować działalności przestępczej, że część ich pieniędzy trafi na słuszny cel. Warto wiedzieć, że w wielu przypadkach organizacje charytatywne nie mogą przyjmować pieniędzy od takich ugrupowań i przelewy będą zamrażane. O ile w ogóle zostaną wykonane.
4. Cyberprzestępcy uważnie analizują skradzione dane i rynek. Przed opublikowaniem informacji zdobytych od ofiary, która nie zapłaciła okupu, atakujący sprawdzają jej kontakty i identyfikują dobrze znanych klientów, partnerów, a także konkurencję. Badacze z firmy Kaspersky uważają, że głównym celem tych działań jest maksymalizacja szkód i zastraszenie ofiar, a tym samym zwiększenie szans na otrzymanie okupu.
5. Grupa Darkside funkcjonuje zgodnie z własnymi zasadami etycznymi, tak jak prawdziwe korporacje. Przestępcy utrzymują, że nigdy nie atakują firm z sektora medycznego, zakładów pogrzebowych, instytucji edukacyjnych oraz organizacji non-profit i rządowych.

Więcej informacji na temat zmian w działaniu cybergangów stosujących ataki ransomware znajduje się na oficjalnym blogu firmy Kaspersky – Kaspersky Daily: https://kas.pr/9np1.

Wyciekły dane osobowe ponad 20 000 policjantów, strażaków, celników, pograniczników

20.04.2021 r. - Jeden z użytkowników serwisu ArcGIS poszukiwał w nim informacji na temat szczepień. Tak natknął się na ciekawy plik. O swoim znalezisku poinformował portal niebezpiecznik.pl.

Plik programu Excel zawierał dane osobowe ponad 20 000 funkcjonariuszy publicznych: policjantów (także z CBŚP), celników, pracowników Służby Ochrony Państwa, Administracji Skarbowej, Straży Granicznej, Straży Pożarnej (także ochotniczej), Inspekcji Transportu Drogowego, Straży Miejskiej, a nawet SOK-u czy Służby Więziennej.

Udostępniony plik składa się z 2 arkuszy zawierający poniższe dane:

- imię i nazwisko,
- adres e-mail,
- numer telefonu,
- pełna nazwa jednostki,
- adres (ulica i numer budynku, kod pocztowy, miejscowość),
- imię i nazwisko pracownika,
- numer telefonu komórkowego do pracownika,
- PESEL pracownika,
- seria i numer dowodu tożsamości / paszportu (na szczęście ta kolumna była pusta),
- CreationDate.

Na liście znaleźli się funkcjonariusze i pracownicy różnych rządowych instytucji, których zgłoszono do szczepień w okresie od 12-20 kwietnia 2021 r.

Co prawda w opisywanym wycieku danych nie znalazły się ich prywatne adresy zamieszkania, ale w przypadku niektórych osób dostępne są numery telefonów komórkowych, które są tzw. uni-

katowym identyfikatorem i występują także w innych wyciekach danych (np. z Facebooka czy z Morele). Na podstawie numeru komórki ktoś może uzupełnić brakujące dane osobowe konkretnego funkcjonariusza o np. jego adres zamieszkania, pod jaki w przeszłości zamówił przesyłkę podczas zakupów w internetowym sklepie, którego baza danych wyciekła.

Pozytywnym dla funkcjonariuszy aspektem tej sprawy jest to, że plik mogli pobrać tylko zalogowani użytkownicy ArcGIS-u, którzy zazwyczaj są etycznymi badaczami, choć warto podkreślić, że konto na tej platformie założyć może każdy. Do policjantów wysłano stosowne ostrzeżenie, a Policja zobowiązała się do refundacji opłat za wykupienie alertu BIK dla pracowników, których dane znalazły się na liście.

Ze wszystkich dostępnych informacji można wywnioskować, że Rządowe Centrum Bezpieczeństwa najprawdopodobniej wykorzystywało do zbierania danych narzędzie survey123.arcgis.com. Pozwala ono na uproszczenie procesu zbierania danych — osoby wypełniające formularz nie muszą posiadać konta w ArcGIS, aby móc go uzupełnić i przekazać dane. Taka otwartość formularza ma jednak swoje konsekwencje — plik, do którego zbiera się dane, ma charakter publiczny. Najprawdopodobniej taka była geneza opisywanego przypadku wycieku.

Zaawansowane cybergangi coraz częściej wykorzystują luki w zabezpieczeniach

27.04.2021 r. - Eksperci z firmy Kaspersky podsumowali ewolucję zaawansowanych cyberataków w I kwartale 2021 r. W ostatnich trzech miesiącach największe fale aktywności APT napędzane były atakami na łańcuch dostaw oraz lukami dnia zerowego. W wyniku złamania zabezpieczeń w oprogramowaniu Orion firmy SolarWinds służącym do monitorowania infrastruktur IT w ponad 18 000 sieciach klientów zainstalowany został niestandardowy trojan dający zdalny dostęp, z kolei luka w zabezpieczeniach Microsoft Exchange Server spowodowała nowe kampanie ataków w Europie, Rosji oraz Stanach Zjednoczonych.

Zaawansowani cyberprzestępcy nieustannie zmieniają swoje taktyki i udoskonalają narzędzia. Aby użytkownicy oraz organizacje wiedzieli, na jakie zagrożenia są narażeni, Globalny Zespół ds. Badań i Analiz firmy Kaspersky (GReAT) tworzy kwartalne raporty dotyczące najistotniejszych trendów w krajobrazie zaawansowanych długotrwałych zagrożeń (APT). W ostatnim raporcie eksperci zwrócili uwagę na dwie główne fale aktywności.

Pierwsza z nich spowodowana była złamaniem zabezpieczeń w oprogramowaniu Orion firmy SolarWinds służącym do monitorowania infrastruktur IT. Umożliwiło to zainstalowanie niestandardowego backdoora o nazwie Sunburst w sieciach ponad 18 000 klientów. Wśród nich znajdowały się duże korporacje oraz organy rządowe w Ameryce Północnej, Europie, na Bliskim Wschodzie oraz w Azji.

Drugą falę aktywności zapoczątkowały załatane już luki dnia zerowego w rozwiązaniu Microsoft Exchange Server. Na początku marca luki te wykorzystało nowe ugrupowanie APT o nazwie HAFNIUM w celu przeprowadzenia serii ataków. W pierwszym tygodniu marca cel ataków stanowiło około 1 400 unikatowych serwerów, większość w Europie i Stanach Zjednoczonych. Biorąc pod uwagę, że niektóre serwery były atakowane kilkukrotnie, wydaje się, że luki te są obecnie wykorzystywane przez różne ugrupowania. W połowie marca badacze z firmy Kaspersky zidentyfikowali kolejną kampanię wykorzystującą te same exploity w Rosji. Wykazywała ona pewne powiązania z HAFNIUM, jak również z nieznanymi wcześniej działaniami atakujących badanych przez firmę Kaspersky.

Odnotowano ponadto nową aktywność, za którą odpowiadało niesławne ugrupowanie APT o nazwie Lazarus – również z wykorzystaniem luki dnia zerowego. Tym razem cybergang zastosował socjotechnikę, aby nakłonić badaczy bezpieczeństwa do pobrania zainfekowanego pliku projektu Visual Studio lub zwabić ofiary na swojego bloga, po to by instalować program wykorzystujący luki w przeglądarce Chrome. Przynęty często dotyczyły luk dnia zerowego i wydaje się, że celem ataku była kradzież badań dotyczących błędów w zabezpieczeniach. Pierwsza fala miała miejsce w styczniu, druga w marcu. Aby skutecznie „nabrać" ofiary, połączono to z nową falą fałszywych profili na mediach społecznościowych oraz fałszywą firmą.

Po dokładniejszej analizie badacze z firmy Kaspersky zauważyli, że wykorzystany w kampanii szkodnik pasuje do ThreatNeedle[6], backdoora stworzonego przez ugrupowanie Lazarus, który ostatnio został zauważony w atakach na branżę obronną w połowie 2020 r.

W innej, określanej jako TurtlePower, interesującej kampanii wykorzystującej luki dnia zerowego, która jest prawdopodobnie powiązana z ugrupowaniem BitterAPT, atakowane były podmioty rządowe oraz z branży telekomunikacyjnej w Pakistanie i Chinach. Odpowiedzialny za tę załataną już lukę w zabezpieczeniach wydaje się być „Moses" – broker, który w ciągu dwóch ostatnich lat stworzył co najmniej pięć programów partnerskich wykorzystujących luki w zabezpieczeniach, z czego niektóre zostały wykorzystane zarówno przez ugrupowanie BitterAPT, jak i DarkHotel.

Więcej informacji na temat krajobrazu zaawansowanych cyberzagrożeń w pierwszym kwartale 2021 r. znajduje się na stronie https://r.kaspersky.pl/WXVJW.

[6] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3371/zaawansowany-cybergang-lazarus-bierze-na-celownik-przemysl-obronny*

Badacze ESET odkryli EmissarySoldier, nową kampanię grupy LuckyMouse – na celowniku organizacje rządowe, przedsiębiorstwa i banki na całym świecie

DAGMA BEZPIECZEŃSTWO IT

29.04.2021 r. - Organizacje rządowe i przedsiębiorstwa potrzebują wsparcia w walce z cyberatakami, a jednym z największych zagrożeń są obecnie grupy APT, takie jak LuckyMouse – wynika z najnowszego raportu ESET, który zaprezentowano 28 kwietnia, podczas wirtualnej konferencji ESET European Cybersecurity Day.

Unia Europejska, jej strategia w zakresie cyberbezpieczeństwa, a także rządy na całym świecie zmagają się z poważnymi wyzwaniami z zakresu cyberprzestępczości. Przeniesienie wielu dziedzin życia do sfery wirtualnej, pandemia COVID-19 i związany z nią zdalny tryb pracy, wprowadzony niemal w każdym przedsiębiorstwie i organizacji, a także cyberszpiegostwo, złośliwe oprogramowanie ransomware czy ataki na łańcuchy dostaw – to tylko niektóre z nich. Największym, wspólnym wrogiem dla wszystkich rządów okazują się jednak zaawansowane grupy cyberwywiadowcze APT (Advanced Persistent Threats).

Grupy APT wykorzystują udoskonalone narzędzia

Najnowszy raport branżowy ESET opisuje zagrożenia przygotowywane przez grupy APT i podkreśla ich złożoną naturę. Eksperci zwracają szczególną uwagę na EmissarySoldier, nową kampanię przeprowadzoną przez grupę LuckyMouse za pomocą zestawu narzędzi SysUpdate. Jej celem jest przejęcie kontroli nad komputerami, z których część korzystała z popularnej aplikacji Microsoft SharePoint.

LuckyMouse wykorzystuje nierozpracowany dotąd zestaw narzędzi SysUpdate – którego pierwsze próbki odkryto w 2018 roku, jednak od tego czasu przeszedł on różne etapy rozwoju. Obecnym sposobem działania grupy cyberprzestępców jest instalowanie złośliwego oprogramowania z wykorzystaniem trzech komponentów: legalnej aplikacji podatnej na przechwytywanie wywołań DLL, szkodliwego kodu binarnego zakodowanego dodatkowo w Shikata Ga Nai oraz niestandardowej biblioteki DLL ładującej ten złośliwy kod.

Ponieważ modułowa architektura SysUpdate umożliwia przestępcom ograniczenie ekspozycji złośliwych komponentów do minimum, kompleksowa analiza zagrożenia jest dość trudna. Niezależnie od tego, LuckyMouse zwiększył swoją aktywność w 2020 roku, najwyraźniej przechodząc przez proces, w którym różne nowe funkcje były stopniowo integrowane z zestawem narzędzi SysUpdate.

Ewolucja narzędzi wykorzystywanych przez grupy APT, takie jak LuckyMouse, powinna znajdować się pod szczególną obserwacją. To na organizacjach rządowych spoczywa odpowiedzialność za zapewnienie bezpieczeństwa oraz stabilności obywatelom, środowisku biznesowemu i relacjom międzynarodowym. Te zadania mogą być zagrożone, skoro LuckyMouse i inne grupy APT, a także podmioty państwowe i ich współpracownicy, korzystają z popularnych platform współpracy, takich jak Microsoft SharePoint i domyślnie cyfrowo świadczone usługi.

Rząd w centrum uwagi

W latach 2020 i 2021 ESET zaangażował się w kilka projektów współpracy badawczej, w tym między innymi z Europejską Organizacją Badań Jądrowych (CERN), Europolem i francuską Narodową Agencją Cyberbezpieczeństwa (ANSSI). Wnioski z nich, przedstawione podczas wirtualnego wydarzenia oraz w raporcie, wskazują, że rządy i ich infrastruktura IT znajdują się stale na celowniku cyberprzestępców.

Raport podkreśla potrzebę dalszego, technologicznego wspierania rządów w usuwaniu luk w zabezpieczeniach, wykrywaniu zagrożeń oraz monitorowaniu taktyk, technik i procedur grup APT za pośrednictwem dostępnych narzędzi.

Raport w wersji angielskiej można znaleźć na stronie: https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf

Operacja TunnelSnake: nieznany wcześniej rootkit wykorzystywany do kontrolowania sieci firm w Azji i Afryce

kaspersky

6.05.2021 r. - Badacze z firmy Kaspersky wykryli TunnelSnake – aktywną kampanię APT prowadzoną od 2019 r., której celem były regionalne placówki dyplomatyczne w Azji oraz Afryce. Atakujący zastosowali nieznanego wcześniej rootkita o nazwie Moriya. Szkodnik ten, posiadający niemal całkowitą kontrolę nad systemem operacyjnym, umożliwił atakującym przechwytywanie ruchu sieciowego oraz ukrywanie szkodliwych poleceń wydawanych zainfekowanym hostom. W efekcie przestępcy przez kilka miesięcy potajemnie kontrolowali sieci atakowanych organizacji.

Rootkity to szkodliwe programy lub zestawy narzędzi zapewniające atakującym niemal nieograniczony i dyskretny dostęp do zainfekowanego urządzenia. Rootkity znane są z ukradkowości i unikania wykrycia dzięki swym umiejętnościom „stapiania się" z systemem operacyjnym. Dzięki wysiłkom podejmowanym od wielu lat przez firmę Microsoft w celu zabezpieczenia systemów, zainstalowanie i wykonanie rootkita, zwłaszcza w przestrzeni jądra systemu, stanowi spore wyzwanie, dlatego większość rootkitów dla systemów Windows jest obecnie wykorzystywanych jedynie w najbardziej zaawansowanych atakach APT, takich jak TunnelSnake.

Dochodzenie w sprawie omawianej kampanii rozpoczęło się po otrzymaniu przez firmę Kaspersky alertów w związku z wy-

kryciem unikatowego rootkita w atakowanych sieciach. Rootkit ten – któremu nadano nazwę Moriya – okazał się wyjątkowo nieuchwytny dzięki dwóm cechom. Po pierwsze, przechwytuje on i przegląda pakiety sieciowe przesyłane z przestrzeni adresowej jądra systemu Windows, czyli regionu pamięci, w którym uruchamiany jest zwykle jedynie uprzywilejowany i zaufany kod.

Z tego powodu ataki mogły pozostawać niewykryte przez mniej zaawansowane rozwiązania bezpieczeństwa. Po drugie, w przeciwieństwie do większości powszechnych backdoorów dających zdalny dostęp do zainfekowanych urządzeń, rootkit Moriya nie łączył się z żadnym serwerem w celu pobierania poleceń, ale otrzymywał je w specjalnie oznaczonych pakietach, wmieszanych w ruch sieciowy. Dzięki temu cyberprzestępcy nie musieli utrzymywać infrastruktury sterowania i kontroli, utrudniając tym samym analizę i śledzenie aktywności.

Rootkit Moriya instalowany był na urządzeniu w wyniku złamania zabezpieczeń podatnych na ataki serwerów WWW w atakowanych organizacjach. Ponadto wraz z rootkitem stosowano zestaw różnych innych narzędzi – dostosowanych do konkretnych potrzeb bądź wykorzystywanych wcześniej przez rozmaite chińskojęzyczne cybergangi – które pozwalały atakującym skanować urządzenia w sieci lokalnej, znajdować nowe cele, infekować je oraz wyprowadzać z nich pliki.

Pełny raport dotyczący kampanii TunnelSnake jest dostępny na stronie https://r.kaspersky.pl/cCU6R.

Każda osoba może sprawdzić na WhatsAppie, kiedy jesteś online, i domyślić się, z kim rozmawiasz

6.05.2021 r. - Za pomocą dostępnych za darmo narzędzi każdy może sprawdzić, kiedy dany użytkownik aplikacji WhatsApp jest online. Co więcej, aktywność jednej osoby na WhatsAppie można nałożyć na aktywność innego użytkownika, co pozwala wywnioskować, że być może te osoby ze sobą rozmawiają, jeśli okresy ich aktywności są zbieżne.

WhatsApp chwali się „prywatnością w swoim DNA", a z drugiej strony na swojej stronie przyznaje[7], że domyślnie każdy jego użytkownik widzi:

- status „Widziano",
- zdjęcie profilowe,
- sekcję „O mnie",
- potwierdzenie odczytania wiadomości.

Powyższe aspekty można zmienić w ustawieniach prywatności, jednak problem w tym, że większość osób uważa, że wybranie takich ustawień, aby NIKT ich nie widział, powoduje, że są bezpieczni. Tymczasem WhatsApp w swojej dokumentacji ostrzega, że nie można ukryć statusu „aktywny(-a)" ani „pisze...".

Dlaczego stwarza to problem? Z WhatsAppa korzysta wiele osób, a dzięki tej luce pokazującej, kiedy ktoś jest online, można próbować ustalać siatkę kontaktów i powiązania danych osób, namierzać prawdziwą tożsamość (w przypadku osób anonimowych), a nawet typować lokalizację, w której przebywają. Namierzanie czasów czyjejś aktywności w internecie może więc być przydatne dla detektywów, służb, ale także stalkerów i marketerów.

Warto mieć świadomość, że sprawdzenie, które osoby w określonym czasie korzystały z aplikacji WhatsApp, nie jest niezbitym dowodem na to, że się ze sobą kontaktowały. Każdą informację należy zweryfikować w wielu źródłach, a bazowanie wyłącznie na jednej technice może być tragiczne w skutkach.

Jeśli jednak wiemy o relacji dwóch osób i obserwujemy ich wzajemną aktywność bardzo często i w różnych dniach i zawsze się ona pokrywa, trudno będzie uznać to za czysty przypadek (zwłaszcza jeśli te dwie osoby nie używają WhatsAppa bardzo często do rozmów z innymi).

Taka technika może być przydatna do wykazania, że:

- w trakcie wypadku samochodowego kierowca korzystał z WhatsAppa,
- ochrona w obiekcie ma przerwy w konkretnych, powtarzalnych godzinach,
- dyrektor właśnie skończył spotkanie i można zajrzeć do niego z ofertą, bo właśnie patrzy w telefon.

Jedną z darmowych usług, które pozwalają każdemu sprawdzić i porównać okresy aktywności dowolnej osoby na WhatsAppie, jest Wacheck.Online. Wystarczy wpisać numer i sprawdzić, kiedy ktoś jest online.

Drugą usługą jest Chatwatch.net. Jest ona płatna, ale można wypróbować ją za darmo w ramach 8-godzinnego testu. Po wprowadzeniu numeru telefonu można sprawdzić, kiedy jego użytkownik był online w ciągu ostatnich 24 godzin albo w jakimś wcześniejszym dniu. Można dodać 2 lub więcej numerów (w ramach bezpłatnych testów tylko 2) i dzięki temu sprawdzić, czy momenty aktywności dwóch numerów się pokrywają. To zaś może prowadzić do ustalenia, czy dwie osoby prowadzą ze sobą rozmowy na WhatsApp.

Podobnych aplikacji jest wiele. Jeden z nich, WaRadar, reklamuje się jako narzędzie do monitorowania, ile czasu korzysta dziecko z komunikatorów i mediów społecznościowych. Wspomniane dziecko jest tu wymienione tylko formalnie, gdyż firma Google zabrania umieszczania w swoim sklepie aplikacji reklamowanych wprost jako produkty do szpiegowania.

[7] *https://faq.whatsapp.com/iphone/security-and-privacy/configuring-your-privacy-settings*

Powrót do normalności: po styczniowym wzroście liczba ataków DDoS w I kwartale 2021 r. wraca do poziomu sprzed lockdownu

11.05.2021 r. - W pierwszych trzech miesiącach 2021 r. liczba ataków DDoS spadła o 29% w stosunku do analogicznego okresu w 2020 r. oraz zwiększyła się o 47% w porównaniu z IV kwartałem 2020 r. – wynika z danych pochodzących z rozwiązania Kaspersky DDoS Protection. Wzrost ten spowodowany był nietypowym, nagłym skokiem w styczniu, który odpowiadał za 43% wszystkich ataków w analizowanym kwartale, podczas gdy pozostałe dwa miesiące nadal były spokojne.

Na początku 2021 r. wiele osób nadal pracowało zdalnie i spędzało czas wolny w domu. Cyberprzestępcy przeprowadzali więc ataki DDoS na podmioty, które były wtedy najbardziej „kluczowe" dla użytkowników, np. na dostawców usług telekomunikacyjnych[8], co powodowało problemy z dostępem do internetu, lub na strony z grami online[9]. Chociaż zasoby te nadal pozostają na celowniku cyberprzestępców, statystyki pokazują, że ogólna sytuacja dotycząca ataków DDoS stabilizuje się.

Eksperci z firmy Kaspersky tłumaczą spadek liczby ataków w porównaniu z analogicznym kwartałem poprzedniego roku nietypową aktywnością[10] z początku 2020 r. Pospieszne przechodzenie na pracę zdalną spowodowało, że celem ataków DDoS stały się korporacyjne bramy VPN oraz zasoby online, takie jak poczta czy firmowe bazy wiedzy, które wcześniej dostępne były jedynie wewnątrz organizacji. Na przestrzeni roku firmy w większości wdrożyły ochronę dla tych elementów infrastruktury IT. W efekcie ataki DDoS na takie zasoby stały się mniej skuteczne, a ich liczba spadła, wracając w lutym i marcu 2021 r. do poziomu sprzed lockdownu.

Pod względem liczby ataków DDoS zdecydowanie wyróżnia się styczeń 2021 r. Potwierdzają to również statystyki pochodzące z systemu Kaspersky DDoS Intelligence, który przechwytuje i analizuje polecenia otrzymywane przez szkodliwe narzędzia z serwerów cyberprzestępczych. Na przykład 10 i 11 stycznia liczba zarejestrowanych ataków przekroczyła 1 800, a przez kilka dni w miesiącu wynosiła ponad 1 500.

Pełny raport firmy Kaspersky poświęcony ewolucji ataków DDoS w I kwartale 2021 r. jest dostępny na stronie https://r.kaspersky.pl/CrVWZ.

[8] *https://www.tt.com/artikel/30780033/ddos-attacke-sorgte-fuer-stoerung-bei-a1-internet-problem-behoben*

[9] *https://esports-news.co.uk/2021/01/22/lol-clash-ddos-attack/*

[10] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3262/trzykrotny-wzrost-liczby-atakow-ddos-na-edukacje-i-administracje-podczas-pandemii-koronawirusa*

Nagrano rozmowę ze złodziejami, którzy od wielu miesięcy okradają Polaków

11.05.2021 r. - Pewien mężczyzna odebrał telefon od oszustów podszywających się pod pracowników banków. Nagrał tę rozmowę, dzięki czemu wiadomo, jak cwani są złodzieje i jak dokładnie przebiega jeden najpopularniejszych obecnie przekrętów — oszustwo „na pracownika infolinii banku".

Na czym polega to oszustwo? Złodzieje:

1. Pozyskują Twoje dane z wycieków, np. ze sklepu internetowego. Mają imię, nazwisko, numer telefonu i cztery ostatnie cyfry karty płatniczej, którą opłacane było zamówienie.
2. Dzwonią do Ciebie z prawdziwego numeru Twojego banku i prawie zawsze mają ukraiński akcent. Numer wygląda na prawdziwy, lecz w rzeczywistości pod numery telefonów można się podszyć.
3. Twierdzą, że bank wykrył podejrzaną transakcję na Twoim rachunku i jest ona wynikiem infekcji smartfona szkodliwym oprogramowaniem.
4. Nalegają, by „zgodnie z regulaminem banku" pracownik działu technicznego przeskanował Twoje urządzenie pod kątem wirusów. W tym celu chcą się połączyć z Tobą przez aplikację Teamviewer QuickSupport lub Anydesk, którą rzekomo masz mieć zainstalowaną, a jeśli jej nie masz, to musisz ją zainstalować, bo „regulamin banku tego wymaga".
5. Z Twoją pomocą wykonują operacje „weryfikacji" na Twoim koncie. Widzą wszystko, co Ty, także kody potrzebne do autoryzowania „testowych" transakcji. W ten sposób przejmują kontrolę nad rachunkiem i okradają Cię z pieniędzy, ale z punktu widzenia banku okradłeś się sam, zatem reklamacja zostanie odrzucona.

Do wspomnianej osoby oszuści dzwonili 2 razy. Była ona świadoma, że jest to atak, więc zaczęła nagrywać rozmowę. Nagranie zatytułowane „Rozmowa ze złodziejami, którzy od miesięcy oszukują Polaków" zostało opublikowane przez portal Niebezpiecznik w serwisie YouTube[11].

Co sprawia, że oszuści są tak przekonujący i nabierają tak wiele osób?

1. W trakcie rozmowy złodziej powołuje się na współpracę z policją i czyta fragmenty skryptu, co ma na celu wymuszenie pośpiechu i wzbudzenie poczucia zagrożenia. Wielu osobom takie zapewnienia wyłączają trzeźwe myślenie.
2. Oszust cytuje ofierze poprawny numer karty płatniczej. Redakcja portalu Niebezpiecznik dowiedziała się, że niedoszła ofiara korzystała z serwisu Aliexpress, a zatem jej dane mogą pochodzić z wycieku od jednego ze kontrahentów tego serwisu. Inne osoby wskazywały, że oszuści zwracali się do nich fałszywymi imionami, jakie podali podczas zakupów przez aplikację Joom.

To jednak nie oznacza, że gdy ktoś nie kupował na Aliexpress lub nie korzystał z serwisu Joom, to nie będzie ofiarą tego ataku. Informacje na temat kart bankowych i numerów telefonu złodzieje zbierają z wielu różnych wycieków, których niestety nie brakuje.

3. Oszust uwiarygadnia się. Podaje swoje dane i informuje, że za chwilę będzie dzwonić policjant, który zapyta o te dane. Ujawnia też dane oszusta, na którego konto miały rzekomo zostać przekazane środki potencjalnej ofiary na skutek fałszywej transakcji. Ponieważ połączenie pochodzi z prawdziwego numeru infolinii, wszystko dodaje wiarygodności atakowi.
4. Na drodze manipulacji oszust sprawia, że ofiara zaczyna wierzyć, że jej urządzenie jest zainfekowane. W tym celu zadaje jej pytania, na które większość osób odpowiedziałby „tak", podświadomie przyznając rację historii snutej przez oszusta. Oto pytania:
   - — Czy otrzymywał Pan jakieś podejrzane e-maile w ciągu ostatnich 2 tygodni?
   - — Czy robił Pan zakupy na Allegro, Aliexpress, OLX w ciągu ostatni 2 miesięcy?
   - — Czy zawsze zabiera Pan potwierdzenie po zakupach?
   - — Czy Pan korzysta z sieci Wi-Fi w ogólnodostępnych miejscach?
5. Oszust służy nawet dobrą radą! Edukuje zupełnie jak prawdziwy pracownik banku, że należy uważać na strony internetowe, na których nie ma certyfikatu bezpieczeństwa.
6. Następnie naciągacz pyta, czy ofiara ma aplikację mobilną banku oraz „dodatkową aplikację" Quick Support (Teamviewer), którą według regulaminu banku powinno się mieć zainstalowaną, jeśli konto było założone po 2015 roku. Osoba ta twierdzi, że jest to aplikacja banku, które została stworzona w odpowiedzi na wiele ataków na telefony, a dzięki niej bank może szybko pomagać klientom. Jeśli Quick Support nie działa, to oszust nakłania do zainstalowania aplikacji AnyDesk.
7. Oszust przekonuje, że jest to standardowa procedura. Nie chce żadnych kodów uwierzytelniających, a rozmowa jest nagrywana (zapewnia nawet, że gdyby poprosił o kody z SMS-ów, zostałby ukarany przez bank). Oczywiście nie musi prosić o te kody, ponieważ dobrze wie, że będzie mieć do nich dostęp — po instalacji aplikacji Quick Support będzie widzieć wszystko to, co ofiara.

Jeśli ktoś padł ofiarą tego oszustwa, powinien zgłosić reklamację do banku i udać się na policję. Im więcej zgłoszeń, tym lepsza reakcja różnych instytucji.

Warto również pamiętać, że oszuści dzwonią na dane pochodzące z różnych wycieków. Po odebraniu takiego telefonu można założyć, że znalazł się on w bazie, która wyciekła.

[11] *https://www.youtube.com/watch?v=SbCcmLqmQSs*

Operatorzy ransomware i gdzie ich znaleźć: Kaspersky rzuca nieco światła na ekosystem cyberprzestępczy

kaspersky **12.05.2021 r. - Za każdym razem, gdy pojawia się temat cyberzagrożeń dla firm, jednym z pierwszych przykładów jest ransomware. Cyberprzestępcy wypracowali dobrze działające mechanizmy, a ich poczynania jeszcze nigdy nie były tak śmiałe, o czym świadczą nieustanne doniesienia medialne o atakach na organizacje z wykorzystaniem oprogramowania wymuszającego okup. Aby pomóc organizacjom zrozumieć, jak działa ten ekosystem oraz jak można z nim walczyć, na potrzeby badacze z firmy Kaspersky zagłębili się w fora darknetu, przyjrzeli się dokładnie cybergangom Revil i Babuk oraz rozwiali kilka mitów dotyczących ransomware.**

Jak każda branża, ekosystem ransomware składa się z wielu graczy, którzy pełnią w nim różne role. Chociaż panuje przekonanie, że gangi ransomware są zwartym tworem niczym mafia rodem z „Ojca Chrzestnego", rzeczywistość bardziej przypomina świat z filmu „Dżentelmeni" Guya Ritchiego. W większości ataków bierze udział spora liczba różnych uczestników – deweloperów, specjalistów od botów, sprzedawców „dostępu", operatorów ransomware – świadczących sobie wzajemnie usługi za pośrednictwem darkwebowego rynku.

Gracze ci spotykają się na specjalistycznych forach darknetu, gdzie można znaleźć regularnie aktualizowane ogłoszenia oferujące usługi oraz partnerstwa. Stron tych nie odwiedzają działające niezależnie „grube ryby", jednak znane ugrupowania, takie jak Revil, które w minionych kwartałach przeprowadzały coraz więcej ataków na organizacje, regularnie publikują swoje oferty oraz informacje poprzez programy partnerskie. Ten rodzaj relacji opiera się na współpracy pomiędzy operatorem ugrupowania ransomware oraz podmiotem stowarzyszonym, przy czym operator ransomware otrzymuje udział w zyskach na poziomie 20-40%, podczas gdy pozostałe 60-80% zgarnia podmiot stowarzyszony.

Wybór takich partnerów stanowi rygorystyczny proces, w którym ogólne zasady zostają określone przez operatorów ransomware już na samym początku – łącznie z ograniczeniami geograficznymi, a nawet poglądami politycznymi. Jednocześnie, ofiary ransomware wybierane są w sposób oportunistyczny.

Ponieważ osoby infekujące organizacje oraz te, które obsługują ransomware, to w rzeczywistości różne grupy, połączone jedynie chęcią zysku, najczęściej infekowane są organizacje stanowiące „łatwą zdobycz" – zasadniczo te, do których atakujący mają łatwiejszy dostęp. Mogą to być zarówno gracze działający w ramach podmiotów stowarzyszonych, jak i niezależni operatorzy, którzy sprzedają następnie „dostęp". Tacy atakujący są najczęściej właścicielami sieci zainfekowanych urządzeń (tzw. botnetów), które pozwalają na przeprowadzanie masowych oraz szeroko zakrojonych kampanii. Prowadzą oni także hurtową sprzedaż dostępu do maszyn ofiar, ujawnionych publicznie luk w zabezpieczeniach, urządzeń VPN, serwerów e-mail itd.

Na forach dotyczących ransomware znaleźć można również inne rodzaje ofert. Niektórzy operatorzy ransomware sprzedają próbki szkodliwego oprogramowania oraz kreatory ransomware za kwotę rzędu 300 – 4 000 dolarów, podczas gdy inni oferują usługi przeprowadzania ataków, np. sprzedaż ransomware wraz z nieprzerwanym wsparciem jego twórców, co może kosztować, w zależności od pakietu miesięcznego lub rocznego, od 120 do 1 900 dolarów.

Więcej informacji na temat ekosystemu ransomware znajduje się na stronie https://r.kaspersky.pl/URhLI.

Kaspersky wykrywa kolejnego brazylijskiego trojana bankowego atakującego na skalę globalną

17.05.2021 r. - Badacze z firmy Kaspersky wykryli nowe szkodliwe oprogramowanie bankowe z Brazylii o nazwie Bizarro, które zaatakowało 70 banków w różnych państwach Europy i Ameryki Południowej. W zeszłym roku eksperci zauważyli, że kilka trojanów bankowych z Ameryki Południowej (Guildma, Javali, Melcoz oraz Grandoreiro) rozszerzyło swoje operacje na cały świat. Określane łącznie jako Tetrade[12]**, rodziny te stosowały szereg nowych, innowacyjnych i wyrafinowanych technik. Podobną tendencję zaobserwowano w 2021 r. – nowy gracz lokalny, Bizarro, zaczął działać na skalę globalną.**

Bizarro to nowa rodzina trojanów bankowych, która została stworzona w Brazylii, a teraz znaleźć ją można również w innych państwach, takich jak Argentyna, Chile, Niemcy, Hiszpania, Portugalia, Francja oraz Włochy. Podobnie jak Tetrade, Bizarro wykorzystuje sieci partnerskie lub rekrutuje słupy do przeprowadzania swoich ataków, wypłacania środków lub po prostu pomocy w tłumaczeniach na kolejne języki. Jednocześnie stojący za tą rodziną szkodników cyberprzestępcy stosują różne metody techniczne w celu komplikowania analizy oraz wykrywania szkodliwego oprogramowania, jak również sztuczki socjotechniczne, za pomocą których nakłaniają ofiary do ujawnienia swoich bankowych danych uwierzytelniających.

Bizarro jest rozprzestrzeniany za pośrednictwem pakietów MSI (pliki instalacyjne systemu Windows) pobieranych przez ofiary z odsyłaczy zamieszczonych w wiadomościach spamowych. Po zainstalowaniu Bizarro pobiera z zainfekowanej strony archiwum ZIP w celu wykonania dalszych szkodliwych funkcji. Po wysłaniu danych na serwer telemetryczny Bizarro inicjuje moduł przechwytywania ekranu. Jak zaobserwowali eksperci z firmy Kaspersky, w celu przechowywania szkodliwego oprogramowania i zbierania telemetrii Bizarro wykorzystywał do tej pory serwery na platformach Azure i Amazon, jak również zhakowane serwery WordPress.

Badacze z firmy Kaspersky podkreślają, że głównym komponentem Bizarro jest backdoor. Zawiera on ponad 100 poleceń, z czego większość wykorzystywana jest do wyświetlania użytkownikom fałszywych wiadomości wyskakujących. Niektóre z nich próbują nawet imitować systemy bankowości online.

Szczegóły techniczne dotyczące szkodliwego programu Bizarro są dostępne na stronie: https://r.kaspersky.pl/TwFqY.

[12] https://www.kaspersky.pl/o-nas/informacje-prasowe/3293/tetrade-brazylijscy-cyberprzestepcy-atakuja-swiat-nowa-generacja-trojanow

Złośliwy FluBot wciąż atakuje użytkowników urządzeń mobilnych, podszywając się pod firmy kurierskie

20.05.2021 r. - Złośliwe oprogramowanie mobilne znane jako FluBot nadal wywołuje chaos w wielu krajach europejskich, w tym w Polsce. – Wykorzystująca wizerunek firm kurierskich akcja daje przestępcom m.in. dostęp do numerów kart kredytowych czy bankowości online nieświadomych użytkowników. Wersja 4.0 zagrożenia została opracowana z myślą o szerokim działaniu – przestrzegają eksperci ds. cyberbezpieczeństwa.

FluBot został po raz pierwszy zidentyfikowany przez specjalistów ESET w Hiszpanii, w grudniu 2020 r. Od tego czasu złośliwe oprogramowanie atakowało m.in. w Niemczech, Polsce, we Włoszech i Holandii. Kod rozprzestrzeniającej się obecnie wersji 4.0 sugeruje, że jej twórcy planują szeroką akcję w wielu krajach na całym świecie. Kampania wymierzona jest głównie w użytkowników urządzeń mobilnych korzystających z systemu Android, ale istnieją także mutacje atakujące właścicieli iPhone'ów.

FluBot to podstępny gracz, który po zainstalowaniu umożliwia hakerom pełen dostęp do urządzenia. Został opracowany tak, by wyłączać ochronę Play Protect, a także pozyskiwać dane kolejnych potencjalnych ofiar. Tak jak aktywny w ostatnich dniach i oparty na podobnym mechanizmie TeaBot (znany również jako Anatsa lub Toddler), FluBot jest wykrywany i blokowany przez produkty ESET jako wariant zagrożenia z rodziny Android/TrojanDropper.Agent.

Jak działa FluBot?

Ofiara najpierw otrzymuje wiadomość SMS od nadawcy, który podszywa się pod popularną markę, zajmującą się przewozem przesyłek i logistyką, taką jak FedEx, DHL, UPS. Hakerzy wykorzystują też marki lokalnych usługodawców (np. InPost w Polsce czy Correos w Hiszpanii). Wiadomość nakłania użytkownika Androida do kliknięcia łącza w celu pobrania i zainstalowania aplikacji, w której nazwie również pojawia się marka przewoźnika.

W rzeczywistości to złośliwe oprogramowanie FluBot. Wiadomości SMS mają różną treść, np. „Twoja paczka jest w drodze, śledź ją tutaj (tu link)" lub „Nie byliśmy w stanie dostarczyć Twojej paczki. Kliknij, aby utworzyć nową datę dostawy (tu link)". Z kolei mutacja kampanii wymierzona w posiadaczy telefonów z systemem iOS zawiera ankietę, która wyłudza dane, wyświetla fałszywą informację o wygranej i zachęca do opłacenia przesyłki z nagrodą.

Po zainstalowaniu i przyznaniu żądanych uprawnień, FluBot uruchamia szereg szkodliwych funkcji. Jest w stanie spamować SMS-ami, wykraść numery kart kredytowych i dane uwierzytelniające do kont bankowych, działa także jak oprogramowanie szpiegowskie. Lista kontaktów z urządzenia jest wysyłana na serwery kontrolowane przez cyberprzestępców, dostarczając kolejnych danych, przydatnych do dalszych ataków na potencjalne ofiary. FluBot jest też w stanie przechwytywać wiadomości SMS i powiadomienia od operatorów telekomunikacyjnych, otwierać strony przeglądarki i pozyskiwać dane uwierzytelniające. Aby uniemożliwić usunięcie złośliwego oprogramowania, atakujący wdrożyli mechanizmy zatrzymujące wbudowaną ochronę, oferowaną przez system operacyjny Android. Aplikacja dezaktywuje Google Play Protect, uniemożliwia też instalowanie niektórych pakietów zewnętrznego oprogramowania zabezpieczającego.

Jak namierzono adres ministra Niedzielskiego?

25.05.2021 r. - Na udostępnionym w internecie 4-minutowym materiale wideo widać, jak grupa osób wyposażona w kamery towarzyszy ministrowi Niedzielskiemu od klatki wejściowej aż do windy, a kiedy ta rusza, grupa wbiega schodami na piętro, na którym mieszka minister. Sytuację opisał m.in. portal Niebezpecznik, który na swoich stronach wyjaśnia, w jaki sposób ktoś mógł namierzyć adres ministra.

Na profilu pana ministra na Twitterze można zauważyć wpis, na którym widoczny jest zrzut ekranu z pewnej aplikacji służącej do logowania aktywności fizycznej.

Na podstawie powyższego można całkiem precyzyjnie oszacować miejsce, z którego minister w weekend ruszył na rowerową przejażdżkę. Oczywiście start wcale nie musiał znajdować się w bloku, w którym mieszka pan minister — ale mógł. Na wszelki wypadek redakcja Niebezpiecznika ocenzurowała więc punkt początku i końca tej trasy zielonym prostokątem. Możliwości wyznaczenia adresu jest kilka:

1. Chociaż z mapy opublikowanej przez pana Niedzielskiego nie można odczytać dokładnego adresu, wystarczy obserwować wyznaczoną okolicę, aby prędzej czy później zauważyć, do którego budynku wchodzi.
2. Mając przybliżony obszar zamieszkania jakiejś osoby, można także ustalić numery ksiąg wieczystych okolicznych budynków. Jeśli lokal, w którym mieszka pan minister, należy do niego, to dzięki tej technice będzie można konkretny adres odczytać właśnie ze zdobytych za darmo z ministerialnego serwisu ksiąg wieczystych.
3. W kontekście ustalania adresu, zwłaszcza osoby ważnej, nie można też pominąć tzw. osobowych źródeł informacji, czyli ludzi-informatorów. Pan minister to postać znana; zapewne wielu z jego sąsiadów wie, obok kogo mieszka. Można więc powiedzieć, że sąsiedzi również stanowią zagrożenie dla naszej prywatności, ponieważ w każdej chwili mogą ujawnić nasz adres na jakiejś grupie dyskusyjnej.
4. Istnieje jeszcze jedno zagrożenie związane z prywatnością — każdą osobę można śledzić aż do jej miejsca zamieszkania.

Od masowych kampanii po polowanie na „grubego zwierza": jak oprogramowanie ransomware JSWorm wyewoluowało w ciągu zaledwie dwóch lat

27.05.2021 r. - Ukierunkowane oprogramowanie ransomware wciąż nęka firmy na całym świecie, dlatego warto przyjrzeć się bliżej operacjom konkretnych cybergangów. Dzięki temu będzie można lepiej je zrozumieć, a także opracować bardziej zaawansowaną ochronę przed ich atakami. Badacze z firmy Kaspersky rozłożyli na czynniki pierwsze i zbadali ciekawy okaz (a dokładniej — okazy) należący do grupy JSWorm, który pokazuje, jak sprawnie potrafi ona aktualizować swój zestaw narzędzi. Ugrupowanie to, które wcześniej koncentrowało się na operacjach przeprowadzanych na skalę masową, zdołało szybko zaadaptować się oraz rozwinąć wysoce ukierunkowaną operację w ciągu zaledwie dwóch lat, tworząc ponad osiem odrębnych „marek" szkodliwych narzędzi.

W każdym „przemianowanym" wariancie zmieniono różne aspekty kodu, nazwy rozszerzeń plików, schematy kryptograficzne oraz klucze szyfrowania. Oprócz zmian nazw twórcy tego oprogramowania ransomware zmodyfikowali również swój kod i wypróbowali różne podejścia do dystrybucji, co świadczy o ich niezwykłej adaptacyjności oraz posiadaniu ogromnych zasobów.

JSWorm był wykrywany na całym świecie – od Ameryki Północnej i Południowej (Brazylia, Argentyna, Stany Zjednoczone) po Bliski Wschód oraz Afrykę (Afryka Południowa, Turcja, Iran), Europę (Włochy, Francja, Niemcy) oraz region Azji i Pacyfiku (Wietnam).

Jeśli chodzi o atakowane branże, nie ma wątpliwości, że na celowniku omawianej rodziny znajduje się infrastruktura krytyczna oraz główne sektory na całym świecie. Niemal połowa (41%) ataków JSWorm była wymierzona w firmy z branży inżynieryjno-produkcyjnej. Atakowane były również podmioty z ta-

kich branż jak: energia i usługi komunalne (10%), finanse (10%), usługi profesjonalne i konsumencie (10%), transport (7%) oraz służba zdrowia (7%).

Pełny raport dotyczący różnych wersji oprogramowania JSWorm jest dostępny na stronie https://r.kaspersky.pl/2CEa9.

Cyberprzestępcy polują na kryptowalutę: liczba nowych modyfikacji szkodliwych koparek w marcu 2021 r. wzrosła ponad czterokrotnie w stosunku do poprzedniego miesiąca

31.05.2021 r. - Z raportu firmy Kaspersky poświęconego ewolucji szkodliwego oprogramowania w pierwszym kwartale 2021 r. wynika, że cyberprzestępcze koparki kryptowalut wracają do gry po ponadrocznym spadku aktywności.

Szkodliwe koparki kryptowalut to narzędzia cyberprzestępców służące do kradzieży kryptowaluty z zainfekowanych urządzeń. Po tym, jak zostaną zainstalowane – zazwyczaj bez wiedzy użytkowników – zaczynają stopniowo wyprowadzać różne rodzaje kryptomonet, w niektórych przypadkach warte miliony. Koparki stały się cenionym narzędziem w arsenale cyberprzestępców z początkiem 2018 r., jednak na przestrzeni roku 2020 ich popularność stopniowo malała.

Wszystko zmieniło się w I kwartale 2021 r. Od lutego do marca 2021 r. liczba unikatowych modyfikacji koparek zwiększyła się ponad czterokrotnie, z 3 815 do 16 934. W I kwartale 2021 r. badacze z firmy Kaspersky wykryli łącznie 23 894 nowych modyfikacji koparek.

Stopniowo wzrastała również – z 187 746 w styczniu do 200 045 w marcu 2021 r. – liczba użytkowników produktów firmy Kaspersky, którzy byli atakowani zagrożeniami związanymi ze szkodliwymi koparkami. W I kwartale 2020 r. łączna liczba takich użytkowników wynosiła 432 171.

Pozostałe trendy, o których mowa w raporcie, obejmują spadek liczby użytkowników, którzy zetknęli się z trojanami bankowymi, rozprzestrzeniającymi się zarówno na urządzeniach mobilnych, jak i komputerach, oraz wzrost liczby modyfikacji trojanów ransomware wyłudzających okup – z 3 096 w IV kwartale 2020 r. do 4 354 w I kwartale 2021 r.

Pełny raport poświęcony ewolucji szkodliwego oprogramowania w pierwszym kwartale 2021 r. jest dostępny na stronie https://r.kaspersky.pl/jHLhv.

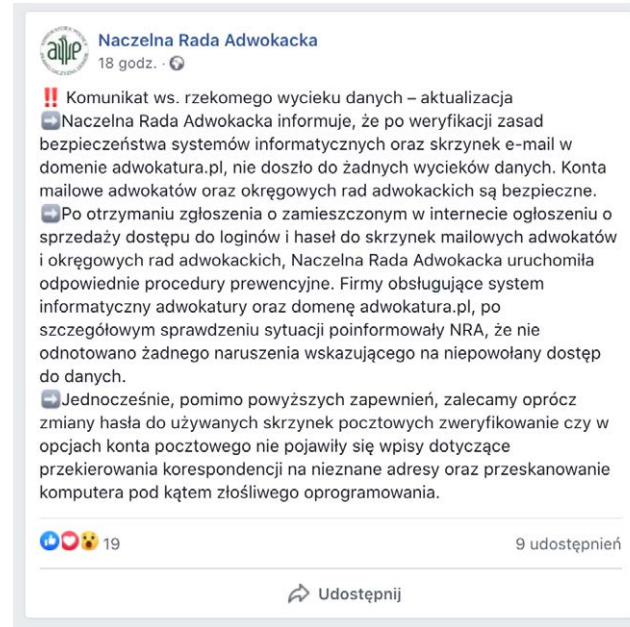
Ktoś twierdzi, że przejął skrzynki e-mail polskich adwokatów i wystawił je na sprzedaż

31.05.2021 r. - W maju tego roku na jednym z polskojęzycznych forów dla cyberprzestępców pojawiło się ogłoszenie zatytułowane „Egzamin Adwokacki 2021 – dostępy do skrzynek rad adwokackich". Naczelna Rada Adwokacka nazwała ten incydent „rzekomym wyciekiem danych" i w wydanym przez siebie oświadczeniu[13] zarekomendowała adwokatom prewencyjną zmianę hasła do używanych skrzynek pocztowych.

Nie wiadomo, czy do wycieku faktycznie doszło, ale jest to prawdopodobne z dwóch powodów.

- Użytkownik Roooj, który oferuje na sprzedaż dostępy do skrzynek adwokatów, ma bogatą historię i handlował już danymi w przeszłości. Ponadto ktoś od pewnego czasu atakował prawników i próbował przejmować ich konta. Nie wiadomo, czy za tymi atakami stał ten sprzedawca.
- Adwokaci mają najczęściej fatalne zabezpieczenia swoich skrzynek i nieadekwatną do rangi piastowanych funkcji wiedzę dotyczącą cyberbezpieczeństwa. Wielu z nich zawodowo korzysta ze skrzynek na np. WP czy Onecie. Niestety, łatwo też nabrać ich na proste ataki phishingowe.

Jak zwraca uwagę Niebezpiecznik, sprzedający nie mówi wprost, że na wspomnianych skrzynkach faktycznie znajduje się lista pytań. Egzamin adwokacki jest przez niego wykorzystywany raczej jako przynęta w ogłoszeniu. Można się jednak spodziewać, że w dobie pandemii opracowywanie egzaminu odbywało się elektronicznie, a to oznacza, że treści pytań lub loginy i hasła do systemu, w którym pytania zbierano, faktycznie mogły znaleźć się na skrzynkach, które udało się przejąć Rooojowi.



Naczelna Rada Adwokacka wystosowała oświadczenie w sprawie tego incydentu:

Co ważne, w oświadczeniu jest mowa o bezpieczeństwie skrzynek w domenie „adwokatura.pl" i samym serwisie adwokatura.pl, podczas gdy ogłoszenie o sprzedaży danych dotyczy innego serwisu — paneladwokata.pl oraz prywatnych skrzynek adwokatów. Należy tu jednak podkreślić, że nie każdy adwokat ma konto w serwisie paneladwokata.pl.

Po nagłośnieniu incydentu do Niebezpiecznika odezwał się rzekomy sprzedawca. Roooj poinformował, że nie dokonał, nie uczestniczył, ani nie pomagał w żadnych tego typu atakach na serwery/skrzynki e-mail adwokatury, złamaniu jakichkolwiek zabezpieczeń teleinformatycznych, naruszeniu tajemnicy państwowej, jak również nie sprzedał ani nie opublikował żadnych danych dostępowych do ww. serwerów.

Na pytanie, skąd miał „dostępy do kont w serwisie protaladwokata.pl" oraz „loginy i hasła do prywatnych skrzynek adwokatów", mężczyzna odpowiedział, że „dane adwokatów pochodziły z ogólnie dostępnych combo list z całego internetu". Podkreślił przy tym, że nie sprawdzał, czy działają. Dodał, że „nie stosował phishingu, sqlinjection, malware ani innych technik ataków". Wedle jego relacji chętnych do zakupu nie było, a gdyby tacy się pojawili, to „odmówiłby transakcji". Roooj podkreślił, że „to, co zrobił, jest kierowane pasją, a nie chęcią zarobku".

Trudno stwierdzić, czy ogłoszenie o sprzedaży było prawdziwe, a prowadzona z serwisem Niebezpiecznik komunikacja była elementem kampanii dezinformacyjnej (ewentualnie próbą załagodzenia afery, która się rozpętała, i śledztwa, które ruszyło), czy może faktycznie była to jedynie prowokacja.

[13] *https://www.ora-warszawa.com.pl/aktualnosci/wiadomosci/komunikat-nra-ws-rzekomego-wycieku-danych/*

5 typowych cyberoszustw, wymierzonych w nastolatki – jak dbać o bezpieczeństwo dzieci w sieci?

DAGMA BEZPIECZEŃSTWO IT

1.06.2021 r. - Internet to naturalne środowisko dla większości nastolatków. Zbyt duża ufność, niewinność i otwartość na znajomości mogą jednak sprawić, że dzieci staną się celem oszustów. Eksperci ds. cyberbezpieczeństwa ESET przyglądają się niektórym typowym działaniom, wymierzonym w nastolatków.

Oszustwa w mediach społecznościowych

Media społecznościowe są naturalnym, cyfrowym miejscem spotkań dla większości nastolatków. Przedsiębiorczy oszuści próbują zatem atakować tam, gdzie młodzież spędza najwięcej czasu. Oszustwa w social mediach przybierają różne formy i czasem, nawet doświadczonym użytkownikom, bardzo trudno jest określić, czy dany post jest prawdziwy i nie stanowi zagrożenia. Jednym z działań wymierzonych między innymi w nastolatków, są wpisy zawierające fałszywe linki do artykułów z szokującymi nagłówkami o celebrytach, np. członkach popularnych zespołów czy influencerach. Jednak po kliknięciu takiego linku następuje przekierowanie do złośliwej witryny internetowej.

Oszuści nierzadko także kontaktują się ze swoimi ofiarami bezpośrednio, za pośrednictwem wiadomości, z ofertami udziału w konkursach lub loteriach. Często są one atrakcyjne graficznie, opatrzone emotikonami i sprawiają wrażenie autentycznych, ale udostępnione linki mogą przekierować nastolatka na fałszywą witrynę, która albo zainfekuje jego urządzenia złośliwym oprogramowaniem, albo spróbuje wyłudzić poufne informacje.

Markowe ciuchy w super niskiej cenie

Innym powszechnym oszustwem, które rozprzestrzenia się w Internecie, w tym za pośrednictwem fałszywych reklam umieszczanych w mediach społecznościowych, jest oferowanie dóbr luksusowych w rażąco niskich cenach. Aby uczynić swoje oferty atrakcyjnymi dla nastolatków, oszuści powołują się na marki i towary, które są popularne i pożądane wśród młodzieży, np. drogie trampki z limitowanej edycji czy ubrania marek, które są zwykle zbyt drogie dla przeciętnego nastolatka.

Podstęp polega na stworzeniu fałszywej witryny, która oferuje szeroki asortyment produktów. Niestety, po dokonaniu zakupu ofiara otrzyma najpewniej podrobiony produkt lub nie otrzyma go wcale. W najgorszym przypadku, jeśli wprowadzimy dane karty płatniczej, cyberprzestępcy mogą całkowicie wyczyścić nasze konto bankowe.

Fałszywe stypendia

Gdy zbliża się koniec szkoły średniej, młodzież zaczyna zastanawiać się nad kolejnym krokiem w życiu. Większość przyszłych studentów decyduje się na pierwsze próby samodzielnego życia. Jednak taka decyzja wiąże się z dużymi kosztami i niekiedy szukaniem źródeł finansowania, w tym również stypendiów naukowych, czy programów typu „work and travel", które mogłyby pokryć część wydatków. Oszuści próbują żerować na studentach szukających pomocy finansowej, tworząc fałszywe stypendia, które przybierają różne formy. Fałszywe programy stypendialne często wymagają od wnioskodawcy uiszczenia „opłaty rejestracyjnej". W rzeczywistości nie ma jednak żadnego stypendium, a to oszust pobiera opłatę. Ewentualne oszustwo może też przybrać formę loterii stypendialnej, która będzie wymagać od uczestnika uiszczenia „opłaty manipulacyjnej" lub „opłaty za wypłatę".

Oszustwa związane z zatrudnieniem

Bycie nastolatkiem nie jest łatwe. Bycie nastolatkiem o różnorodnych zainteresowaniach muzycznych, modowych i podróżniczych, a niskim kieszonkowym – to podwójna trudność. Wielu młodych ludzi poszukuje pracy w niepełnym wymiarze godzin, żeby pokryć swoje wydatki. Cyberprzestępcy coraz częściej wykorzystują tę sytuację i tworzą fałszywe oferty zatrudnienia, które zwykle brzmią bardzo kusząco. Oszuści publikują oferty pracy na legalnych ta-

blicach ogłoszeń i zazwyczaj oferują stanowiska, które pozwalają pracować z domu i jednocześnie zarabiać duże pieniądze.

Ostatecznym celem jest jednak zebranie danych osobowych, które zostaną następnie wykorzystane w różnych nielegalnych działaniach, takich jak otwieranie kont bankowych na nazwiska ofiar lub wykorzystywanie ich tożsamości do fałszowania dokumentów.

Oszustwa randkowe

Poszukiwanie znajomości w Internecie jest dla nastolatków czymś naturalnym. Niestety internetowe platformy randkowe stały się terenem łowieckim dla oszustów. Cyberprzestępcy potrafią podszywać się pod osobę, która będzie atrakcyjna dla potencjalnej ofiary. Po zdobyciu zaufania nieświadomego użytkownika, najczęściej starają się wyłudzić od niego pieniądze. Nierzadko stosują bardzo krzywdzące taktyki, takie jak wmanipulowanie ofiar w udostępnianie intymnych zdjęć, które w dalszych etapach posłużą do szantażu. Grożąc opublikowaniem zdjęć, oszuści wyłudzają pieniądze i wszelkie dane, również do kont bankowych.

Luki dnia zerowego w systemie Windows oraz przeglądarce Chrome wykorzystane w serii zaawansowanych cyberataków

kaspersky

8.06.2021 r. - W kwietniu eksperci z firmy Kaspersky wykryli wiele ataków precyzyjnie wycelowanych w liczne firmy. Użyto w nich nieznanego wcześniej łańcucha szkodliwych narzędzi wykorzystujących luki dnia zerowego w przeglądarce Google Chrome i systemie Microsoft Windows. Jedno z tych narzędzi służy do zdalnego wykonywania szkodliwego kodu w przeglądarce, a drugie pozwala na zwiększanie uprawnień w atakowanym systemie. Luki zostały już załatane przez firmę Microsoft.

W ostatnich miesiącach miała miejsce fala aktywności obejmującej zaawansowane zagrożenia wykorzystujące luki dnia zerowego. W połowie kwietnia eksperci z firmy Kaspersky odkryli kolejną partię wysoce ukierunkowanych ataków na liczne firmy z wykorzystaniem exploitów, które pozwoliły atakującym ukradkowo zainfekować atakowane sieci. Firma Kaspersky nie powiązała jeszcze tych ataków z żadnymi znanymi ugrupowaniami cyberprzestępczymi, a sprawcy są określani jako „PuzzleMaker".

Wszystkie ataki zostały przeprowadzone za pośrednictwem przeglądarki Chrome i wykorzystywały exploita umożliwiającego zdalne wykonanie kodu. Chociaż badacze z firmy Kaspersky nie byli w stanie dotrzeć do kodu exploita, porządek chronologiczny — jak również dostępność — sugerują, że atakujący wykorzystywali załataną już lukę CVE-2021-21224. Była ona związana z błędem niezgodności typów w silniku JavaScript wykorzystywanym przez przeglądarki Chrome i Chromium.

Eksperci z firmy Kaspersky zdołali znaleźć i przeanalizować drugi exploit: narzędzie umożliwiające podniesienie uprawnień, które wykorzystuje dwie różne luki w jądrze Microsoft Windows OS. Pierwsza z nich to luka powodująca wyciek wrażliwych informacji dotyczących jądra systemu, której nadano kod CVE-2021-31955. Luka ta jest związana z funkcją wstępnego ładowania do pamięci, która po raz pierwszy została wprowadzona do systemu Windows Vista w celu skrócenia czasu uruchamiania oprogramowania.

Druga luka – podnosząca uprawnienia w systemie – otrzymała nazwę CVE-2021-31956. Atakujący wykorzystali ją wraz z systemem powiadomień systemu Windows w celu m.in. uruchamiania modułów szkodliwego oprogramowania z uprawnieniami systemu.

Po wykorzystaniu exploitów dla Chrome'a i Windowsa w celu przedostania się do atakowanego systemu szkodnik pobiera ze zdalnego serwera kolejny moduł. Jest on odpowiedziany za pobranie i zainstalowanie dwóch plików wykonywalnych, które podszywają się pod legalne moduły systemu Windows. Jeden z nich potrafi pobierać i przesyłać pliki, tworzyć procesy, pozostawać w uśpieniu przez pewien czas oraz usuwać się z zainfekowanego systemu.

Firma Microsoft opublikowała już poprawkę na obie luki w systemie Windows w ramach tzw. poprawkowego wtorku.

Produkty firmy Kaspersky wykrywają i chronią przed szkodliwymi narzędziami wykorzystującymi omawiane luki w zabezpieczeniach oraz powiązanymi z nimi modułami szkodliwego oprogramowania.

Szczegóły techniczne dotyczące luk i szkodliwych narzędzi wykrytych przez badaczy z firmy Kaspersky są dostępne na stronie https://r.kaspersky.pl/7gPXS.

Kaspersky wykrywa szkodliwe aplikacje podszywające się pod popularną grę

kaspersky

9.06.2021 r. - Minecraft, najlepiej sprzedająca się gra wszech czasów, przyciąga uwagę nie tylko graczy, którzy oddają się jej z entuzjazmem, ale również oszustów. W ubiegłym roku badacze z firmy Kaspersky wykryli[14] ponad 20 narzędzi reklamowanych w sklepach z aplikacjami, które rzekomo oferowały dodatkowe funkcje do Minecrafta. Chociaż szkodniki te zostały usunięte z oficjalnych sklepów, eksperci z firmy Kaspersky zidentyfikowali nowe niebezpieczne aplikacje, wykorzystujące tę znaną grę do oszukańczych celów.

Badacze z firmy Kaspersky przeanalizowali różne aplikacje, łącznie z tymi, które można pobrać w sklepie Google Play, podszywające się pod pakiety wprowadzające modyfikacje (tzw. mody), czyli stworzone przez użytkowników pakiety z dodatko-

wymi elementami gry. W rezultacie znaleziono różne szkodliwe aplikacje rozprzestrzeniające oprogramowanie adware lub kradnące dane uwierzytelniające dostęp do kont w mediach społecznościowych.

Przede wszystkim badacze wykryli kilka aplikacji rozprzestrzeniających oprogramowanie adware, które bombarduje użytkowników niechcianymi reklamami, zakłócając korzystanie z urządzenia. Nie trzeba nawet otwierać tych aplikacji, aby – na polecenie oszusta – wyświetlały reklamy. Co więcej, mogą one ładować dodatkowe moduły, które pozwalają ukryć ikonę, jak również otwierać nieoczekiwanie przeglądarkę, strony aplikacji w Google Play czy odtwarzać filmy na YouTubie, przeszkadzając tym samym w korzystaniu ze smartfona.

Badacze z firmy Kaspersky znaleźli dwa takie szkodliwe mody z podstawową funkcjonalnością. W aktualnej wersji aplikacja wyświetla reklamy pełnoekranowe (także wtedy, kiedy nie jest uruchomiona), jednak nie posiada funkcji ukrywania ikony ani uruchomiania przeglądarki, YouTube'a czy sklepu Google Play. W celu uzyskania dodatkowego zarobku twórcy aplikacji wykorzystują funkcję „zakup w aplikacji".

Kilka innych wykrytych aplikacji kradnie konta w mediach społecznościowych. W jednym przypadku w sklepie Google Play dostępna była fałszywa aplikacja sieci reklamowej wykorzystywana do reklamowania na TikToku. Podanie przez użytkownika swoich danych uwierzytelniających do portalu społecznościowego skutkowało kradzieżą jego konta.

Niezwłocznie po wykryciu nowych zagrożeń badacze z firmy Kaspersky zwrócili się go Google'a z kompletem informacji o nowych szkodliwych aplikacjach w sklepie Google Play.

[14] *https://plblog.kaspersky.com/minecraft-mod-adware-google-play/14208/*

Premier przyznaje, że zaatakowano całą „polską klasę polityczną"

15.06.2021 r. - W czerwcu tego roku w przestrzeni publicznej pojawiły się oświadczenia ministra Dworczyka, premiera i serwisu WP, z których wynika, że skrzynka wspomnianego ministra została zhakowana. Jak zauważa portal niebezpiecznik.pl, nie oznacza to jednak, że wszystkie publikowane przez włamywaczy treści e-maili są prawdziwe lub faktycznie pochodzą z tego źródła. W operacjach dezinformacji celowo miesza się prawdę z fałszywkami.

Do ataku odniósł się premier Morawiecki:

„(...) Doszło do bezprecedensowego ataku, który kierowany jest według wszelkiego prawdopodobieństwa zza naszej wschodniej granic (...) Trzeba sobie wprost powiedzieć: dzisiaj mamy do czynienia z atakami różnego rodzaju, atakami hybrydowymi, atakami cyfrowymi. (...) poprzez tak zwane skompromitowanie (...) szeregu skrzynek zakładanych na portalu Wirtualna Polska z rozszerzeniem wp.pl (...) doszło do przejęcia tych skrzynek przez innych, nieuprawnionych do tego podmiotów".

Wywołana do tablicy Wirtualna Polska odpowiedziała, że:

„(...) Wejście na konto ministra Michała Dworczyka i co za tym idzie uzyskanie dostępu do jego emaili nastąpiło na skutek podania poprawnego loginu i hasła. Naszym zdaniem przestępcy albo wyłudzili hasło od żony ministra, albo używała ona takiego samego hasła u innych usługodawców i tam był wyciek. (...) Premier Mateusz Morawiecki mówił dziś o potrzebie uwierzytelniania dwuskładnikowego. Chcemy jasno i wyraźnie zaznaczyć, że taki system uwierzytelnienia funkcjonuje w poczcie WP od dawna. Przykro nam to stwierdzić, ale minister Michał Dworczyk w momencie tego zdarzenia nie korzystał z takiego systemu".

Jak zauważa Niebezpiecznik, uwierzytelnienie dwuskładnikowe stosowane przez Wirtualną Polskę nie chroni przed atakami phishingowymi.

Kaspersky odkrywa 6-letnią kampanię cyberszpiegowską prowadzoną na Bliskim Wschodzie

16.06.2021 r. - Badacze z firmy Kaspersky odkryli długotrwałą kampanię cyberszpiegowską wymierzoną w perskojęzyczne osoby w Iraku. Stojące za nią ugrupowanie – określone jako Ferocious Kitten – działa od co najmniej 2015 r. i rozprzestrzenia niestandardowe szkodliwe oprogramowanie o nazwie MarkiRAT, które kradnie dane i potrafi wykonywać polecenia na maszynie ofiary. Szkodnik posiada również wersje, które potrafią przejmować kontrolę nad przeglądarką Chrome oraz aplikacją Telegram użytkownika zainfekowanego urządzenia.

Ugrupowanie Ferocious Kitten, aktywne co najmniej od 2015 r., atakuje swoje ofiary przy użyciu dokumentów-wabików zawierających szkodliwe makra. Dokumenty te są ukrywane pod postacią zdjęć lub filmów przedstawiających działania przeciwko reżimowi irańskiemu. Początkowe wiadomości związane z dokumentami wabikami próbują przekonać potencjalną ofiarę do otwarcia załączonych zdjęć lub filmów. Jeśli ofiara wykona takie działanie, do jej systemu przesyłane są szkodliwe pliki wykonywalne, podczas gdy na ekranie w dalszym ciągu wyświetlana jest przynęta.

Pobierane pliki dostarczają główną szkodliwą funkcję – niestandardowe szkodliwe oprogramowanie o nazwie MarkiRAT. Po aktywacji w zainfekowanym systemie szkodnik inicjuje keyloggera, który kopiuje całą zawartość systemowego schowka i prze-

chwytuje wszystkie znaki wprowadzane na klawiaturze. Ponadto MarkiRAT umożliwia atakującym pobieranie i przesyłanie plików oraz wykonywanie rozmaitych poleceń na zainfekowanej maszynie.

Badacze z firmy Kaspersky wykryli również kilka innych wariantów szkodnika MarkiRAT. Jeden z nich potrafi przechwytywać moment uruchamiania aplikacji Telegram i aktywować wraz z nią szkodliwe oprogramowanie. W tym celu MarkiRAT szuka na zainfekowanym urządzeniu repozytorium danych wewnętrznych Telegrama. Jeśli je znajdzie, kopiuje się do niego, a następnie dokonuje modyfikacji, w wyniku których szkodliwe moduły są uruchamianie wraz z Telegramem.

Inny wariant w podobny sposób modyfikuje skrót przeglądarki Chrome na zainfekowanym urządzeniu. W efekcie przy każdym uruchomieniu Chrome'a aktywowana jest wraz z nim szkodliwa funkcja MarkiRAT. Jeszcze inny wariant stanowi zawierającą backdoora wersję Psiphona – otwartego narzędzia VPN, które jest często wykorzystywane do obchodzenia cenzury w internecie. Badacze z firmy Kaspersky znaleźli również dowody na to, że ugrupowanie Ferocious Kitten przygotowało szkodliwe implanty atakujące urządzenia z systemem Android, jednak nie udało im się zdobyć konkretnych próbek do analizy.

Ofiarami opisywanej kampanii wydają się być osoby perskojęzyczne oraz mieszkające w Iraku. Zawartość dokumentów wabików sugeruje, że atakujący mają na celowniku zwolenników ruchów protestacyjnych w kraju.

Więcej informacji na temat omawianych cyberataków znajduje się na stronie https://r.kaspersky.pl/eI8TW.

ABW i SKW potwierdza, że to Rosjanie zhackowali Dworczyka i resztę polskich polityków

22.06.2021 r. - W internecie opublikowano oficjalne oświadczenie[15] polskich służb dotyczące ataków na polskich polityków, w tym ministra Dworczyka. ABW i SKW ustaliły, że na liście celów było co najmniej 4350 adresów e-mail.

Jak sugeruje Niebezpiecznik, po wykryciu operacji dokonano inspekcji infrastruktury wykorzystywanej przez włamywaczy, namierzając w ten sposób logi, z których udało się pozyskać adresy, pod które rozesłano phishing.

Co najmniej 500 osób dało się skutecznie podejść atakującym, co świadczy o 12-procentowej skuteczności ataku. Wniosek jest więc taki, że atak musiał być słabo przygotowany pod kątem języka (przez co potencjalne ofiary uznały go za mało wiarygodny), albo pod kątem technicznym (i w efekcie został zablokowany przez coraz lepiej działające systemy chroniące przed spamem).

Należy tu jednak podkreślić, że nawet pojedyncza ofiara, na której skrzynkę uda się wejść, może dać atakującemu cenne informacje (szablony pism, aktualnie realizowane projekty, dostęp do wspólnych systemów, np. CRM), co pomoże mu dopracować atak na pozostałe, powiązane z nią osoby. I dla tej jednej ofiary czasem warto startować całą operację.

Jak ustalono, za atakami stoi grupa UNC1151[16] powiązana z rosyjskimi służbami.

[15] https://www.gov.pl/web/sluzby-specjalne/ustalenia-abw-i-skw-dot-atakow-hakerskich

[16] https://niebezpiecznik.pl/tag/unc1151/

Jak przejąć czyjś Profil Zaufany?

24.06.2021 r. - Serwis Niebezpiecznik opisuje kolejne przypadki użycia luki w bezpieczeństwie systemu związanego z Profilem Zaufanym. Pozwala ona na przejmowanie cudzych Profili Zaufanych — wystarczy dysponować imieniem i nazwiskiem oraz numerem PESEL ofiary.

Po przejęciu Profilu Zaufanego oszuści uzyskują dostęp do pozostałych danych o ofierze (np. tych z dokumentów tożsamości), dzięki czemu są w stanie brać na ofiarę pożyczki w bankach[17]. Co gorsza, mają też dostęp do najbardziej wrażliwych informacji, np. tych o zdrowiu.

Wykorzystanie tej luki nie wymaga założenia na czyjeś dane konta w banku. Do Profilu Zaufanego można też logować się przez Envelo, czyli przez usługę Poczty Polskiej. Z tej metody najchętniej korzystają oszuści, ponieważ weryfikacja na poczcie nie wydaje się szczególnie mocna. Oszust może się posłużyć fałszywym dowodem z dowolnie wygenerowanym numerem, ponieważ Poczta Polska nie sprawdza zgodności numeru dowodu z Rejestrem Dowodów Osobistych.

Poczta Polska stwierdziła, że skala wyłudzeń nie jest duża[18], a w reakcji na problem wprowadzono „ponadnormatywne" procedury. Niestety nie powstrzymały one kolejnych przejęć profili.

Mając czyjś Profil Zaufany, oszust może:

- sprawdzić dane osoby w rejestrze PESEL[19],
- sprawdzić dane w Rejestrze Dowodów Osobistych[20],
- sprawdzić punkty karne kierowcy[21],
- wysyłać wnioski przez praca.gov.pl (np. o pożyczkę COVID-ową[22]),
- zapoznać się z zeznaniem podatkowym przez podatki.gov.pl[23],
- sprawdzić dane w Krajowym Rejestrze Karnym[24],
- sprawdzić dane osoby w PUE ZUS[25],
- założyć firmę[26] na czyjeś dane,
- podpiąć aplikację mObywatel i mieć dostęp do recept oraz certyfikatu potwierdzającego szczepienie, a także elektronicznych wersji dokumentów, takich jak dowód osobisty i prawo jazdy.

Niestety nieposiadanie Profilu Zaufanego nikogo przed niczym

nie uchroni. Oszust zawsze może go założyć ofierze przez Envelo, a zatem lepiej mieć Profil Zaufany, by ewentualnie dostać powiadomienie o tym, że się go już nie ma... Wydział Cyfryzacji KRPM odpowiedzialny za Profil Zaufany ciągle „rozważa usunięcie" luki, która na to nadużycie pozwala.

[17] https://niebezpiecznik.pl/post/oszustowi-do-wziecia-pozyczki-wystarczyly-publicznie-dostepne-dane/

[18] https://niebezpiecznik.pl/post/poczta-polska-proby-przejecia-profili-zaufanych-dotycza-0019-wszystkich-kont/

[19] https://www.gov.pl/web/gov/sprawdz-swoje-dane-w-rejestrze-pesel

20 https://www.gov.pl/web/gov/sprawdz-swoje-dane-w-rejestrze-dowodow-osobistych1

21 https://www.gov.pl/web/gov/sprawdz-swoje-punkty-karne

22 https://niebezpiecznik.pl/post/ktos-moze-wyludzic-pozyczke-z-tarczy-w-imieniu-twojej-firmy-sprawdz-czy-juz-tego-nie-zrobil/

23 https://www.podatki.gov.pl/pit/twoj-e-pit/

24 https://www.gov.pl/web/gov/uzyskaj-zaswiadczenie-z-krajowego-rejestru-karnego

25 https://www.zus.pl/portal/logowanie.npi

26 https://prod.ceidg.gov.pl/ceidg.cms.engine/

Cyberprzestępcy biorą na celownik infrastrukturę wodną

STORMSHIELD

29.06.2021 r. - Informacje o cyberatakach skierowanych w stacje uzdatniania wody, zapory wodne, systemy nawadniania i oczyszczalnie ścieków coraz częściej trafiają na główne strony gazet i czołówki portali internetowych. Rośnie świadomość, że zagrożenie tego rodzaju atakiem jest poważnym wyzwaniem strategicznym – nie tylko dla przedsiębiorstw, ale i całego kraju. Sektor wodno-kanalizacyjny jest bowiem jednym pozbawienie miast dostępu do wody pitnej lub skażenie jej na dużym obszarze niebezpiecznymi substancjami. W Polsce wciąż wiele podmiotów z sektora wod-kan nie posiada zabezpieczeń, które są kluczowym aspektem przeciwdziałania hakerom. Wdrożenie odpowiednich zabezpieczeń sieciowych rekomenduje m.in. rządowy Departament Cyberbezpieczeństwa.

Transformacja cyfrowa jest dla sektora wodnego szansą na optymalizację działalności. Możliwość automatycznego sterowania funkcjonowaniem systemu z wykorzystaniem nowoczesnych rozwiązań i przemysłowego Internetu Rzeczy (IoT) ułatwia obsługę skomplikowanej sieci. Jednocześnie fakt, że przedsiębiorstwa wodociągowe korzystają z rozwiązań cyfrowych, powoduje, że stają się one celem cyberprzestępców. Zapewnienie bezpieczeństwa i stabilności działania systemu wodnego to jedno z najważniejszych wyzwań dla podmiotów odpowiedzialnych za infrastrukturę wodnokanalizacyjną. Jak wynika ze sprawozdania amerykańskiej spółki Gray Matter, w 2019 roku w samych Stanach Zjednoczonych odnotowano ponad 22 cyberataki na tego rodzaju infrastrukturę. Głównym narzędziem stosowanym przez cyberprzestępców jest oprogramowanie ransomware.

W 2017 roku zajmujący się cyberbezpieczeństwem eksperci Georgia State University, w ramach eksperymentu, opracowali nową formę złośliwego oprogramowania zdolnego do zatruwania wody poprzez zmianę stężenia chloru w zakładach uzdatniania wody pitnej. Kilka lat później, w lutym 2021 roku, podobnego typu atak miał miejsce w rzeczywistości w hrabstwie Pinellas na Florydzie. Po włamaniu do systemu w zakładzie uzdatniania wody, przestępcy chcieli dodać do wody pitnej niebezpieczną ilość wodorotlenku sodu. Atak został udaremniony.

Opublikowane w lutym 2021 roku rekomendacje dla sektora wod-kan polskiego rządowego Departamentu Cyberbezpieczeństwa odniosły się między innymi do ataku na Florydzie. Eksperci podkreślili winę zarówno obsługi, jak i nieadekwatnych procedur i słabej organizacji systemu bezpieczeństwa wykorzystywanych narzędzi do kontroli i nadzoru procesu. Wśród głównych przyczyn skuteczności ataku wskazano:

- Słabe zasady zarządzania hasłami - wszystkie komputery posiadały to samo hasło umożliwiające zdalny dostęp
- Podłączenie do Internetu wszystkich komputerów służących do zarządzania usługą
- Brak firewalla

Ochrona przed cyberatakami jest możliwa, wymaga jednak filtrowania wszystkich danych, które trafiają do obiektów z zewnątrz. Przedsiębiorstwa prowadzące działalność w sektorze wodno-kanalizacyjnym chronią infrastrukturę wdrażając zasady wielopoziomowej segmentacji. Polega ona na oddzielaniu wszystkich obiektów operacyjnych i kontroli przepływu komunikacji i danych. Kolejnym krokiem jest oddzielenie środowiska IT, w tym komputerów, serwerów i użytkowników od środowiska operacyjnego OT. Dzięki temu w przypadku ataku środowisko operacyjne jest odizolowane. Twórcy oprogramowania wspierają podmioty z sektora wod-kan w zakresie segmentacji i wdrażania kolejnych zabezpieczeń, na przykład w sprawdzaniu niezawodności i zgodności ich protokołów sieciowych. Wspólnym celem jest bezpieczeństwo systemów wodnych.

Uwaga na nowe warianty oszustwa na pracownika infolinii banku!

30.06.2021 r. - Portal niebezpiecznik.pl opisał nowe warianty popularnego w Polsce ataku.

1. Wariant na automat proszący o wciśnięcie 1 lub 2

Dzwoni telefon. Numer, który się wyświetla, zgadza się z oficjalnym numerem infolinii banku Millennium. Automatyczne nagranie informuje, że wniosek o kredyt został rozpatrzony pozytywnie i kwota 15.tys zł zostanie przelana na konto. Aby otrzymać kwotę, należy wcisnąć 1, a jeśli odbiorca nie składał wniosku, ma wcisnąć 2.

Osoby, które wcisną „2" (bo o kredyt nie wnioskowały), zostaną połączone z fałszywym pracownikiem banku. Zatroskany (ale fałszywy) konsultant wypyta o dane, będzie starał się pomóc, przełączał do swoich współpracowników, aż w końcu poprosi ofiarę o zainstalowanie „specjalnej aplikacji" lub podanie danych, które... umożliwią złodziejom wyprowadzenie pieniędzy z jej konta.

2. Wariant na pracownika BIK-u

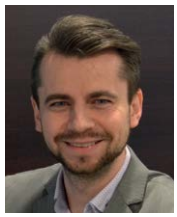
a) Ofiara odbiera telefon z infolinii BIK — z numeru 223104444. Jakiś mężczyzna mówi, że udzielono pożyczki na 20 tysięcy złotych. Człowiek ten nie mówi jak rodowity Polak, lecz zna imię i nazwisko oraz adres zamieszkania rozmówcy oraz wie, w jakim banku ma on konto. Twierdzi, że wniosek jest pozytywnie rozpatrzony i pójdzie na konto zagraniczne.
Oczywiście ofiara przyznaje, że nie wnioskowała o żaden kredyt. Wtedy oszust mówi, że to może być próba wyłudzenia. Musi zgłosić ten incydent do banku i na policję, aby uratować potencjalną ofiarę przed kradzieżą środków. Pyta o informacje (np. nazwy banków, z których korzysta ofiara) i informuje, że zapewne zaraz ktoś z banku oddzwoni. Tak się też dzieje — dzwoni ktoś (kolega, także złodziej), kto podszywa się pod bank ofiary.

b) Dzwoni kobieta przedstawiająca się jako pracownik Biura Informacji Kredytowej. Zwracając się do odbiorcy imieniem i nazwiskiem, pyta, czy osoba ta potwierdza złożenie wniosku o kredyt na kwotę 30 tysięcy złotych w Banku PKO BP. Gdy rozmówca zaprzecza, kobieta informuje, że wniosek wpłynął do banku w danym dniu o godzinie 8.30 i został zaakceptowany. Wykonywany przez nią telefon ma na charakter wyłącznie formalnego potwierdzenia. Kobieta po chwili zapewnia, że sprawa jest poważna, gdyż być może doszło do wycieku danych osobowych. Oświadcza, że sprawę skieruje niezwłocznie na policję i zabezpieczy dane potencjalnej ofiary. W ciągu 10 minut powinny się skontaktować z nią banki, w których posiada ona konta, aby zabezpieczyć dane. Dla formalności dopytuje, w jakich bankach ofiara posiada rachunki (żeby wysłać powiadomienie o wycieku danych) i jaki ma numer dowodu osobistego. Po 5 minutach pojawia się kolejne połączenie przychodzące z jednego z banków, które ofiara wspomniała. Numer jest jej znany, autentyczny, podobnie jak powitanie i komunikat, że za chwilę nastąpi połączenie z konsultantem działu bezpieczeństwa. Zgłasza się pan, który przedstawia jako pracownik Departamentu Ochrony Danych, i informuje, że otrzymał pilne zawiadomienie z Biura Informacji Kredytowej, że doszło do poważnego wycieku danych. Rzekomo sprawdza, czy było jakieś włamanie. Mężczyzna mówił płynnie, spokojnie, jest opanowany i brzmi przekonująco. W celu dopełnienia kwestii formalnych zadaje kilka pytań do weryfikacji — data ostatniej transakcję dokonanej z rachunku, ile obecnie znajduje się środków na rachunku bankowym, czy ofiara posiada rachunek oszczędnościowy, w jakiej walucie. Sprawdza logowania i w międzyczasie pyta, czy ofiara nie zgubiła dowodu, czy ktoś mógł mieć dostęp. Wszystko odbywa się bardzo wiarygodnie. Zapewnia, że po stronie banku wszystko jest w porządku, więc wyciek nie nastąpił z tej instytucji. Przełącza do następnego działu, niby w celu zabezpieczenia konta.

W opisywanym przypadku potencjalna ofiara straciła cierpliwość i zaczęła nabierać podejrzeń. Dzwoniąc samodzielnie na numer Biura Informacji Kredytowej, dowiedziała się, że instytucja ta nie posiada infolinii wychodzącej, a dziennie rejestruje ok. 40 zgłoszeń tego typu. Sprawa została zgłoszona na Policji, która nie do końca wiedziała, jak w tej sytuacji zareagować.

Naciągacze podszywają się też pod numer 22-348-4444. Gdy się odbierze taki telefon, należy się rozłączyć i samodzielnie znaleźć numer do swojego banku lub firmy, która rzekomo dzwoniła, i wykonać połączenie na własną rękę.

Jak chronić małe firmy przed zaawansowanymi atakami, nie wydając na to fortuny?



Piotr Kupczyk,
Dyrektor biura
komunikacji
z mediami
Kaspersky Lab Polska

Od tego, jak szybko uda się wykryć incydent naruszenia cyberbezpieczeństwa, może zależeć, jak poważne będą jego konsekwencje. Z najnowszego badania[1] firmy Kaspersky wynika, że małe i średnie firmy (zatrudniające poniżej tysiąca pracowników), które zidentyfikowały problem natychmiast po jego wystąpieniu, poniosły o 17% mniejsze szkody finansowe na skutek wycieku danych niż te, które wykryły atak po tygodniu lub później. Na podstawie tej samej ankiety stwierdzono, że jedynie 10% firm tej skali zdołało od razu wykryć naruszenie bezpieczeństwa. Jak to możliwe, że firmy przeoczyły tak ważny problem?

Zaawansowane ataki stały się bardziej przystępne kosztowo

Cyberprzestępcy chętniej przeprowadzą zaawansowany atak, jeśli jego koszt będzie niższy niż potencjalne zyski, czyli np. wysokość okupu otrzymanego w zamian za odszyfrowanie plików lub przychód ze sprzedaży skradzionych wrażliwych danych. Właśnie dlatego celem wyrafinowanych ataków są zwykle duże przedsiębiorstwa – po prostu szanse na zgarnięcie dużych pieniędzy są w tym przypadku wyższe.

Jednak ataki na małe i średnie firmy również stały się opłacalne. Po pierwsze, nie wymagają one od sprawców przygotowania własnego szkodliwego oprogramowania, które wymknie się jakoś rozwiązaniu bezpieczeństwa. Atakujący mogą po prostu wykorzystać „najlepsze praktyki" swoich „kolegów po fachu", na przykład kupując[2] niezbędny zestaw narzędzi. Zatem zaawansowane ataki na średnie przedsiębiorstwa również są warte zachodu.

Poza tym cyberprzestępcy mogą w ogóle nie stosować szkodliwego oprogramowania. Wystarczy, że wykorzystają legalne funkcje systemu operacyjnego lub oprogramowanie zdalnej administracji, by – niepostrzeżenie dla rozwiązań chroniących punkty końcowe – gromadzić dane uwierzytelniające lub uzyskiwać dostęp do informacji. Zespół ds. reagowania na incydenty działający w ramach firmy Kaspersky oszacował, że tego rodzaju legalne oprogramowanie dotyczyło niemal jednej trzeciej zapytań klientów[3], którzy doświadczyli cyberincydentu.

Takie zagrożenia są nie tylko trudne do wychwycenia, ale również często nie mogą być automatycznie zablokowane, ponieważ bardzo przypominają codzienne działania wykonywane przez administratora bezpieczeństwa IT. Bez przeprowadzenia dochodzenia działania podejmowane w ramach reagowania na zagrożenia mogą zakłócić istotne procesy biznesowe.

Zasoby firm nadal są ograniczone

Ogólnie rzecz biorąc, aby poradzić sobie z takimi zagrożeniami, firmy potrzebują zarówno zaawansowanych rozwiązań potrafiących gromadzić i korelować dane dotyczące bezpieczeństwa, jak również doświadczonego zespołu ds. bezpieczeństwa – w celu przeanalizowania incydentu i zareagowania na niego.

Jednak budżety przeznaczane na bezpieczeństwo nie pokrywają potrzeb w zakresie ochrony. Z badania[4] firmy Kaspersky wynika, że organizacje zatrudniające poniżej tysiąca pracowników wydały w 2020 r. średnio około 275 tys. dolarów na ochronę IT. Kwota ta nie była znacząco wyższa w stosunku do poprzedniego roku. W obecnych trudnych warunkach gospodarczych nie ma w tym nic dziwnego i oznacza po prostu, że firmy inwestują w obszary pozwalające zwiększyć zyski.

Ponadto, jeśli chodzi o wykwalifikowany personel, małe firmy zmuszone są robić więcej, mając do dyspozycji mniej. Kiedy za cyberbezpieczeństwo odpowiada jeden pracownik, co stanowi rzeczywistość w wielu małych i średnich firmach, zespołowi trudno jest zajmować się podejrzanymi zdarzeniami 24 godziny na dobę.

W takiej sytuacji najbardziej opłacałoby się „dzielić" z innymi firmami koszty centrum operacji bezpieczeństwa lub wy-

specjalizowanej jednostki odpowiedzialnej za proaktywne wyszukiwanie potencjalnych zagrożeń oraz analizę alertów. Właśnie takie rozwiązanie oferuje usługa zarządzanego wykrywania i reagowania (ang. Managed Detection and Response, MDR). Specjaliści z branży dostarczania usług badają informacje pochodzące z rozwiązań bezpieczeństwa zainstalowanych w organizacjach klientów i sugerują, w jaki sposób firma powinna zareagować na określony atak.

Na co zwracać uwagę, wybierając dostawcę usługi MDR

Głównym czynnikiem, na który należy zwrócić uwagę, są kwalifikacje w zakresie wykrywania ataków. Oczywistym dowodem potwierdzającym takie możliwości jest własny rozbudowany dział badawczy dostawcy. Prowadząc własne badania, analitycy z centrum operacji bezpieczeństwa mogą szybko znaleźć nowe zagrożenia w infrastrukturze klienta, ponieważ poznali już nowe szkodliwe taktyki i nie muszą czekać, aż informacje na ten temat staną się publicznie dostępne.

Warto również zwrócić uwagę na wykorzystywane w usłudze technologie. Przede wszystkim powinny one być wystarczająco skuteczne, aby większości zagrożeń można było zapobiec bez angażowania analityków bezpieczeństwa dostawcy czy wewnętrznego personelu ds. IT. Ponadto niektórzy dostawcy stosują algorytmy uczenia maszynowego w przetwarzaniu alertów. Dzięki automatyzacji rutynowych zadań analitycy bezpieczeństwa mogą zająć się rzeczywistymi incydentami, co pozwala skrócić czas reakcji na atak.

Po drugie, warto rozważyć koszt rozwiązania oraz łatwość wdrożenia. Dostawca usługi MDR pracuje z informacjami pochodzącymi z zaawansowanego rozwiązania wykrywania i reagowania na punktach końcowych (ang. Endpoint Detection and Response, EDR), które gromadzi i analizuje dane, aby analitycy uzyskali większą widoczność bezpieczeństwa. Takie narzędzie może okazać się zbyt drogim nabytkiem i ze względu na to, że wymaga doświadczenia, prawdopodobnie będzie wykorzystywane jedynie przez specjalistów w zakresie MDR. Takie podejście nie jest opłacalne i niweluje wszelkie korzyści finansowe outsourcingu.

Należy również zwrócić uwagę na oferowane przez dostawcę możliwości reagowania na incydenty. Najlepiej, aby było ono elastyczne i łączyło dwie możliwości: w niektórych przypadkach zespół MDR przeprowadza działania w ramach reagowania w sposób zdalny, w innych natomiast reagowanie wykonywane jest samodzielnie przez personel wewnętrzny zgodnie z dostarczonymi instrukcjami oraz z wykorzystaniem przekazanego zestawu narzędzi. Druga opcja jest pomocna na początku współpracy, kiedy klient chce się upewnić, że otrzymywane zalecenia działają i uwzględniają specyfikę jego sieci oraz procesów biznesowych. Poza tym niektóre firmy wolą reagować samodzielnie, np. w sytuacji gdy incydenty dotyczą zasobów krytycznych, takich jak komputer dyrektora. Pozwala to lepiej kontrolować sytuację oraz wynik, ponieważ nawet godzina braku dostępu do sieci w komputerze osoby ze ścisłego zarządu może spowodować utratę możliwości biznesowych.

Bardzo ważne jest również, aby w umowach o poziomie świadczonych usług został wyraźnie określony czas reakcji w zależności od priorytetu przypisanego wykrytemu incydentowi. Należy wybrać dostawcę usługi MDR, który jest w stanie najszybciej zareagować na incydenty, które mogą wyrządzić firmie ogromne szkody. Naturalnie operacje w trybie 24/7 mają istotne znaczenie w zapobieganiu atakom na wczesnym etapie niezależnie od tego, kiedy będą miały miejsce.

Istotnym czynnikiem jest również możliwość skonsultowania się z analitykami z centrum operacji bezpieczeństwa w ramach zespołu MDR. Przyda się to w sytuacjach, gdy wewnętrzny zespół będzie potrzebował bardziej zaawansowanej pomocy lub porady.

EDR, MDR, a może jedno i drugie?

Usługa MDR może pomóc organizacjom, które potrzebują szybko poprawić swoje możliwości wykrywania zagrożeń i reagowania na nie. Jednak korzystanie z niej nie oznacza zaprzestania przez firmę rozwijania wewnętrznej wiedzy eksperckiej oraz doświadczenia. Wszystko zależy od indywidualnej strategii.

Jeśli firma chciałaby rozwinąć dojrzały, wewnętrzny dział odpowiedzialny za cyberbezpieczeństwo, usługa MDR będzie pomocna w okresie przejściowym. Później może pełnić rolę wspierającą, pozwalając wewnętrznym analitykom ds. bezpieczeństwa skoncentrować się na najbardziej krytycznych incydentach.

[1] *https://r.kaspersky.pl/QruUD*
[2] *https://www.infosecurity-magazine.com/news/society-increasingly-risk-cyber*
[3] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3302*
[4] *https://calculator.kaspersky.com/app/repor*

Od cyberbezpieczeństwa do cyberodporności: jak to osiągnąć

Irina Skrypnik, Szefowa działu rozwoju produktów z systemem KasperskyOS w firmie Kaspersky

Uzarania dziejów bezpieczeństwa komputerowego, pod koniec lat osiemdziesiątych, w odpowiedzi na pojawienie się pierwszego szkodliwego programu powstał antywirus[1]. Od tamtego czasu branża IT próbuje dotrzymać kroku cyberprzestępcom, a celem rozwiązań cyberbezpieczeństwa jest jak najszybsze rozpoznanie nowych szkodliwych programów i technik oraz oferowanie odpowiedniej ochrony. Siła akcji jest równa sile reakcji.

W ciągu ponad trzydziestu lat tej rozgrywki jej stawka znacząco wzrosła. Obecnie cyberbezpieczeństwo, ochrona danych oraz zwalczanie zaawansowanych ataków APT stają się priorytetem na najwyższym szczeblu rządowym[2], a korporacje przeznaczają prawie jedną trzecią swojego budżetu IT[3] na ochronę przed cyberzagrożeniami.

Tak jak w wielu innych branżach, również w obszarze cyberbezpieczeństwa może – prędzej czy później – nastąpić ewolucyjny przeskok, który zmieni charakter gry. Być może ten moment już nadszedł: przejście od ochrony przed cyberzagrożeniami do odporności na nie.

Kiedy dotychczasowe rozwiązania bezpieczeństwa już nie wystarczają

W niektórych obszarach, takich jak ochrona korporacyjna, dotychczasowe rozwiązania okazują się bardzo skuteczne. Ale istnieją też systemy, np. urządzenia Internetu Rzeczy czy elektroniczne jednostki sterujące, w których zainstalowanie klasycznych rozwiązań antywirusowych nie jest możliwe.

Tymczasem wykorzystywanie niebędących komputerami urządzeń mających dostęp do internetu nabiera rozpędu i według prognoz[4] odnotuje 25% wzrost w latach 2019-2027. W przypadku krytycznych infrastruktur oraz inteligentnych miast digitalizacja i wykorzystywanie chmury wymagają stosowania dodatkowych środków cyberbezpieczeństwa w celu uniknięcia poważnych konsekwencji. O tym, jak bardzo mogą być one bolesne, przekonaliśmy się niedawno na przykładzie cyberincydentu, który dotknął organizację Colonial Pipeline[5].

Innym problemem jest to, że takiego ryzyka nie można z góry oszacować. Dlatego oprócz tradycyjnych sposobów ochrony potrzebne jest nowe podejście, w którym bezpieczeństwo jest cechą urządzenia, systemu lub samego rozwiązania ochrony.

Czym jest cyberodporność?

Celem cyberodporności jest scenariusz, w którym ataki nie mogą wpłynąć na funkcje systemu. System, który jest cyberodporny, opiera się na zasadzie: wszystko, co nie jest dozwolone, jest zabronione. To oznacza, że jego komponenty mogą wykonywać tylko te funkcje, które zostały zdefiniowane podczas tworzenia go.

Jak to osiągnąć?

Aby system był cyberodporny, należy rozwijać go według określonej metodologii i z zastosowaniem odpowiednich komponentów.

Po pierwsze, należy jasno określić cel systemu pod względem bezpieczeństwa – np. zapewnienie poufności oraz integralności danych przenoszonych z urządzenia do chmury. System musi spełnić ten cel w każdym przypadku użycia. Na przykład, jeżeli ktoś buduje dom na terenie narażonym na trzęsienia ziemi, musi uwzględnić odpowiednie środki ochronne już na etapie projektowania.

Po drugie, wszystkie komponenty systemu, takie jak aplikacje i sterowniki, muszą być odizolowane od siebie nawzajem. W ten sposób złamanie zabezpieczeń jednego komponentu nie zapewni dostępu do innego. To tak, jakby umieścić jabłka, pomarańcze i brzoskwinie w oddzielnych koszykach: jeśli owoce z jednego koszyka zaczną się psuć, te w innym koszyku pozostaną nietknięte.

Po trzecie, należy kontrolować komunikację między komponentami, zezwalając wyłącznie na jej określony rodzaj. Jądro takiego cyberodpornego systemu powinno być tak kompaktowe, jak to możliwe, w celu zminimalizowania ewentualnych błędów i luk w zabezpieczeniach oraz zawężenia powierzchni ataków.

W efekcie bezpieczeństwo staje się integralną cechą systemu. W praktyce oznacza to, że np. próba zdalnego połączenia się z dowolnym komponentem zaawansowanego układu wspomagającego, który odpowiada za funkcję autopilota w samochodzie, do niczego nie doprowadzi. Żadna zewnętrzna aplikacja nie będzie mogła przejąć kontroli nad systemem, ponieważ atakowany komponent pozostanie odizolowany, przez co nie będzie możliwe złamanie zabezpieczeń pozostałych części.

Dlaczego teraz?

Idea podejścia, zgodnie z którym systemy IT są projektowane z myślą o bezpieczeństwie, dojrzewała[6] w firmie Kaspersky od 2002 r. W tym czasie firma opracowała KasperskyOS — system operacyjny, który umożliwia spełnienie powyższych wymagań bezpieczeństwa. Badano również jego zastosowanie w różnych dziedzinach oraz rozpoczęto rozwijać pierwsze urządzenia wykorzystujące tę platformę.

Odporność stała się „cenionym" słowem w latach 2020/21 ze względu na pandemię. Przypadkowo również w 2020 r. koncepcja cyberodporności oparta na systemie KasperskyOS została urzeczywistniona w pierwszym produkcie ogłoszonym[7] w kwietniu 2021 r. Jest to brama dla urządzeń Internetu Rzeczy umożliwiająca klientom bezpieczne gromadzenie danych telemetrycznych z podłączonego sprzętu przemysłowego oraz przesyłanie ich do chmury w celu przetworzenia w aplikacjach biznesowych.

Cyberodporność ma przed sobą długą drogę: jej zastosowanie rozszerzy się na różne projekty i rozwiązania, które charakteryzują się wyższymi wymogami dotyczącymi cyberbezpieczeństwa w obszarze infrastruktury krytycznej, inteligentnych miast, motoryzacji oraz w wielu innych zastosowaniach. Firma Kaspersky ma nadzieję, że w dającej się przewidzieć przyszłości podejście to pomoże zapewnić jakościowo nowy poziom bezpieczeństwa w tych branżach oraz zmniejszyć prawdopodobieństwo cyberataków oraz ich konsekwencji.

[1] *https://kas.pr/8907*
[2] *https://www.cnbc.com/2021/05/12/biden-signs-executive-order-to-strengthen-cybersecurity-after-colonial-pipeline-hack.html*
[3] *https://kas.pr/2r84*
[4] *https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307*
[5] *https://en.wikipedia.org/wiki/Colonial_Pipeline_cyber_attack*
[6] *https://kas.pr/8AD4*
[7] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3392*

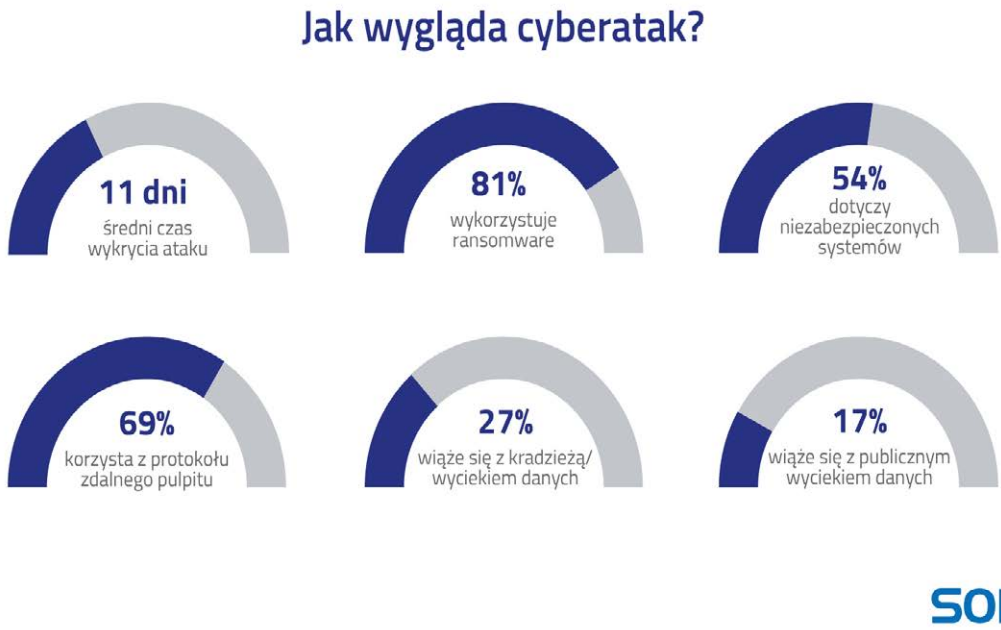
Cyberprzestępcy spędzają w firmowej sieci średnio 11 dni, zanim zostaną wykryci

Grzegorz Nocoń,
inżynier systemowy
w firmie Sophos

W trakcie pandemii ponad połowa polskich firm (54%) zauważyła wzrost liczby cyberataków. W opublikowanej w maju br. analizie pt. „Active Adversary Playbook 2021" analitycy firmy Sophos ujawniają, że przestępcy zostają wykryci średnio dopiero po 11 dniach od przeniknięcia do firmowej sieci. W tym czasie mogą swobodnie poruszać się po zasobach i wykradać dane przedsiębiorstwa. Coraz trudniej namierzyć złośliwą działalność, jednak pomocna w tym zakresie może okazać się pandemia. W ubiegłym roku wzrosły bowiem umiejętności i szybkość reagowania zespołów IT.

Nawet rok na wykradanie danych i złośliwe działania

Mimo że średnio atakujący mają aż 11 dni na działania w firmowych systemach, zanim zostaną wykryci, to według analityków Sophos w niektórych przypadkach cyberprzestępcy są namierzani nawet dopiero po 15 miesiącach. W tym czasie



mogą swobodnie przemieszczać się w sieci, przeglądać firmowe zasoby, pobierać dane uwierzytelniające i wykradać poufne informacje. W większości przypadków do ich powstrzymania nie wystarczy VPN czy wieloskładnikowe uwierzytelnianie. Metody te zabezpieczają przed nieuprawnionym dostępem z zewnątrz, jednak w aż 69% ataków zabezpieczenia te są obchodzone poprzez wykorzystanie do poruszania się wewnątrz sieci protokołu pulpitu zdalnego.

Setki narzędzi, dziesiątki grup przestępczych

Środowisko cyberzagrożeń jest złożone – w 2020 r. analitycy Sophos zidentyfikowali aż 37 różnych grup atakujących, które stosowały ponad 400 narzędzi. Wiele z nich w pełni legalnych i wykorzystywanych na co dzień także przez administratorów czy specjalistów IT. Dlatego dostrzeżenie różnicy między niegroźną a złośliwą aktywnością jest coraz trudniejsze. Sytuację dodatkowo utrudnia fakt, że przestepcy często instalują sterowniki wyłączające programy zabezpieczające, które mogłyby przerwać atak.

Czujność specjalistów powinno wzmóc wykrycie legalnego narzędzia lub aktywności w nietypowym miejscu. Ważne jest sprawdzanie każdego incydentu: fakt zablokowania pewnego działania nie oznacza, że zagrożenie w pełni zneutralizowano. Atakujący już naruszył zabezpieczenia serwera i może wypróbować inne techniki, które nie zostały wykryte. Warto ustanowić odpowiednie zasady dostępu pracowników i urządzeń do narzędzi czy aplikacji. Łatwiej wtedy namierzyć podejrzane działania.

Zespoły IT szybsze i skuteczniejsze

Według badania pt. „IT Security Team: 2021 and Beyond" ponad połowa zespołów IT w Polsce w trakcie pandemii zauważyła wzrost liczby cyberataków. Intensyfikacja zagrożeń i nakładów pracy umożliwiła im jednak nabycie nowych doświadczeń. Aż 53% zespołów uważa, że w ostatnim roku rozwinęło swoje umiejętności i wiedzę z zakresu cyfrowego bezpieczeństwa. Pomimo nowych wyzwań 36% stwierdziło, że ich morale wzrosło. Ponad połowa (52%) zauważa też, że szybciej reaguje na incydenty.

Z drugiej strony 54% zespołów IT na świecie uważa, że cyberataki są obecnie zbyt zaawansowane, aby móc sobie z nimi poradzić samodzielnie. Znaczenia nabierają więc rozwiązania bazujące na sztucznej inteligencji. Jednak nie można zapominać, że równie ważnym jak cyfrowe techniki elementem ochrony firmy jest człowiek i jego zdolność reagowania. Rozwój umiejętności i doświadczenia specjalistów IT, związany ze wzrostem nakładu pracy, przełoży się na zwiększenie bezpieczeństwa firm. Specjaliści będą potrafili korzystać z dostępnych narzędzi tak, aby w pełni chronić zasoby.

Badanie zatytułowane „IT Security Team: 2021 and Beyond" zostało przeprowadzone przez Vanson Bourne, niezależną agencję badawczą, w styczniu i lutym 2021 roku. W badaniu wzięło udział 5,4 tys. decydentów z branży IT w 30 krajach: Stanach Zjednoczonych, Kanadzie, Brazylii, Chile, Kolumbii, Meksyku, Austrii, Francji, Niemczech, Wielkiej Brytanii, Włoszech, Holandii, Belgii, Hiszpanii, Szwecji, Szwajcarii, Polsce, Czechach, Turcji, Izraelu, Zjednoczonych Emiratach Arabskich, Arabii Saudyjskiej, Indiach, Nigerii, RPA, Australii, Japonii, Singapurze, Malezji i na Filipinach. Wszyscy respondenci pochodzili z firm zatrudniających od 100 do 5 tys. pracowników.

Analizę ekspertów Sophos dotyczącą cyberataków i narzędzi wykorzystywanych przez przestępców można znaleźć na stronie: https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021.

Bezpieczny powrót do biura: w jaki sposób przedsiębiorstwa mogą ustrzec się przed ukrytymi zagrożeniami

Rick Vanover,
dyrektor ds. strategii produktowej w firmie Veeam

Dave Russell,
wiceprezes ds. strategii korporacyjnej w firmie Veeam

Wiele firm planuje wznowić normalny tryb pracy. Większość pracowników nie może się doczekać powrotu do standardowego środowiska biurowego: brakuje im bezpośredniego kontaktu z kolegami i koleżankami, wypadów na lunch i różnych elementów kultury organizacyjnej, których nie da się odtworzyć na platformie Zoom czy Teams.

Administratorzy systemów informatycznych dostrzegają jednak inne aspekty powrotu do normalności. Oczywiście również cieszą się z możliwości funkcjonowania na standardowych zasadach, ale perspektywa pojawienia się w sieci wszystkich użytkowników po dłuższym okresie pracy zdalnej budzi ich poważny niepokój. Obawiają się, że pracownicy, którzy przez ostatni czas zwracali mniejszą uwagę na kwestie bezpieczeństwa, wrócą do biura wraz ze swoimi zainfekowanymi urządzeniami, co narazi firmę na nowe zagrożenia.

Takie obawy są uzasadnione. W czasie pandemii służbowe komputery służyły do wielu różnych celów — do obsługi spotkań towarzyskich, programów treningowych i nauki przez internet, do robienia zakupów i do oglądania seriali na Netfliksie. Dzieci pożyczały sprzęt od rodziców, żeby pograć online w ulubioną grę, a wszyscy członkowie rodziny przekazywali sobie ważne hasła. Kwestie zachowania należytej staranności zabezpieczeń zeszły niestety na dalszy plan.

Cyberprzestępcy zdają sobie doskonale sprawę ze stopnia podatności środowisk pracowników — już w czasie wiosennego lockdownu w 2020 roku miała miejsce seria ataków phishingowych. Obecnie administratorzy obawiają się, że hakerzy umieścili w niezabezpieczonych laptopach szkodliwy kod, który zostanie uaktywniony w momencie ponownego podłączenia urządzeń do szerszej grupy zasobów w ramach sieci przedsiębiorstwa.

Niektóre firmy podjęły odpowiednie działania, które mają im pomóc w uniknięciu takich zagrożeń. Kiedy praca zdalna stała się ogólnie przyjętym rozwiązaniem, pracownicy otrzymywali standardowe urządzenia służbowe objęte regularnymi aktualizacjami oprogramowania antywirusowego. Większość przedsiębiorstw skupiła się jednak na działaniach zmierzających do szybkiego udostępnienia odpowiedniego środowiska roboczego, niewymagającego regularnych aktualizacji, poprawek i kontroli zabezpieczeń.

Wyniki przeprowadzonej w lutym ankiety dotyczącej cyberbezpieczeństwa[1] wskazują, w jakim stopniu przedsiębiorstwa są nieprzygotowane na zagrożenia związane z powrotem personelu do pracy. Aż 61% ankietowanych używało w domu prywatnych urządzeń, a nie sprzętu przydzielanego przez pracodawcę. Jedynie 9% korzystało z korporacyjnego systemu antywirusowego, a tylko 51% uzyskało wsparcie informatyczne podczas przechodzenia na zdalne stacje robocze.

Administratorzy przygotowują się na kłopoty. W sieci pojawi się duża liczba potencjalnie źle zabezpieczonych urządzeń, a do tego należy uwzględnić warunki tzw. nowej normalności i działanie w modelu hybrydowym, czyli obecność pracowni-

ków zarówno w domach, jak i w biurze. Według raportu firmy Veeam o ochronie danych[2] aż 89% przedsiębiorstw znacznie zwiększyło zakres wykorzystania usług chmurowych w związk u z pracą zdalną. Należy się spodziewać utrzymania takiego trendu, wzrośnie zatem liczba urządzeń końcowych, które powinny zostać objęte ochroną.

W jaki sposób przedsiębiorstwa mogą przygotować się do zmiany środowiska pracy? Przedstawiamy kilka kroków, nad podjęciem których warto się zastanowić.

Rygorystyczny proces przygotowania do powrotu do pracy

W ramach tego etapu administratorzy infrastruktury informatycznej fizycznie kontrolują wszystkie zasoby i sprawdzają, czy są one przygotowane do pracy w standardowym środowisku.

Pierwszym krokiem powinno być dokonanie oceny ryzyka dla każdego pracownika i każdego urządzenia. Konieczne jest ustalenie, które urządzenia podlegały aktualizacjom i regularnemu serwisowaniu. Na komputerach używanych do pracy zdalnej znajdują się zapewne poufne dane przedsiębiorstwa — należy sprawdzić, gdzie i na czyim koncie zostały one zapisane. Celem takich działań jest minimalizacja ryzyka i zapewnienie zgodności ze standardami i przepisami, np. z rozporządzeniem RODO.

Należy również ustalić, czy pracownicy przekazywali hasła członkom rodziny korzystającym ze służbowych komputerów, a jeśli tak, to czy później je zmienili. Konieczne jest także sprawdzenie, czy używali tych samych haseł na kontach firmowych i prywatnych oraz czy instalowali nowe aplikacje lub usuwali oprogramowanie w okresie pracy zdalnej. Administratorzy muszą poznać odpowiedzi na takie pytania, zanim zezwolą użytkownikom na rozpoczęcie pracy w sieci.

Kolejnym krokiem powinno być sprawdzenie wszystkich urządzeń w celu wyszukania niedozwolonych aplikacji i innego oprogramowania. Użytkownicy często musieli szukać kreatywnych rozwiązań ułatwiających realizację codziennych zadań w środowisku roboczym, mogli jednak przy tej okazji skorzystać z zasobów niespełniających standardów bezpieczeństwa. Należy uruchomić skanowanie wszystkich urządzeń końcowych ponownie podłączanych do sieci w celu wykrycia potencjalnych luk w zabezpieczeniach. Cyberprzestępcy często za cel ataku obierają punkty końcowe, więc zespoły informatyków muszą przeskanować wszystkie firmowe i prywatne urządzenia, które mają znaleźć się w sieci przedsiębiorstwa.

Zwiększenie poziomu „higieny cyfrowej" pracowników

W okresie pracy zdalnej część użytkowników mogła nie przywiązywać wagi do kwestii cyberbezpieczeństwa, lecz po powrocie do biura osoby te muszą znów przestrzegać ściślejszych zasad cyfrowej higieny. Powinny one używać odrębnych haseł na urządzeniach służbowych i prywatnych, a także tworzyć hasła według złożonych reguł, tak aby były one trudne do złamania. Warto wrócić do regularnych szkoleń przedstawiających sposoby wykrywania różnych zagrożeń, m.in. rozpoznawania wiadomości stanowiących próbę wyłudzenia informacji. Trzeba określić zasady korzystania z publicznych sieci Wi-Fi i pobierania materiałów. W trakcie powrotu pracowników do biura administratorzy muszą zmodyfikować poszczególne procedury informatyczne, dążąc do ochrony przedsiębiorstwa przed największymi zagrożeniami.

Monitorowanie wszystkich działań

Najlepszą metodą wykrycia problemów jest skonfigurowanie systemu, który oznaczy odpowiednie sytuacje w momencie ich wystąpienia. Taką procedurą można objąć narzędzia i zachowania pracowników, którzy zaczynają ponownie używać wszystkich aplikacji w sieci przedsiębiorstwa. Narzędzia do monitorowania pozwalają zidentyfikować zmiany w sposobie użycia zasobów i programów. Jeśli pracownik dokonuje zmiany w aplikacji, administratorzy powinni o tym wiedzieć, ponieważ może chodzić o wprowadzenie błędnego fragmentu kodu. Może to być również wcześniejsza zmiana, wprowadzona świadomie lub nieświadomie przez informatyków, którą należy obecnie wycofać. Administratorzy powinni wyrobić sobie nawyk sprawdzania narzędzi do monitorowania co najmniej kilka razy dziennie. Zwykle zajmuje to kilka minut, a pozwala na bieżąco kontrolować stan cyberzabezpieczeń w przedsiębiorstwie.

Wdrożenie skutecznych metod zarządzania danymi w chmurze i tworzenia kopii zapasowych

W obecnej sytuacji administratorzy systemów informatycznych muszą zadbać o prawidłowe funkcjonowanie wszystkich usług zarządzania danymi i tworzenia kopii zapasowych. Konieczne są procedury zapewniające ochronę i pełną dostępność danych oraz sprawnie działający system tworzenia kopii zapasowych na wypadek, gdyby przejęte urządzenie powodowało zagrożenie bezpieczeństwa pewnych informacji. Warto pamiętać o tzw. regule 3-2-1: powinny istnieć co najmniej trzy kopie danych przedsiębiorstwa, ważne dane muszą być zapisane na co najmniej dwóch rodzajach nośników, a jedna z kopii zapasowych powinna być przechowywana w innej lokalizacji. W związku z rozpowszechnieniem ataków typu ransomware zalecamy rozszerzenie reguły 3-2-1 do 3-2-1-1-0: dodajemy kolejną jedynkę oznaczającą nośnik odłączony od sieci i wskazujemy, że podczas odtwarzania żadne ze stosowanych rozwiązań nie ma prawa generować błędów.

Wnioski

Administratorzy systemów informatycznych, podobnie jak pozostali pracownicy, cieszą się z możliwości powrotu do normalnych warunków współpracy w firmie i nieformalnych, swobodnych kontaktów, jednak mają uzasadnione obawy dotyczące kwestii cyberbezpieczeństwa, związane z ponownym pojawieniem się w sieci dużej grupy użytkowników. Z taką sytuacją rzeczywiście wiążą się poważne wyzwania. Jednak właściwe planowanie i odpowiednie działania mogą sprawić, że przedsiębiorstwo będzie w stanie umiejętnie zarządzać ryzykiem i wzmocnić strategie ochrony zasobów.

[1] *https://www.pcmatic.com/news/covid-19/*
[2] *https://www.veeam.com/wp-2021-data-protection-trends.html*

Cyfrowa transformacja opiera się na zaufaniu

Edwin Weijdema, globalny specjalista ds. technologii, dział strategii produktowej w firmie Veeam

Jesteśmy coraz bardziej uzależnieni od technologii, z której korzystamy w celach związanych z pracą, komunikacją i rozrywką. Musimy więc jej zaufać. Jeśli wybraliśmy pracę z domu zamiast dojeżdżania do biura, to chcemy mieć pewność, że nasz laptop jest w pełni sprawny, łącze internetowe stabilne, a niezbędne aplikacje chmurowe zawsze dostępne. Jest jednak naturalne, że podświadomie bardziej boimy się awarii urządzeń i połączeń podczas pracy w domu niż w biurze, gdzie w tym samym budynku pracuje zespół informatyków.

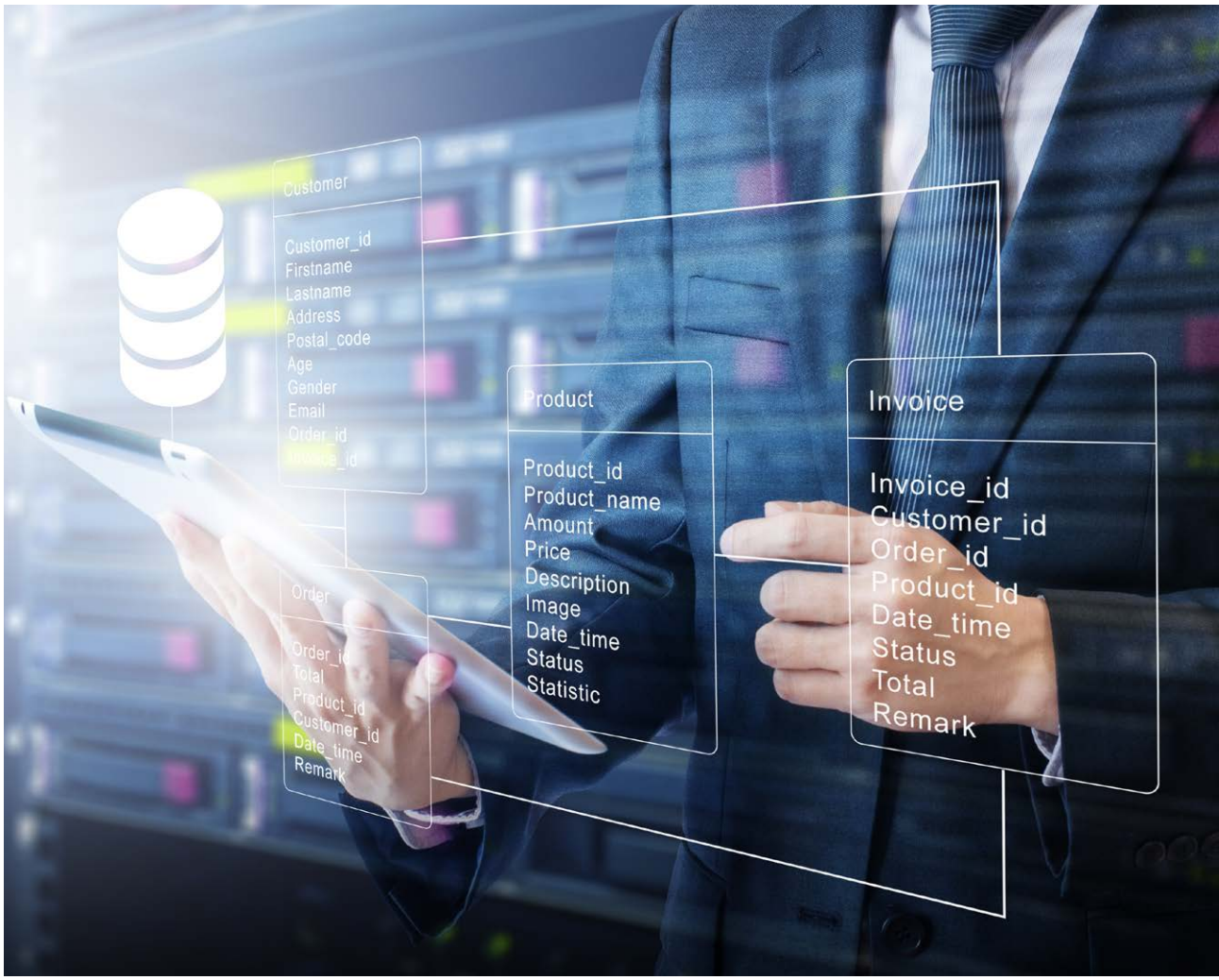
Obdarzenie zaufaniem technologii często oznacza zawierzenie czemuś nieznanemu. Na tym zresztą polega istota zaufania. Czy potrafimy uwierzyć komuś lub czemuś w stopniu, który pozwoli nam przezwyciężyć uczucie niepewności? Bez zaufania nie podejmiemy ryzyka i nie zrobimy kroku w nieznane, więc nigdy niczego nie zmienimy. Przedsiębiorstwa realizują dziś transformację cyfrową. Czy brak zaufania do technologii nie zniechęci ich do podjęcia ryzyka niezbędnego w przypadku każdej zmiany?

Proces obdarzania zaufaniem produktu lub usługi technologicznej jest bardzo podobny jak w przypadku człowieka. Wiąże się z nim kilka mechanizmów. Pierwszy z nich jest oparty na naszym pierwotnym instynkcie. Często wiemy, czy możemy komuś zaufać, już po 30 sekundach od chwili jego poznania. To samo dotyczy technologii. Co decyduje o tym, czy uznamy urządzenie, stronę WWW lub wiadomość za godne zaufania? Wszystko — od logotypu marki po pierwszą interakcję z interfejsem użytkownika. Jak wynika z badań, istnieje większe prawdopodobieństwo, że odbierzemy połączenie telefoniczne z numeru, który znamy. Gdy mamy udostępnić dane osobowe podczas rejestracji na stronie usług online, stajemy się podejrzliwi. Nie wahamy się jednak podać tych samych danych urzędnikowi bankowemu lub doradcy kredytowemu.

Choć nasze instynkty mają wielką siłę, czasem nas zawodzą. W realnym świecie zdarza się, że wierzymy w coś, co nasz przyjaciel powiedział tylko żartem, lub jedziemy w niedzielę do biura, ponieważ nasz mózg przełączył się w tryb „autopilota". W sferze cyfrowej zawierzenie instynktom lub błąd w rozumowaniu może spowodować, że klikniemy odsyłacz mający na celu wyłudzenie informacji, narazimy na niebezpieczeństwo dane osobowe lub uznamy fałszywą wiadomość za prawdziwą.

Zaufanie nie opiera się jednak tylko na instynktownej reakcji. Nabieramy go z czasem, na podstawie doświadczeń nie tylko naszych, lecz również innych ludzi. Gdy przeczytamy relacje osób, których nigdy nie spotkaliśmy, możemy zmniejszyć poczucie niepewności i niechęć do ryzyka, aby odważniej zrobić krok w nieznane. Można to nazwać zaufaniem dystrybuowanym. Łatwiej zaufamy dekoratorowi wnętrz i powierzymy mu odnowienie mieszkania, jeśli przeczytamy w internecie, że ma on duże doświadczenie i dobre oceny, oraz obejrzymy jego prace. To samo odnosi się do technologii. Przykładowo, większość ludzi nie należy do konsumentów, którzy jako pierwsi kupują nowe produkty lub korzystają z nowych rozwiązań technologicznych, zanim wejdą one do powszechnego użytku. Technologia pomaga nam w zmniejszeniu niepewności, zapewniając dostęp do ogromnej liczby informacji, które można nazwać „wyzwalaczami zaufania".

Większość użytkowników technologii i informatyków woli jednak poczekać. Niezależnie od tego, czy chodzi o nowy smartfon, czy o przeniesienie danych do chmury publicznej, wielu z nas chce przed zakupem zasięgnąć opinii osób, które wcześniej używały już takiego produktu czy usługi. Szukamy tych osób wśród kolegów i znajomych, pracowników innych firm, niezależnych konsultantów, a także ludzi zupełnie nam nieznanych, czasem mieszkających na drugim końcu świata. W branży IT nie bez powodu mówi się, że żaden pracownik nie zostanie zwolniony za korzystanie z produktów niektórych marek. Chodzi o marki, które stały się znane i cenione dzięki swojej niezawodności, spójności i świetnej obsłudze klienta. Ludzie ufają, że produkty i usługi tych marek będą działać zgodnie z zapewnieniami ich dostawców, wspartymi długą historią sukcesów. Postrzegają więc ryzyko inwestycji w taki zakup jako mniejsze niż w przypadku mniej znanych marek.



Jednym z najważniejszych czynników, od których zależy zaufanie do technologii w przedsiębiorstwie, jest bezpieczeństwo. Czy dane będą bezpieczne i skutecznie chronione? Firmy chcą również wiedzieć, co się stanie, gdy coś pójdzie nie tak — na przykład zawiedzie technologia. Jak przywrócić dostęp do usług online i szybko odzyskać dane? Dlatego dziś, gdy zarząd każdej firmy realizuje transformację cyfrową, dyrektorzy ds. informatycznych i informatycy muszą mieć pewność, że dostawcy technologii, którym zaufali, spełnią ich oczekiwania. Jak wynika z raportu[1] firmy Veeam na temat ochrony danych w 2021 roku, 27% dyrektorów przedsiębiorstw w regionie EMEA uważa, iż zagrożenia cybernetyczne mogą im utrudnić transformację cyfrową w ciągu najbliższych 12 miesięcy. Dyrektorzy mają więc coraz większą świadomość, że incydenty z zakresu cyberbezpieczeństwa mogą pogorszyć wyniki finansowe firmy. Z pewnością nie pozostanie to bez wpływu na wybór partnerów w zakresie transformacji cyfrowej.

Przedsiębiorstwa zaczynają również rozumieć, że naruszenie bezpieczeństwa danych, zarówno na skutek kradzieży, jak i zgubienia, jest jedną z najpewniejszych dróg do utraty zaufania. Jak wynika z naszych badań, 51% szefów przedsiębiorstw uważa, iż przestoje i utrata danych mogą osłabić zaufanie klientów, a 34% obawia się w takim przypadku utraty wiary w firmę przez pracowników. Zdaniem 43% ankietowanych incydenty takie szkodzą integralności marki, co wskazuje na nierozerwalny związek między ochroną danych i zaufaniem.

Jeśli chodzi o obecną skuteczność zabezpieczenia danych w przedsiębiorstwach, to na skutek awarii systemu tworzenia kopii zapasowych i ich niekompletności nawet 58% danych może pozostawać poza ochroną. Problemy związane z ochroną danych i cyberbezpieczeństwem stwarzają jednak zagrożenie dla transformacji cyfrowej. Jest oczywiste, że w relacjach człowieka z technologią — niezależnie od tego, czy chodzi o klienta, pracownika czy osobę decyzyjną w firmie — najważniejsze jest zaufanie. Przedsiębiorstwa powinny więc zwracać się do zaufanych doradców w zakresie technologii, którzy pomogą im przeprowadzić transformację cyfrową w oparciu o solidne podstawy, z zastosowaniem odpowiednio dobranych zabezpieczeń.

[1] *https://www.veeam.com/wp-2021-data-protection-trends.html*

Włamanie na konto nie zawsze musi mieć miejsce – cyberprzestępcy chętnie sięgają po publiczne dane

Zespół analityków Fortinet

W czasie pandemii COVID-19 media społecznościowe stały się dla wielu osób kluczowym narzędziem do utrzymywania kontaktu z bliskimi. Korzystanie z popularnych platform może być jednak obarczone pewnym ryzykiem, a cyberprzestępcy wcale nie muszą wykradać danych, bo użytkownicy sami podają im jak na talerzu wiele cennych informacji.

Dla cyberprzestępców dane publicznie udostępniane przez użytkowników, takie jak adresy e-mail czy numery telefonów, są bardzo atrakcyjne. Każdy, kto podaje je w mediach społecznościowych, powinien mieć świadomość, że mogą one zostać wykorzystane do wysyłania spamowych SMS-ów czy e-maili. Tego typu dane są sprzedawane na czarnym rynku, a następnie wykorzystywane w kampaniach phishingowych. Osoby, które podają do publicznej wiadomości numer telefonu, muszą szczególnie uważać na tzw. smishing, czyli próby wyłudzenia za pomocą SMS-ów.

Jak rozpoznać phishing?

Jakiego rodzaju wiadomości powinny wzbudzać szczególną ostrożność użytkowników? Eksperci Fortinet wskazują kilka elementów. Pierwszym z nich jest zachęta do natychmiastowego działania. Cyberprzestępcy lubią motywować odbiorców wiadomości do tego, aby od razu kliknęli przesłany link lub otworzyli załączony dokument. W tym celu często wywołują określone emocje: w phishingu najczęściej wykorzystywane jest poczucie strachu (e-mail informuje np. o niezapłaconych mandatach), ale także zaangażowanie (e-mail informuje np. o możliwości szybszego otrzymania szczepionki przeciw COVID-19) czy też litość (fałszywe zbiórki charytatywne).

Ponadto przestępcy podszywają się chętnie pod firmy, które prowadzą częstą komunikację z klientami – kurierskie, sklepy internetowe czy dostawców internetu lub telewizji. Wysyłają wówczas informacje o dodatkowych lub zaległych rachunkach, promocjach czy konieczności wniesienia dodatkowych opłat, np. za

dezynfekcję paczki.

Warto też zwrócić uwagę na niepoprawny język. Wiadomości wysyłane przez hakerów często są napisane niepoprawną gramatyką, zawierają liczne błędy i literówki. Wynika to głównie z faktu, że cyberprzestępcy niewładający językiem polskim korzystają z niedoskonałych tłumaczeń automatycznych.

Jeśli wiadomość wzbudza wątpliwości, ale jednocześnie jest napisana poprawnie, należy dokładnie sprawdzić domenę adresu, z którego została wysłana, oraz umieścić kursor na znajdującym się w treści wiadomości linku (lub na grafice, jeśli umieszczony został w niej link), aby sprawdzić rzeczywisty adres.

W przypadku, gdy zweryfikowanie powyższych elementów nie rozwiewa wątpliwości, należy skontaktować się nadawcą e-maila np. telefonicznie lub za pomocą zweryfikowanego adresu e-mail i w ten sposób sprawdzić, czy otrzymana wiadomość pochodzi z prawdziwego źródła.

Chrońmy prywatność w internecie

Zachowanie bezpieczeństwa w platformach społecznościowych zależy w dużej mierze od samych użytkowników. Każdy z nich powinien z rozwagą publikować informacje o sobie i swojej rodzinie i starać się nie upubliczniać takich danych jak data urodzenia, miejsce pracy czy wizerunek dzieci.

To tak, jak byśmy w realnym świecie chodzili w miejscu publicznym z tabliczką, na której byłyby wypisane wrażliwe informacje na nasz temat. Nikt tak nie postępuje, zatem warto uświadomić sobie, że bardzo podobne konsekwencje ma udostępnianie informacji o swoim życiu w cyberprzestrzeni.

Podczas korzystania z serwisów społecznościowych warto więc pamiętać o odpowiednim zabezpieczeniu konta za pomocą silnego hasła oraz weryfikacji wieloetapowej, a następnie o wyborze odpowiednich ustawień prywatności. Ostatecznie, podobnie jak w przypadku korzystania z każdego zasobu w internecie, wiele zależy od samych użytkowników i zachowania przez nich zdrowego rozsądku.

Wyróżnione ryzyko: zagrożenia występujące po dostarczeniu wiadomości e-mail

Działania podejmowane po tym, jak złośliwy e-mail ominie zabezpieczenia organizacji i znajdzie się w skrzynce odbiorczej użytkownika, mogą być równie ważne jak te, które są podejmowane na wcześniejszym etapie.

Aby lepiej zrozumieć wzorce zagrożeń i praktyki reagowania na nie, analitycy z firmy Barracuda przeanalizowali działania i wzorce zachowań w ponad 3500 organizacjach. Okazało się, że przeciętna organizacja licząca 1100 użytkowników doświadcza miesięcznie około 15 incydentów związanych z bezpieczeństwem poczty elektronicznej, a każdy atak phishingowy, który zdoła się przedostać, dotyka średnio 10 pracowników.

Stwierdzono również, że 3% pracowników kliknie łącze w szkodliwym e-mailu, narażając całą organizację na atak. Mimo że liczby bezwzględne mogą wydawać się niewielkie, potencjalna skala zagrożenia jest znacząca, ponieważ hakerom wystarczy jedno kliknięcie lub odpowiedź, aby atak zakończył się sukcesem.

Zidentyfikowano także działania, które mogą przynieść wymierne korzyści po dostarczeniu wiadomości. Analiza wykazała, że organizacje, które przeszkolą swoich użytkowników, już po dwóch kampaniach szkoleniowych odnotują 73-procentowy wzrost w zasadności zgłoszeń podejrzanych wiadomości e-mail.

Oto bliższe spojrzenie na wzorce zagrożeń i praktyki reagowania, które odkryli analitycy firmy Barracuda, a także kroki, które można podjąć, aby usprawnić reakcję organizacji na zagrożenia związane z wiadomościami e-mail po ich dostarczeniu.

Zagrożenia występujące po dostarczeniu wiadomości e-mail

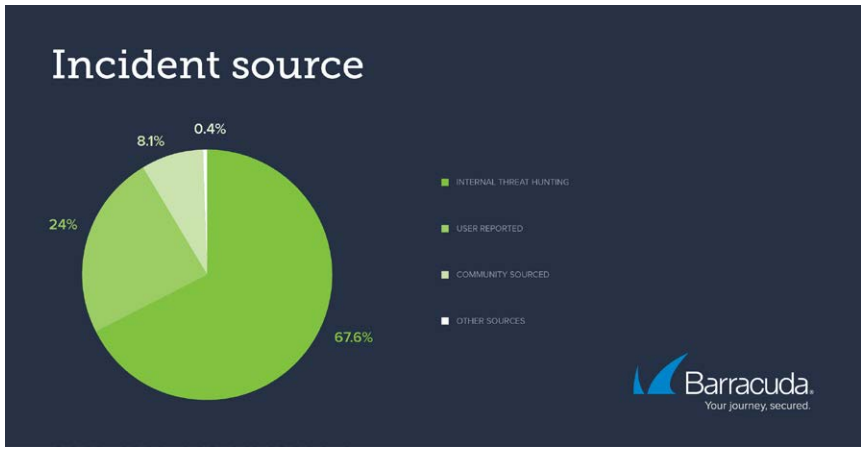
Działania, których celem jest zarządzanie następstwami naruszenia bezpieczeństwa i zagrożeniami występującymi po dostarczeniu wiadomości e-mail, są powszechnie określane mianem reagowania na incydenty. Skuteczna reakcja na incydenty ma na celu szybkie usunięcie zagrożenia, aby zatrzymać rozprzestrzenianie się ataku i zminimalizować potencjalne szkody.

Coraz częstsze ataki z wykorzystaniem poczty elektronicznej stanowią poważne zagrożenie dla organizacji. Ponieważ hakerzy wykorzystują coraz bardziej wyrafinowane techniki socjotechniczne, zagrożenia związane z pocztą elektroniczną stają się trudne do wykrycia zarówno przez mechanizmy kontroli technicznej, jak i użytkowników poczty elektronicznej. Nie istnieje rozwiązanie zabezpieczające, które potrafi zapobiec wszystkim atakom. Ponadto użytkownicy nie zawsze zgłaszają podejrzane wiadomości e-mail, ponieważ albo nie przeszli odpowiedniego szkolenia, albo zapominają o konkretnych procedurach bezpieczeństwa. Z drugiej strony, gdy pracownicy informują o incydencie, często dokładność tych zgłoszeń jest niska, co skutkuje marnowaniem zasobów IT. Bez skutecznej strategii reagowania na incydenty zagrożenia często pozostają niewykryte do momentu, aż jest za późno.

Szczegóły

Zgodnie z raportem przygotowanym przez ekspertów firmy Barracuda uwzględniającym ponad 3500 podmiotów przeciętna organizacja licząca 1100 użytkowników doświadcza około 15 incydentów związanych z bezpieczeństwem poczty elektronicznej miesięcznie. „Incydent" w tym przypadku odnosi się do złośliwych wiadomości e-mail, które przedostały się przez techniczne rozwiązania zabezpieczające do skrzynek odbiorczych użytkowników. Po zidentyfikowaniu tych incydentów należy ustalić priorytety, zbadać ich zakres i poziom zagrożenia, a jeśli zostaną uznane za zagrożenie, konieczne jest również podjęcie działań zaradczych.

Zagrożenia dla poczty elektronicznej



Rys. 1 Źródło incydentu

występujące po dostarczeniu wiadomości można identyfikować na wiele sposobów: zgłoszenia od użytkowników, wewnętrzne programy wykrywania zagrożeń uruchamiane przez działy IT lub informacje od społeczności w innych organizacjach, które zajmują się usuwaniem skutków ataków. Dane o usuniętych zagrożeniach, współdzielone przez organizacje, są zazwyczaj bardziej wiarygodne niż dane zgłoszone przez użytkowników.

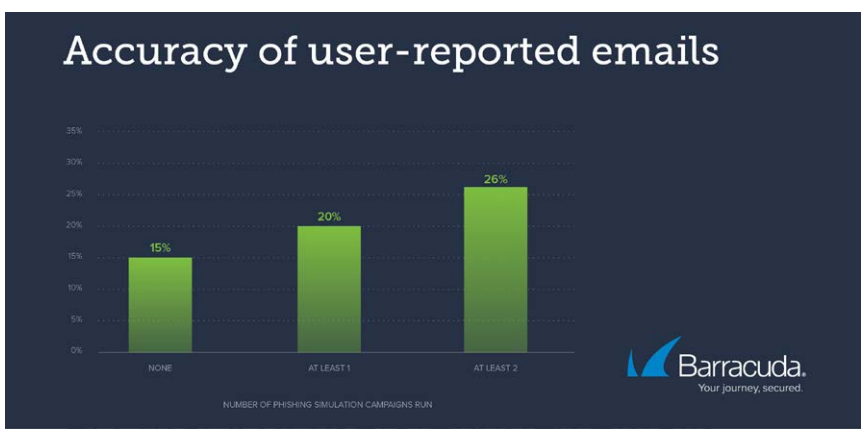
Analitycy firmy Barracuda ustalili, że większość incydentów (67,6%) została odkryta w wyniku wewnętrznych dochodzeń dotyczących zagrożeń, wszczętych przez zespół IT. Dochodzenia te mogą być inicjowane na różne sposoby. Powszechne praktyki obejmują przeszukiwanie logów wiadomości lub wyszukiwanie słów kluczowych lub nadawców w już dostarczonej poczcie. Kolejne 24% incydentów zostało stworzonych na podstawie wiadomości e-mail zgłoszonych przez użytkowników, 8,1% odkryto przy użyciu wywiadu środowiskowego, a pozostałe 0,4% poprzez inne źródła, takie jak zautomatyzowane lub wcześniej rozwiązane incydenty.

Organizacje powinny zawsze zachęcać użytkowników do zgłaszania podejrzanych wiadomości e-mail, ale napływ zgłoszeń może być uciążliwy dla zespołów IT dysponujących ograniczonymi zasobami. Dobrym sposobem na zwiększenie dokładności zgłoszeń jest konsekwentne prowadzenie szkoleń z zakresu świadomości bezpieczeństwa. Nasze badania wykazały, że organizacje, które szkolą swoich użytkowników, już po dwóch kampaniach szkoleniowych odnotowują 73% wzrost dokładności raportowanych przez nich wiadomości e-mail.

3% użytkowników klika łącza w złośliwych e-mailach

Po zidentyfikowaniu i potwierdzeniu złośliwych wiadomości e-mail administratorzy IT muszą zbadać potencjalny zakres i wpływ ataku. Bez odpowiednich narzędzi identyfikacja wszystkich osób w organizacji, które otrzymały złośliwe wiadomości, może być niezwykle czasochłonna. Badania Barracudy wykazały, że średnio 10 pracowników jest dotkniętych każdym atakiem phishingowym, który zdoła się przedostać.

Ponadto 3% pracowników kliknie łącze w złośliwym e-mailu, narażając całą organizację na atak. Innymi słowy, przeciętna organizacja licząca 1100 użytkowników będzie miała około pięciu użytkowników, którzy klikną link w złośliwej wiadomości e-mail każdego miesiąca. Pracownicy będą również przesyłać dalej lub odpowiadać na złośliwe wiadomości, rozprzestrzeniając ataki dalej w obrębie swojej firmy lub nawet na zewnątrz. Wystarczy 16 minut, aby użytkownicy kliknęli złośliwy link[1], dlatego szybkie zbadanie sprawy i usunięcie skutków ataku jest kluczowe dla zapewnienia bezpieczeństwa organizacji.



Rys. 2 Dokładność zgłoszeń od użytkowników w sprawie e-maili

Złośliwe e-maile pozostają w skrzynkach użytkowników przez 83 godziny, zanim zostaną usunięte

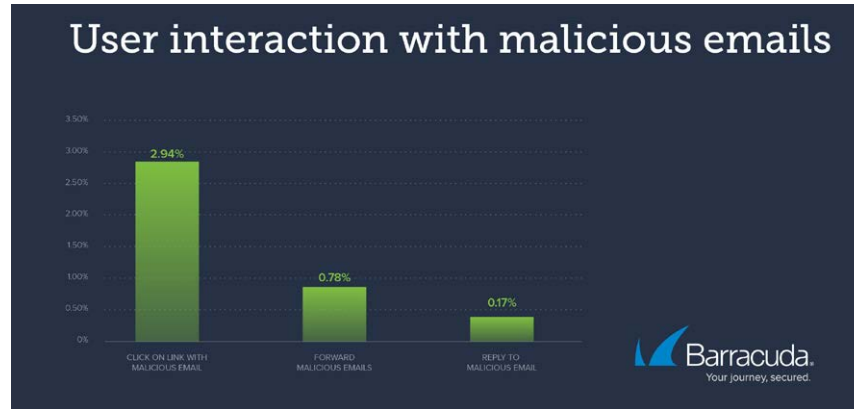
Usuwanie skutków ataków może być procesem długotrwałym i czasochłonnym. Analitycy firmy Barracuda ustalili, że od momentu, w którym atak trafia do skrzynek użytkowników, do momentu wykrycia go przez zespół bezpieczeństwa lub zgłoszenia przez użytkowników i ostatecznego usunięcia, mija średnio trzy i pół dnia (ok. 84 godziny). Czas ten można znacznie skrócić dzięki ukierunkowanym szkoleniom z zakresu bezpieczeństwa[2], które poprawią dokładność zgłoszeń od użytkowników, oraz wdrożeniu zautomatyzowanych narzędzi naprawczych[3], które mogą automatycznie identyfikować i usuwać ataki, uwalniając czas pracowników działu bezpieczeństwa.

Wiele zespołów ds. bezpieczeństwa wykorzystuje również informacje o zagrożeniach pochodzące z rozwiązanych incydentów do aktualizacji polityk bezpieczeństwa i zapobiegania przyszłym atakom. Na przykład 29% organizacji regularnie aktualizuje utworzone przez siebie listy zawierające określonych nadawców lub regiony geograficzne, których wiadomości są blokowane. Jednak tylko 5% organizacji będzie aktuali-

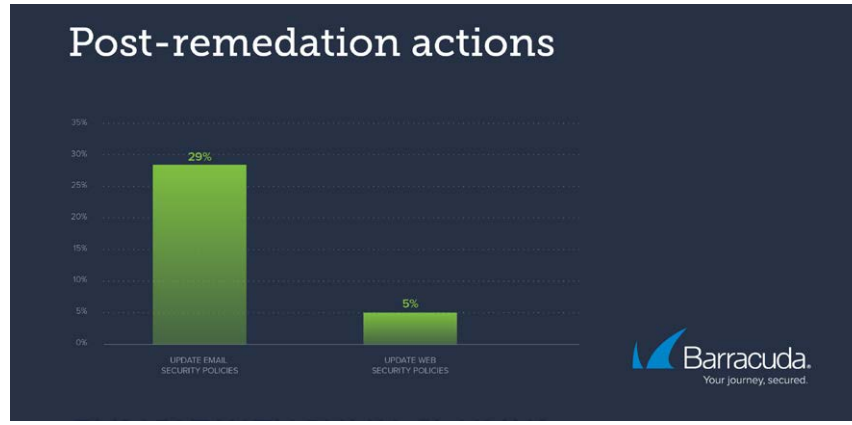
zować swoje zabezpieczenia internetowe, aby zablokować dostęp do złośliwych witryn dla całej organizacji. Ten niewielki odsetek wynika z braku integracji pomiędzy reagowaniem na incydenty a bezpieczeństwem sieciowym w większości organizacji.

Jak chronić się przed zagrożeniami po dostarczeniu wiadomości e-mail

- **Wyszkol swoich użytkowników, aby zwiększyć dokładność i liczbę zgłaszanych ataków.**
  Wyedukowany użytkownik poczty elektronicznej może zapobiec niszczącym skutkom udanego ataku. Ciągłe szkolenie w zakresie świadomości bezpieczeństwa[4] zwiększy prawdopodobieństwo, że użytkownicy będą zgłaszać potencjalne zagrożenia do swojego zespołu IT, zamiast odpowiadać, klikać lub przesyłać je dalej. Szkolenia dla użytkowników końcowych powinny być częste, tak aby najlepsze praktyki bezpieczeństwa zostały na stałe przyswojone, a dokładność zgłaszanych zagrożeń chroniła dział IT przed poświęcaniem zbyt dużej ilości czasu na badanie wiadomości niechcianych, które nie stwarzają zagrożenia.
- **Polegaj na społeczności jako źródle potencjalnych zagrożeń.**
  Dzielenie się danymi o zagrożeniach to skuteczny sposób zapobiegania zagrożeniom, które ewoluują i narażają na szwank dane i użytkowników. Powiązane, a czasami identyczne zagrożenia związane z wiadomościami e-mail mogą dotyczyć więcej niż jednej organizacji, ponieważ hakerzy często wykorzystują te same techniki ataków na wiele celów. Zamiast korzystania wyłącznie z danych o zagrożeniach zebranych przez indywidualną sieć organizacji, skutecznym podejściem do pokonywania ataków na dużą skalę jest wykorzystanie danych wywiadowczych gromadzonych przez inne organizacje. Upewnij się, że firmowe rozwiązanie reagowania na incydenty może uzyskać dostęp i wykorzystać współdzielone dane o zagrożeniach w celu skutecznego wyszukiwania zagrożeń i ostrzegania o potencjalnych incydentach.
- **Wykorzystaj narzędzia do wyszukiwania zagrożeń w celu szybszego badania ataków.**
  Odkrywanie potencjalnych zagrożeń, jak również identyfikacja zakresu ataku i wszystkich dotkniętych użytkowników może zająć godziny, a nawet dni. Organizacje powinny wdrożyć narzędzia do wyszukiwania zagrożeń, które dają im wgląd w pocztę po jej dostarczeniu. Narzędzia te mogą być wykorzystywane do identyfikacji anomalii w już dostarczonej poczcie, szybkiego wyszukiwania zaatakowanych użytkowników i sprawdzania, czy weszli oni w interakcję ze złośliwymi wiadomościami.
- **Automatyzuj działania zaradcze tam, gdzie to możliwe.**
  Zautomatyzowane systemy reagowania na incydenty[5] mogą znacznie skrócić czas potrzebny na zidentyfikowanie podejrzanych wiadomości e-mail, usunięcie ich ze skrzynek wszystkich użytkowników, których dotyczą, oraz zautomatyzowanie procesów, które wzmocnią obronę przed przyszłymi zagrożeniami. Wdrażając zautomatyzowane przepływy pracy, klienci firmy Barracuda skrócili czas reakcji nawet o 95%, skracając czas rozprzestrzeniania się zagrożenia i uwalniając swoje zespoły IT, które mogą skupić się na innych zadaniach związanych z bezpieczeństwem.
- **Wykorzystaj punkty integracji.**
  Organizacje muszą nie tylko zautomatyzować swoje przepływy pracy, ale także zintegrować reagowanie na incydenty z zabezpieczeniami poczty elektronicznej i stron internetowych, aby zapobiec dalszym atakom. Dane zebrane podczas reagowania na incydenty mogą być również wykorzystane do automatycznych działań naprawczych i pomocy w identyfikacji powiązanych zagrożeń.



Rys. 3 Interakcje użytkowników ze złośliwymi e-mailiami



Rys. 4 Działania po rozwiązaniu incydentu

[1] *https://blog.barracuda.com/2019/09/26/threat-spotlight-inefficient-incident-response/*
[2] *https://www.barracuda.com/products/phishline*
[3] *https://www.barracuda.com/products/forensics*
[4] *https://www.barracuda.com/products/phishline*
[5] *https://www.barracuda.com/products/forensics*

Od dyskietek do zaawansowanych modeli biznesowych – ransomware ma już ponad 30 lat

Zespół analityków Fortinet

Ransomware to złośliwe oprogramowanie blokujące dostęp do systemu i żądające okupu za przywrócenie stanu pierwotnego. Według raportu Fortinet „Global Threat Landscape"[1], obejmującego drugie półrocze 2020 roku, w grudniu codziennie na świecie 17,2 tys. urządzeń stawało się celem ataków tego typu. Przychody z cyberprzestępczości z użyciem szyfrującego oprogramowania wzrosły w 2020 roku o 311% (w porównaniu z rokiem poprzednim) i osiągnęły szacunkową wartość 350 milionów dolarów[2]. Ransomware to dzisiaj powszechne zagrożenie wpływające na funkcjonowanie wielu gałęzi gospodarki. Eksperci FortiGuard Labs pokazują drogę, jaką ransomware przeszło w ciągu ostatnich 30 lat – od ataków z użyciem dyskietek aż do usług działających w złożonych modelach biznesowych.

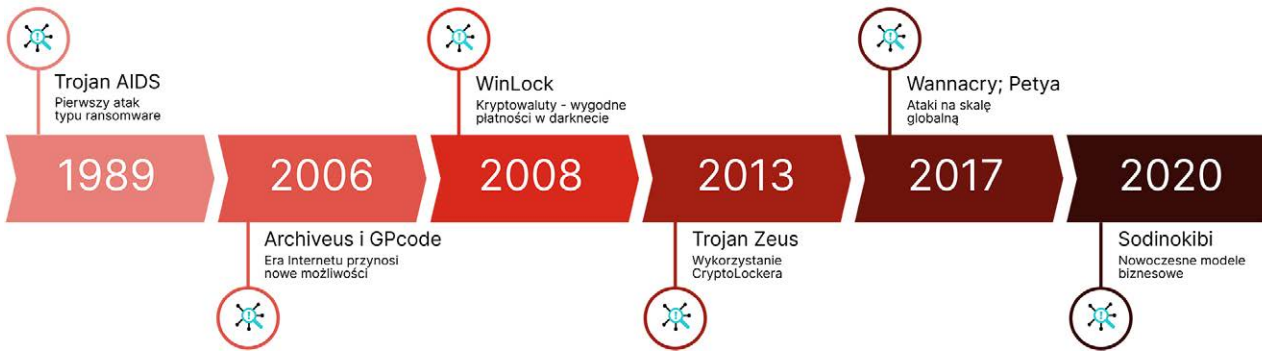
Trojan AIDS z 1989: pierwszy atak ransomware

Pierwszy w historii atak ransomware został wymierzony w branżę medyczną. W czasie konferencji Światowej Organizacji Zdrowia poświęconej tematyce AIDS rozdano 20 tysięcy zainfekowanych dyskietek. Zawierały one program do analizy ryzyka zachorowania oraz złośliwe oprogramowanie, które uruchamiało się automatycznie wraz z 91 uruchomieniem komputera. Ukrywało ono katalogi i szyfrowało nazwy wszystkich plików znajdujących się na dysku C, a następnie wyświetlało komunikat o żądaniu okupu.

Użyte w ataku oprogramowanie otrzymało nazwę „trojan AIDS", ale było również znane jako „wirus PC Cyborg" – od fikcyjnej nazwy firmy żądającej zapłaty (PC Cyborg Corporation). W kolejnych latach pojawiły się podobne ataki, ale oprogramowanie ransomware pozostawało stosunkowo niewielkim zagrożeniem, aż do przełomu wieków.

Era internetu i nowe możliwości: Archiveus i GPcode

Już na samym początku XXI wieku dostęp do internetu w krajach rozwiniętych przekroczył 50 procent. W okolicach 2005 roku



łącza szerokopasmowe stały się normą. Stworzyło to warunki do rozwoju nowych form cyberprzestępczości.

W 2006 roku pojawił się trojan Archiveus, który był pierwszym oprogramowaniem ransomware korzystającym z szyfrowania RSA. Blokował on wszystkie pliki w katalogu „Dokumenty" i wymagał od ofiar zakupu produktów w aptece internetowej, w celu uzyskania 30-cyfrowego kodu klucza, dającego możliwość odzyskania dostępu.

W tym samym roku złośliwe oprogramowanie GPcode infekowało komputery poprzez ataki z użyciem phishingu ukierunkowanego. Trojan rozsyłany był jako załącznik do wiadomości e-mail wyglądających jak podania o pracę. GPcode, podobnie jak Archiveus, używał 660-bitowego klucza publicznego RSA do szyfrowania plików w katalogu „Dokumenty". Aby uzyskać kod dostępu, ofiary były zmuszone zapłacić okup.

Kryptowaluty – wygodne płatności w darknecie

W 2008 roku stworzono bitcoina, zdecentralizowaną cyfrową kryptowalutę. Cyberprzestępcy szybko wyczuli jej potencjał, który wynika z braku powiązania transakcji z konkretną osobą. Liczba wykrywanych ataków typu ransomware zaczęła szybko i systematycznie wzrastać. W pierwszym i drugim kwartale 2011 roku zarejestrowano ich około 30 tysięcy. W trzecim – liczba ta podwoiła się. Pod koniec 2012 r. ransomware osiągnęło na czarnym rynku wartość 5 milionów dolarów.

Jednym z głównych graczy w tej dziedzinie był wówczas trojan WinLock. Zamiast pojedynczych plików, blokował on całe systemy. Atakował system operacyjny Windows i uniemożliwiał użytkownikom dostęp do wszystkich zasobów, aż do momentu zakupu klucza.

Ransomware jako usługa

Ostatnia dekada przyniosła intensywny rozwój cyberprzestępczości za sprawą modelu usługowego Ransomware-as-a-Service (RaaS). Umożliwia on kupno gotowych narzędzi i daje możliwość przeprowadzania ataków bez konieczności posiadania zaawansowanej wiedzy technicznej.

Trojan Zeus, który został zidentyfikowany już w roku 2007, w latach 2013-2014 posłużył do przeprowadzenia wielu ataków poprzez instalowanie ransomware o nazwie CryptoLocker.

Ataki na skalę globalną: WannaCry i Petya

W 2017 roku ataki ransomware wciąż przybierały na sile i były wymierzane równocześnie w komputery na całym świecie. W maju 2017 r. oprogramowanie WannaCry – przygotowane pod kątem systemu operacyjnego Windows – zainfekowało ponad 200 tys. komputerów w 150 krajach, co wywołując szkody sięgające miliardów dolarów.

W czerwcu 2017 roku nowy wariant znanego wcześniej oprogramowania Petya, nazwany NotPetya, wywołał globalny cyberatak, który zarejestrowano w Rosji, Ukrainie, Francji, Niemczech, Włoszech, Polsce, Wielkiej Brytanii i Stanach Zjednoczonych. W samej Ukrainie ucierpiało ponad 1500 osób fizycznych i prawnych, w tym instytucje finansowe.

Nowoczesne modele biznesowe

Współcześni cyberprzestępcy często działają jak duże, rozproszone firmy, i dysponują centralami telefonicznymi do obsługi płatności okupu. Celem ich ataków są głównie korporacje lub znane osoby.

Grupa znana jako Sodinokibi (lub REvil) wykorzystała koncepcję RaaS do budowy zaawansowanego modelu dystrybucji swojego oprogramowania. Dzięki temu udało się jej pozyskać blisko terabajt danych dużej firmy prawniczej. Niedawno przestępcy znani jako DarkSide uzyskali dostęp do sieci Colonial Pipeline, największego systemu rurociągów do transportu pochodnych ropy naftowej w Stanach Zjednoczonych.

[1] *https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-2h-2020.pdf*
[2] *https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021*

Europejski rynek chmury: wyzwania dla Europy oraz pięć scenariuszy do 2027 oraz 2030 roku

Francuski oddział firmy KPMG, na zlecenie liderów branży – InfraNum, Talan, OVHcloud oraz Linkt – opracował bezprecedensowy raport analizujący główne wyzwania związane z chmurą na Starym Kontynencie na nadchodzące lata oraz prognozujący pięć scenariuszy do roku 2027 oraz 2030.

Kluczowe wnioski

- Pandemia COVID-19 zdynamizowała wdrażanie usług chmurowych w firmach. Migracja motywowana jest optymalizacją operacyjną i finansową.
- Europejski rynek chmury czekają wyzwania: szacuje się, że do 2027 roku powstanie tu ponad 500 000 miejsc pracy, a skumulowane inwestycje wyniosą około 200 mld euro.
- Rośnie rola europejskich ekspertów na lokalnych rynkach w sektorze uprzednio zdominowanym już przez trzech amerykańskich graczy.
- Bez podjęcia strategicznych decyzji Europa może stracić nawet połowę zarówno ekonomicznych, jak i społecznych korzyści wynikających z rozwoju rynku technologii chmurowych.

Europejski rynek chmury kwitnie, ale jest mało konkurencyjny

W latach 2017–2019 rynek przetwarzania danych w chmurze (zogniskowany wokół trzech modeli usług: SaaS – oprogramowanie jako usługa, PaaS – platforma jako usługa, IaaS – infrastruktura jako usługa) rósł w Europie o 27 proc. rocznie. Szacuje się, że w 2020 roku osiągnął wartość 53 mld euro. Wartość ta ma w latach 2027-2030 wzrosnąć do 300-500 mld euro. Pandemia COVID-19 przyśpieszyła przechodzenie na usługi chmurowe, co dowiodło ich strategicznej roli jako kluczowego składnika infrastruktury i czynnika odporności. Pandemia sprawiła, że aż 82 proc. ankietowanych zaczęło w szerszym zakresie korzystać z chmury.

Europejski rynek chmury jest zdominowany przez trzech głównych graczy (hiperskalerów), którzy mają aż 70 proc. udziału w rynku IaaS: Amazon AWS (53 proc.), Microsoft Azure (9 proc.) i Google Cloud (8 proc.). Jednak europejscy dostawcy usług chmurowych i operatorzy telekomunikacyjni wciąż zyskują na znaczeniu na swoich macierzystych rynkach. Na przykład OVHcloud i Deutsche Telekom zajmują odpowiednio trzecie i czwarte miejsce w swoich krajach na rynku infrastrukturalnym i platformowym.

Niezbędna, lecz restrykcyjna migracja

Migracja firm i organizacji do chmury jest motywowana optymalizacją operacyjną i finansową. Główne powody wykorzystywania chmu ry wymienione w raporcie to:

- zmienność kosztów,
- elastyczność użycia zasobów,
- współpraca między zespołami i bezpieczna wymiana danych,
- elastyczność i płynność wdrożeń,
- bezpieczeństwo i odporność,
- elastyczność we wdrażaniu działań strategicznych.

Dla decydentów ważnymi kryteriami wyboru dostawcy usług chmurowych są zgodność z RODO oraz suwerenność danych.

Drażliwa kwestia suwerenności danych

Od 2016 roku w Stanach Zjednoczonych i UE wdrożono szereg przepisów dotyczących danych (RODO, Tarcza Prywatności UE-USA, Cloud Act), których celem jest ustanowienie ścisłych ram prawnych dotyczących przepływu danych. Jednak unieważnienie Tarczy Prywatności przez Trybunał Sprawiedliwości UE w 2020 roku uwidoczniło głęboką niezgodność przepisów amerykańskich z zasadami RODO, które wydają się nie do pogodzenia.

W rezultacie firmy przekazujące dane osobowe Europejczyków do serwerów firm spoza Europy (nawet jeśli mają one swoje siedziby w Europie) w większości przypadków zostały pozbawione rzetelnej podstawy prawnej i tym samym narażają się na ryzyko prawne oraz gospodarcze, wiedząc, że globalni dostawcy usług chmurowych mają często dostęp do ich poufnych danych i własności intelektualnej. Sytuacja ta budzi obawy i wiąże się z zagrożeniami finansowymi oraz operacyjnymi, które wykraczają poza kompetencje działów technicznych i zaczynają wkraczać w sferę ładu korporacyjnego.

Suwerenność danych europejskich opiera się na połączeniu ośmiu kryteriów, które należy traktować jako całość, aby zapewnić pełną zgodność i zapobiegać ryzyku. Prawdopodobnie w nadchodzących latach suwerenność danych stanie się kluczową kwestią ze względu na rosnące oczekiwania europejskich konsumentów w tym obszarze.

Pięć scenariuszy dla europejskiego rynku

W tym kontekście sytuacja na europejskim rynku chmury musi ulec transfor-

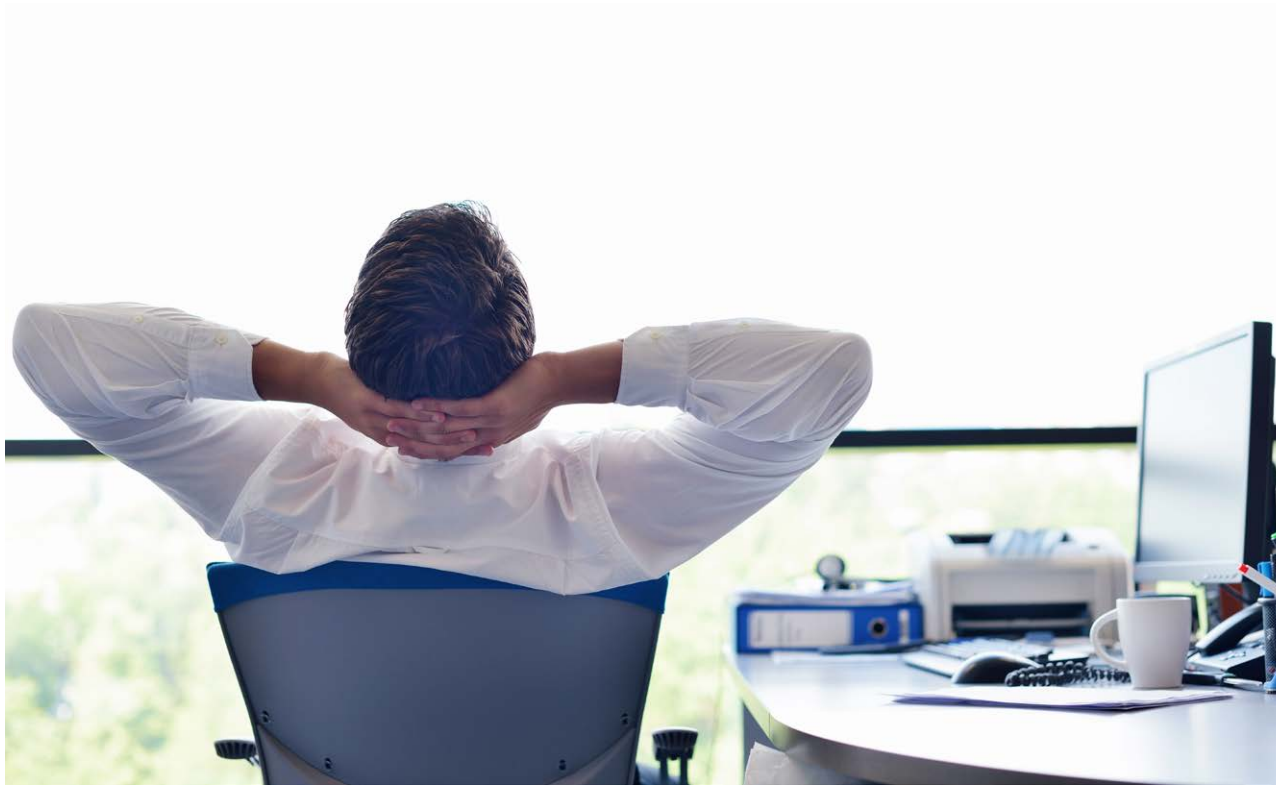
macji, a zmiany te mogą przebiegać według kilku scenariuszy. Raport francuskiego oddziału firmy KPMG wskazuje pięć możliwości:

- **Chmura rozumiana jako dobro wspólne**, cechująca się większym stopniem dobrowolnej interoperacyjności między usługami chmurowymi, a nawet federacją dostawców skupioną wokół wspólnych sektorowych ekosystemów chmurowych.
- **Wzrost znaczenia graczy europejskich** dzięki powstaniu nowych segmentów rynku, przetwarzania brzegowego, rozwoju sztucznej inteligencji (zwłaszcza w sektorze przemysłowym), suwerennych ofert itd.
- **Wprowadzenie daleko idących regulacji,** w szczególności poprzez powołanie Organu Regulacyjnego ds. Chmury, ściślejsze regulowanie praktyk biznesowych, wymagana interoperacyjność między operatorami oraz większa regulacja innowacji bazujących na chmurze.
- **Europeizacja działalności głównych nieeuropejskich graczy,** w zależności od regulacji gwarantujących regionalne tworzenie wartości dla Europy oraz ścisłą zgodność z przepisami europejskimi.
- **Funkcjonalne lub strukturalne oddzielenie działalności chmurowej od innych rodzajów działalności operatorów chmurowych,** w tym utworzenie oddzielnych podmiotów prawnych, zgodnie z aktualnymi propozycjami dotyczącymi sektora Big Tech w Stanach Zjednoczonych.

Raport pokazuje, że przyszłość europejskiej chmury może łączyć kilka scenariuszy z różnym horyzontem czasowym. Przy braku znaczących zmian w porównaniu z obecną sytuacją, gdyby dominacja hiperskalerów miała się umocnić, Europa może stracić od 20 do 50 proc. szacowanych korzyści gospodarczych z rynku przetwarzania danych w chmurze.

Metodologia

Raport firmy KPMG we Francji powstał na podstawie danych z różnych źródeł, w tym z ponad 250 wywiadów z osobami podejmującymi decyzje w europejskim sektorze prywatnym i publicznym. Badanie przeprowadzono w okresie od stycznia do marca 2021 roku, przy wsparciu i aktywnym udziale firm Infra-Num, Talan, OVHcloud i Linkt.



Rynek pracy w cyberbezpieczeństwie – brakuje specjalistów, firmy kuszą wysokimi zarobkami

Zespół analityków Fortinet

Na rynku pracy brakuje specjalistów ds. cyberbezpieczeństwa. W tej szybko rozwijającej się dziedzinie potrzebnych jest wielu nowych pracowników. Niestety trudno wypełnić tę lukę, ale nadzieją na rozwiązanie tego problemu jest podjęcie działań edukacyjnych. Na rynku dostępne są programy umożliwiające nawet osobom początkującym uzyskanie wiedzy i certyfikatów specjalistów.

Duże zapotrzebowanie na specjalistów

Cyberbezpieczeństwo to obecnie najszybciej rozwijająca się dziedzina w branży teleinformatycznej. Wraz ze zwiększającą się aktywnością cyberprzestępców jej znaczenie stało się kluczowe dla przedsiębiorstw z każdego sektora. Zapotrzebowanie na rynku pracy na wykwalifikowanych specjalistów ds. ochrony danych znacznie wzrosło zarówno w sektorze prywatnym, jak i publicznym.

W Polsce powstaje wiele nowych, państwowych jednostek organizacyjnych zajmujących się cyberochroną, którym także brakuje odpowiednio przygotowanych kadr. Zgodnie z przyjętą Strategią Cyberbezpieczeństwa RP 2019-2024[1] powstały zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT GOV, CSIRT MON, CSIRT NASK). W planach są kolejne, m.in. branżowe zespoły bezpieczeństwa (np. CSIRT Telco), operacyjne centra bezpieczeństwa (SOC) u operatorów usług kluczowych oraz eksperckie centra wymiany i analizy informacji na temat podatności, zagrożeń i incydentów (ISAC). Eksperci szacują, że liczba jednostek zajmujących się cyfrową ochroną w niedługim czasie podwoi się. Konsekwencją tego będzie jeszcze większe zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa.

Co warto wiedzieć o pracy w cyberbezpieczeństwie

W wyniku zwiększonej aktywności użytkowników internetu w czasie pandemii, chociażby w postaci pracy zdalnej czy masowo prowadzonych e-zakupów, wzrosła także aktywność cyberprzestępców. Wobec tego na rynku zaistniało większe zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa. Dodatkowo luka kompetencyjna sprawia, że znalezienie zatrudnienia w tym obszarze może być wyjątkowo łatwe. Pracodawcami, którzy poszukują takich specjalistów, są przede wszystkim duże banki, firmy technologiczne i podmioty zajmujące się bezpieczeństwem informacji.

W Polsce pracodawcy kuszą specjalistów ds. cyberbezpieczeństwa wysokimi zarobkami. Według danych pochodzących z Ogólnopolskiego Badania Wynagrodzeń z 2021 r.[2] zarabiają oni przeciętnie od 6 do 12 tys. zł brutto. Kierownik ds. bezpieczeństwa IT zarabia najczęściej ok. 13 tys. zł brutto, a ¼ najwyżej wynagradzanych otrzymuje ponad 20 tys. zł brutto.

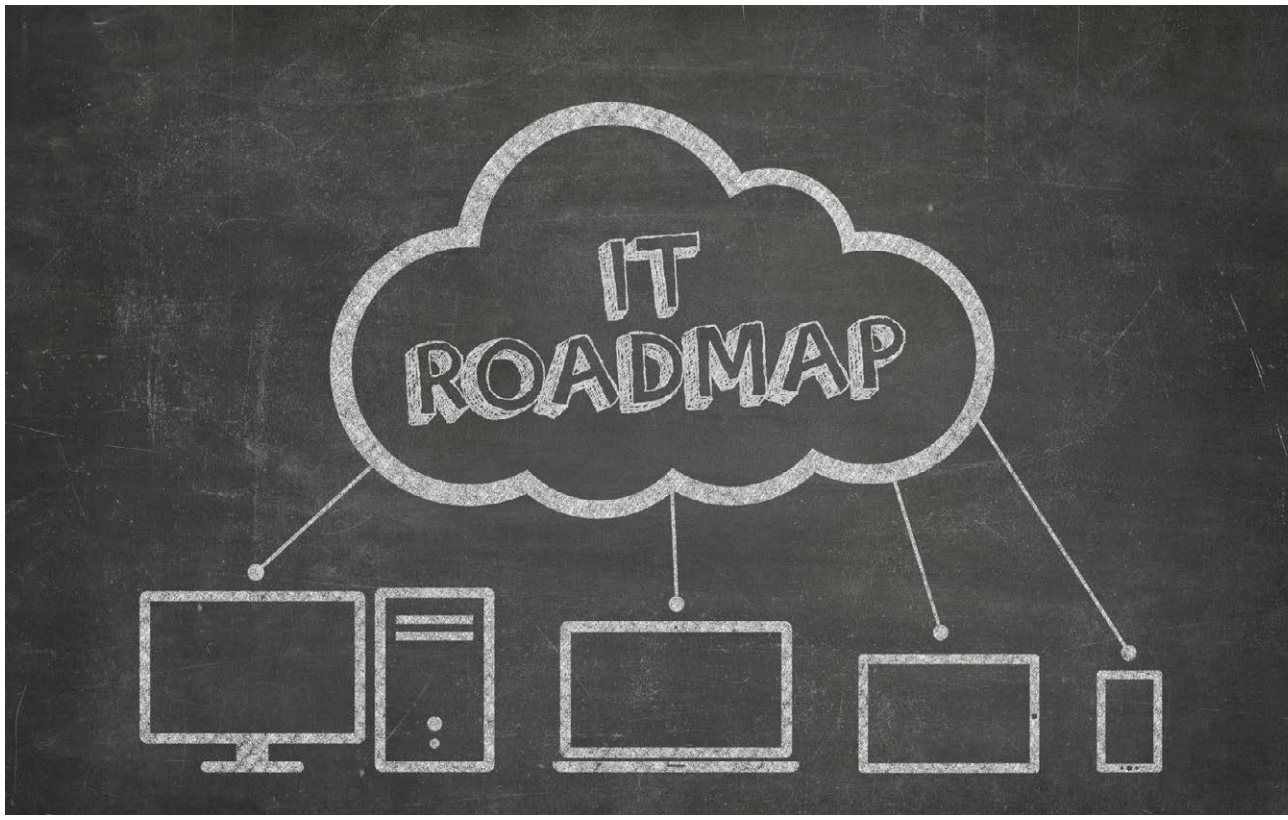
Należy przy tym wspomnieć, że w obszarze bezpieczeństwa IT istnieje wiele zawodów i specjalizacji. Jak wyjaśniają **Aamir Lakhani** i **Jonas Walker**, eksperci FortiGuard Labs firmy Fortinet, zadaniem np. osoby pracującej na stanowisku badacza zagrożeń jest odnalezienie źródła ataku i zrozumienie, w jaki sposób go przeprowadzono[3]. To oznacza, że gdy przestępca użyje do przeprowadzenia ataku poczty elektronicznej, osoba ta musi odkryć, która skrzynka e-mail znajduje się na początku łańcucha ataku. Z kolei pracownik na stanowisku strateg ds. bezpieczeństwa odpowiada za tworzenie strategii zabezpieczania środowiska IT, co wymaga połączenia wiedzy z różnych dziedzin.

Nowe rodzaje cyberzagrożeń, jak np. popularne w ostatnich latach ataki z wykorzystaniem zabiegów socjotechnicznych, wymagają od specjalistów nieustannego poszerzania wiedzy i rozwijania kwalifikacji na różnych płaszczyznach, nawet prawa czy psychologii[4].

Certyfikat, czyli pierwszy krok do kariery w cyberbezpieczeństwie

Do załatania luki kompetencyjnej najważniejsza jest edukacja. Problem z niedoborem specjalistów na rynku można próbować rozwiązać na dwa sposoby. Po pierwsze, firmy powinny inwestować w szkolenia dla swoich obecnych pracowników, którzy są zainteresowani karierą w obszarze cyberbezpieczeństwa. Jest to o tyle łatwe, że na rynku dostępnych jest wiele bezpłatnych kursów, dzięki którym można uzyskać stosowne certyfikaty. Po drugie, firmy i instytucje zajmujące się bezpieczeństwem IT mogą nawiązywać współpracę z uczelniami wyższymi, które kształciłyby specjalistów. To jednak wymaga dostosowania programu kursów do bieżących wymogów rynku.

[1] *https://www.dziennikustaw.gov.pl/M2019000103701.pdf*
[2] *https://wynagrodzenia.pl/moja-placa/ile-zarabia-specjalista-do-spraw-bezpieczenstwa-it*
[3] *https://www.fortinet.com/blog/industry-trends/establishing-a-career-in-the-field-of-cybersecurity*
[4] *https://www.sciencedirect.com/science/article/pii/S0167404820303539*



Cisco wskazuje najważniejsze trendy w zakresie cyberzagrożeń

Jeśli chodzi o bezpieczeństwo, decyzja o tym, na co przeznaczyć zasoby, ma kluczowe znaczenie. Aby zrobić to optymalnie, firmy muszą wiedzieć, jakie zagrożenia na tym polu mają największą szansę pojawić się w ich organizacjach w niedalekiej przyszłości i jaki mogą mieć na nie wpływ. Wyzwanie polega na tym, że peleton najbardziej aktywnych niebezpieczeństw zmienia się niezwykle dynamicznie, a częstotliwość poszczególnych ataków jest bardzo zróżnicowana. Dlatego tak pomocna staje się wiedza na temat kluczowych trendów w krajobrazie zagrożeń. Może ona dostarczyć amunicji do skutecznej obrony oraz informacji, gdzie najlepiej alokować zasoby.

Analizując ruch z platformy Umbrella, chmurowej platformy bezpieczeństwa obsługującej dziennie 620 miliardów zapytań DNS na całym świecie, eksperci Cisco przyglądają się aktywnościom, które występują w środowisku zagrożeń, jednocześnie analizując ruch na zainfekowanych stronach i protokoły DNS. Najpierw patrzą na organizację jak na całość, a na kolejnym etapie analizują liczby: punkty końcowe, które mogą potencjalnie łączyć się ze złośliwymi witrynami, oraz zapytania, które te strony otrzymują. dzięki temu mają wgląd w to, jak wielu użytkowników klika zainfekowane linki w poczcie e-mail, jak bardzo aktywne są trojany umożliwiające dostęp zdalny lub czy popularność kopania kryptowalut nadal rośnie. Zebrane dane mogą być źródłem wiedzy o tym, gdzie należy zainwestować większe zasoby: np. czy lepiej jest skupić się na szkoleniach z zakresu bezpieczeństwa czy poradnikach dotyczących polowania na cyberzagrożenia.

Analizując zapytania DNS wysyłane do podejrzanych domen oraz tych zainfekowanych konkretnymi wirusami w okresie od stycznia do grudnia 2020 roku, eksperci Cisco przejrzeli szereg trendów związanych z cyberzagrożeniami. Na tej podstawie wyróżnili te, z którymi organizacje mogą zetknąć się najczęściej.

Organizacje i złośliwa aktywność DNS

Jak pokazują dane[1] zebrane przez usługę Cisco Umbrella, chmurową platformę bezpieczeństwa obsługującą dziennie 620 miliardów zapytań DNS na świecie, w 86% organizacji przynajmniej jeden użytkownik próbował połączyć się z witryną phishingową, prawdopodobnie poprzez kliknięcie linku znajdującego się w wiadomości.

Co ciekawe, podobne scenariusze pojawiają się w innych kategoriach:

- W 70% organizacji część użytkowników obejrzała złośliwe reklamy w przeglądarce.
- 51% firm spotkało się z aktywnością związaną z ransomware.
- 48% organizacji wykryło złośliwe oprogramowanie wykradające informacje.

Wydobywanie kryptowalut

Nie jest zaskoczeniem, że ten typ ataków generował najwięcej ruchu DNS spośród wszystkich kategorii. Ataki te są stosunkowo łatwe do odnotowania po stronie DNS, ponieważ regularnie pingują serwery w celu uzyskania większej mocy obliczeniowej.

Ich częstotliwość w dużej mierze pokrywa się z wahaniami wartości popularnych kryptowalut.

Phishing

Liczba aktywności DNS związanych z phishingiem utrzymywała się na dość stabilnym poziomie przez cały rok, z wyjątkiem grudnia, w którym odnotowano 52-procentowy wzrost w okresie świątecznym. Jeśli chodzi o liczbę punktów końcowych odwiedzających strony wyłudzające dane, znaczący wzrost nastąpił w sierpniu i wrześniu. Ma to związek m.in. z bardzo dużą kampanią phishingową realizowaną pomiędzy lipcem a wrześniem.

Trojany

Podobnie jak w przypadku kopania kryptowalut, dość intensywnie były dystrybuowane trojany. Niezwykle wysoka liczba punktów końcowych łączących się z witrynami trojanów była w dużej mierze spowodowana przez Ursnif/Gozi oraz IcedID – dwa groźne wirusy znane z tego, że współpracują ze sobą w celu rozprzestrzeniania ransomware. Te dwa złośliwe programy odpowiadały za 82% ataków na punkty końcowe z użyciem trojanów w styczniu, a było to prawdopodobnie związane z kampanią świąteczną prowadzoną przez atakujących. Wraz z upływem roku odsetek ten spadł i ustabilizował się.

Pod koniec lipca doszło do reaktywacji jednego z groźniejszych trojanów ostatnich lat o nazwie Emotet. Generował on ogromny ruch, który narastał przez cały wrzesień. Zagrożenie to jest odpowiedzialne za duży wzrost aktywności DNS w okresie od sierpnia do września. W sumie zetknęło się z nim 45% organizacji.

Ransomware

Przez większą część roku dominowały dwa kluczowe zagrożenia typu ransomware — jedno pod względem zasięgu, drugie pod względem wysokości okupu. Począwszy od kwietnia, liczba komputerów zaatakowanych przez oprogramowanie Sodinokibi (znane jako REvil) znacząco rosła aż do jesieni. W efekcie z zagrożeniem tym zetknęło się aż 46% organizacji. We wrześniu ogólna liczba zapytań dotyczących tej konkretnej grupy ransomware wzrosła pięciokrotnie w porównaniu z sierpniem, co może sugerować, że dostarczany przez szkodliwe oprogramowanie ładunek został najprawdopodobniej aktywowany na wielu zaatakowanych systemach.

To jednak nadal kropla w morzu w porównaniu z aktywnością wirusa Ryuk, który jest w dużej mierze odpowiedzialny za listopadowo-grudniowy skok aktywności. Liczba punktów końcowych łączących się z domenami powiązanymi z Ryukiem pozostawała stosunkowo niewielka i stała przez cały rok, wykazując jedynie niewielki skok przed gwałtownym wzrostem aktywności zapytań. W zamian oprogramowanie to żądała znacznie większego okupu niż Sodinokibi.

Skuteczne zapobieganie atakom

„Dane wykorzystane do zilustrowania tych trendów pochodzą z Cisco Umbrella, usługi bezpieczeństwa dostarczanej w chmurze, która obejmuje zabezpieczenia DNS, bezpieczną bramę internetową, zaporę sieciową i funkcje brokera bezpieczeństwa dostępu do chmury (CASB) oraz informacje o zagrożeniach" – mówi **Łukasz Bromirski**, Engineering Product Manager, Cisco Security Business Group.

„W każdym z tych przypadków złośliwe działanie zostało zatrzymane przez usługę Umbrella. Użytkownik, który kliknął phishingową wiadomość e-mail, nie był w stanie połączyć się ze złośliwą witryną" – dodaje **Artur Czerwiński**, Dyrektor ds. Technologii, Cisco Polska.

Umbrella to wiele funkcji bezpieczeństwa w jednym rozwiązaniu, dzięki czemu można rozszerzyć ochronę na urządzenia, użytkowników zdalnych i rozproszone lokalizacje. Umbrella to najprostszy sposób na skuteczną ochronę użytkowników w dowolnym miejscu w ciągu kilku minut.

Dodatkowo narzędzie Umbrella Investigate zapewnia najbardziej kompletny obraz zależności i ewolucji domen internetowych, adresów IP i plików, pomagając w identyfikowaniu infrastruktury napastników i przewidywaniu przyszłych zagrożeń. Żaden inny dostawca nie oferuje takiego samego poziomu interaktywnej informacji o zagrożeniach.

Trendy dotyczące bezpieczeństwa cyfrowego związane z poszczególnymi branżami

Oczywiście znajomość dominujących trendów w krajobrazie zagrożeń pozwala lepiej lokować zasoby bezpieczeństwa tam, gdzie są one najbardziej potrzebne, jednak istotne jest także to, że różne branże są w różnym stopniu narażone na pewne typy zagrożeń. Na przykład w branży usług finansowych można zaobserwować większą aktywność złodziei informacji, podczas gdy sektor produkcji jest bardziej narażony na oprogramowanie ransomware.

Sektor IT

Zdecydowaną większość złośliwego ruchu DNS w sektorze technologicznym – branżą związaną z rozwojem i/lub dystrybucją produktów i usług IT – można przypisać do dwóch kategorii: kopanie kryptowalut i wyłudzanie informacji. Te dwie kategorie odpowiadały za aż 70% złośliwego ruchu w organizacjach z tego sektora. Nic dziwnego, że w IT zaobserwowano znacznie więcej ruchu związanego z kopaniem kryptowalut niż w jakiejkolwiek innej branży: oprócz tego, że za znaczną część tej aktywności odpowiadają cyberprzestępcy, większa dostępność wiedzy na temat kryptowalut zachęca pracowników tej branży do zainstalowania koparek kryptowalut na swoich komputerach firmowych. Jednak wówczas usługa Cisco Umbrella zablokuje DNS

z powodu naruszenia polityki organizacji.

Co ciekawe, sektor technologii odnotował drugi najwyższy poziom ruchu związanego z ransomware, głównie za sprawą ataków z wykorzystaniem oprogramowania Sodinobiki i Ryuk. Jednak niezwykle wysoki udział generowania kryptowalut obniżył ogólny odsetek, który wyniósł 6%. Aktywność trojanów była również wysoka, biorąc pod uwagę, że Emotet i Trickbot zostały wykorzystane do dystrybucji Ryuka.

Sektor usług finansowych

W sektorze usług finansowych za najwyższy poziom złośliwego ruchu DNS odpowiadały ataki phishingowe. Analizując krajobraz zagrożeń, eksperci z firmy Cisco zaobserwowali o 60% więcej przypadków ataków tego typu niż np. w szkolnictwie wyższym. Możliwe, że sektor ten jest celem ataków phishingowych częściej niż inne ze względu na większą możliwość zarobku. Potwierdzeniem tej tezy jest fakt, że w sektorze usług finansowych zaobserwowano więcej zagrożeń polegających na kradzieży informacji niż w jakiejkolwiek innej branży.

Opieka zdrowotna

W branży ochrony zdrowia zaobserwowano więcej trojanów niż w jakimkolwiek innym sektorze, ale także największą liczbę wirusów typu dropper (służących do instalowania na komputerach ofiar złośliwego kodu). Większość aktywności opartych na trojanach można przypisać Emotetowi — odpowiadał on za prawie 70% ataków w sektorze opieki zdrowotnej. Dodając do statystyk jego bliskiego kuzyna, Trickbota, otrzymujemy 83% całego ruchu związanego z trojanami.

Nie będzie zapewne zaskoczeniem, że ataki ransomware również zaznaczyły swoją obecność w sektorze opieki zdrowotnej. Szczególnie aktywny był Ryuk, co bez wątpienia było efektem dużej aktywności Emoteta. Sektor ten znalazł się na drugim miejscu pod względem ruchu związanego z ransomware.

Sektor produkcji

Podobnie jak w branży IT, aktywność w zakresie wydobywania kryptowalut była wysoka również w sektorze produkcyjnym. Odnotowano tu mniej więcej połowę aktywności zaobserwowanej w sektorze technologicznym, ale co ciekawe, w produkcji było prawie trzy razy więcej punktów końcowych zaangażowanych w generowanie kryptowalut. Gdy większa liczba maszyn skutkuje mniejszą aktywnością DNS, można wysnuć wniosek, że te punkty końcowe miały mniejsze moce obliczeniowe w porównaniu do tych z sektora technologicznego. Możliwe, że zaatakowane maszyny były zaangażowane w sam proces produkcji — w takich przypadkach generowanie kryptowalut odbywałoby się prawdopodobnie wolniej, ale nadal mogłoby obniżać szybkość produkcji.

Okazuje się, że sektor produkcyjny również jest najbardziej narażony na ransomware. W branży tej odnotowano prawie tyle samo ataków związanych z ransomware co w dwóch najbliższych branżach łącznie (technologie i ochrona zdrowia). To wyraźny sygnał, że branża ta jest regularnie obierana za cel cyberprzestępców, prawdopodobnie ze względu na polowanie na dużych graczy i wysokość potencjalnej zapłaty, jaką mogą otrzymać atakujący.

Szkolnictwo wyższe

Pandemia COVID-19 spowodowała zamknięcie szkół i uczelni na całym świecie, a nauka odbywała się w trybie zdalnym lub hybrydowym. Ponieważ w dużej mierze zajęcia odbywały się online, wiele szkodliwych działań, które zostałyby zablokowane w uczelnianej infrastrukturze IT, pojawiło się w sieciach domowych uczniów i studentów. Spowodowało to spadek aktywności cyberprzestępców w tym sektorze w wielu kategoriach począwszy od marca, a także znacznie niższe ogólne liczby w 2020 roku niż w latach poprzednich.

Nie oznacza to, że aktywność cyberprzestępców gwałtownie spadła — część działań wymagających dostępu do zasobów związanych ze szkolnictwem przełożyła się na aktywność DNS. Na przykład w zestawieniu branżowym działania phishingowe uplasowały szkolnictwo wyższe na drugim miejscu. Firmy zajmujące się wydobywaniem kryptowalut również często celują w sektor szkolnictwa wyższego, próbując wyłudzić zasoby komputerowe lub dostęp do chmury studentów, aby uruchomić swoje koparki.

Administracja rządowa

Spośród wszystkich analizowanych przez Cisco branż sektor rządowy wydaje się być najbardziej równomiernie obłożony pod względem głównych kategorii ataków – phishingu, generowania krytpowalut, ransomware i trojanów. W obszarze administracji publicznej zaobserwowano także dość równomierny rozkład dla każdej z tych kategorii, porównując miesiąc do miesiąca.

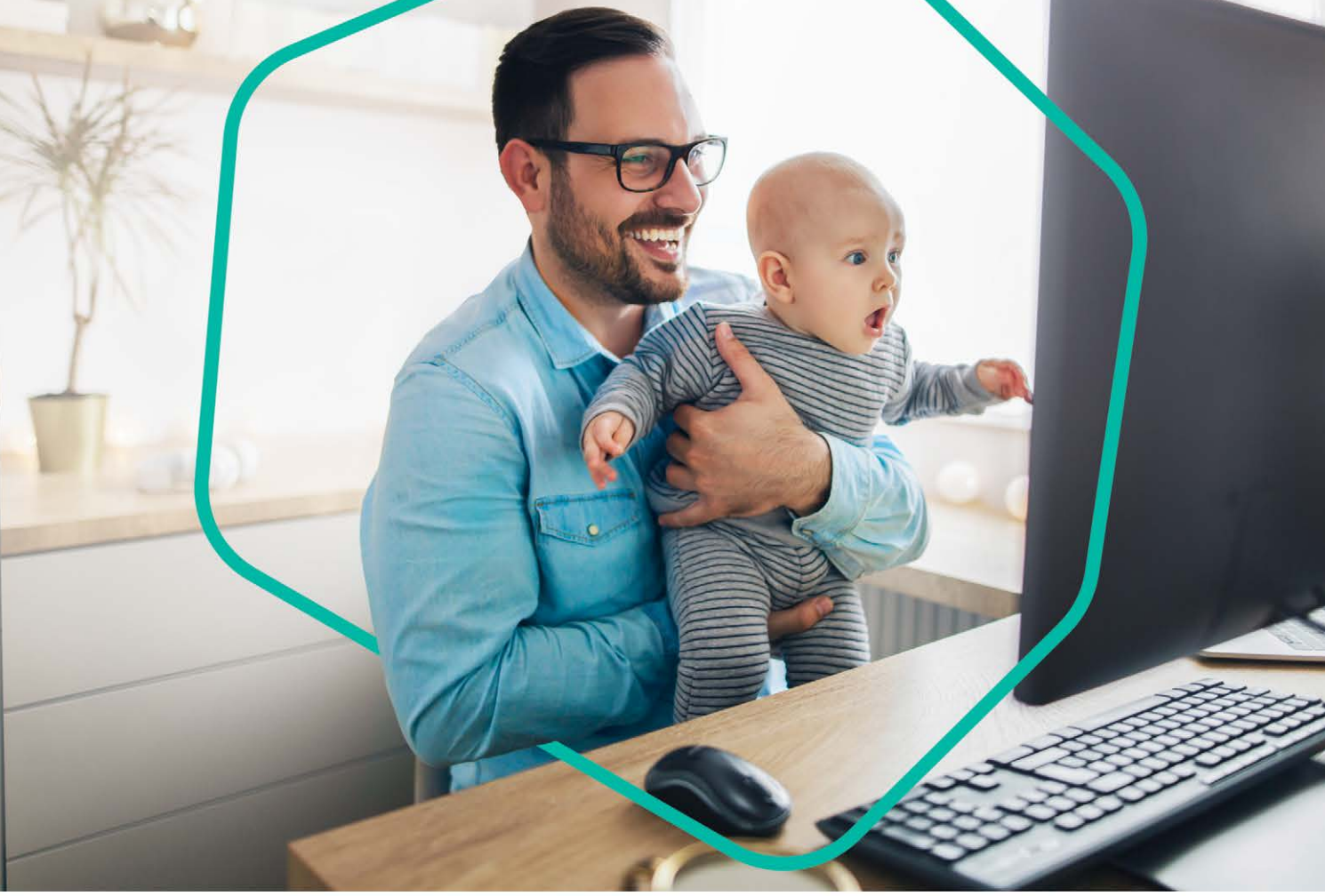
Jedynym wyjątkiem od tego trendu było wydobywanie kryptowalut, które w pierwszych trzech kwartałach 2020 roku odbywało się na niewielką skalę, by w październiku skoczyć w górę (kryptowaluty osiągnęły wtedy najwyższą wartość). Jednak w ostatnim kwartale wspomnianego roku liczby — porównując miesiąc do miesiąca — nie ulegały wahaniom i przeważnie pozostawały na tym samym wysokim poziomie.

Zapobieganie udanym atakom

Nie ma wątpliwości, że analizowanie trendów w krajobrazie zagrożeń może przynieść korzyści. Wiedząc, gdzie mogą pojawić się ataki, łatwiej jest podjąć decyzję, gdzie należy skierować zasoby, aby się przed nimi bronić. Obecnie wydobywanie kryptowalut i wyłudzanie informacji są powszechnie spotykane, podobnie jak trojany wykorzystywane do instalacji oprogramowania ransomware.

Oczywiście różne sektory są narażone na różne zagrożenia, dlatego warto zrozumieć specyficzne trendy dla własnego obszaru działania. Na przykład ekspert z sektora usług finansowych powinien uważnie śledzić trendy związane z phishingiem, podczas gdy osoba odpowiedzialna za bezpieczeństwo w firmie produkcyjnej powinna przyjrzeć się bliżej oprogramowaniu ransomware.

[1] Dane obejmują okres styczeń-grudzień 2020 r. i zostały ujęte w dwuc częściowym raporcie pt. „DNS Threat Report 2021": https://blogs.cisco.com/security/threat--trends-dns-security-part-1, https://blogs.cisco.com/security/threat-trends-dns-security-part-2



Zapewnij swoim pracownikom bezpieczną pracę - niezależnie od miejsca

Dzięki Kaspersky ASAP - platformie edukacyjnej online - możesz zadbać, by Twoi pracownicy byli gotowi na cyberzagrożenia, zarówno gdy pracują w biurze jak i w domu. Nasza platforma powstała przy udziale czołowych ekspertów ds. cyberbezpieczeństwa, dzięki czemu obejmuje najbardziej aktualne i istotne zagadnienia. Zarządzanie szkoleniami jest zautomatyzowane, a pracownicy biorą udział w praktycznych i angażujących lekcjach, które budują ich świadomość i umiejętności z zakresu cyberbezpieczeństwa.

Kaspersky Automated Security Awareness Platform

Wypróbuj wersję testową już teraz: asap.kaspersky.pl

kaspersky AKTYWUJ PRZYSZŁOŚĆ

www.dlp-expert.pl

Zarejestruj się,

aby pobrać magazyn w wersji elektronicznej

Zdecydowaliśmy się przejść na formę elektroniczną, ponieważ daje nam ona znacznie większe możliwości rozwoju magazynu, między innymi poprzez zastosowanie elementów interaktywnych. Nie bez znaczenia jest także możliwość wyeliminowania konieczności trzymania się ram objętościowych, które narzuca forma drukowana. Ponadto planujemy zintensyfikować nasze działania zarówno na stronie internetowej jak i na naszych kontach w mediach społecznościowych.

Nie oznacza to jednak, że w przypadku szczególnie ciekawych wydarzeń związanych z cyberbezpieczeństwem całkowicie zrezygnujemy z publikowania materiałów również w postaci drukowanej. Mogą one jednak przybrać nieco inną formę niż dotychczas.