Numer 1/2021 (36)
ISSN 2720-0604

DLP expert

Data Leak Prevention

www.dlp-expert.pl

Nauka poprzez grywalizację

Phising związany ze szczepieniami

Jak bronić się przed kradzieżą tożsamości

Kradzieże danych kart płatniczych

Jak zmienił się krajobraz cyberzagrożeń podczas pandemii

W nowych szatach króla

Szwajcaria do niedawna była symbolem solidności, precyzji i dyskrecji. Obecnie, jak onegdaj rzekł słowem pisanym wieszcz, ideał sięgnął bruku. Kompania z kraju bankierów, SITA, zabrała się za robienie oprogramowania do rezerwacji rozmaitych usług, w szczególności dla podróżnych. System rezerwacji jej autorstwa wykorzystuje globalny alians przewoźników *Star Alliance*.

I zdarzyło się iż z kompanii *SITA* wyciekły dane. Efektem bezpośrednim jest ujawnienie danych osobowych pasażerów (jakieś 4.5 mln) hinduskiego przewoźnika *Air India*. Inne kompanie, *Malaysia Airlines, Singapore Airlines, Jeju Air, Air New Zealand,* ***Polish Airlines****, Finnair, Scandinavian Airlines, Cathay Pacific i Lufthansa* także ucierpiały i do niedawna nie były w stanie określić nawet tego, jakie dane zostały utracone i stały się towarem bazarowym.

SITA poinformowała o incydencie jeszcze w marcu tego roku i dopiero teraz Air India opublikowała analizę incydentu. Niegodziwiec, bliżej nieznany, uzyskał dostęp do danych osobowych pasażerów, którzy rezerwowali bilety w systemie *SITA* w okresie od 2011/04/16 do 2021/02/03. Ponieważ wszystko jest na sprzedaż, to i dane też. Dane są dostępne w oficjalnej sieci handlarzy danymi i nie tylko*: […]Dark Leak Market posted on Darkweb site that it was selling breach information about 4.5 million customers of Air India[…]*

A nasz magazyn, w nowoczesnej i ekologicznej postaci, prezentuje efekty wysiłków firm parających się orką na ugorach ludzkich umysłów, jako że najsłabszym ogniwem w każdym systemie jest człowiek. Który sądzi, że jest panem wszelkiego stworzenia *(list do Kolosan 1:15).*

Życzymy Wam, czytelnicy naszego DLP immunitetu względem wirusów żywych i martwych.
Redakcja

DLP Expert
kwartalnik
numer 1/2021 (36)
kwiecień 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

Kwartalnik DLP Expert
jest wydawnictwem bezpłatnym dostępnym w subskrypcji.

Spis treści

Cyberprzestępcy wykorzystują zainteresowanie szczepieniami na COVID-19 i oferują szybszy dostęp do nich

5.01.2021 r. - Cyberprzestępcy testują nowe metody ataków, związane z trwającą właśnie akcją szczepień na COVID-19. To m.in. fałszywe propozycje pomocy w szybszym przystąpieniu do szczepienia. Pierwsze tego typu oszustwa odnotowano już w USA. – Dla cyberprzestępców nie ma żadnego tabu, prędzej czy później próby takich działań pojawią się w innych krajach.

FinCEN, oddział Departamentu Skarbu USA zajmujący się wykrywaniem przestępstw finansowych, wydał właśnie ostrzeżenie przed atakami ransomware, oszustwami i innymi cyberprzestępstwami, związanymi tematycznie ze szczepionkami na COVID-19 i ich dystrybucją.

W alercie zwrócono uwagę na fakt, iż cyberprzestępcy od początku wykorzystują pandemię do ataków, a budząca ogromne emocje i zainteresowanie akcja szczepień otwiera przed nimi nowe perspektywy. FinCEN zaapelował więc do banków i innych instytucji finansowych, by szczególnie uważały na ataki ransomware wymierzone w procesy produkcji i dystrybucji szczepionek oraz łańcuchy dostaw z nimi związane. Wymieniono także działania przestępców takie jak: oferowanie nieistniejących lub podrobionych szczepionek, nielegalne przekierowywanie oryginalnych preparatów na czarny rynek czy proponowanie dostępu do szczepień poza obowiązującym harmonogramem.

W ostatnich miesiącach firmy farmaceutyczne, badacze i organizacje zajmujące się przechowywaniem oraz transportem szczepionek były celem wielu grup cyberszpiegowskich. Wśród nich znalazł się na przykład atak grupy Lazarus wykorzystujący złośliwe oprogramowanie, zidentyfikowany przez badaczy ds. cyberbezpieczeństwa z firmy ESET.

Od soboty rano WhatsApp będzie płatny? Łańcuszek związany z popularnym komunikatorem oszukuje po raz kolejny

8.01.2021 r. - Użytkownicy aplikacji WhatsApp masowo przesyłają sobie informację o wprowadzeniu opłat w tym popularnym komunikatorze. – To fałszywa wiadomość, bazująca na znanym od dawna mechanizmie łańcuszków – ostrzegają eksperci ds. cyberbezpieczeństwa ESET.

Łańcuszek dotyczący WhatsAppa od kilku lat inicjowany jest wraz z początkiem nowego roku. W 2021 roku brzmi on podobnie jak w latach poprzednich: „Od soboty rano WhatsApp będzie płatny. Jeśli masz co najmniej 10 kontaktów, wyślij do nich tę wiadomość" – zachęcają oszuści. „W ten sposób można pokazać, że jesteś zapalonym użytkownikiem i logo będzie niebieskie i pozostanie darmowe. Wiadomość wg dziennika TF1. WhatsApp kosztować będzie 0,01 $ za wiadomość. Wyślij tę wiadomość do 10 osób. Gdy już to zrobisz, lampka zapala się na niebiesko (inaczej aktywuje się WhatsApp rozliczeń.)" – brzmi dalsza część komunikatu.

To fałszywa wiadomość, której głównym celem jest wzbudzenie zaniepokojenia użytkowników. Tego typu akcje często jednak „przecierają szlaki" innym, szeroko zakrojonym działaniom, związanym np. z wyłudzaniem danych. Przykładem może być choćby kampania spamowa z 2019 roku, którą wykryli badacze cyberbezpieczeństwa z ESET, także wymierzona w użytkowników komunikatora WhatsApp. Otrzymywali wtedy wiadomość, w której obiecywano 1000 GB darmowego Internetu po kliknięciu w załączony link i wypełnieniu krótkiej ankiety. Oszuści zarabiali na każdym kliknięciu w link zawarty w wiadomości.

Jednocześnie WhatsApp rzeczywiście wprowadza zmiany, ale są one związane z aktualizacją regulaminu i polityki prywatności. Mają wejść w życie w dniu 8 lutego 2021. Obejmują usługę WhatsApp i sposób przetwarzania danych użytkownika oraz sposób, w jaki firmy mogą używać usług Facebooka do przechowywania czatów WhatsApp i zarządzania nimi. Komunikat o tej aktualizacji i konieczności akceptacji nowego regulaminu użytkownicy otrzymują jednak oficjalnym kanałem, zaraz po uruchomieniu aplikacji, nim rozpoczną korzystanie z niej.

Brakujące ogniwo: badacze z firmy Kaspersky łączą atak na firmę SolarWinds z backdoorem Kazuar

11.01.2021 r. - W połowie grudnia 2020 r. firmy FireEye, Microsoft oraz SolarWinds poinformowały o wykryciu dużego, wyrafinowanego ataku na łańcuch dostaw, w którym wykorzystano nieznane wcześniej szkodliwe oprogramowanie – Sunburst – i którego ofiarą padli klienci oprogramowania Orion firmy SolarWinds. Eksperci z firmy Kaspersky zidentyfikowali różne podobieństwa w kodzie pomiędzy szkodnikiem Sunburst oraz znanymi wersjami backdoora Kazuar, zapewniającego atakującym zdalny dostęp do urządzeń ofiar. Nowe ustalenia ujawniają szczegóły, które mogą pomóc badaczom w dochodzeniach związanych z tym atakiem..

Badając backdoora wykorzystanego przez szkodnika Sunburst, eksperci z firmy Kaspersky odkryli wiele cech wspólnych ze szkodnikiem Kazuar, który został wcześniej zidentyfikowany jako backdoor napisany przy użyciu platformy .NET Framework.

Po raz pierwszy poinformowała o nim firma Palo Alto w 2017 r.[1], a sam szkodnik był wykorzystywany w atakach cyberszpiegowskich na całym świecie. Liczne podobieństwa w kodzie sugerują związek pomiędzy Kazuarem oraz Sunburstem, aczkolwiek charakter powiązania nie został jeszcze określony.

Szkodniki łączy m.in. algorytm generowania identyfikatorów użytkownika (UID) odnoszących się do ofiar, podobieństwa w kodzie odpowiadającym za pozostawanie szkodnika w uśpieniu w pierwszej fazie ataku oraz intensywne wykorzystywanie funkcji skrótu FNV1a. Po pojawieniu się szkodnika Sunburst w lutym 2020 r. Kazuar ciągle ewoluował i podobieństwa obserwowane w jego wersjach z późniejszej części ubiegłego są jeszcze większe.

Eksperci z firmy Kaspersky zaobserwowali ciągły rozwój szkodnika Kazuar w okresie jego ewolucji, łącznie z pojawianiem się nowych, istotnych funkcji wskazujących na podobieństwo ze szkodnikiem Sunburst. Chociaż podobieństwa te są godne uwagi, mogą one wynikać z kilku przyczyn: Sunburst mógł zostać stworzony przez to samo ugrupowanie co Kazuar; twórcy Sunbursta mogli wykorzystać Kazuara jako inspirację; twórca Kazuara mógł dołączyć do zespołu, który stworzył Sunbursta; lub też ugrupowania stojące za Sunburstem i Kazuarem mogły uzyskać kod źródłowy szkodnika z tego samego źródła.

Dalsze szczegóły techniczne dotyczące podobieństw między szkodnikami Sunburst oraz Kazuar zawiera raport dostępny na stronie https://r.kaspersky.pl/54hZf.

[1] *https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/*

Złośliwe aplikacje mogą nas szpiegować – nowy rodzaj ataku na urządzenia z Androidem

SOPHOS 12.01.2021 r. – Badacze firmy Sophos zidentyfikowali nowy rodzaj ataku na użytkowników urządzeń z systemem Android. Cyberprzestępcy stworzyli fałszywe wersje m.in. oficjalnej aplikacji rządowej Pakistanu, aplikacji firmy ubezpieczeniowej oraz porównywarki cen operatorów telefonicznych. Złośliwe wersje programów przechwytują z urządzeń kontakty, treść wiadomości SMS, dane z dokumentów tożsamości, informacje o lokalizacji czy zdjęcia, a następnie przesyłają je na serwery przestępców. Dotychczas celem były aplikacje dla użytkowników w Pakistanie, jednak atak może zostać łatwo powtórzony w każdym miejscu na świecie.

Telefony na podsłuchu

Fałszywe aplikacje są identyczne jak ich legalne odpowiedniki dostępne w Google Play Store, umożliwiają też korzystanie z tych samych funkcji. Przestępcy wybrali pięć programów działających w Pakistanie: oficjalną aplikację rządową Pakistan Citizen Portal, muzułmański zegar modlitewny, aplikację do porównywania ofert operatorów telefonicznych, narzędzie do sprawdzania ważności karty SIM oraz program firmy ubezpieczeniowej.

Złośliwe narzędzia po uruchomieniu przechwytują unikalny identyfikator IMEI urządzenia, informacje o lokalizacji, pełną listę kontaktów, treść wiadomości tekstowych, zestawienie połączeń czy katalogi karty SD. Aplikacja Pakistan Citizen Portal skłania też użytkowników do podania swojego numeru dowodu osobistego, danych paszportowych, haseł do Facebooka i innych serwisów. Niektóre ze sfałszowanych aplikacji zawierają mechanizm umożliwiający nagrywanie rozmów telefonicznych i dźwięków rejestrowanych przez urządzenie. Funkcje te nie zostały jednak jeszcze aktywowane przez przestępców.

„Czerwona lampka" dla wszystkich użytkowników

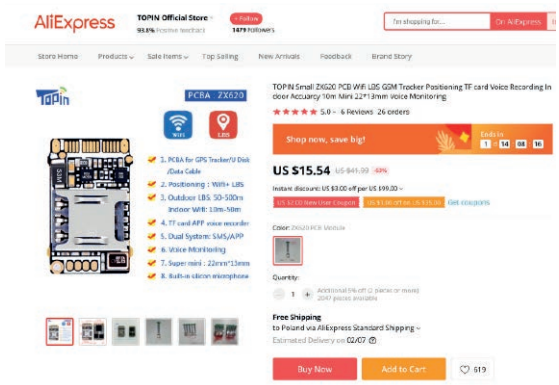
Fałszywe wersje aplikacji nie są dostępne w oficjalnym sklepie Google Play Store, ale na stronach imitujących m.in. pakistański

serwis rządowy. Użytkownicy mogli otrzymać linki z instrukcją pobrania programów m.in. SMS-em lub mailem. Cyberprzestępcy szyfrują przy tym stworzony przez siebie kod, instalowana aplikacja nie jest więc identyfikowana jako złośliwa podczas wstępnego skanowania przez urządzenie.

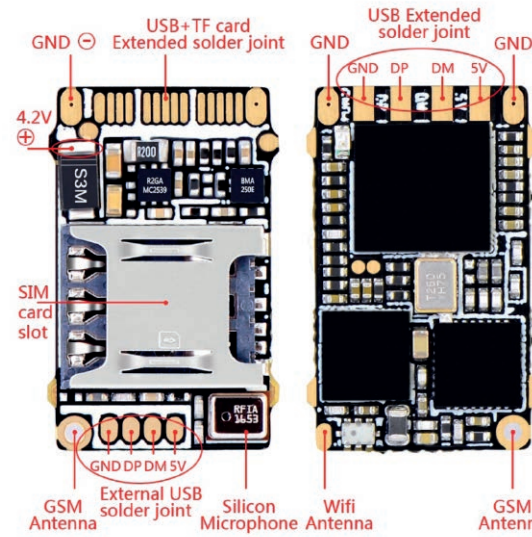
Odkryte programy szpiegujące to sygnał ostrzegawczy dla użytkowników nie tylko w Pakistanie, ale i na całym świecie. Przestępcy coraz częściej przeprowadzają bowiem ataki na telefony komórkowe, aby przechwycić wrażliwe dane i uzyskać dostęp w czasie rzeczywistym do lokalizacji zainfekowanego urządzenia, a nawet rozmów odbywających się w jego zasięgu.

Ktoś wlutował sprzętowy podsłuch do iPhone'a rosyjskiego aktywisty

14.01.2021 r - Portal Niebezpiecznik.pl przytoczył ciekawą historię: Aleksiej Nawalny udostępnił na Twitterze[2] nagranie, na którym prezentowany jest iPhone X. Urządzenie należy do jednego z aktywistów podejrzewanego przez służby o nękanie oficera zamieszanego w sprawę otrucia Nawalnego. Aktywista został zatrzymany, a jego smartfon trafił do depozytu. Po uwolnieniu mężczyzna zauważył, że jego iPhone wygląda trochę inaczej. Okazało się, że do baterii urządzenia ktoś podpiął dodatkowy układ zawierający osobną kartę SIM.



Po pewnym czasie jeden z użytkowników serwisu Twitter poinformował, że taką pluskwę można kupić w internecie za 15 dolarów. Działają one jak zwyczajny telefon, lecz miniaturowych rozmiarów, bez ekranu i klawiatury, ale za to z mikrofonem i modułem pseudo GPS (w rzeczywistości lokalizacja bazuje na okolicznych sieciach Wi-Fi i BTS-ach).



Aby kogoś podsłuchać, należy zadzwonić na numer włożonej do pluskwy karty SIM — pluskwa automatycznie odbierze połączenie i aktywuje mikrofon, co umożliwi dzwoniącemu podsłuchiwanie. Na numer pluskwy można też wysłać SMS, a w zamian wyśle ona przybliżoną lokalizację. W przeciwieństwie do Pegasusa pluskwa nie będzie miała dostępu do danych z aplikacji na telefonie, nie ustali wpisywanych treści na klawiaturze smartfona ani nie zobaczy niczego, co pojawia się na jego ekranie. Będzie jednak słyszeć każdą rozmowę prowadzoną przy i przez smartfona głosowo — nawet jeśli ktoś rozmawia przez bezpieczny, szyfrowany komunikator.

[2] *https://twitter.com/navalny/status/1349627228175253506*

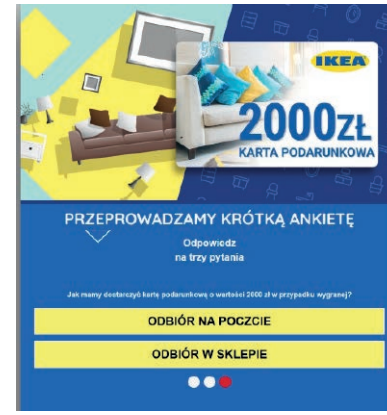
Bon do IKEA? Nie dostaniesz 2000 zł, ale możesz stracić cyfrową tożsamość!

21.01.2021 r. - Eksperci ds. cyberbezpieczeństwa ESET zidentyfikowali nową kampanię spamową. Wykorzystuje ona markę i identyfikację graficzną IKEA, kusząc możliwością otrzymania karty podarunkowej o wartości 2000 zł. Popularna sie ć nie ma z nią jednak nic wspólnego. To kolejna odmiana kampanii wabiącej internautów fikcyjnymi nagrodami przyznawanymi rzekomo przez znane marki handlowe. – Nieświadomi użytkownicy mogą w ten sposób przekazać swoje dane podmiotom, które będą je nieuczciwie wykorzystywać – wyjaśniają specjaliści.

Kampania spamowa, która od kilku dni trafia na skrzynki polskich użytkowników, bazuje na prostym mechanizmie scamu, oszustwa wzbudzającego zaufanie. Mail pułapka miewa różne tytuły. „Gratulacje", „Zostałeś wybrany", „Potwierdź nagrodę" – to sformułowania, które pojawiają się najczęściej. Nazwa nadawcy to zwykle „Ikea", ale maskuje ona tylko adresy, z jakich maile

napływają, założone m.in. na francuskich serwerach pocztowych.

Ci internauci, których skusi perspektywa „odebrania prezentu", trafiają następnie na stronę internetową, zachęcającą do odpowiedzi na kilka zamkniętych pytań i uzupełnienia formularza z danymi osobowymi. Na stronie znajduje się regulamin, informacja o danych firmy organizującej promocję (zlokalizowanej w Singapurze), a nawet klauzule dotyczące ochrony danych osobowych. Uważna lektura zgód marketingowych, towarzyszących formularzowi pokazuje, że za jego pośrednictwem można przekazać swoje dane osobowe szeregowi podmiotów m.in. w Polsce, Niemczech, we Francji i na Malcie. Dodatkowo pod stronę podpięte są reklamowe banery, oszuści zarabiają zatem także na każdym jej otwarciu.



Ochrona pojazdów: firma Kaspersky uruchamia raporty analizy zagrożeń przeznaczone dla branży motoryzacyjnej

21.01.2021 r. - Firma Kaspersky wprowadziła dostępne wcześniej dla wybranych klientów zindywidualizowane raporty analizy zagrożeń (Threat Intelligence), przeznaczone dla organizacji działających w branży motoryzacyjnej. Raporty te dostarczają producentom samochodów dogłębną analizę specyficznych dla branży cyberzagrożeń i wskazują informacje, które mogą zostać wykorzystane przez przestępców do opracowania ataków na pojazdy, infrastrukturę samochodów połączonych z internetem oraz inne systemy związane z pojazdami.

Istnieją liczne przykłady[3] świadczące o coraz większym zainteresowaniu bezpieczeństwem motoryzacyjnym, zarówno wśród niezależnych badaczy, entuzjastów, jak i cyberprzestępców. W efekcie wzrosła liczba technik ataków, a z drugiej strony wprowadzono nowe wymogi regulacyjne, których producenci muszą przestrzegać, aby zabezpieczyć się przed nimi.

Usługa Automotive Threat Intelligence firmy Kaspersky pomaga organizacjom – od producentów pojazdów po dostawców – monitorować problemy związane z bezpieczeństwem, które mogą dotyczyć branży motoryzacyjnej, oraz pozwala niezwłocznie podjąć odpowiednie czynności naprawcze. Ta dostosowana do potrzeb klienta usługa pozwala zidentyfikować istniejące oraz nowe zagrożenia dla komponentów wewnątrz pojazdów, jak dla również infrastruktury połączonych samochodów.

Każdy raport zawiera przegląd i analizę trendów technologicznych związanych z cyberatakami w branży motoryzacyjnej, która obejmuje cyberincydenty, najnowsze badania bezpieczeństwa, konferencje, wystąpienia, fora społeczności, a także informacje dotyczące potencjalnych wektorów ataków na pojazdy oraz infrastrukturę serwisową. Główne elementy usługi to: raport wraz ze streszczeniem, opisy i zalecenia dotyczące zagrożeń oraz powiadomienia o działaniach wysokiego ryzyka i lukach w zabezpieczeniach dopasowane do potrzeb danego producenta.

Jeśli w raporcie Threat Intelligence znajdzie się zagrożenie wymagające pilnego działania, klienci zostaną o nim natychmiast powiadomieni.

Więcej informacji na temat rozwiązań i usług firmy Kaspersky przeznaczonych dla branży motoryzacyjnej znajduje się na stronie https://www.kaspersky.pl/ochrona-dla-korporacji/transportation-security.

[3] *https://plblog.kaspersky.com/cybersecurity-automotive/14039/*

Firmy Kaspersky oraz Waterfall Security Solutions zapewniają kompatybilność swoich rozwiązań w celu udoskonalenia ochrony sieci przemysłowych

26.01.2021 r. - Kaspersky łączy siły z Waterfall Security Solutions w celu lepszego zabezpieczania sieci przemysłowych. Kaspersky Industrial CyberSecurity for Networks wraz z Waterfall for Intrusion Detection Systems umożliwia nieinwazyjną inwentaryzację sieci przemysłowych, wykrywanie zagrożeń oraz wymuszoną sprzętowo ochronę przed atakami sieciowymi.

Przedsiębiorstwa przemysłowe muszą sprostać nowym wyzwaniom w zakresie cyberbezpieczeństwa, jakie pojawiają się w związku z cyfryzacją sieci technologii operacyjnej (OT). 55% organizacji uważa[4], że Internet Rzeczy zmieni stan bezpieczeństwa przemysłowych systemów sterowania (ICS). W kontekście tego zapotrzebowania produkty takie jak te oferowane przez firmy Kaspersky i Waterfall prezentowane są obecnie jako opłacalny sposób zapewnienia odpowiednio wczesnej ochrony przed zagrożeniami sieciowymi. Dlatego zagwarantowanie kompatybilności tych dwóch przełomowych produktów ma istotne znaczenie dla organizacji przemysłowych.

Kaspersky Industrial CyberSecurity for Networks wykrywa anomalie i włamania wewnątrz sieci OT, dzięki czemu

przedsiębiorstwa przemysłowe mogą zapobiec wszelkim negatywnym wpływom takich incydentów na procesy przemysłowe. Waterfall for Intrusion Detection Systems umożliwia sensorom wykrywającym włamania sieciowe łączenie się z sieciami OT i ICS oraz monitorowanie ich bez narażania na ryzyko operacji fizycznych. Zespół złożony z inżynierów z firm Waterfall oraz Kaspersky przeprowadził obszerne testy w celu weryfikacji kompatybilności obu produktów, aby zagwarantować zarówno technologiczne, jak i operacyjne korzyści rozwiązania końcowego.

Korzyści te obejmują rozszerzenie widoczności całkowicie odizolowanych sieci przemysłowych, możliwość analizy w czasie rzeczywistym ruchu sieciowego w celu wykrycia podejrzanych aktywności oraz możliwość połączenia sieci przemysłowych do infrastruktury monitorowania, analizy i ostrzegania przedsiębiorstwa bez ryzyka zakłóceń w procesie przemysłowym.

[4] *https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2020/*

Większa kontrola prywatności dla wszystkich dzięki narzędziu TinyCheck

27.01.2021 r. - W celu zapewnienia lepszej kontroli prywatności danych użytkowników dwóch ekspertów z firmy Kaspersky połączyło wyniki swoich badań i uaktualniło ogólnodostępne narzędzie TinyCheck. Stworzony pierwotnie jako narzędzie wykrywania oprogramowania stalkerware z myślą o organizacjach wspierających ofiary przemocy domowej, TinyCheck pomaga teraz wykrywać wszelkiego rodzaju aplikacje śledzące lokalizację.

W grudniu 2020 r. firmy Apple i Google zakazały umieszczania w swoich sklepach jakichkolwiek aplikacji, które wykorzystują technologię firmy X-Mode umożliwiającą śledzenie i sprzedaż danych lokalizacyjnych posiadaczy urządzeń mobilnych. Kilka miesięcy przed decyzją tych gigantów technologicznych analizą takich aplikacji zajął się dyrektor Globalnego Zespołu ds. Badań i Analiz (GReAT) firmy Kaspersky, Costin Raiu, po tym, jak zobaczył wizualizację identyfikującą przemieszczanie się osób na podstawie ich danych GPS udostępnionych przez X-Mode.

Raiu znalazł ponad 240 oddzielnych aplikacji z technologią śledzenia X-Mode, które łącznie zostały zainstalowane ponad 500 milionów razy. Tego rodzaju gromadzenie danych możliwe jest w sytuacji, gdy twórcy osadzają w swojej aplikacji pewien komponent – zestaw narzędzi programistycznych SDK. Problem polega na tym, że użytkownik nie jest w stanie rozpoznać, czy dana aplikacja zawiera komponenty śledzenia lokalizacji.

Ponadto aplikacja może zawierać więcej niż jedno śledzące narzędzie SDK. Na przykład, badając aplikację zawierającą SDK firmy X-Mode, Costin Raiu wykrył pięć komponentów innych firm, które również gromadziły dane lokalizacyjne.

Jak pomieszać szyki szpiegom

Wyniki badań Costina Raiu zostały wykorzystane w TinyCheck[5] – narzędziu open-source, które zostało opracowane i opublikowane[6] w listopadzie ubiegłego roku przez Féliksa Aimé, innego eksperta z zespołu GReAT firmy Kaspersky.

Początkowo TinyCheck został stworzony z myślą o zwalczaniu oprogramowania stalkerware, czyli narzędzi wykorzystywanych do szpiegowania życia prywatnego innej osoby za pośrednictwem urządzenia mobilnego. Teraz TinyCheck może wykrywać zarówno stalkerware, jak i aplikacje śledzące i w zależności od tego będzie wyświetlał użytkownikowi stosowne ostrzeżenia.

Narzędzie opiera się na powszechnie dostępnym, miniaturowym komputerze Raspberry Pi. Przy użyciu zwykłego połączenia Wi-Fi TinyCheck skanuje ruch wychodzący urządzenia przenośnego oraz identyfikuje interakcje ze znanymi szkodliwymi źródłami, takimi jak serwery powiązane z oprogramowaniem szpiegowskim. Do poprawnego działania komputer Raspberry Pi musi być wyposażony w dwa interfejsy Wi-Fi (jeden w celu połączenia się z internetem, drugi dla łączności telefonu) lub w jeden interfejs Wi-Fi (dla telefonu) oraz połączenie Ethernet (dla internetu). W obu przypadkach idealnie sprawdzi się komputer Raspberry Pi 3 lub nowszy z niewielkim ekranem dotykowym.

[5] *https://github.com/KasperskyLab/tinycheck*

[6] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3338/kaspersky-i-koalicja-przeciwko-stalkerware-mija-rok-walki-o-prywatnosc-cyfrowa*

Nowe badanie przeprowadzone przez firmę Barracuda pokazuje wzrost zaufania specjalistów IT do chmury publicznej pomimo obaw o bezpieczeństwo

28.01.2021 r. – Firma Barracuda, zaufany partner i wiodący dostawca chmurowych rozwiązań w zakresie bezpieczeństwa, przedstawia raport[7] pt. Cloud networks: Shifting into hyperdrive. Badanie zrealizowane na zlecenia firmy Barracuda objęło globalnych decydentów IT, aby poznać ich opinie na temat chmury publicznej, ograniczeń dostępu, obaw związanych z bezpieczeństwem, nowych rozwiązań oraz innych zagadnień.

Najważniejsze informacje:

- Ponad trzy czwarte organizacji korzysta z usług wielu dostawców chmury, takich jak Amazon Web Services, Microsoft Azure i Google Cloud Platform.
- 56% respondentów ma problem z zapewnieniem ciągłego, bezproblemowego dostępu do aplikacji w chmurze dla swoich organizacji.
- Prawie 70% uczestników badania doświadcza problemów z opóźnieniami i wydajnością podczas uruchamiania obciążeń SaaS, takich jak Office 365.

– Ponad 60% respondentów twierdzi, że koszty MPLS znacznie wzrosną z powodu sezonowych szczytów obciążenia.

Badanie przeprowadzone przez niezależną firmę badawczą Censuswide zawiera odpowiedzi 800 członków zarządów, niezależnych konsultantów oraz szefów zespołów odpowiedzialnych za infrastrukturę chmury w ich organizacjach. Badanie przeprowadzono w firmach o różnej wielkości z regionów EMEA, APAC i USA, reprezentujących szereg różnych branż, takich jak budownictwo, edukacja, finanse, służba zdrowia, technologie, produkcja, handel detaliczny, transport i inne.

Wyniki badania pokazują, że chociaż specjaliści IT mają coraz większe zaufanie do chmury, organizacje napotykają na rosnące ograniczenia w zakresie dostępu do niej.

Najważniejsze wnioski z raportu obejmują:

1. Specjaliści IT mają coraz większe zaufanie do chmury
   – Ponad trzy czwarte respondentów korzysta z usług wielu dostawców usług chmurowych, takich jak Amazon Web Services, Microsoft Azure i Google Cloud Platform.
   – Prawie 80% twierdzi, że ich organizacja wdrożyła sieć opartą na platformie Azure.
2. Organizacje napotykają na rosnące ograniczenia w dostępie do chmury.
   – 56% respondentów zmaga się z zapewnieniem stałego i bezproblemowego dostępu do aplikacji w chmurze dla swoich organizacji.
   – Prawie 70% doświadcza problemów z opóźnieniami i wydajnością podczas uruchamiania obciążeń SaaS, takich jak Office 365.
3. Obecna infrastruktura sieciowa staje się coraz bardziej kosztowna.
   – Ponad 70% respondentów korzysta z tradycyjnych metod dostępu, takich jak MPLS.
   – Ponad 60% twierdzi, że ich koszty MPLS poważnie wzrosły z powodu sezonowych szczytów obciążenia.
4. Specjaliści IT szukają łatwiejszej i bardziej ekonomicznej łączności.
   – Ponad 70% respondentów planuje wdrożenie rozwiązania SD-WAN w ciągu najbliższych 12 miesięcy w celu rozwiązania problemów z łącznością w chmurze.
   – Jednocześnie prawie 60% twierdzi, że ich organizacja waha się, czy wdrożyć rozwiązanie SD-WAN z powodu obaw co do złożoności i ceny.

[7] *https://www.barracuda.com/sase-report*

Kaspersky przedstawia prognozy dotyczące prywatności w 2021 r.

29.01.2021 r. - W ubiegłym roku przekonaliśmy się, jak istotne dla codziennego funkcjonowania społeczeństwa słały się usługi cyfrowe i infrastruktura połączona z internetem. W efekcie zmieniło się podejście do prywatności, jak również jej postrzeganie przez obywateli, organizacje oraz rządy. Eksperci ds. prywatności z firmy Kaspersky przygotowali swoje prognozy dotyczące zmian w tym zakresie, jakie czekają nas w 2021 r. Wśród wyzwań wyraźnie wybija się jeden trend – starcie przeciwnych sił reprezentujących różne interesy. Producenci zaczną gromadzić coraz więcej różnorodnych danych, na co rządy zareagują wprowadzeniem nowych regulacji, a użytkownicy zaczną postrzegać prywatność jako korzyść, za którą są skłonni zapłacić.

Pre zentowane prognozy zostały opracowane na podstawie zmian i trendów obserwowanych przez ekspertów ds. prywatności firmy Kaspersky w 2020 r. Według badaczy poważny impas pomiędzy różnymi uczestnikami dialogu na temat prywatności i gromadzenia danych jest wynikiem następujących tendencji:

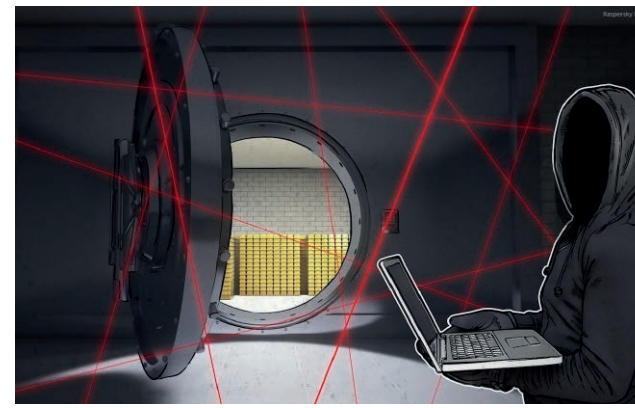
1. **Prywatność konsumentów będzie stanowić propozycję wartości i, w większości przypadków, będzie kosztowała pieniądze.** Podczas pandemii gromadzone były większe ilości danych oraz nasilił się chaos polityczny, który przeniósł się także na platformy cyfrowe. To wszystko spowodowało, że szybko zdaliśmy sobie sprawę ze zjawiska niekontrolowanego gromadzenia danych. Coraz więcej użytkowników dąży do zachowania prywatności, dlatego organizacje oferują produkty stworzone z myślą o takich możliwościach. Ich liczba i różnorodność wzrośnie.
2. **Producenci inteligentnych gadżetów związanych ze zdrowiem będą gromadzić coraz bardziej różnorodne dane i wykorzystywać je na znacznie więcej różnych sposobów.** Dane gromadzone przez urządzenia monitorujące kondycję fizyczną, ciśnienie krwi oraz inne tego typu gadżety dostarczają tak cenną wiedzę, że były już wykorzystywane w sprawach sądowych, a także naturalnie przez handlowców i ubezpieczycieli, którzy również uważają je za niezwykle przydatne. W sytuacji rosnącego zaniepokojenia kwestiami zdrowotnymi popyt na takie dane z pewnością wzrośnie.
3. **Rządy będą coraz bardziej przyglądać się danym gromadzonym przez firmy z grupy Big Tech i aktywne regulować ten proces.** Dostęp do danych użytkowników otwiera ogromne spektrum możliwości – np. zwalczanie przemocy wobec dzieci czy usprawnienie ruchu miejskiego. Z drugiej strony, może również ułatwić uciszenie sprzeciwów. W związku z odmową udostępnienia takich danych przez większość prywatnych organizacji rządy z pewnością wprowadzą więcej regulacji ograniczających prywatność danych, a najgorętsze debaty toczyć się będą wokół technologii pozwalających na zachowanie prywatności, takich jak kompleksowe szyfrowanie, DNS-over-HTTPS czy kryptowaluty.
4. **Firmy, których działalność opiera się na danych, będą rozwijać jeszcze bardziej kreatywne, a niekiedy natarczywe, źródła danych napędzających machinę analizy zachowania.** Analiza zachowania w oparciu o dane to niebezpieczna gra. Błędy mogą przynieść szkody ludziom, podczas gdy rzeczywista jakość tych systemów często stanowi tajemnicę handlową. To jednak nie powstrzyma organizacji z tej branży przed szukaniem kreatyw-

niejszych sposobów profilowania użytkowników na podstawie ich upodobań i aktywności – a tym samych wpływania na ich życie.

5. **Prywatność różnicowa oraz uczenie federacyjne będą coraz powszechniej stosowane, podobnie jak technologia przetwarzania na brzegu sieci.** Ponieważ firmy coraz lepiej orientują się, jakiego rodzaju dane są im potrzebne, a klienci sprzeciwiają się niekontrolowanemu gromadzeniu informacji, powstają i rozpowszechniają się bardziej zaawansowane narzędzia prywatności, podczas gdy organizacje z grupy Big Tech zaczynają gwarantować użytkownikom nowe i ścisłe standardy prywatności. Należy spodziewać się bardziej zaawansowanego sprzętu, który umożliwi tworzenie narzędzi zdolnych do zaawansowanego przetwarzania danych, a tym samym zmniejszenie ilości danych udostępnianych organizacjom przez użytkowników.

Liczba incydentów przejęcia kont bankowych zwiększyła się o 20% w porównaniu z 2019 r.

3.02.2021 r. - W 2020 roku przejęcie konta stanowiło co drugą oszukańczą transakcję w branży finansowej – wynika z raportu[8] firmy Kaspersky. Według zanonimizowanych danych statystycznych dotyczących zdarzeń wykrytych przez rozwiązanie Kaspersky Fraud Prevention w okresie od stycznia do grudnia 2020 r., udział tego rodzaju incydentów zwiększył się z 34% w 2019 r. do 54% w 2020 r. Wśród najpopularniejszych sposobów uzyskiwania dostępu do kont bankowych można wyróżnić dwa – „na ratownika" oraz „na inwestora" – które stosowane są od 2019 r.



Wzrost znaczenia cyfrowych usług finansowych oraz e-handlu w 2020 r. jest w dużej mierze związany z tym, że z powodu pandemii spędzaliśmy więcej czasu w domu. Według ekspertów z firmy Kaspersky spowodowało to wzrost wykorzystywania socjotechniki przez cyberprzestępców. Dlatego tak istotne jest, aby zarówno instytucje finansowe, jak i klienci wiedzieli, jakie są typowe oszustwa, i potrafili się przed nimi bronić.

Zespół ekspertów odpowiedzialnych za rozwiązanie Kaspersky Fraud Prevention wyróżnił dwie powszechne metody stosowane przez osoby atakujące w celu uzyskania dostępu do kont – obie stanowiły kontynuację podobnych trendów zaobserwowanych w 2019 r. Pierwsza taktyka polega na wcieleniu się w rolę „osoby ratującej": oszuści podszywali się pod ekspertów ds. bezpieczeństwa i próbowali „ratować" użytkowników. W tym celu dzwonili do klientów banków, podając się za pracowników ds. bezpieczeństwa, informowali ich o podejrzanych obciążeniach lub płatnościach i oferowali swoją pomoc. Taki ratownik mógł poprosić klientów o zweryfikowanie ich tożsamości przy pomocy kodu wysłanego przy użyciu wiadomości SMS lub powiadomienia push, powstrzymanie podejrzanej transakcji lub przelanie środków na „bezpieczny rachunek". Atakujący mógł również poprosić o zainstalowanie aplikacji do zdalnego zarządzania, twierdząc, że jest ona wymagana do rozwiązywania problemów. Oszuści często przedstawiali się jako pracownicy największego banku w regionie potencjalnej ofiary i wykorzystywali sfałszowany identyfikator dzwoniącego w celu podszycia się pod rzeczywisty bank.

Drugą metodą było odgrywanie „inwestora". W tym przypadku oszuści podawali się za pracowników firmy inwestycyjnej lub konsultantów inwestycyjnych z banku. Dzwonili do klientów, by zaproponować im możliwość szybkiego zarobienia pieniędzy poprzez zainwestowanie w kryptowalutę lub akcje bezpośrednio z konta klienta bez konieczności udania się do oddziału banku. Jako warunek wykonania „usługi inwestycji" potencjalna ofiara musiała podać kod otrzymany w wiadomości tekstowej lub powiadomieniu push.

Raport Kaspersky Fraud Prevention opiera się na incydentach związanych z cyberprzestępczością oraz danych uzyskanych przez rozwiązanie Kaspersky Fraud Prevention na podstawie szczegółowej analizy zachowania klientów sektora bankowego oraz e-handlu.

[8] *https://kfp.kaspersky.com/resources*

Jak cyberprzestępcy próbowali nas oszukać w ostatnim sezonie wyprzedażowym?

4.02.2021 r. - Skończył się kolejny sezon wyprzedaży, będący czasem szczególnej aktywności cyberprzestępców. Ze względu na zamknięcie sklepów, wiele osób chętniej niż w ubiegłych latach korzystało z handlu online. Tymczasem oszuści, jak co roku, stosowali inżynierię społeczną, aby żerować na emocjach ofiary, a następnie podjąć próbę kradzieży pieniędzy i danych osobowych.

Według analizy ekspertów z Fortinetu, cyberprzestępcy podczas ostatniego okresu świątecznych wyprzedaży korzystali

ze sprawdzonych i wypróbowanych metod. Warto je poznać i uświadomić sobie, że ostrożność wobec niżej wymienionych zjawisk jest potrzebna zawsze, a nie tylko od święta.

- **Fałszywe strony internetowe** – Podczas zakupów online zawsze należy upewnić się, czy odwiedzamy oficjalne strony sklepów. Trzeba uważać na adresy URL, które mogą zawierać nazwy znanych marek ze zmienionymi niektórymi znakami oraz zwracać uwagę na obecność symbolu kłódki i „https" przy adresach, aby upewnić się, że strona jest chroniona.
- **Okazje w social media** – Cyberprzestępcy mają sposoby na śledzenie wyników wyszukiwania ofiary i mogą reklamować w mediach społecznościowych akurat te produkty, których ona szuka, po zaskakująco niskich cenach. Reklama może wydawać się godna zaufania, ale należy pamiętać, że każdy – w tym przestępcy – może zapłacić za umieszczenie reklamy w mediach społecznościowych i skierować ją do określonej grupy docelowej.
- **Fałszywe powiadomienia o wysyłce** – W razie otrzymania podejrzanego powiadomienia o dostawie paczki albo konieczności dopłaty za jej dezynfekcję, nie wolno klikać w żadne dołączone linki! Takie wiadomości zawierają łącza lub załączniki, które instalują na komputerze złośliwe oprogramowanie lub prowadzą na fałszywe strony internetowe.
- **Fałszywe organizacje charytatywne** – W okresie świąt ludzie są często w życzliwym nastroju, a cyberprzestępcy chcą to wykorzystać. Tworzą fałszywe strony organizacji charytatywnych w mediach społecznościowych, wysyłają wiadomości e-mail, a nawet SMS-y. Przed przekazaniem jakiegokolwiek datku trzeba upewnić się, że dana organizacja działa legalnie, a jej dane, w szczególności numer konta, są prawidłowe.
- **Nietypowe formy płatności** – Należy uważać na sklepy lub

osoby, które proszą o opłacenie zakupów za pomocą kart przedpłaconych, przelewów bankowych, osób trzecich, itp. W przypadku oszustwa, takiej płatności często nie da się cofnąć. Zamiast tego należy używać kart kredytowych, gdyż mają one zabezpieczenia na wypadek oszustwa, płatności można łatwo prześledzić, a odpowiedzialność leży nie tylko po stronie konsumenta.

- **Darmowe karty podarunkowe** – Wyskakujące reklamy lub wiadomości e-mail z ofertami bezpłatnych kart podarunkowych mogą być zarówno legalną ofertą, jak też próbą wyłudzenia informacji i kradzieży tożsamości. Jeśli okazja brzmi zbyt dobrze, żeby była prawdziwa, to prawdopodobnie mamy do czynienia z oszustwem.

Dla cyberprzestępców czasem nawet jedna ofiara jest warta inwestycji. Dlatego warto korzystać z wygody zakupów online, ale robić to rozsądnie i mieć się na baczności. Cyberprzestępcy wykorzystają bowiem każdą nadarzającą się okazję, zwłaszcza w czasie zwiększonego ruchu w e-commerce.

AV-Comparatives przyznaje rozwiązaniu Kaspersky Internet Security tytuł Produkt Roku

5.02.2021 r. - Kaspersky Internet Security – flagowe rozwiązanie zabezpieczające firmy Kaspersky przeznaczone do użytku domowego – już szósty raz z rzędu otrzymuje wyróżnienie Produkt Roku 2020[9] w corocznym raporcie opublikowanym przez niezależne laboratorium testowe AV-Comparatives. Firma Kaspersky wyprzedziła 16 konkurentów, zdobywając wyróżnienia Advanced+ w siedmiu rygorystycznych testach w ciągu 2020 r.

W minionym roku użytkownicy w większym niż zwykle stopniu polegali na technologii[10], aby utrzymać kontakt z najbliższymi oraz pracować zdalnie, po tym jak zamknięto biura oraz szkoły. Przez cały ten czas firma Kaspersky chroniła swoich klientów przed ewoluującymi cyberzagrożeniami za pomocą najbardziej niezawodnych i skutecznych produktów na rynku. Jej zaangażowanie zostało zauważone i potwierdzone sześcioma corocznymi kluczowymi wyróżnieniami przyznanymi przez laboratorium AV-Comparatives za doskonałe działanie produktów firmy przez ostatnie 12 miesięcy.

Zdobywając wyróżnienie Produkt Roku 2020, rozwiązanie Kaspersky Internet Security wyprzedziło 16 konkurentów w okresie objętym testem i otrzymało wyróżnienia Advanced+ za maksymalne wyniki pod względem skuteczności we wszystkich siedmiu testach przeprowadzonych w okresie całego roku. Wśród nich znajdują się dwa półroczne testy Real-World Protection (ochrona w warunkach odwzorowujących realne korzystanie z komputera i internetu), dwa testy Malware Protection (ochrona przed szkodliwym oprogramowaniem), dwa testy Performance Measurement (pomiar skuteczności) oraz test Enhanced Real-World (rozszerzone badanie jakości ochrony).

Dalsze informacje na temat corocznego raportu AV-Comparatives 2020 są dostępne na stronie https://www.av-comparatives.org/tests/summary-report-2020.

[9] *https://www.av-comparatives.org/awards/kaspersky-lab/*

[10] *https://www.thinkwithgoogle.com/intl/en-cee/future-of-marketing/digital-transformation/covid-accelerated-digital-adoption/*

Firma CD Projekt zaatakowana ransomware

9.02.2021 r. - Jak można przeczytać w serwisie niebezpiecznik.pl, w lutym br. firma CD Projekt poinformowała, że padła ofiarą ataku ransomware[11]. Jak wynika z jej oświadczenia, dane na niektórych serwerach zostały zaszyfrowane, jednak dzięki regularnie wykonywanym kopiom bezpieczeństwa wszystkie są możliwe do przywrócenia. Ponadto maszyny, które zostały zaszyfrowane, nie przetwarzały danych klientów. CD Projekt nie sprecyzował, jakie dane znajdowały się na serwerach; atakujący z kolei wskazywali, że były to serwery zawierające kody źródłowe gier Cyberpunk 2077, Witcher, GWent, Witcher 3 oraz dane finansowo-księgowe i kadrowe.

Firma zdecydowała się nie negocjować z przestępcami, a wręcz przeciwnie — ujawniła ich notatkę i założyła, że jeśli jakieś dane zostały wykradzione, to mogą zostać ujawnione. Jak zauważają redaktorzy wspomnianego portalu, wiadomość od przestępców nie przypomina żadnej innej „automatycznie generowanej" notatki publikowanej przez powszechnie znane rodziny oprogramowania ransomware, co pozwalałoby przypisać atak któremuś ze znanych ugrupowań wykorzystujących to zagrożenie, jak np. Dopple, Ragnar czy Avaddon.

CD Projekt poinformował o incydencie odpowiednie służby.

[11] *https://twitter.com/CDPROJEKTRED/status/1359048125403590660*

Haker zatruł wodę w wodociągach, przez internet

10.02.2021 r. - W lutym br. szeryf z Florydy poinformował[12] o incydencie, który mógł zagrażać życiu i zdrowiu kilkunastu tysięcy ludzi. O sprawie poinformował m.in. portal niebezpiecznik.pl: nieznana osoba włamała się do wodociągów w hrabstwie Pinellas i zwiększyła stężenie wodorotlenku sodu stukrotnie. Substancja ta jest stosowana przez wodociągi na Florydzie do sterowania kwasowością wody, a włamywacz zmienił jej stężenie do wartości 11000 ppm. Na szczęście pracownik wodociągów zauważył tę groźną w skutkach modyfikację i błyskawicznie przywrócił poprawne parametry. Władze uspokajają, że nawet jeśli pracownik nie przywróciłby ustawień ręcznie, to zadziałałyby inne systemy bezpieczeństwa m.in. monitorujące pH wody. Dodają też, że woda o zmienionych parametrach trafiłaby do mieszkańców i tak najwcześniej następnego dnia. Gdyby jednak tak się nie stało, skutki kontaktu z wodorotlenkami sodu mogły być tragiczne.

Jak się okazało, atakujący uzyskał dostęp do systemu dwukrotnie. Za każdym razem włamanie trwało kilka minut, podczas których swobodnie zmieniał parametry w interfejsie. Chociaż jego aktywność w systemie była obserwowana przez pracownika, nie wzbudziła żadnych podejrzeń, gdyż do tego systemu zdalny dostęp regularnie wykorzystywał przełożony pracownika. Poruszający się po ekranie kursor myszy był nie był więc niczym dziwnym. Po incydencie władze wodociągów zdecydowały się na zablokowanie zdalnego dostępu do swoich systemów.

Wodociągi korzystały z rozwiązania TeamViewer; nie wiadomo, w jaki sposób włamywacz przejął nad nim kontrolę. Dziś, zwłaszcza z uwagi na pandemię, zdalny dostęp jest coraz bardziej pożądany, ale niestety nie zawsze wdrażany z głową i odpowiednimi zabezpieczeniami.

[12] *https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/*

100 tys. zł kary za wyciek danych sędziów i prokuratorów

18.02.2021 r - Jak przypomina portal Niebezpiecznik.pl, w kwietniu 2020 r. na pewnym forum internetowym opublikowano bazę danych z portalu KSIP.gov.pl[13] **zawierającą imiona, nazwiska, adresy e-mail, adresy IP, numery telefonów oraz miasta sędziów, asesorów i referendarzy. Do incydentu miało dojść w wyniku błędu podmiotu przetwarzającego. Prokuratura Regionalna w Lublinie poinformowała o zatrzymaniu Krzysztofa J.[14], pracownika spółki zewnętrznej, która na drodze przetargu świadczyła usługi utrzymania serwerów dla KSSIP. Mężczyzna ten miał rzekomo omyłkowo przenieść dane do katalogu, któremu nadane zostały uprawnienia publiczne.**

Urząd Ochrony Danych Osobowych uznał, że problem był po stronie szkoły i nałożył na nią karę w wysokości 100 tys. zł. Jego zdaniem szkoła nie zastosowała odpowiednich środków technicznych i organizacyjnych, które pozwoliłyby zapewnić poufność przetwarzania danych. Nie testowano i nie szacowano skuteczności środków technicznych i organizacyjnych, które miały służyć bezpieczeństwu. Nie uwzględniono ryzyka, jakie wiązało się z przetwarzaniem takich danych.

W komunikacie prasowym[15] napisano, że:

Na zasobach informatycznych KSSiP znajdowała się kopia bazy danych, której istnienie i bezpieczeństwo, po wykonaniu czynności migracyjnych, w żaden sposób nie zostało zweryfikowane przez

administratora, co jest jego prawnym obowiązkiem wynikającym z przepisów o ochronie danych osobowych. KSSIP, w związku ze zmianami w procesie przetwarzania, nie podjęła wystarczających działań mających na celu zweryfikowanie bezpieczeństwa środowiska przetwarzania przed rozpoczęciem działań migracyjnych, jak i po ich zakończeniu.

Z komunikatu wynika również, że KSSIP nie zawarła w umowie przetwarzania istotnych aspektów, np. nie uwzględniła kategorii osób i nie doprecyzowała rodzaju danych osobowych przez wskazanie ich kategorii. W umowie zabrakło też zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora. Jak stwierdza UODO, KSSIP „nie miała pełnej świadomości, jak kształtują się prawa i obowiązki, pomiędzy administratorem a podmiotem przetwarzającym" zarówno przed naruszeniem, jak i po jego stwierdzeniu.

Podmiot przetwarzający nie został ukarany. Zdaniem UODO wypełniał on obowiązki wynikające z umowy powierzenia i umowy głównej, a także stosował przyjęte przez siebie środki organizacyjne mające na celu zapewnienie bezpieczeństwa. To administrator nie podjął się analizy, czy wskazując podmiotowi przetwarzającemu miejsce do wykonania kopii zapasowej bazy danych, nie naraża danych osobowych w niej zawartych na naruszenie ich poufności. W opinii UODO nie ma podstaw do zarzucenia podmiotowi przetwarzającemu naruszenia obowiązku wspierania administratora w wywiązywaniu się z obowiązków.

[13] *https://niebezpiecznik.pl/post/dane-dziesiatek-tysiecy-sedziow-i-prokuratorow-wyciekly-z-kssip-i-ciagle-wisza-w-sieci/*

[14] *https://niebezpiecznik.pl/post/jak-doszlo-do-wycieku-danych-sedziow-i-prokuratorow/*

[15] *https://uodo.gov.pl/pl/138/1909*

Zaawansowany cybergang Lazarus bierze na celownik przemysł obronny

25.02.2021 r. - Badacze z firmy Kaspersky zidentyfikowali nową, nieznaną wcześniej kampanię, za którą stoi Lazarus – niezwykle aktywne, zaawansowane ugrupowanie cyberprzestępcze działające od 2009 r. i powiązane z wieloma wyrafinowanymi atakami. Od początku 2020 r. cybergang atakował przemysł obronny z pomocą szkodliwego narzędzia o nazwie ThreatNeedle, które rozprzestrzenia się w zainfekowanych sieciach, gromadząc poufne informacje.

Lazarus[16] to obecnie jedno z najaktywniejszych ugrupowań cyberprzestępczych. Działając od co najmniej 2009 r., grupa ta przeprowadzała kampanie szpiegowskie[17] na dużą skalę – także w polskim sektorze finansowym, kampanie z wykorzystaniem ransomware[18], a nawet ataki na rynek kryptowaluty[19]. Chociaż przez ostatnie kilka lat Lazarus koncentrował się na instytucjach finansowych, wygląda na to, że na początku 2020 r. wziął na swój celownik również przemysł obronny.

Badacze z firmy Kaspersky po raz pierwszy wpadli na trop wspomnianej kampanii, gdy pewna organizacja zwróciła się do nich o pomoc w zareagowaniu na incydent. Odkryli wówczas, że padła ona ofiarą szkodliwego programu umożliwiającego pełną zdalną kontrolę nad zainfekowanymi urządzeniami (tzw. backdoor). Szkodnik ten, któremu nadano nazwę ThreatNeedle, rozprzestrzenia się w zainfekowanych sieciach, wydobywając z nich poufne informacje. Do tej pory zaatakowane zostały organizacje w kilkunastu krajach.

Na początkowym etapie infekcji stosowany jest phishing ukierunkowany: potencjalne ofiary otrzymują wiadomości e-mail zawierające szkodliwy załącznik pod postacią pliku Worda lub odsyłacz do dokumentu przechowywanego w chmurze. Często wiadomości te zawierają rzekomo pilne aktualizacje związane z pandemią, a atakującym zdarza się podszywać pod uznane centrum medyczne.

ThreatNeedle należy do rodziny szkodników o nazwie Manuscrypt, której właścicielem jest ugrupowanie Lazarus i która wcześniej atakowała firmy związane z kryptowalutą. Po zainstalowaniu się na urządzeniu ofiary ThreatNeedle potrafi przejąć nad nim całkowitą kontrolę, co oznacza, że może zrobić tam wszystko: od manipulowania plikami po wykonywanie otrzymanych poleceń.

Jedna z najbardziej interesujących technik w tej kampanii dotyczyła możliwości kradzieży danych zarówno z sieci biurowej (zawierającej komputery z dostępem do internetu), jak i z maszyn odizolowanych od internetu, zawierających zasoby krytyczne. Zgodnie z zasadami stosowanymi w wielu firmach, między tymi dwiema sieciami nie mogą być przesyłane żadne dane. Mogą jednak łączyć się z nimi administratorzy w celu utrzymania systemów. Lazarus zdołał przejąć kontrolę nad stancjami roboczymi administratorów, a następnie skonfigurować „szkodliwą" bramę, aby atakować odizolowaną sieć, a następnie kraść i wydobywać z niej poufne dane.

Więcej informacji na temat kampanii ThreatNeedle można uzyskać na stronie internetowej zespołu Kaspersky ICS CERT: https://r.kaspersky.pl/sBn4F.

[16] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3355/kaspersky-ujawnia-dwa-incydenty-cyberprzestepcze-dotyczace-badan-nad-szczepionka*

[17] *https://www.kaspersky.pl/o-nas/informacje-prasowe/2768*

[18] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3298/cybergang-lazarus-poluje-na-grubego-zwierza-wykorzystujac-wlasne-oprogramowanie-ransomware*

[19] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3213/cybergang-lazarus-pokazuje-udoskonalony-warsztat-w-ataku-applejeus-majacym-na-celu-kradziez-kryptowaluty-takze-w-polsce*

Cyberzagrożenia czające się za produkcjami nominowanymi do Złotych Globów

1.03.2021 r. - W niedzielę odbyła się 78 ceremonia wręczenia Złotych Globów, a wraz z nią rozpoczął się sezon przyznawania wyróżnień w branży filmowej i telewizyjnej w 2021 r. Jednak seriale i filmy dostarczają nie tylko rozrywkę, ale stanowią również atrakcyjną przynętę wykorzystywaną przez cyberprzestępców do dystrybucji zagrożeń, stron phishingowych oraz wiadomości spamowych. Dlatego to istotne wydarzenie branżowe wzbudza zainteresowanie zarówno kinomanów, jak i wszelkiej maści oszustów. Aby dowiedzieć się, w jaki sposób cyberprzestępcy próbują zarobić na widzach małego i dużego ekranu, eksperci z firmy Kaspersky przeanalizowali szkodliwe pliki ukrywające się pod nominowanymi filmami, a także związane z filmami strony internetowe stworzone w celu kradzieży danych uwierzytelniających użytkowników.

Do analizy wybrano następujące nominowane produkcje: „Kolejny film o Boracie", „Emily w Paryżu", „Ozark", „Palm Springs", „Ratched", „The Crown", „The Mandalorian", „Gambit królowej", „Proces siódemki z Chicago" oraz „Unorthodox".

Badacze z firmy Kaspersky ustalili, że w pierwszych trzech tygodniach stycznia próby infekcji przy użyciu plików kryjących różne zagrożenia podszywające się pod nominowane produkcje dotyczyły najczęściej serialu „The Mandalorian" (68% prób infekcji). Drugie miejsce zajął hit sieci Netflix – serial „Gambit królowej" (11% atakowanych użytkowników), natomiast pierwszą trójkę zamknął serial „Ozark" (6% atakowanych użytkowników).

Eksperci zidentyfikowali również liczne strony phishingowe przygotowane w celu kradzieży danych uwierzytelniających użytkowników. Niektóre z nich żądają podania danych dotyczących karty bankowej w celu potwierdzenia, że dany użytkownik zlokalizowany jest w regionie objętym licencją zasobu online na dystrybuowanie zawartości; inne po prostu przekierowują do zasobów zewnętrznych. W każdym przypadku użytkownik zostaje oszukany, jego dane wydostają się na zewnątrz, a informacje uwierzytelniające zostają skradzione.

Szczepionki przeciwko COVID-19 do kupienia na czarnym rynku za kwotę od 200 do 1 200 dolarów

4.03.2021 r - Obecnie na całym świecie prowadzona jest jedna z największych i najbardziej skomplikowanych w historii akcji szczepień. W tej sytuacji nie mogło zabraknąć oszustów oraz nielegalnych sprzedawców chcących wzbogacić się na tym procesie. Analizując 15 różnych rynków w Darknecie, badacze z firmy Kaspersky znaleźli reklamy trzech głównych szczepionek przeciwko COVID-19: preparatów firm Pfizer/BioNTech, AstraZeneca oraz Moderna. Pojawili się również sprzedawcy reklamujący niezatwierdzone szczepionki.

Większość sprzedawców pochodziła z Francji, Niemiec, Wielkiej Brytanii oraz Stanów Zjednoczonych, a ceny za dawkę wahały się w granicach od 200 do 1 200 dolarów, przy czym średnio wynosiły około 500 dolarów. Komunikacja odbywała się za pośrednictwem komunikatorów umożliwiających wymianę wiadomości zabezpieczonych szyfrowaniem, takich jak Wickr oraz Telegram, natomiast żądaną formą płatności była kryptowaluta, głównie bitcoin, która jest znacznie trudniejsza do śledzenia niż tradycyjne przelewy.

Większość nielegalnych sprzedawców wykonała od 100 do 500 transakcji, co oznacza, że osoby te coś sprzedawały, jednak to, co dokładnie kupili użytkownicy Darknetu, pozostaje niewiadomą. Na podstawie dostępnych informacji nie można stwierdzić, jaka część reklamowanych online dawek szczepionek jest prawdziwa, a jaka jest zwykłym oszustwem.

Więcej informacji na temat szczepionek sprzedawanych w Darknecie znajduje się na oficjalnym blogu firmy Kaspersky – Kaspersky Daily: https://kas.pr/4cs1.

Podstępne malware. W jaki sposób złośliwe oprogramowanie może zainfekować komputer?

5.03.2021 r. - Znalazłeś w publicznym miejscu pendrive, dostałeś maila z prośbą o pilne kliknięcie linka lub pobranie nowej aplikacji związanej z koronawirusem? Wszystko to może być próba zainfekowania złośliwym oprogramowaniem. – Coraz bardziej wyrafinowane akcje wykorzystujące malware to jedno z głównych cyberzagrożeń według prognoz na 2021 rok. Tymczasem internauci wciąż padają także ofiarami znanych od lat scenariuszy.

Mimo że świadomość zagrożenia ze strony złośliwego oprogramowania regularnie rośnie, użytkownicy nadal niewiele wiedzą o możliwych mechanizmach ataków. Dlatego eksperci ESET opracowali listę sześciu najpopularniejszych sposobów, za pośrednictwem których hakerzy wykorzystują malware.

Wiadomości e-mail typu phishing i złośliwy spam

Zwykle celem akcji phishingowych jest wyłudzanie poufnych informacji, takich jak dane karty płatniczej, kod PIN lub dane dostępu do różnych usług. Jednak udające np. korespondencję od zaufanej instytucji maile mogą zawierać także załączniki lub linki, których celem będzie zainfekowanie urządzenia złośliwym oprogramowaniem. Dlatego zawsze należy dokładnie czytać maile, nim klikniemy zawarte w nich linki czy pobierzemy załączniki. Co powinno wzbudzić podejrzenie? Najczęstszymi znakami ostrzegawczymi są błędy ortograficzne, nadmierne akcentowanie potrzeby pilnego kliknięcia, prośby o podanie danych osobowych lub podejrzany adres mailowy, z którego pochodzi wiadomość.

Fałszywe witryny internetowe

Aby nakłonić ofiary do pobrania złośliwych aplikacji, cyberprzestępcy podszywają się także pod strony internetowe znanych marek lub organizacji. Oszuści często tworzą fałszywe strony, które do złudzenia przypominają legalne odpowiedniki. Różnią się one łatwymi do przeoczenia szczegółami. Często są to dodane w adresie strony litery, symbole, a czasem całe wyrazy. Aby uniknąć zagrożenia, adres strony należy wpisywać ręcznie w pasku adresu w przeglądarce.

Zewnętrzna pamięć

Zewnętrzne urządzenia typu flash to od dawna najpopularniejsza forma przechowywania i przekazywania plików. Ta furtka bardzo szybko została dostrzeżona i wykorzystana przez cyberprzestępców. Najczęstsze ataki tego typu wykorzystują m.in. motyw „zagubionych" pendrive'ów, które pozostawiane są w ogólnodostępnych miejscach. Osoby, które znalazły taki sprzęt nierzadko, choćby z ciekawości, podłączają go do swoich komputerów, nie mając świadomości, że mogą dać w ten sposób hakerom dostęp do osobistych danych. Jeśli komputer nie będzie wyposażony w aktualne oprogramowanie antywirusowe zabezpieczające punkty końcowe i skanujące wszelkie nośniki zewnętrzne podłączone do urządzenia, bez wątpienia zostanie zainfekowany.

Zainfekowane oprogramowanie

Rzadkim, ale równie niebezpiecznym zjawiskiem jest infekowanie legalnego oprogramowania. Jednym z przykładów takiego naruszenia bezpieczeństwa jest z pewnością przypadek CCleaner z 2017 roku. Złośliwe oprogramowanie zostało wtedy „wstrzyknięte" bezpośrednio do aplikacji, która była następnie wykorzystywana do rozprzestrzeniania malware. Ponieważ CCleaner to zaufany i znany program, użytkownicy niczego nie podejrzewali. To przykład ataku, w którym zagrożenie pochodzi ze źródła pozornie niebudzącego wątpliwości.

Reklamy i banery

Niektóre witryny są pełne agresywnych reklam typu pop-up, które szybko przenoszą użytkowników w inne miejsca strony, czy poza pierwotną witrynę. Chociaż celem tych reklam jest najczęściej generowanie przychodów z ich wyświetlania, bywają także reklamy „obciążone" różnymi typami złośliwego oprogramowania. Klikając w nie, użytkownik może pobrać niepożądane aplikacje. Bardzo częstym zjawiskiem, szczególnie w przypadku urządzeń mobilnych, są reklamy, które wykorzystują metodę zastraszania. Sugerują one, że urządzenie zostało przejęte i tylko rozwiązanie oferowane w reklamie może pomóc w odzyskaniu pełnej funkcjonalności sprzętu. Tego typu zagrożeń można uniknąć używając zaufanych rozszerzeń blokujących reklamy w przeglądarce i nie wchodząc na podejrzane witryny.

Fałszywe aplikacje mobilne

Ostatnią pozycją na liście potencjalnych zagrożeń są fałszywe aplikacje mobilne, które udają prawdziwe i próbują nakłonić użytkowników do podjęcia określonych działań. Mogą np. udawać aplikacje do ćwiczeń fitness, kryptowalut, a nawet te związane tematycznie z COVID-19. Dlatego zaleca się korzystanie tylko z aplikacji pochodzących z zaufanego źródła, oferowanych przez firmy i instytucje z weryfikowalną historią i recenzjami.

Połowa firm zabrania dzielenia się wynikami analizy zagrożeń ze społecznościami zawodowymi

9.03.2021 r. - Dwie trzecie (66%) analityków cyberzagrożeń należy do społeczności zawodowych, jednak 52% osób odpowiedzialnych za IT oraz cyberbezpieczeństwo w firmach nie może dzielić się w obrębie takich społeczności wykrytymi artefaktami analizy zagrożeń – wynika z nowego raportu[20] firmy Kaspersky.

Kaspersky od dawna nawołuje do międzynarodowej współpracy w cyberprzestrzeni oraz bierze udział we wspólnych inicjatywach globalnej społeczności związanej z bezpieczeństwem IT[21], uważając, że jest to najlepszy sposób na zapewnienie ochrony przed nieustannie ewoluującymi cyberzagrożeniami. Do celów nowego raportu firma przeprowadziła ankietę wśród ponad 5 200 praktyków w zakresie IT oraz cyberbezpieczeństwa, aby przekonać się, czy ich firmy są otwarte na współpracę oraz dzielenie się wynikami analizy zagrożeń.

W badaniu stwierdzono, że respondenci odpowiedzialni za analizę zagrożeń szczególnie często korzystają ze specjalistycznych forów (45%), forów dark webu (29%) czy też grup w mediach społecznościowych (22%).

Jeśli chodzi o dzielenie się własnymi ustaleniami, jedynie 44% respondentów upubliczniło swoje odkrycia. Z kolei w firmach, w których przekazywanie takich informacji na zewnątrz jest dozwolone, postąpiło w ten sposób 77% analityków bezpieczeństwa. W 8% przypadków eksperci dzielili się swoimi ustaleniami w zakresie analizy zagrożeń mimo zakazu organizacji, w których pracowali.

Specjaliści z firmy Kaspersky zauważyli, że takie zakazy wynikają częściowo z obaw, że jeśli pewne obiekty zostaną publicznie ujawnione, zanim firma zdoła zareagować na atak, cyberprzestępcy zorientują się, że ich działania zostały wykryte, i zmienią taktyki. Aby pomóc zespołom ds. bezpieczeństwa IT w analizowaniu podejrzanych obiektów bez narażania prowadzonego dochodzenia, firma Kaspersky oferuje tryb prywatnego przesyłania podejrzanych obiektów poprzez darmowy dostęp do usługi Kaspersky Threat Intelligence Portal[22]. W ten sposób cyberprzestępca nie dowie się, że ktoś udostępnił próbki zagrożeń, a analityk będzie mógł otrzymać żądane dane.

[20] *https://www.kaspersky.com/blog/it-security-economics-2020-part-4/*

[21] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3374/budowa-zaufania-i-bezpieczenstwa-w-cyberprzestrzeni-kaspersky-wspolprzewodniczy-wraz-ze-stowarzyszeniem-cigref-grupie-roboczej-w-ramach-inicjatywy-paris-call*

[22] *https://opentip.kaspersky.com/#_blank*

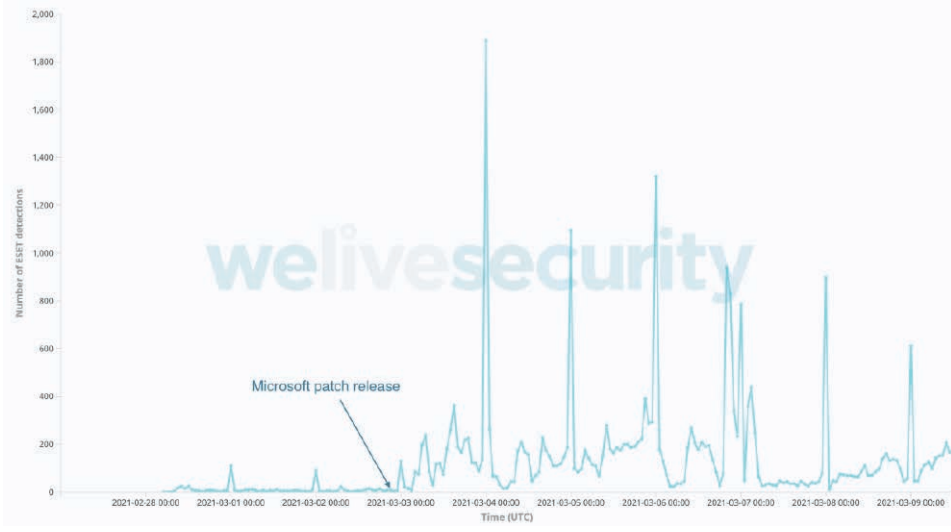
Ponad 5 tysięcy serwerów padło ofiarą ataków związanych z lukami w zabezpieczeniach Microsoft Exchange

DAGMA BEZPIECZEŃSTWO IT

12.03.2021 r - W minionym tygodniu ponad dziesięć różnych grup hakerskich APT wykorzystało istniejące luki w Microsoft Exchange, aby włamać się do serwerów pocztowych. Badacze ESET odkryli, że złośliwą aktywność zarejestrowano na ponad 5000 serwerów poczty e-mail, należących do różnego rodzaju organizacji, zarówno firm, jak i rządów z całego świata. – Aktywność grupy Hafnium, o której najgłośniej w mediach, to zaledwie wierzchołek góry lodowej. Biorąc pod uwagę popularność oprogramowania Microsoft, skala zagrożenia jest bardzo poważna.

Z początkiem marca firma Microsoft udostępniła łatki dla Exchange Server 2013, 2016 i 2019, które naprawiają szereg luk w zabezpieczeniach i chronią przed zdalnym wykonaniem kodu (RCE). Dla cyberprzestępców, luki te stanowią furtkę do swobodnego przejęcia podatnej wersji serwera Exchange i to bez konieczności znajomości jakichkolwiek istotnych danych logowania do konta. Okazało się, że serwery połączone z Internetem stanowią łatwy cel dla grup hakerskich, a ogromna liczba użytkowników Microsoft Exchange może oznaczać ryzyko nadużyć na ogromną skalę.

Krótko po wypuszczeniu łatek, eksperci ESET bacznie przyglądali się bieżącej sytuacji i odnotowali zwiększoną aktywność cyberprzestępców, którzy skanowali i atakowali serwery Exchange.



Detekcje ESET dla skryptów typu webshell w okolicy dodania ostatniej łatki Microsoft Exchange, godzina po godzinie.

Zgodnie z ich obserwacjami, wzmożoną aktywność odnotowano w szczególności w Stanach Zjednoczonych, Wielkiej Brytanii oraz Niemczech, niemniej jednak ataki zaobserwowano w wielu innych krajach.

Telemetria ESET zgłosiła obecność złośliwych programów lub skryptów, które umożliwiają zdalne sterowanie serwerem za pośrednictwem przeglądarki internetowej, na ponad 5000 serwerach rozmieszczonych w ponad 115 krajach.

Kaspersky uplasował się w pierwszej trójce w 81% testów porównawczych w 2020 r.

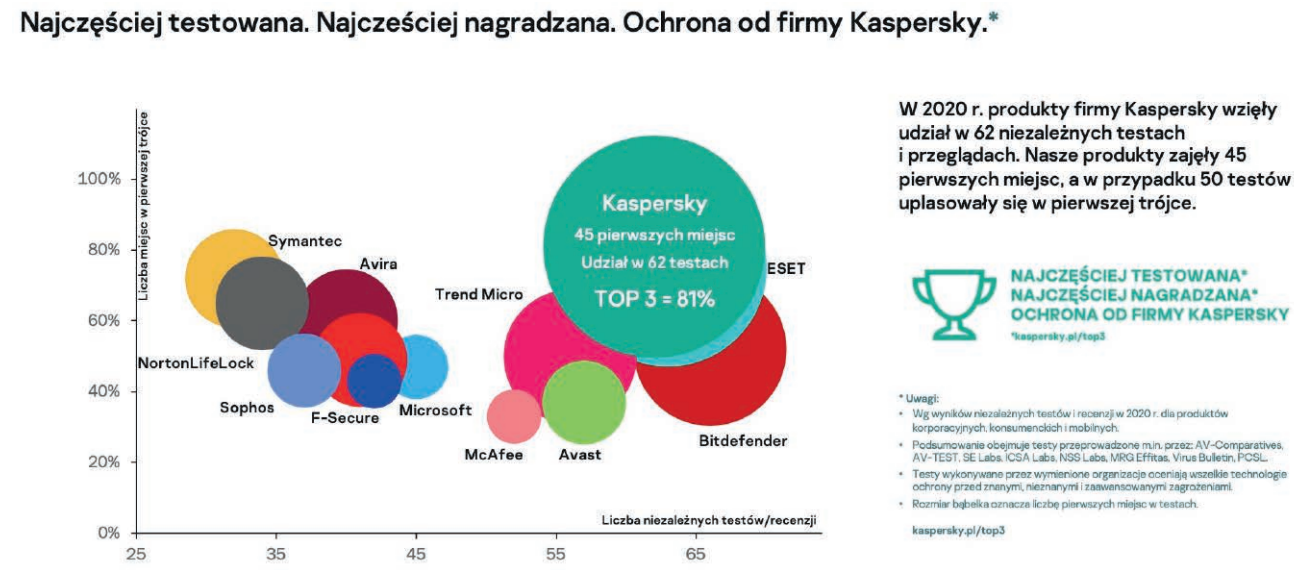
12.03.2021 r. - Ósmy rok z rzędu firma Kaspersky znalazła się na szczycie rankingu TOP3: jej rozwiązania bezpieczeństwa uplasowały się w pierwszej trójce w 50 na 62 niezależne testy, w których wzięły udział w 2020 r. Firma uplasowała się na podium w 81% testów porównawczych. Wynik ten stanowi potwierdzenie, że produkty firmy Kaspersky nieustannie wyprzedzają konkurencję pod względem ochrony zarówno przedsiębiorstw, jak i konsumentów przed znanymi, nieznanymi oraz zaawansowanymi zagrożeniami.

Coroczny ranking TOP3 wskazuje, ile razy rozwiązania danego producenta zdobyły pierwsze, drugie lub trzecie miejsce w najbardziej rygorystycznych w branży niezależnych testach. Są one przeprowadzane przez tak szanowane instytucje testujące jak AV-Test, AV-Comparatives, SELabs, NSS Labs, VirusBulletin, MRG Effitas czy ICSA Labs. Firma Kaspersky zdobyła pierwsze miejsce w 73% testów, w których wzięła udział, 45 razy pokonując konkurencję w rywalizacji o najwyższy stopień podium.

Rok 2020 okazał się kolejnym wyśmienitym rokiem dla firmy Kaspersky. Jej flagowe rozwiązanie bezpieczeństwa dla użytkowników domowych – Kaspersky Internet Security – po raz szósty otrzymało wyróżnienie Produkt Roku przyznane przez AV-Comparatives. Produkt ten osiągnął również najwyższe wyniki w teście ochrony przed zaawansowanymi zagrożeniami i po raz drugi z rzędu został uhonorowany corocznym wyróżnieniem ATP 2020 Gold. Ponadto osiągnął najwyższy wskaźnik Total Accuracy Rating spośród wszystkich uczestników wszystkich czterech kwartalnych testów przeprowadzonych przez SE Labs, otrzymując cztery najwyższe oceny AAA. Z kolei Kaspersky Mobile Antivirus otrzymał certyfikat MRG Effitas za osiągnięcie 100% współczynnika wykrywania w programie oceny Android 360.

Produkty dla sektora B2B, Kaspersky Endpoint Security oraz Kaspersky Small Office Security, osiągnęły najwyższe wskaźniki Total Accuracy Rating w zakresie ochrony przed znanymi i ukierunkowanymi atakami spośród wszystkich uczestników testów SELabs przeprowadzonych w trzech kwartałach i czterokrotnie zdobyły certyfikat AAA. Z kolei Kaspersky Endpoint Security for Business został wyróżniony przez SELabs tytułem najlepszego produktu dla punktów końcowych przedsiębiorstw na podstawie ciągłego udziału w testach publicznych, prywatnych ocen oraz informacji zwrotnych od klientów. NSS Labs zwrócił uwagę na wysokie możliwości Kaspersky Endpoint Security for Business w zakresie ochrony przed atakami, łącznie ze szkodliwym oprogramowaniem, exploitami, zagrożeniami mieszanymi, przyznając mu bardzo mocną ocenę AA. Kaspersky Web Traffic Security otrzymał swój trzeci certyfikat VBWeb po zablokowaniu wszystkich 650 zestawów exploitów, na które został wystawiony.

Wyróżniane nagrodami rozwiązania cyberbezpieczeństwa firmy Kaspersky chronią ponad 400 milionów użytkowników. W okresie od listopada 2019 r. do października 2020 r. zablokowały 666 809 967 ataków przeprowadzonych z zasobów online. Ponadto rozpoznały 173 335 902 szkodliwych adresów URL i zablokowały 33 412 568 unikatowych szkodliwych obiektów. Rozwiązania firmy Kaspersky odparły również 549 301 ataków ransomware oraz 668 619 prób infekcji przez szkodliwe oprogramowanie stworzone w celu kradzieży pieniędzy poprzez konto bankowe użytkownika.

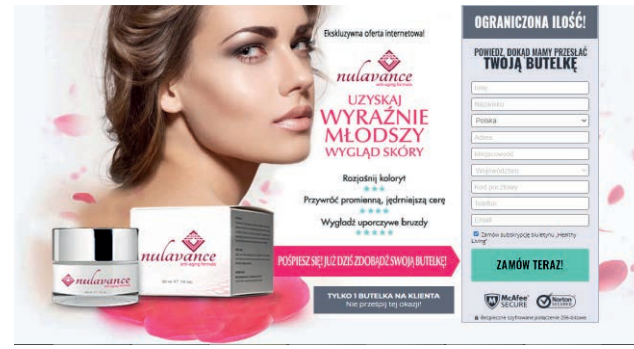


Nowe cyberoszustwo „na cudowny krem”

16.03.2021 r. - „Wyraźnie młodszy wygląd”, „wygładzenie zmarszczek”, „promienną, jędrniejszą cerę” obiecują maile reklamujące nowy, cudowny krem do twarzy. Niestety, nie zadziała. Zainteresowanie ofertą może przynieść odwrotny efekt. To bowiem najnowsza kampania spamowa, jaką zidentyfikowali właśnie eksperci ds. cyberbezpieczeństwa ESET.

Fałszywy preparat o nazwie Nulavance nie usunie zmarszczek, a zainteresowanie nim może przyczynić się do utraty danych i pieniędzy. Po kliknięciu w grafikę, dołączoną do maila z reklamą, zostajemy przekierowani do formularza. Żąda on od nas m.in. podania szczegółowych danych teleadresowych, a w kolejnym kroku także danych karty płatniczej.

Reklama preparatu trafia na skrzynki mailowe z różnych adresów, niepowiązanych z polską domeną produktu. Ta bowiem nie istnieje. Informacje o kremie, który – zgodnie z grafiką dołączaną do maila – ma być rzekomo dystrybuowany w „ekskluzywnej ofercie internetowej”, rozsiane są na różnych, zwykle bezpłatnych serwisach internetowych, które umożliwiają wrzucanie treści każdemu. W oczy rzuca się słaba jakość językowa i graficzna przygotowanych materiałów. „Nulavance być odpowiedzią! Co więcej, zaczyna się od odżywienia skóry balsamem odmładzającym i naturalnie zwiększyć kolagen, a także utrzymać nawilżenie skóry” – to tylko próbka z jednego z artykułów promujących nieistniejący produkt.

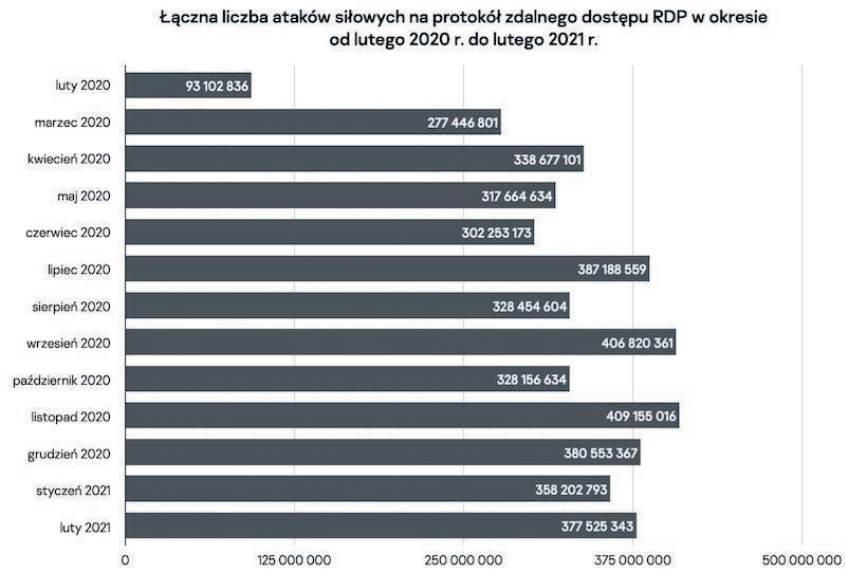


Materiały zawierają hasła marketingowe, które mają podkreślać ekskluzywny i ograniczony charakter rzekomej oferty – m.in. „jedna butelka na klienta”, „niski stan magazynowy”, „ryzyko wykupienia wysokie”. W grafice dołączanej do maila oszuści wykorzystują natomiast logotypy znanych dostawców rozwiązań antywirusowych, zapewniając o „bezpiecznym szyfrowaniu”. To kolejna kampania spamowa, która próbuje wzbudzić wśród użytkowników zaufanie, powołując się cynicznie na standardy z zakresu cyberbezpieczeństwa.

Efekt pandemii: covidowy krajobraz cyberprzestępczy

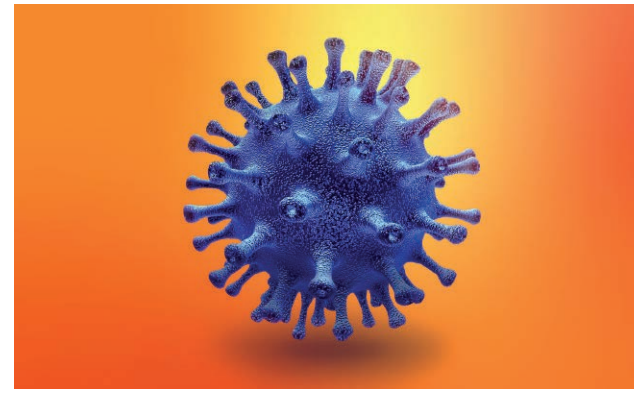
17.03.2021 r. - Po tym, jak Światowa Organizacja Zdrowia oficjalnie ogłosiła w połowie marca zeszłego roku, że mamy do czynienia z pandemią, państwa zaczęły pospiesznie podejmować środki mające na celu powstrzymanie jej rozprzestrzeniania się. Popularnym posunięciem w ramach walki z pandemią było przechodzenie firm na tryb pracy zdalnej. Ponieważ działania te były wykonywane w dużym pośpiechu i często bez uprzedniego przygotowania, wiele firm nie miało czasu na wdrożenie właściwych środków, narażając się na wiele nowych zagrożeń dla cyberbezpieczeństwa. Według badaczy z firmy Kaspersky do najczęstszych należały ataki na protokoły wykorzystywane przez pracowników do uzyskiwania zdalnego dostępu do zasobów firmowych.

Protokół RDP, wykorzystywany do uzyskiwania dostępu do systemu Windows lub serwerów, stanowi prawdopodobnie najpopularniejszy mechanizm zdalnego pulpitu. Gdy pracownicy przeszli na pracę zdalną, liczba ataków siłowych na ten protokół błyskawicznie wzrosła. W ramach takich działań atakujący wypróbowują różne nazwy użytkowników oraz hasła, dopóki nie trafią na poprawną kombinację – i uzyskają dostęp do zasobów firmowych.



Na przestrzeni minionego roku liczba ataków siłowych wahała się, jednak w porównaniu z okresem sprzed pandemii nastąpił wyraźny wzrost.

Według telemetrii firmy Kaspersky, gdy w marcu 2020 r. na całym świecie wprowadzano lockdowny, liczba ataków siłowych na protokoły RDP wzrosła z 93,1 mln w lutym 2020 r. do 277,4 mln w marcu 2020 r. — czyli o 197 proc. Od kwietnia 2020 r. miesięczna liczba takich ataków nigdy nie spadła poniżej 300 milionów, a w listopadzie wynosiła 409 milionów, ustanawiając nowy światowy rekord. W lutym 2021 r., niemal rok od wybuchu pandemii, odnotowano 377,5 mln ataków — nieporównywalnie więcej niż rok wcześniej.



Państwowa Agencja Atomistyki zhackowana

17.03.2021 r. - W marcu br. na łamach portalu Niebezpiecznik.pl została opisana ciekawa sytuacja. Państwowa Agencja Atomistyki poinformowała, że jej strona została zhakowana. Incydent polegał na tym, że nieznana osoba umieściła na niej komunikat ostrzegający o skażeniu radiologicznym, którego źródłem miała być Litwa. Równocześnie przejęte zostało konto Marka Budzisza, znanego publicysty zajmującego się tematyką Wschodu i bezpieczeństwa.

Litewski odpowiednik PAA szybko zdementował informację, że jest źródłem jakiegokolwiek skażenia. Okazało się, że oryginalny wpis o skażeniu, do którego nawiązywał fałszywy komunikat opublikowany w naszym kraju i który miał znajdować się na stronie litewskiego odpowiednika PAA, został umieszczony na podstawionej domenie — różniącą się ostatnią literą.

PAA nie tłumaczy w swoim oświadczeniu, jak doszło do opublikowania na jej stronach fałszywego komunikatu. W wypowiedzi dla Pulsu Biznesu PAA poinformowała, że nie stwierdziła, żeby ucierpiały jej systemy, ale trwają ustalenia w tej sprawie.

Jak zauważają redaktorzy Niebezpiecznika, wcześniejsze wpisy na Twitterze opublikowane na zhakowanym koncie Pana Budzisza prowadziły również do serwisu zdrowie.gov.pl. Na stronach organizacji Concept Intermedii, która była odpowiedzialna za te publikacje, można dowiedzieć się, że obsługuje ona Ministerstwo Zdrowia oraz kilka innych instytucji. Wygląda więc na to, że za fałszywe komunikaty w Polsce odpowiada jedna firma, która obsługuje instytucje administracji rządowej. Takie organizacje są łakomym kąskiem dla osób trudniących się dezinformacją.

Potężny atak na użytkowników OLX w Polsce

19.03.2021 r. - W drugiej połowie 2020 roku na polski rynek przestępczy weszli „nowi gracze" zza wschodniej granicy. Na celownik wzięli sprzedawców korzystających z platformy OLX. Każda z oszukanych osób traci od kilku do kilkudziesięciu tysięcy złotych. Atak polega na udawaniu kupującego i wyciągnięciu od ofiary (sprzedającego) jej numeru karty płatniczej oraz innych danych pod pretekstem otrzymania zapłaty za zakupiony produkt.

Portal Niebezpiecznik.pl opisuje schemat działania następująco:

1. Ofiara wystawia coś na OLX.
2. Odzywa się do niej osoba, która jest zainteresowana tym przedmiotem. Komunikacja może odbywać się poprzez OLX — wówczas atakujący prosi o adres e-mail, na który wysyła fałszywą wiadomość podszywającą się pod serwis OLX. Inną drogą komunikacji jest komunikator WhatsApp (atakujący ma numer telefonu ofiary z ogłoszenia na OLX) — wtedy w rozmowie wysyła link do fałszywej strony OLX.
3. Niezależnie od formy kontaktu oszust wysyła link do podrobionej strony i informuje, że należy tam przejść, aby zaakceptować odbiór pieniędzy. Najczęściej fałszywa strona udaje OLX, ale oszuści podszywają się też pod firmy kurierskie.

Na fałszywej stronie najczęściej należy podać dane karty płatniczej (co od razu umożliwi kradzież pieniędzy z powiązanego z kartą rachunku bankowego), jednak coraz częściej ofiary są proszone o podanie dodatkowych danych (np. danych dostępowych do konta bankowego lub danych osobowych, takich jak np. PESEL i nazwisko panieńskie matki, a także kod z otrzymanego SMS-a, co pozwala oszustowi podpiąć do rachunku bankowego ofiary aplikację mobilną i wyczyścić konto do zera).

Zarówno e-maile wysyłane rzekomo od OLX, jak i linki kierujące do strony „potwierdzającej odbiór pieniędzy" są fałszywe i dość łatwe do wykrycia na pierwszy rzut oka. Ponieważ jednak atak często odbywa się poprzez komunikator WhatsApp, oznacza to, że ofiara korzysta ze smartfona, więc nie widzi prawdzi-

wych adresów docelowych (na komputerze łatwiej jest je zidentyfikować). Część programów pocztowych maskuje też pole nadawcy i mało kto je klika, aby zobaczyć pełen adres:

Na etapie otrzymania łącza lub wiadomości e-mail ofiara może nie zorientować się, że coś jest nie tak. Niestety nadal wiele osób nie zastanawia kolejny etap oszustwa i bez wahania podaje numer swojej karty, aby rzekomo odebrać pieniądze za „sprzedany" produkt. Okazuje się, że wiele z nas zupełnie nie rozumie, jak działają karty płatnicze.

Jak zauważają redaktorzy portalu, w wiadomościach od oszustów często znajdują się charakterystyczne dla naszych wschodnich sąsiadów elementy, np. uśmiechanie się przez kilka nawiasów, bez użycia dwukropka. Wiele wskazuje na to, że za atakami na OLX stoją rekrutowani na potęgę Rosjanie i Ukraińcy. Potwierdza to opublikowany na stronie group-ib.com raport[23], który wskazuje, że na Telegramie znaleźć można boty ułatwiające przeprowadzenie ataku. Wystarczy, że oszust wklei botowi dane dotyczące ofiary, a w odpowiedzi otrzyma odpowiednie linki i materiały do przesłania ofierze.

Osoby zatrudnione do realizacji oszustwa nie muszą mieć żadnych umiejętności. Od prawdziwych cyberprzestępców otrzymują dostęp do narzędzi, w tym botów na Telegramie, które pozwalają im szybko generować fałszywe strony internetowe, automatycznie generowane na podstawie linku do ogłoszenia oszukiwanej osoby.

Jak można przeczytać we wspomnianym raporcie, w 2020 roku działało tak ok. 40 grup. Ofiarom pozostaje ścieżka reklamacji w banku (standardowa dla kradzieży przez przelew) i procedura Chargeback (dla operacji z użyciem danych kartach płatniczych). Niekiedy zdarza się, że na szczęście zadziałały zastosowane w banku mechanizmy chroniące przed oszustwami i pieniądze zostały zablokowane albo transakcja na karcie nie została potwierdzona kodem 3DSecure. Ale najczęściej bank odrzuca reklamację, bo wszystkie operacje, zarówno te na karcie, jak i te na koncie, zostały poprawnie autoryzowane poprzez wpisanie kodu z SMS-a na fałszywej stronie, mimo że treść SMS-a z kodem informowała, że użytkownik nie odbiera płatności z OLX, a na przykład:

– dodaje do konta nowe urządzenie/aplikację,
– autoryzuje operację kartową 3D Secure na konkretną kwotę.

Bank uznaje takie działania za rażącą niedbałość i trudno z tym polemizować. Niektórzy poszkodowani próbują walczyć w sądzie i coraz częściej wygrywają[24].

Redaktorzy Niebezpiecznika mają dla wszystkich użytkowników internetu cenną radę: nigdy nie wolno podawać numeru karty płatniczej, aby otrzymać pieniądze. Podanie numeru karty oznacza, że ktoś pobierze z niej pieniądze. Pobierze — a nie wpłaci.

Ponadto każda osoba sprzedająca w internecie powinna stosować się do następujących zasad:

– Preferuj odbiór osobisty przedmiotu, korzystaj z przesyłek OLX lub wysyłaj towary kurierem tylko po upewnieniu się, że pieniądze za przedmiot dotarły na Twój rachunek bankowy. Nie ufaj zrzutom ekranu lub plikom PDF z potwierdzeniem nadania przelewu — mogą być podrobione.
– Ograniczaj ryzyko utraty pieniędzy. Nie trzymaj wszystkich oszczędności na jednym koncie w jednym banku. Skonfiguruj też odpowiednie limity na karcie płatniczej i włącz pozostałe zabezpieczenia, jakie oferuje bank.
– Gdy otrzymasz wiadomość od osoby, która nie posługuje się poprawną polszczyzną, zachowaj wzmożoną czujność.

[23] *https://www.group-ib.com/media/classiscam-in-europe/*

[24] *https://niebezpiecznik.pl/post/sad-nabranie-sie-na-phishing-nie-jest-razacym-niedbalstwem-bank-ma-oddac-pieniadze/*

Strzeż się trojana udającego aplikację Clubhouse na systemy Android

DAGMA BEZPIECZEŃSTWO IT

23.03.2021 r. - Rosnąca popularność aplikacji społecznościowej Clubhouse została zauważona i wykorzystana przez cyberprzestępców, którzy umieścili jej spreparowaną wersję na fałszywej stronie internetowej. – Trojan o nazwie BlackRock, kryjący się w złośliwej aplikacji, wyświetla fałszywe okna logowania do Facebooka, Twittera, Netflixa oraz do 455 innych popularnych aplikacji – informują eksperci ds. cyberbezpieczeństwa ESET.

Popularność nowej aplikacji społecznościowej o nazwie Clubhouse rośnie w ogromnym tempie. Wielu użytkowników widzi w niej świetną alternatywę dla takich serwisów jak Facebook, Twitter czy Snapchat. Obecnie z aplikacji mogą korzystać jedynie właściciele iPhone'ów. W ostatnim czasie internauci mogli jednak natrafić na fałszywe informacje o jej wersji na system operacyjny Android. Czyżby Clubhouse zmienił politykę dystrybucji? Nie, to cyberprzestępcy postanowili wykorzystać zainteresowanie aplikacją do swoich celów.

Do pobrania nieistniejącej oficjalnie aplikacji Clubhouse na system Android zachęca spreparowana strona internetowa, wyglądająca i działająca niemal jak prawdziwa. Po kliknięciu fałszywa witryna instaluje groźnego trojana o nazwie „BlackRock", wykrywanego przez ESET pod nazwą Android/TrojanDropper.Agent.HLR, który jest w stanie wykraść dane logowania nieświadomych użytkowników do ponad 450 usług online, wśród których znajdziemy najpopularniejsze aplikacje finansowe, zakupowe, jak i giełdy kryptowalut. BlackRock może wykraść również dane logowania do popularnych mediów społecznościowych, platform do przesyłania wiadomości, a nawet platform streamingowych – skąd bardzo blisko do uzyskania danych bankowych.

Złośliwa strona to przykład dobrze wykonanej kopii legalnej witryny Clubhouse. Gdy jednak użytkownik kliknie „Pobierz

w Google Play", szkodliwa aplikacja zostanie automatycznie pobrana na jego urządzenie mobilne. Tymczasem legalnie działające strony internetowe zawsze przekierowują użytkownika do sklepu Google Play.

Czujni użytkownicy z pewnością dostrzegą, że coś jest nie tak – pierwsza oznaka to połączenie ze stroną, które nie jest szyfrowane (HTTP zamiast HTTPS). Drugim sygnałem jest fakt, że fałszywa witryna używa zupełnie innego rozszerzenia domeny - „.mobi" zamiast „.com", które jest używane przez legalną aplikację (patrz Rysunek 1). Najistotniejszym elementem, który powinien wzbudzić czujność, jest fakt, że autentyczna platforma jest obecnie dostępna tylko i wyłącznie dla iPhone'ów, a w oficjalnych źródłach brak informacji o tym, że Clubhouse już uruchomił wersję aplikacji na Androida (choć jest ona faktycznie w planach).

W momencie, gdy ofiara pobierze i zainstaluje złośliwe oprogramowanie BlackRock, trojan będzie próbował wykraść dane uwierzytelniające za pomocą ataku typu overlay. Co oznacza, że za każdym razem, gdy użytkownik uruchomi jedną z atakowanych aplikacji, szkodliwe oprogramowanie utworzy nakładkę żądającą logowania się. Zamiast się logować, użytkownik nieświadomie przekazuje swoje dane cyberprzestępcom. Korzystanie z uwierzytelniania dwuskładnikowego opartego na wiadomościach SMS (2FA), by zapobiec infiltracji kont, może być w tym przypadku niewystarczające, ponieważ złośliwe oprogramowanie zainstalowane na smartfonie jest w stanie przechwytywać wiadomości tekstowe. Trojan prosi także ofiarę o włączenie usług ułatwień dostępu, skutecznie umożliwiając przestępcom przejęcie kontroli nad urządzeniem.

Niemal jedna czwarta użytkowników zawsze zezwala aplikacjom i usługom na dostęp do mikrofonu i kamery

24.03.2021 r. - Z nowego badania[25] firmy Kaspersky przeprowadzonego wśród 15 000 osób na całym świecie wynika, że aż 23% użytkowników bez zastanowienia zezwala aplikacjom i usługom na dostęp do mikrofonów i kamer. Jednocześnie 59% osób niepokoi się tym, że ktoś mógłby je ukradkowo podglądać przez kamerę komputera, a 60% obawia się bycia śledzonym za pośrednictwem szkodliwego oprogramowania.

Popularność wideokonferencji w ostatnim roku spowodowała gigantyczny wzrost liczby aplikacji takich jak Microsoft Teams, która począwszy od czerwca 2020 r. zwiększyła się o 894% w stosunku do lutego 2020 r. Jednocześnie niemal na całym świecie zaczęło brakować kamer internetowych, a wielu czołowych dostawców odnotowało znacząco wyższy popyt na ten sprzęt.

Ponieważ tego typu technologie i aplikacje pomagały wykonywać obowiązki zawodowe oraz zaspokajać potrzeby społeczne w ubiegłym roku, nic dziwnego, że ludzie skłonni byli zezwalać im na dostęp do swojej kamery oraz mikrofonu. Narzędzia te wzbogacają i ułatwiają przechodzenie na system cyfrowy – dlatego, jak wynika z badania firmy Kaspersky, 27% osób w wieku 25-34 lat zawsze zezwala na taki dostęp. W znacznie mniejszym stopniu dotyczy to osób starszych, bo aż 38% respondentów w wieku co najmniej 55 lat nigdy nie udziela aplikacjom i usługom takiego dostępu.

Aby zachować ostrożność, a jednocześnie nadal korzystać z dobrodziejstw współczesnych środków komunikacji, należy dokładnie przyglądać się aplikacjom oraz usługom, z jakich korzystamy, jak również uprawnieniom, jakich od nas żądają. Na przykład, jeśli aplikacja do wideorozmów żąda dostępu do kamery, wszystko jest w porządku. Jeśli jednak aplikacja nie zawiera odpowiednich funkcji i bez uzasadnionego powodu chce mieć dostęp do mikrofonu, lepiej zbadać jej uprawnienia.

[25] *https://media.kasperskydaily.com/wp-content/uploads/sites/92/2021/03/16090300/consumer-appetite-versus-action-report.pdf*

Kaspersky z tytułem lidera w zakresie usług analizy cyberzagrożeń

25.03.2021 r. - Forrester, wpływowa organizacja badawczo-doradcza, przyznała firmie Kaspersky tytuł lidera w zakresie usług analizy zagrożeń w swoim raporcie[26] „The Forrester Wave™: External Threat Intelligence Services Q1, 2021". Raport ten stanowi istotny test porównawczy dla organizacji, zainteresowanych usługami analizy zagrożeń na całym świecie.

Coraz więcej firm postrzega analizę zagrożeń jako obszar inwestycji po doświadczeniu incydentu naruszenia bezpieczeństwa danych. Wyróżnienie przyznawane przez Forrestera pozwala wskazać czołowych dostawców organizacjom, które poszukują najbardziej kompletnej analizy w oparciu o niezależ-

ną ocenę. Raport oferuje przegląd trendów w krajobrazie analizy zagrożeń, oceniając wiedzę ekspercką dwunastu dostawców. Firma Kaspersky jako jeden z zaledwie trzech dostawców zdobyła w tym porównaniu miano lidera.

W swoim raporcie Forrester stwierdził, że firma Kaspersky stanowi lidera jakości analizy, przyznając jej jedną z dwóch najwyższych ocen w kategorii dot. oferty dostępnej na rynku. Firma otrzymała również najwyższą możliwą ocenę pod względem „hakowania" zagrożeń, oddającą jej doskonały wgląd w operacje posiadające powiązania państwowe oraz bezpośrednie obserwacje, jak również tropienie zagrożeń przestępczych i haktywistycznych.

Forester zwrócił również uwagę na możliwości firmy Kaspersky w zakresie odpowiadania na żądania od klientów: klienci referencyjni byli bardzo zadowoleni z jakości informacji przekazywanych przez firmę Kaspersky, jak również jej procesu pomagania firmom w pomiarze wydajności i wyników.

Wspierane przez globalny zespół badaczy i analityków, usługi Kaspersky Threat Intelligence zostały ocenione przez Forrestera jako odpowiednie dla firm dowolnych rozmiarów.

[26] *https://r.kaspersky.pl/evhUy*

Cyberzagrożenia przemysłowe w II połowie 2020 r. – większa aktywność atakujących

kaspersky

29.03.2021 r. - Po spadku, jaki rozpoczął się w drugiej połowie 2019 r., odsetek komputerów stosowanych w przemysłowych systemach sterowania (ICS), na których zablokowano szkodliwe obiekty, w drugiej połowie 2020 r. zaczął ponownie rosnąć. W skali globalnej odsetek zaatakowanych komputerów ICS wynosił w drugiej połowie 33,4% – co stanowi wzrost o 0,85 proc. Odsetek takich komputerów w sektorze energetycznym zwiększył się o niemal 8%, w sektorze naftowo-gazowym – o prawie 7%, natomiast w sektorze inżynieryjnym oraz integracji ICS – o 6,2%.

Ataki na organizacje przemysłowe charakteryzują się szczególnie dużym potencjałem destrukcyjności, zarówno pod względem zakłócenia produkcji, jak i strat finansowych. Ponadto organizacje przemysłowe stanowią atrakcyjny cel ataków, ponieważ posiadają wysoce poufne informacje. Jednak począwszy od drugiej połowy 2019 r. eksperci z firmy Kaspersky odnotowali spadek odsetka komputerów ICS, na których wykryto szkodliwe obiekty, ponieważ przestępcy w większym stopniu skupiali się na atakach ukierunkowanych. W drugiej połowie 2020 r. zagrożenia dla komputerów ICS zaczęły ponownie wzrastać pod każdym względem, zwiększył się bowiem zarówno globalny odsetek zaatakowanych maszyn (o 0,85%), jak i różnorodność rodzin wykorzystywanych szkodników (o 30%).

Spośród analizowanych przez badaczy z firmy Kaspersky branż największy odsetek zaatakowanych komputerów ICS odnotowano w sektorze naftowo-gazowym (46,7%, wzrost o niemal 7% w stosunku do pierwszej połowy 2020 r.), w sektorze inżynierii oraz integracji ICS (44%, wzrost o ponad 6% w stosunku do pierwszej połowy 2020 r.) oraz w sektorze energetycznym (39,3%, wzrost o niemal 8%). Zagrożenia dla branży naftowo-gazowej oraz inżynieryjnej nasilały się od pierwszej połowy 2019 r. Pozostałe dwie branże analizowane przez badaczy z firmy Kaspersky (automatyka budynków oraz przemysł motoryzacyjny) również odnotowały wzrost liczby ataków.

Na komputerach przemysłowych zablokowano zagrożenia należące do 5 365 rodzin szkodliwego oprogramowania – o 30% więcej w stosunku do pierwszej połowy 2020 r. Najczęstszymi zagrożeniami były backdoory (niebezpieczne trojany dające atakującym zdalny dostęp do zainfekowanych maszyn), oprogramowanie spyware (szkodliwe programy stworzone w celu kradzieży danych), inne rodzaje trojanów oraz szkodliwe skrypty i dokumenty.

Łącznie 62% państw analizowanych przez badaczy z firmy Kaspersky odnotowało wzrost odsetka zaatakowanych komputerów ICS. Co więcej, w 73,4% wszystkich badanych państw (w porównaniu z 23,6% w drugiej połowie 2019 r.) zwiększył się odsetek komputerów przemysłowych, na których zablokowano szkodliwe załączniki e-mail. W skali globalnej wzrost ten wynosił średnio 0,7%.

Więcej informacji na temat krajobrazu zagrożeń dla systemów przemysłowych w drugiej połowie 2020 r. znajduje się na stronie https://r.kaspersky.pl/CmLIE.

Doxing w biznesie: wzrost liczby spersonalizowanych ataków za pośrednictwem e-maili

kaspersky

30.03.2021 r. - Szkodliwi użytkownicy zrozumieli, że stosowanie niektórych sztuczek typowych dla zaawansowanych cybergangów, takich jak wykorzystywanie oprogramowania ransomware w atakach ukierunkowanych na organizacje, pozwala osiągnąć różne cele. Według badaczy z firmy Kaspersky kolejnym zagrożeniem, na które trzeba uważać, jest tzw. „corporate doxing", czyli gromadzenie poufnych informacji na temat organizacji i jej pracowników bez ich zgody w celu wyrządzenia szkody bądź osiągnięcia zysku. Szybki wzrost ilości dostępnych publicznie informacji, wycieki danych oraz postęp technologiczny sprawiają, że podstępne nakłonienie pracowników do ujawnienia poufnych informacji, a nawet przelania środków pieniężnych, staje się łatwiejsze niż kiedykolwiek wcześniej.

Jedną z metod wykorzystywanych w celu pozyskania

prywatnych informacji dotyczących firm, aby rozpowszechnić je następnie w internecie w złych intencjach, stanowią ataki Business Email Compromise (BEC). Są to ataki ukierunkowane polegające na inicjowaniu wymiany e-maili z pracownikami poprzez podszycie się pod kogoś z firmy. W lutym 2021 r. eksperci z firmy Kaspersky wykryli 1 646 takich ataków, co pokazuje, jak bardzo organizacje są podatne na wykorzystywanie publicznie dostępnych informacji. Ogólnie celem takich ataków jest uzyskanie poufnych informacji, takich jak bazy danych klientów, lub kradzież środków. Badacze z firmy Kaspersky regularnie analizują przypadki, w których przestępcy podszywają się pod jednego z pracowników organizacji, wykorzystując wiadomości e-mail do złudzenia przypominające te autentyczne w celu wyłudzenia środków pieniężnych.

Takie ataki nie byłyby możliwe na skalę masową, gdyby przestępcy nie mogli gromadzić i analizować publicznych informacji dostępnych m.in. w mediach społecznościowych, takich jak nazwiska i stanowiska pracowników, ich adresy zamieszkania, kontakty itd.

Jednak ataki BEC to tylko jeden z wielu rodzajów działań wykorzystujących publicznie dostępne informacje w celu zaszkodzenia organizacji. Paleta sposobów pozwalających na oszukanie firm jest szokująca i oprócz bardziej oczywistych metod, takich jak phishing czy tworzenie profili organizacji przy użyciu danych, które wyciekły, obejmuje również te bardziej kreatywne i oparte na technologii.

Prawdopodobnie najpopularniejszą strategią corporate doxingu jest kradzież tożsamości. Doxerzy wykorzystują zwykle informacje do profilowania określonych pracowników, a następnie posłużenia się ich tożsamością. Zadanie to staje się łatwiejsze za sprawą nowych technologii, takich jak deepfake. Na przykład film wykorzystujący technologię deepfake, w którym rzekomo występuje pracownik jakiejś organizacji, mogłoby zaszkodzić reputacji owej firmy, a do jego stworzenia doxerzy potrzebowaliby wizualnej reprezentacji danego pracownika oraz jego podstawowych informacji osobowych. Do swoich celów mogliby wykorzystać również głos – np. nagrywając, a następnie imitując popularnego prezentera, dzwoniąc do jego księgowego z poleceniem wykonania pilnego przelewu bankowego lub przesłania bazy danych klientów.

Więcej informacji na temat metod wykorzystywanych przez doxerów w celu atakowania organizacji znajduje się na stronie https://r.kaspersky.pl/ld1vF.

Ponad połowa ofiar oprogramowania ransomware płaci okup, ale tylko jedna czwarta w pełni odzyskuje swoje dane

31.03.2021 r. - Z badania[27] firmy Kaspersky przeprowadzonego wśród 15 000 klientów wynika, że w ubiegłym roku ponad połowa (56%) ofiar oprogramowania ransomware zapłaciła okup w celu odzyskania dostępu do swoich danych. W przypadku 17% z nich zapłata okupu nie zagwarantowała odzyskania skradzionych danych.

Ransomware to rodzaj szkodliwego oprogramowania wykorzystywanego przez przestępców do wyłudzania pieniędzy. Przetrzymuje ono dane dla okupu poprzez zaszyfrowanie ich lub zablokowanie użytkownikom dostępu do urządzeń. Z raportu firmy Kaspersky wynika, że odsetek ofiar, które zapłaciły okup w celu odzyskania dostępu do swoich danych w 2020 r., był najwyższy wśród osób w wieku 35-44 lat, z których dwie trzecie (65%) przyznało się do spełnienia żądania okupu. Dla porównania, w grupie osób w wieku 16-24 lat odsetek ten stanowił 52% i jedynie 11% wśród osób w wieku powyżej 55 lat, co pokazuje, że młodsi użytkownicy są bardziej skłonni zapłacić okup niż ci w wieku powyżej 55 lat.

Niezależnie od tego, czy zapłacono okup, jedynie 29% ofiar zdołało odzyskać wszystkie pliki, które zostały zaszyfrowane lub zablokowane w wyniku ataku. Połowa (50%) utraciła przynajmniej kilka plików, 32% – znaczną część, a 18% – niewielką. Z kolei 13% osób, które doświadczyły takiego incydentu, straciło niemal wszystkie swoje dane.

Około czterech na 10 badanych (39%) twierdziło, że miało świadomość zagrożenia ransomware na przestrzeni minionych 12 miesięcy. Ważne jest, aby wraz ze wzrostem popularności pracy zdalnej liczba takich osób była coraz większa. Aby klienci mogli lepiej ochronić się przed tego rodzaju cyberatakiem, muszą wiedzieć, na co powinni uważać i co robić, jeśli zetkną się z oprogramowaniem ransomware.

[27] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3381/niemal-jedna-czwarta-uzytkownikow-zawsze-zezwala-aplikacjom-i-uslugom-na-dostep-do-mikrofonu-i-kamery*

Nauka poprzez grywalizację

– w jaki sposób firmy mogą ją wykorzystać w szkoleniach zwiększających świadomość w zakresie bezpieczeństwa?

Piotr Kupczyk,
Dyrektor biura
komunikacji
z mediami
Kaspersky Lab Polska

Na ogół mało kto przepada za szkoleniami firmowymi. Na przykład, 42% respondentów[1] pracujących w firmach zatrudniających ponad 1 000 pracowników przyznało, że większość programów szkoleniowych, w których uczestniczyli, była bezużyteczna i nieciekawa. W podobny sposób postrzegana jest często edukacja mająca rozwijać świadomość w zakresie cyberbezpieczeństwa.

Często słyszymy od naszych klientów, że mają już dość tradycyjnych, nudnych szkoleń z podstaw bezpieczeństwa. Wypróbowują więc szkolenia całkowicie oparte na grze, które zapewniają zabawę i rozrywkę. Z drugiej strony obserwujemy również przeciwny kierunek myślenia: niektórzy klienci mają opory przed wprowadzeniem do szkoleń firmowych jakichkolwiek technik związanych z grami. Uważają, że gry zarezerwowane są wyłącznie dla dzieci i nastolatków i bzdurą jest sugerowanie, że dorośli – zwłaszcza ci zajmujący kierownicze stanowiska w firmach – powinni uczyć się poprzez gry.

Jednak w rzeczywistości zarówno gry (format, w którym osoba działa w wymyślonym świecie lub wciela się w inną postać), jak i proces grywalizacji (gdy wykorzystuje się tylko niektóre elementy gier) to doskonałe techniki nauki. I jak wszystkie inne metody, dają najlepsze efekty, gdy uwzględni się szczegółowe cele i ograniczenia.

Dlaczego nie można po prostu zagrać w grę rozwijającą świadomość bezpieczeństwa?

Przede wszystkim zakres nawet podstawowych zasad cyberbezpieczeństwa jest dość spory. Zawartość naszej platformy szkoleniowej Kaspersky Security Awareness Platform[2] jest niemal trzykrotnie większa niż wszystkie tomy „Sagi rodu Forsyte'ów" Johna Galsworthy'ego. Gdyby przerobić te treści na szkolenie oparte na symulacji, musiałoby ono zawierać wszelkie możliwe sytuacje pozwalające „sprawdzić" każdą opcję. A zatem ukończenie takiego modułu edukacyjnego zajęłoby mnóstwo czasu.

Czas nie jest tu jednak jedynym czynnikiem, jaki należy wziąć pod uwagę. Format gry wymaga od osoby zanurzonej w wirtualne środowisko koncentracji i zaangażowania. Badania pokazują, że ciało ludzkie reaguje na stres podczas gry tak samo jak podczas problematycznych sytuacji w prawdziwym życiu[3]. To dlatego gry wideo mogą prowadzić nawet do uczucia zmęczenia[4]. W grze opartej na podstawach cyberbezpieczeństwa gracz będzie nieustannie mierzył się z dylematami – w końcu od jego decyzji będą zależały jego wirtualne pieniądze czy też kariera. Dlatego po kilku godzinach takiego szkolenia pracownicy nie będą w stanie od razu wrócić do swoich obowiązków – będą potrzebowali czasu na odpoczynek.

Najważniejsza jest inspiracja…

Czy to oznacza, że wdrożenie takiego szkolenia i uczenie się z wykorzystaniem technik gier jest zbyt trudne? Aby odpowiedzieć na to pytanie, należy uświadomić sobie, jaki jest ostateczny cel szkolenia rozwijającego świadomość bezpieczeństwa.

Firmy wprowadzają tego rodzaju szkolenia nie tylko w celu zachęcenia personelu do zapoznania się z zasadami cyberbezpieczeństwa, ale również po to, by pracownicy zdobyli i stosowali w praktyce określone umiejętności. Przykładem może być udostępnianie firmowych dokumentów – znacznie łatwiej jest udostępnić taki plik za pośrednictwem tego samego magazynu w chmurze, który wykorzystuje się do przechowywania zdjęć swojego kota, niż skorzystać z bezpiecznej, wyznaczonej w tym celu usługi firmowej. Dlatego, aby zmienić takie nawyki, konieczne jest nie tylko przekazanie instrukcji i rozwijanie praktycznych umiejętności, ale również praca nad motywacją i skłonnościami.

Pod tym względem gra okazuje się najskuteczniejszym narzędziem motywującym pracowników. Ucząc się na własnych błędach, najłatwiej zrozumieć, dlaczego należy postępować w określony sposób. W przypadku cyberbezpieczeństwa firma nie może pozwolić pracownikom, aby coś „zawalili" – nie może czekać, aż np. dojdzie do wycieku poufnego dokumen-

tu – po to, by przekonali się, jak poważne mogą być konsekwencje cyberataku. Ale może dać im grę, w której „przeżyją" określoną sytuację i doświadczą jej skutków, tak jakby zdarzyły się w rzeczywistości, jednak bez szkody dla firmy.

…i wyzbycie się uprzedzeń

Techniki wywodzące się z gier pomagają również w przezwyciężeniu początkowego oporu wobec nauki. Szkolenie w zakresie cyberbezpieczeństwa zwykle postrzegane jest jako coś nudnego, trudnego i skomplikowanego. Gdy jednak pracownicy widzą zabawne obrazki ukazujące znajome sytuacje w kontekście symulacji w formie gry, okazuje się, że szkolenie wcale nie jest takie straszne.

Ponadto zawsze znajdą się pracownicy przekonani o tym, że opanowali już umiejętności z danego zakresu i szkolenie będzie dla nich stratą czasu. O wiele łatwiej dadzą się przekonać, jeśli dostaną krótki test w stylu komiksowym, w którym trzeba obstawić jakąś odpowiedź. Zwykle pracownicy podchodzą z większym entuzjazmem do udziału w takich krótkich sprawdzianach, a grywalizacja sprawia, że są bardziej zaciekawieni tym, jak wypadną w teście. Gdy zauważają u siebie luki w wiedzy, z większą chęcią biorą udział w szkoleniu rozwijającym świadomość w zakresie bezpieczeństwa.

Co więcej, z naszego doświadczenia wynika, że — mimo wątpliwości menedżerów ds. szkoleń — osoby zajmujące kierownicze stanowiska również angażują się w formaty oparte na grach. Oferujemy np. specjalną grę Kaspersky Interactive Protection Simulation, w której dyrektorzy najwyższego szczebla próbują wcielić się w specjalistów ds. bezpieczeństwa IT. Dzięki temu przekonują się, w jaki sposób cyberbezpieczeństwo może wpłynąć na firmę, w tym na krytyczne kwestie, takie jak utrata zysków.

Jeśli pracownicy przezwyciężą uprzedzenia, przygotuje to grunt pod kurs teoretyczny i nauka da lepsze rezultaty. Naturalnie, początkowa motywacja z czasem słabnie, dlatego nie wystarczy jednie zacząć od gry. Zalecamy włączanie elementów gry lub symulacji jako wzmocnienie programu szkolenia.

Skuteczne szkolenie z podstaw cyberbezpieczeństwa powinno uwzględniać różne formaty. Techniki wywodzące się z gier nie są cudownym środkiem i nie rozwiążą wszystkich problemów związanych z edukacją w firmie. Aby dać pożądane rezultaty, muszą być odpowiednio włączone do całego cyklu nauki i skutecznie połączone ze szkoleniem merytorycznym. Gra powinna być swego rodzaju deserem w menu edukacji, który sprawia, że wszystko staje się odrobinę lepsze. Nie może jednak stanowić jedynego dania.

[1] *https://www.capgemini.com/wp-content/uploads/2017/10/report_the-digital-talent-gap_final.pdf*

[2] *https://asap.kaspersky.pl*

[3] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6037427*

[4] *https://www.reddit.com/r/truegaming/comments/7i24hq/does_anyone_get_really_tired_while_playing_video*

Shadow IT – jak zarządzać niezatwierdzonymi zasobami IT z korzyścią dla firmy i jej pracowników

Aleksander Mojsjejew
Dyrektor biznesowy
Kaspersky

Mieszanka firmowych i niezatwierdzonych usług online w pracy to niestety rzeczywistość. Poszczególne działy mają dostęp do określonych usług w chmurze, w praktyce jednak personel często korzysta z mediów społecznościowych, współdzielenia plików, komunikatorów oraz różnych narzędzi bezpieczeństwa dostępnych w modelu usługowym, bo tak jest wygodniej. A dokładnie, dzieje się tak w przypadku 92% małych i średnich firm oraz w 89% dużych korporacji – wynika z niedawnego globalnego badania firmy Kaspersky[1].

Praktyka ta stała się jeszcze bardziej powszechna w dobie wymuszonej pandemią pracy zdalnej. Po przestawieniu się na „biuro domowe" pracownicy wciąż musieli wykonać swoje zadania, nawet jeśli dział IT nie zapewnił im dostępu do wszystkich usług korporacyjnych. Doszło do zatarcia granic między życiem firmowym a prywatnym, więc ludzie zaczęli wykorzystywać firmowe laptopy do celów niezwiązanych z pracą, takich jak granie, serwisy streamingowe, a nawet oglądanie pornografii[2].

Wygląda na to, że takie zachowanie tworzy nową normę, wciąż jednak pozostaje pytanie, jak do problemu niezatwierdzonych zasobów IT (tzw. shadow IT) powinny podchodzić same firmy. Zastanówmy się więc nad zagrożeniami, gratyfikacjami i potencjalnymi rozwiązaniami.

Dlaczego zjawisko shadow IT może być groźne: bezpieczeństwo danych

Zatwierdzone usługi korporacyjne przeznaczone do komunikacji, współpracy, przechowywania oraz współdzielenia plików powinny być odpowiednio skonfigurowane przez zespoły IT firmy oraz posiadać wymagany poziom kontroli dostępu, ochrony danych oraz zarządzania incydentami. Gdy te warunki są spełnione, firma posiada dobry poziom transparentności i może dopilnować, aby nikt spoza niej nie uzyskał dostępu do przestrzeni i zawartości korporacyjnej (przynajmniej nie bez użycia zaawansowanych szkodliwych narzędzi).

Jeśli chodzi o usługi, które nie mają ściśle firmowego przeznaczenia — takie jak komunikatory, współdzielenie plików, poczta e-mail czy narzędzia CRM — nie ma pewności, czy dane, jakie pracownicy udostępniają za ich pośrednictwem, są chronione. Pojawiają się zatem pytania: Czy pracownicy stosują mocne hasła? W jaki sposób uzyskują dostęp do danej usługi i z jakich urządzeń? Kto zarządza dostępem, gdy ludzie przestają pracować w firmie?

Ludzką rzeczą, która może przydarzyć się każdemu pracownikowi, jest zapomnieć o ustawieniu hasła lub o ograniczeniu grona, które mogą przeglądać bądź edytować współdzielony dokument. Poza tym aplikacje mogą stać się celem szkodliwych działań. Oszuści mogą wykorzystać do własnych celów, a nawet przejąć konta użytkowników, stosując phishing lub socjotechnikę. Taka sytuacja miała miejsce w 2019 r., gdy cyberprzestępcy wykorzystali[3] popularną platformę współdzielenia plików WeTransfer i przesłali za jej pomocą szkodliwe pliki, które po pobraniu przekierowywały ofiary na fałszywą stronę logowania Microsoft Office 365 zaprojektowaną w celu przechwytywania wprowadzonych danych logowania.

Jeśli istnienie zjawiska shadow IT jest nieuniknione, pokaż pracownikom, czego należy unikać

Radykalne podejście do niezatwierdzonych zasobów IT polega na zablokowaniu dostępu do wszystkich niefirmowych usług. Jednak rozwiązanie to nie zawsze jest wykonalne, zwłaszcza w nowych realiach pracy. Niekiedy takie niezatwierdzone zasoby IT mogą pomóc pracownikom lepiej wykonać swoją pracę, dlatego całkowity zakaz może zaszkodzić efektywności firmy. Przykładem jest historia[4] pewnej wiceprezes, która zapłaciła za narzędzie CRM z własnej kieszeni, obchodząc autoryzowany system zalecony przez jej zespół IT. Gdy firma dowiedziała się o tym, kobieta została poddana postępowaniu dyscyplinarnemu, mimo że z pomocą tego narzędzia zdołała zwiększyć przychody firmy o milion dolarów miesięcznie.

Konieczny jest zatem kompromis: by z jednej strony nie wprowadzać tyranii IT, a z drugiej nie narażać firmy na zagrożenia. Firmy powinny zatem odkrywać skalę zjawiska shadow IT — ale jak to zrobić?

Po pierwsze, kluczem do zwiększenia cyberbezpieczeństwa w firmie jest świadomość personelu w zakresie bezpiecznego wykorzystywania usług cyfrowych – od poczty firmowej po wyspecjalizowane oprogramowanie inżynieryjne, a nawet komunikator internetowy. Jeśli istnieje polityka firmowa zabraniająca udostępniania dokumentów biznesowych za pośrednictwem niezatwierdzonych aplikacji, pracownicy powinni o tym wiedzieć. Zarządzając dowolnymi narzędziami, pracownicy powinni mieć świadomość podstawowych kwestii, takich jak udzielanie dostępu i zarządzanie hasłami. Powinni również poznać podstawowe zasady bezpieczeństwa, np. że nie należy otwierać załączników czy klikać odsyłaczy w wiadomościach e-mail od nieznanych nadawców ani pobierać oprogramowania z nieoficjalnych źródeł, a także koniecznie sprawdzać adresy stron internetowych żądających podania danych logowania.

Komunikację dotyczącą cyberbezpieczeństwa należy prowadzić w odpowiednim tonie: zamiast karać, lepiej jest edukować, przypominać, testować i jeszcze raz przypominać. Należy wyjaśnić pracownikom, dlaczego to takie istotne i w jaki sposób wpływa na firmę oraz ich własne bezpieczeństwo. Zespół może nadal korzystać z określonych usług do celów związanych z pracą, powinien jednak przestrzegać zasad i nie naruszać zasad ochrony danych.

Po drugie, ważne jest uzyskanie widoczności niezatwierdzonych zasobów IT oraz zintegrowanie ich z zasobami firmowymi. Istnieją specjalistyczne narzędzia pozwalające zarządzać dostępem do chmur publicznych. Wskazują one, jakie usługi są używane najczęściej, które z nich mogą być wykorzystane do przenoszenia i przechowywania danych i jak wysokie jest ryzyko. Narzędzia te pozwalają także na podejmowanie niezbędnych działań. Mogą stanowić oddzielne rozwiązania lub być zintegrowane z ochroną punktów końcowych. Na przykład, z pomocą naszych technologii ustaliliśmy[5], że YouTube to usługa, do której pracownicy najczęściej uzyskują dostęp na urządzeniach firmowych. Nie daje ona jednak możliwości współdzielenia plików czy jakiegokolwiek przetwarzania danych biznesowych, dlatego ryzyko jest minimalne. Można argumentować, że oglądanie filmów na platformie YouTube wpływa na wydajność pracowników, ale to już inna historia.

Na koniec warto zaznaczyć, jak ważne jest posiadanie jasnych procesów oraz kultury korporacyjnej zachęcającej pracowników, by domagali się usprawnień. Historia podobna do tej, która przytrafiła się pani wiceprezes z jej niezatwierdzonym oprogramowaniem CRM, może zdarzyć się w każdej firmie. Na przykład, zespół IT może niechętnie rozpatrywać kierowane do niego prośby. Może to wynikać z braku czasu lub zasobów, lub też braku kultury organizacyjnej sprzyjającej zmianom. Rozwiązaniem będzie tu wprowadzenie określonych praktyk, które pomogą pracownikom kontaktować się z zespołem wsparcia i uzyskać pomoc.

Korzystanie z niezatwierdzonych zasobów IT jest tak powszechne, ponieważ w ludzkiej naturze leży szukanie najłatwiejszego i najwygodniejszego sposobu, by coś zrobić. Dotyczy to również pracy. Niemniej jednak shadow IT to kwestia, do której należy podchodzić ostrożnie, a przedstawione tu proste zalecenia pokazują, że organizacje mogą sobie z nią poradzić. W ten sposób nie tylko zmniejszą ryzyko związane z ochroną danych, ale również zachęcą do lepszej komunikacji między działem IT a innymi pracownikami. Dodatkowym pozytywnym efektem będzie zaufanie pomiędzy firmą a jej pracownikami i odwrotnie.

[1] *Badanie „IT Security Risks Survey 2020" przeprowadzone przez firmę Kaspersky w czerwcu 2020 r. Przeankietowano 5 226 respondentów z 31 krajów.*

[2] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3261*

[3] *https://threatpost.com/popular-file-sharing-service-wetransfer-used-in-malicious-spam-campaigns/146671*

[4] *https://hbr.org/2019/06/when-employees-are-using-software-that-it-hasnt-approved*

[5] *https://r.kaspersky.pl/Ntulq*

Informacje o zagrożeniach: phishing związany ze szczepionkami

W analizie przeprowadzonej od października 2020 r. do stycznia 2021 r. analitycy z firmy Barracuda odkryli, że w ukierunkowanych atakach phishingowych hakerzy coraz częściej wykorzystują wiadomości e-mail związane ze szczepionkami.

Gdy w listopadzie 2020 r. firmy farmaceutyczne ogłosiły dostępność szczepionek, liczba tego typu ataków zwiększyła się o 12%, a pod koniec stycznia br. wzrost w stosunku do października wyniósł 26%.

Najważniejsze zagrożenia

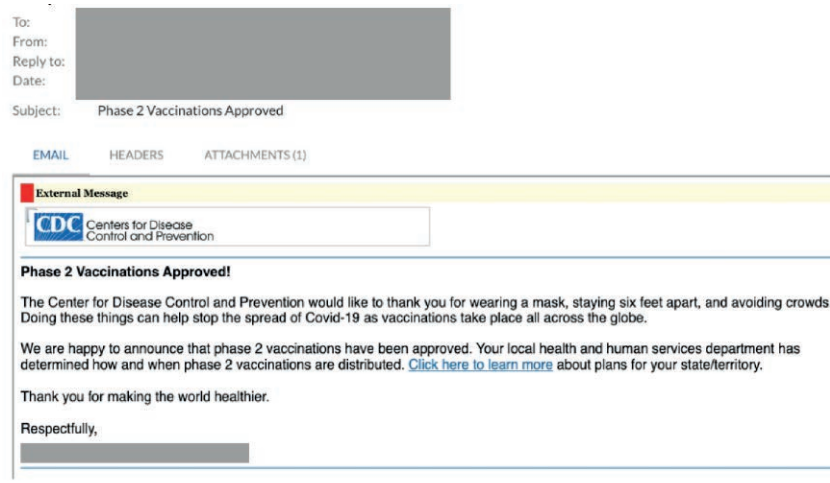
1. Phishing związany ze szczepionkami

Cyberprzestępcy wykorzystują wzmożone zainteresowanie szczepionkami na COVID-19 i przeprowadzają ataki z użyciem phishingu ukierunkowanego. Najczęściej wywołują oni uczucie strachu, niepewności, pilności oraz wykorzystują inżynierię społeczną[1].

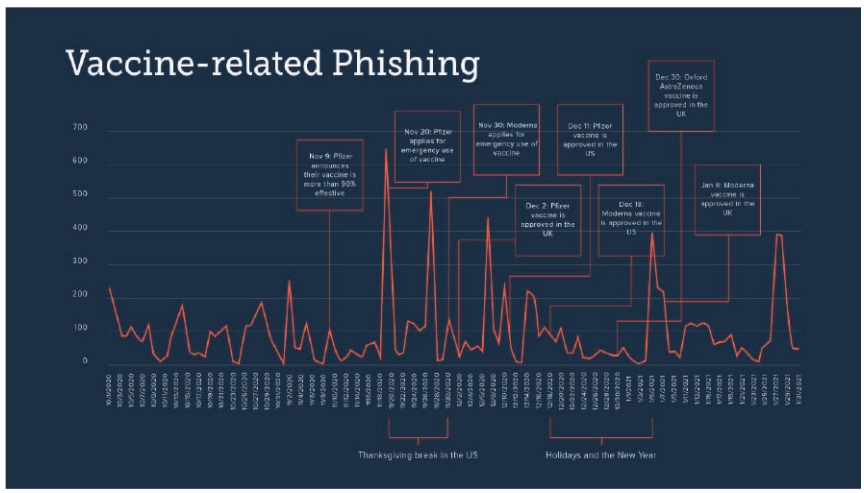
Większość przeanalizowanych przez analityków z firmy Barracuda ataków phishingowych związanych ze szczepionkami to tradycyjne oszustwa, jednak w wielu przypadkach wykorzystano bardziej ukierunkowane techniki, takie jak podszywanie się pod markę i włamania do biznesowej poczty e-mail.

a) Podszywanie się pod markę

Związane ze szczepionkami e-maile phishingowe były przygotowane tak, jakby zostały wysłane przez znaną markę lub organizację. Zawierały odsyłacz do witryny phishingowej, na której reklamowany był wczesny dostęp do szczepionek, oferowane były szczepienia za opłatą, a nawet widniała prośba od rzekomych pracowników służby zdrowia o podanie danych osobowych w celu sprawdzenia uprawnień do szczepienia.



Rys. Przykład treści maila zawierającego phising związany z Covid-19



Rys. Wyłudzanie informacji związane ze szczepionkami

b) Włamania do biznesowej poczty e-mail

W tego typu atakach napastnicy przechwytują dostęp do biznesowej poczty e-mail[2] (ang. Business Email Compromise, BEC), aby móc podszywać się pod pracowników organizacji lub jej partnerów biznesowych. W ostatnich latach było to jedno z najbardziej szkodliwych zagrożeń e-mailowych, które kosztowało biznes ponad 26 miliardów dolarów[3]. Niedawno w tych precyzyjnie celowanych atakach zaczęto wykorzystywać temat szczepionek. Czasami atakujący podszywali się pod pracowników i zwracali się do odbiorcy wiadomości z prośbą o pomoc w dokończeniu spraw firmowych, bo sami muszą stawić się na szczepieniu, a czasami udawali specjalistę działu zasobów ludzkich informującego, że organizacja zdobyła szczepionki dla swoich pracowników.

To:
From:
Reply-to:
Date: Jan 8, 2021

Subject:

Happy New Year would it be possible for you to complete a task for me, before I leave for a covid-19 vaccine meeting. Please give me your personal number? Thanks

Sent from my iPhone

Rys. Przykład treści maila zawierającego phising związany z Covid-19

2. Wykorzystywanie przejętych kont do oszustw związanych ze szczepionkami

Badacze z firmy Barracuda mają wgląd nie tylko w wiadomości e-mail przychodzące spoza organizacji, ale także w komunikację wewnętrzną. Dzięki temu widzą wiele fałszywych wiadomości wysyłanych wewnętrznie – zwykle z konta przejętego przez hakerów.

Cyberprzestępcy wykorzystują ataki phishingowe do włamywania się i przejmowania kont firmowych. Następnie bardziej wyrafinowani hakerzy przed rozpoczęciem ataków ukierunkowanych przeprowadzają rozpoznanie. Najczęściej używają oni takich legalnych kont do wysyłania masowych kampanii phishingowych i spamowych do jak największej liczby osób, zanim ich aktywność zostanie wykryta i utracą dostęp do konta.

Dlatego gdy obserwuje się lateralne ataki phishingowe[4] poza normalnymi godzinami pracy, widać ogromne skoki aktywności. Co ciekawe, wzrost ataków phishingowych tego typu pokrywa się z zatwierdzaniem na całym świecie głównych szczepionek przeciwko COVID-19.

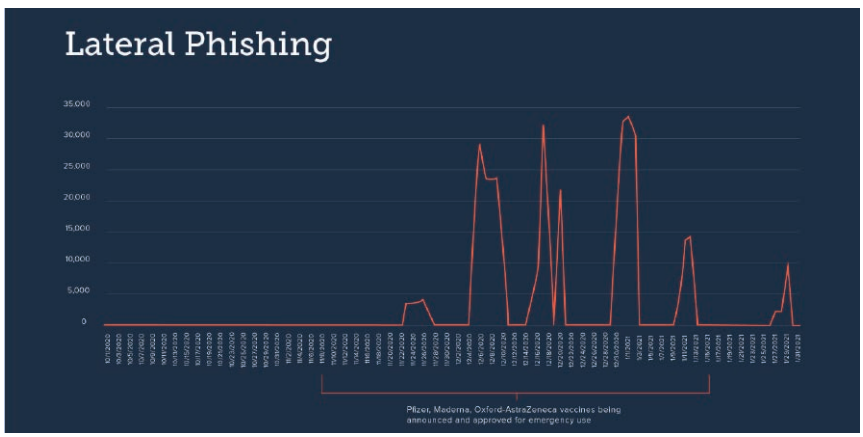
Jak chronić się przed phishingiem związanym ze szczepionkami

1. Podchodź sceptycznie do wszelkich wiadomości dotyczących szczepionek

Niektóre oszustwa e-mailowe zawierają ofertę wcześniejszego otrzymania szczepionki przeciwko COVID-19, dołączenia do listy oczekujących na szczepionkę lub wysłania szczepionki bezpośrednio do adresata. W takich wiadomościach nie należy klikać linków ani otwierać załączników, które zazwyczaj są złośliwe.

2. Wspomagaj się sztuczną inteligencją

W celu ominięcia bram i filtrów spamu oszuści zmieniają sposób działania. Dlatego kluczowe znaczenie ma rozwiązanie, które wykrywa i chroni przed atakami stosującymi phishing ukierunkowany, w tym przed podszywaniem się pod markę czy przejęciem firmowego konta poczty e-mail. Używaj technologii, która wyszukuje złośliwe łącza czy załączniki. Ponadto podczas analizy wzorców komunikacji w organizacji zastosuj uczenie maszynowe, które pozwala wykrywać wskazujące na atak anomalie.



Rys. Lateralne ataki phisingowe

3. Zastosuj ochronę przed przejęciem konta

Nie koncentruj się tylko na zewnętrznych wiadomościach e-mail. Część najbardziej niszczycielskich i skutecznych ataków pochodzi z przejętych kont wewnętrznych. Upewnij się, że oszuści nie używają danej organizacji jako bazy do prowadzenia takich ataków, a także stosuj technologię, która wykorzystuje sztuczną inteligencję do rozpoznawania włamań na konta i działa w czasie rzeczywistym, ostrzegając użytkowników i usuwając złośliwe wiadomości e-mail wysyłane z zainfekowanych kont.

4. Edukuj pracowników poprzez szkolenia, jak rozpoznawać i zgłaszać ataki

Poinformuj pracowników, czym są ukierunkowane ataki phishingowe — w tym wykorzystujące temat szczepień, na czym polegają oszustwa sezonowe oraz jakie są inne potencjalne zagrożenia. Pracownicy muszą potrafić rozpoznawać najnowsze ataki i wiedzieć, jak je zgłaszać do działu IT. W trakcie szkolenia użytkowników w zakresie identyfikowania cyberataków, testowania skuteczności szkolenia i oceny pracowników najbardziej narażonych na ataki możesz wykorzystywać symulacje phishingu wysyłanego pocztą e-mail, pocztą głosową i w SMS-ach.

5. Ustal skuteczne procedury wewnętrzne w celu zapobiegania oszustwom

W celu ograniczenia ryzyka ataku na informacje prywatne i finansowe stwórz odpowiednie procedury wewnętrzne i regularnie je weryfikuj. Procedury potwierdzania wszystkich wniosków e-mail o przelewy i zmiany formy płatności, a także konieczność osobistego lub telefonicznego potwierdzenia i/lub akceptacji transakcji finansowych pomogą uniknąć kosztownych błędów pracowników.

[1] *https://www.barracuda.com/glossary/social-engineering*
[2] *https://www.barracuda.com/glossary/business-email-compromise*
[3] *https://www.securityweek.com/loss-bec-fraud-now-claimed-be-26-billion*
[4] *https://www.barracuda.com/glossary/lateral-phishing*

Jak bronić się przed kradzieżą tożsamości

Ireneusz Wiśniewski,
dyrektor zarządzający
F5 Poland

„Dlaczego cyberprzestępcy mieliby być zainteresowani kradzieżą mojej tożsamości? Przecież nie jestem nikim ważnym". To nieprawda. W tej grze każdy jest istotny.

Statystycznie większość hakerów stara się wręcz unikać bardzo „ważnych" i wartościowych celów. Do wyboru mają niezliczoną liczbę łatwiejszych zdobyczy — ludzi, których uwagę można odwrócić znacznie prostszymi sposobami. Pandemia mocno zwiększyła zasięg i liczbę ataków na niczego niepodejrzewających i bezbronnych użytkowników internetu.

Kradzież tożsamości może nagle wywrócić życie do góry nogami. W niektórych przypadkach może nawet zmniejszyć czyjąś ocenę kredytową, a wyjaśnienie tej sytuacji często zajmuje miesiące i wiąże się z wysokimi kosztami. Poniższe sugestie najlepszych praktyk pomogą każdemu, kto chce aktywnie chronić się przed kradzieżą tożsamości:

- **Wykorzystuj programy do zarządzania hasłami (menedżery haseł).** Przeciętny użytkownik musi pamiętać około 70-80 haseł, co zazwyczaj kończy się na ich ręcznym notowaniu. Ponadto według jednej z ankiet przeprowadzonej przez firmę badawczą Harris Poll jednym z największych błędów jest wykorzystywanie tych samych haseł do różnych kont (przyznaje się do tego dwie trzecie użytkowników). Tymczasem menedżer haseł umożliwia utworzenie silnego, unikalnego hasła dla każdego z kont indywidualnie. Ponadto szyfruje i przechowuje hasła w bezpiecznym schowku, a użytkownik musi pamiętać tylko jedno hasło główne. Jeśli więc hasło główne będzie bezpieczne – bezpieczny będzie także użytkownik.

Jeśli jednak użytkownicy nie są przekonani do menedżera haseł, powinni przynamniej zacząć tworzyć unikalne hasła, które będą zawierały maksymalną dopuszczalną liczbę znaków. Powinni także pamiętać o niezwłocznej zmianie hasła, gdy konto zostało przejęte

przez cyberprzestępców.

Generalna zasada: unikaj zapamiętywania haseł przez przeglądarki i nie używaj tych samych danych logowania do różnych kont (także w mediach społecznościowych). W nazwie użytkownika nie zawieraj imienia, elementów adresu e-mail ani wskazówek odnoszących się do daty urodzenia. Powyższe dane dają cyberprzestępcom połowę informacji wymaganych do złamania dostępu do konta.

- **Używaj identyfikacji wieloskładnikowej.** Uwierzytelnianie wieloskładnikowe wymaga od nas podania nie tylko standardowego loginu i hasła, ale również np.: kodu otrzymanego poprzez SMS. To skuteczna, dodatkowa warstwa ochrony, która powinna być używana dla każdego konta tam, gdzie tylko jest to możliwe.
- **Nie publikuj w Sieci zbyt wielu informacji o sobie.** Przemyśl, jak i co udostępniasz w Sieci. Gdy chętnie udostępniamy prywatne informacje, stajemy się łatwiejszym celem dla złodziejów tożsamości. Cyberprzestępcy w kilka minut połączą udostępnione dane z tymi „w tle", które mogą pozyskać.

Dobrym pomysłem dla zachowania bezpieczeństwa może być usunięcie danych osobistych z kont w mediach społecznościowych i networkingowych (data i miejsce urodzenia, nazwisko panieńskie, nazwisko panieńskie matki, numer telefonu, imię zwierzęcia domowego, hobby itp.).

Warto też używać wyłącznie najsilniejszych ustawień prywatności, ostrożnie wybierać „znajomych" (włącznie z raportowaniem dublujących się próśb o dodanie do znajomych).

Dobrym krokiem jest także rezygnacja z quizów i gier w mediach społecznościowych, ponieważ większość z nich jest zaprojektowana tak, aby zbierać dane osobiste użytkowników.

Nie należy pobierać aplikacji z nieznanych źródeł, a podczas otwierania linków, reklam i wiadomości z podejrzanymi informacjami (również pochodzących od osób, które znamy — ich konta mogą być zhakowane) warto zachować ostrożność. Rozsądne jest również zablokowanie oznaczania lokalizacji i unikanie dzielenia się zdjęciami, jeśli przebywa się poza domem. Oczywiście nie sposób wymienić wszystkich kroków zapobiegawczych, więc za każdym razem należy zadać sobie pytanie do czego jest ta informacja potrzebna, kto z niej skorzysta oraz czy może ona naruszyć moją prywatność albo narazić mnie na kradzież tożsamości.

- **Chroń swoją prywatność we własnym domu.** Chroń swoją domową sieć bezprzewodową, korzystaj tylko z tych urządzeń internetu rzeczy, które pozwalają na zmianę hasła i zarządzanie ustawieniami ochrony, a stare telefony, laptopy i inne urządzenia zawierające dane przechowuj w bezpiecznym miejscu. Nie zapominaj też o zabezpieczeniu tradycyjnej skrzynki pocztowej regularnym odbieraniem listów i rezygnacji z przesyłek reklamowych oraz używaj niszczarki do dokumentów, które mogą zawierać prywatne informacje (włącznie z niechcianą korespondencją). Warto też upewnić się, że nie zostawiamy dokumentów czy innych przedmiotów pozwalających na naszą identyfikację (np.: paszporty, karty ID, portfele) w samochodach czy miejscach publicznie dostępnych.
- **Chroń swoją prywatność w miejscach publicznych.** Trudno uwierzyć, że ktokolwiek potrzebuje przypomnienia, ale jednak — publicznie dostępne sieci Wi-Fi są niezwykle podatne na „podsłuchiwanie". Nigdy nie wykorzystuj takich połączeń do kontaktów z bankiem, zakupów online, żadnych aktywności wymagających używania karty kredytowej czy w kontaktach z usługami sektora zdrowia. Nie dziel się prywatnymi informacjami takimi jak numer karty kredytowej, data urodzenia, PESEL czy jakimikolwiek innymi danymi podczas rozmów telefonicznych i osobistych, gdy jesteś w miejscach publicznych. Podczas korzystania z systemów przyznających punkty za sprzedaż chroń PIN-y i inne dane identyfikacyjne. Warto też zwracać uwagę na czytnik, gdy przeciągamy kartę, i pamiętać, że w przypadku jakichkolwiek wątpliwości można wciąż wykorzystywać gotówkę.

Starajmy się zejść z celownika hakerów – nie ułatwiajmy im zadania

Większość ludzi jest nieświadoma zagrożeń lub zaskoczona liczbą możliwych oszustw online. Dlatego tak ważna jest świadomość i edukacja w tym zakresie. Podjęcie kilku prostych kroków opisanych powyżej znacznie utrudni cyberprzestępcom dotarcie do naszych danych. Oszuści nie lubią przeszkód, więc każde zabezpieczenie zmniejsza ryzyko kradzieży tożsamości. Warto wiedzieć, co robić w ramach swoich możliwości, i pozostać w tych działaniach konsekwentnym.

Kradzieże danych kart płatniczych, nowe oszustwa phishingowe – działania cyberprzestępców w czasie pandemii

Derek Manky,
analityk
FortiGuards Labs

Aamir Lakhani,
analityk
FortiGuards Labs

Po ponad roku od ogłoszenia pandemii i rozpoczęcia pracy zdalnej na masową skalę firmy nadal dostosowują się do nowych okoliczności. Należy oczekiwać, że w 2021 roku nastaną kolejne zmiany w środowiskach pracy czy korzystaniu z internetu. Analitycy Derek Manky oraz Aamir Lakhani z działającego w strukturach Fortinetu laboratorium FortiGuard Labs przedstawili informacje na temat ataków wykrywanych obecnie przez specjalistów ds. cyberbezpieczeństwa. Opowiedzieli też, czego w dziedzinie cyfrowych zagrożeń można spodziewać się w nadchodzącym roku.

W jaki sposób cyberprzestępcy skorzystali na wzroście popularności sprzedaży online w ostatnim roku? Z jakich metod korzystają, aby wykradać informacje dotyczące kart kredytowych?

Ostatnie miesiące były wyjątkowe. Zamiast typowych sezonów wyprzedażowych przez ostatni rok właściwie codziennie mieliśmy „Cyber Monday", czyli akcję wyprzedaży organizowaną zawsze pod koniec listopada. Ten stan rzeczy do tej pory nie uległ zmianie, a sprzedaż online stale rośnie. Zauważyliśmy między innymi ataki na serwery, nastawione głównie na wykradanie informacji z koszyków w sklepach internetowych. W ten sposób cyberprzestępcy chcą zdobyć dane kart kredytowych. Jak już kiedyś wspominali-

śmy, hasła praktycznie tracą popularność wśród hakerów, ale informacje o kartach wciąż mają się dobrze.

W 2020 roku zaczęliśmy zauważać wzrost liczby tzw. ataków e-skimmingowych. Przestępcy odwiedzają zaufane strony i „przejmują" moduł koszyka na zakupy. Instalują własny kod i szukają luk w zabezpieczeniach, z których właściciel nie zdaje sobie sprawy. Działa to na podobnej zasadzie jak atak man-in-the-middle, w ramach którego pobierane są informacje o kartach kredytowych i wysyłane na prywatny serwer przestępcy. Później dane te masowo sprzedaje się lub wykorzystuje do przeprowadzania nielegalnych transakcji.

Cyberprzestępcy coraz częściej stosują skimmery Bluetooth do gromadzenia danych o kartach płatniczych. W jaki sposób unikają wykrycia?

Klasyczny skimmer to fałszywy czytnik kart kredytowych, montowany na standardowych czytnikach. Po włożeniu karty skimmer zbiera informacje, które cyberprzestępcy wykorzystują później do wykonania jej kopii. Takie fałszywe czytniki instaluje się zwykle w bankomatach czy punktach sprzedaży na stacjach paliw. Dawniej przestępca musiał wrócić po takie urządzenie, aby pobrać z niego informacje. Natomiast teraz popularność zyskują sprzedawane masowo w darknecie nowe rodzaje skimmerów, wyposażone w moduł Bluetooth. Wystarczy, że przestępca zainstaluje skimmer na stacji paliw lub w innym miejscu. Później może podjechać z laptopem lub smartfonem, pobrać dane i oddalić się. Nie musi niczego dotykać, a ryzyko bycia złapanym na gorącym uczynku jest znacznie mniejsze. Pozwala to na dużą swobodę działania.

To jest w zasadzie nowoczesna forma wardrivingu. Dawniej była to metoda wykorzystująca Wi-Fi jako wektor dostępu do sieci, aby w bierny sposób wyszukiwać dane do logowania i inne. Jednak w obecnej formie ryzyko dla cyberprzestępcy jest znacznie mniejsze, ponieważ proces trwa krócej. Kiedyś osoba siedząca przez dłuższy czas z laptopem w samochodzie przed budynkiem mogła wzbudzać wątpliwości; nowa metoda pozwala na kradzież informacji w znacznie łatwiejszy, mniej podejrzany sposób.

W jaki sposób cyberprzestępcy mogą wykorzystać do swoich celów temat powstania szczepionki przeciwko COVID-19 oraz jej dystrybucji?

W tym roku zaczęliśmy zauważać ataki phishingowe w formie informacji dających złudną nadzieję na dostęp do tanich szczepionek. Z drugiej strony cyberprzestępcy atakują instytucje ochrony zdrowia, oferując sprzedaż nieistniejących szczepionek w hurtowej ilości. Podobna sytuacja miała miejsce w minionym roku, ale wtedy dotyczyła środków ochrony indywidualnej, kiedy pandemia utrudniła do nich dostęp. Możemy spodziewać się, że w najbliższym czasie takich ataków będzie więcej.

W czasie pandemii cyberprzestępcy wykorzystują ludzkie emocje, które zmieniają się wraz z nowymi informacjami pojawiającymi się w mediach. Bywa, że szczepionka na COVID-19 jest trudnodostępna, również dla pracowników służby medycznej i szpitali. Przestępcy korzystają ze sprawdzonych metod, aby wpłynąć na swoje ofiary. Wysyłają np. wiadomości o treści „Twoja grupa otrzyma szczepionkę dopiero w wakacje, ale możesz ominąć kolejkę". Ludzie klikają łącza w takich wiadomościach, aby zarezerwować dla siebie miejsce, a potem okazuje się, że e-mail był fałszywy i padli ofiarą kradzieży danych.

Jakie są najnowsze zagrożenia związane z dostępem do infrastruktury na brzegu sieci i przeglądarkami?

Kod złośliwego oprogramowania tworzony jest tak, aby był jeszcze bardziej elastyczny i skuteczniejszy. Pojedyncza kampania wykorzystująca szkodliwe oprogramowanie jest w stanie objąć zasięgiem różne rodzaje urządzeń i platform. Dla przykładu, rodzina złośliwego oprogramowania o nazwie Adrozek skutecznie zainfekowała liczne przeglądarki i aplikacje, a obsługująca ją infrastruktura jest bardzo rozległa – cyberprzestępcy kontrolują za jej pomocą setki tysięcy domen. Oprogramowanie to infekuje przeglądarkę tak, aby wyświetlała zmanipulowane wyniki wyszukiwania. Gdy uda mu się zainstalować niebezpieczną wtyczkę DLL, pojawia się duży problem. Tymczasem wiele osób nie zdaje sobie sprawy, że prawie wszystkie podłączone do internetu urządzenia również posiadają przeglądarki.

Przeglądarkę można znaleźć na niemal każdym urządzeniu. Nawet jeśli nie jest obecna w postaci aplikacji, w której użytkownik wpisuje adres witryny, to przeglądarka jest potrzebna do odbierania różnego rodzaju komunikatów. Cyberprzestępcy wykorzystują jej kod wbudowany w urządzenia. Niektórzy użytkownicy z góry zakładają, że przeglądarki są z zasady bezpieczne, bo jest to dość często aktualizowana aplikacja. Jednak w rzeczywistości stanowią one nowy obszar ataku na sieć – nie trzeba koniecznie szukać w nich luk, wystarczy przeanalizować mechanizmy zapewniające działanie przeglądarki, takie jak przetwarzanie wyników wyszukiwania, wyświetlanie reklam lub inne procesy, które dają szansę na skuteczny atak. Dzięki botnetom przestępcy tworzą sieci, które mogą atakować szeroką gamę maszyn z systemami Windows, macOS i Linux, wszystkie urządzenia podłączone do internetu, także internetu rzeczy.

Jakie trendy dotyczące cyberzagrożeń wyróżniają się w tym roku?

Wciąż obserwujemy wspomniane wyżej sytuacje. Ewentualne zniesienie lockdownu z pewnością przyniesie zagrożenia, których nie doświadczyliśmy w poprzednim roku, ale które być może były zauważane w latach wcześniejszych – teraz tylko pojawią się w nowych odmianach. Ataki phishingowe będą wykorzystywać aktualne tematy, jak podróże czy promocje w restauracjach.

W drugiej połowie roku z pewnością nastąpi nasilenie ataków związanych z podróżowaniem. Najprawdopodobniej pojawią się e-maile ze specjalnymi zniżkami na przeloty, hotele i pakiety wakacyjne. Wzrośnie liczba oszustw, ponieważ ludzie zaczną działać pochopnie – widać to zresztą już teraz.

Reguła 3-2-1 ułatwia ochronę przedsiębiorstwa przed atakami ransomware

Rick Vanover, dyrektor ds. strategii produktowej w firmie Veeam

Walka z atakami typu ransomware trwa. W ostatnich latach ten rodzaj ataku stał się realnym zagrożeniem dla przedsiębiorstw. Zakrojone na szeroką skalę działania cyberprzestępców zdążyły już zakłócić funkcjonowanie nie tylko międzynarodowych korporacji, ale także instytucji rządowych, uniemożliwiając im realizację najważniejszych zadań. W roku 2017 atak WannaCry doprowadził do blokady szpitalnych systemów informatycznych w różnych krajach Europy, unieszkodliwiając ponad 200 tysięcy komputerów[1]. Trudno o lepszy przykład destrukcyjnego potencjału tego rodzaju działań.

Najbardziej znane przypadki to jak do tej pory WannaCry i Petya, jednak według przygotowanego przez Europol raportu Internet Organized Crime Threat Assessment (IOCTA)[2] liczba cyberataków w dalszym ciągu rośnie. Przedsiębiorstwa i instytucje muszą zdać sobie sprawę z tego zagrożenia i podjąć odpowiednie kroki w celu przygotowania środowiska i mechanizmów ochrony oraz opracowania środków naprawczych. To kluczowy element, dzięki któremu można uniknąć niezaplanowanych i z dużym prawdopodobieństwem nieskutecznych działań podejmowanych w reakcji na ewentualny incydent. Silne, wielowarstwowe zabezpieczenia i strategia działania muszą oprzeć się na trzech elementach: edukacji użytkowników, wdrożeniu odpowiednich rozwiązań oraz zastosowaniu właściwych środków naprawczych. Krytyczne znaczenie ma również wdrożenie zwiększających odporność środowiska mechanizmów tworzenia kopii zapasowych, odzyskiwania i odtwarzania danych, ponieważ pozwala to zachować ciągłość funkcjonowania firmy w momencie pojawienia się zagrożenia.

Edukacja użytkowników w przedsiębiorstwie

Jeśli chodzi o przekazywanie wiedzy, należy objąć nim dwie istotne grupy pracowników, to jest personel informatyczny i użytkowników biznesowych. Ważne jest uwzględnienie obu grup, ponieważ zagrożenia mogą pojawić się w obu środowiskach pracy.

Ataki typu ransomware realizowane są głównie za pośrednictwem protokołu RDP (Remote Desktop Protocol) lub innych mechanizmów zdalnego dostępu, wyłudzania danych (tzw. phishingu) oraz aktualizacji oprogramowania. W większości sytuacji cyberprzestępcy nie muszą podejmować zbyt wielkich starań, by osiągnąć swój cel. Wiedząc o tych mechanizmach, możemy łatwiej wskazać obszary, w które należy szczególnie zainwestować, jeśli chcemy zapewnić odporność sieci na ataki ransomware i uwzględnić przy tym wektory ataku.

Większość administratorów systemów informatycznych korzysta z protokołu RDP na co dzień, a wiele serwerów RDP jest połączonych bezpośrednio z internetem. Należy zrezygnować z takiej konfiguracji. Administratorzy środowiska informatycznego mogą stosować różne zaawansowane środki, np. specjalne adresy IP, przekierowywanie portów RDP albo skomplikowane hasła, jednak dane jednoznacznie wskazują, że ponad połowa ataków typu ransomware odbywa się za pośrednictwem protokołu RDP. Długoterminowa strategia zapewnienia odporności wyklucza możliwość bezpośredniego łączenia serwerów RDP z internetem.

Inną często stosowaną metodą ataku jest rozsyłanie wiadomości e-mail mających na celu wyłudzenie danych (phishing). Większość użytkowników poczty otrzymało z pewnością wiadomość, która nie wyglądała na autentyczną. Oczywiście taki list należy od razu skasować, jednak nie wszyscy odbiorcy reagują w tej sytuacji we właściwy sposób. Na rynku dostępne są popularne narzędzia, takie jak Gophish[3] i KnowBe4[4], które pomagają w ocenie ryzyka zagrożenia phishingiem. W połączeniu ze szkoleniem, dzięki któremu pracownicy nauczą się rozpoznawać podejrzane wiadomości i odsyłacze, narzędzia do samodzielnej oceny stanowią skuteczną linię obrony przed atakami.

Trzeci istotny obszar ryzyka to wykorzystywanie słabych punktów zabezpieczeń. Konieczność aktualizacji systemów to stały obowiązek wszystkich informatyków, ale obecnie nabiera on szczególnego znaczenia. Zadanie to nie wydaje się wprawdzie zbyt ambitne, jednak przedsiębiorstwo może szybko przekonać się o jego istotności, kiedy wystąpi atak wykorzystujący znaną lukę w zabezpieczeniach, którą dałoby się zlikwidować

po zastosowaniu poprawki. Warto pamiętać o instalowaniu bieżących aktualizacji newralgicznych kategorii zasobów informatycznych, czyli systemów operacyjnych, aplikacji, baz danych i oprogramowania wbudowanego urządzeń. Wiele odmian ataków typu ransomware, w tym WannaCry i Petya, opiera swoje działanie na wcześniej wykrytych lukach w zabezpieczeniach, które zostały już jakiś czas temu usunięte.

Wdrożenie rozwiązań i środki naprawcze

Nawet organizacje, które stosują sprawdzone procedury zapobiegania zagrożeniom typu ransomware, narażone są na pewne ryzyko. Edukacja użytkowników jest bardzo istotnym krokiem, jednak przedsiębiorstwo musi przygotować się także na najgorszy scenariusz. Kierownicy działów informatycznych i biznesowych muszą pamiętać o tym, że konieczna jest pamięć masowa na kopie zapasowe, odznaczająca się maksymalną odpornością.

Firma Veeam zaleca zastosowanie reguły 3-2-1 opisującej ogólną strategię zarządzania danymi. Reguła 3-2-1 zaleca tworzenie co najmniej trzech kopii ważnych danych na co najmniej dwóch rodzajach nośników i przechowywanie co najmniej jednej z tych kopii w innej lokalizacji. Reguła nie wymusza stosowania konkretnych typów sprzętu i jest na tyle elastyczna, że pozwala obsłużyć niemal każdy scenariusz awarii.

Ta „jedna" kopia wskazana w strategii 3-2-1 musi odznaczać się szczególną odpornością. Oznacza to, że powinna być odizolowana fizycznie, odłączona od sieci lub niemodyfikowalna. Istnieją różne typy nośników, na których można zapisać taką kopię danych w wyjątkowo bezpieczny sposób. Obejmuje to pamięci taśmowe, niezmienialne kopie w usłudze S3 lub obiektowej pamięci masowej zgodnej z S3, nośniki odizolowane fizycznie i odłączone od sieci, a także oprogramowanie do tworzenia kopii zapasowych i odzyskiwania danych po awarii działające w modelu usługowym.

Mimo prowadzonych szkoleń i wdrażania różnych technik przedsiębiorstwa muszą być przygotowane na prowadzenie

działań naprawczych w przypadku skutecznego ataku. Firma Veeam zaleca, aby nie płacić okupu, a za jedyną opcję odzyskania danych uważa ich odtworzenie. Ponadto przedsiębiorstwo musi mieć opracowany plan reagowania w momencie wykrycia zagrożenia. W pierwszej kolejności należy skontaktować się ze wsparciem technicznym. Klienci firmy Veeam mają dostęp do specjalnego zespołu stosującego konkretne procedury i gotowego udzielić pomocy w przejściu procesu odzyskiwania danych w incydentach związanych z atakami ransomware.

Niezależnie od rodzaju katastrofy jednym z pierwszych problemów, jakie należy rozwiązać, jest kwestia zapewnienia komunikacji. Musi istnieć plan określający sposoby kontaktu z odpowiednimi osobami bez wykorzystania sieci. Obejmuje to na przykład grupy odbiorców wiadomości tekstowych, odpowiednie numery telefonów i inne mechanizmy komunikacji w ramach rozszerzonego zespołu. W książce adresowej powinni znaleźć się także wewnętrzni lub zewnętrzni eksperci ds. bezpieczeństwa, reagowania na incydenty i zarządzania tożsamością.

Niezbędne jest również skontaktowanie się z osobami odpowiedzialnymi za podjęcie decyzji. Przed wystąpieniem jakichkolwiek incydentów przedsiębiorstwo musi określić, kto podejmuje decyzje o odtwarzaniu lub przełączaniu awaryjnym. Po podjęciu decyzji o odtwarzaniu danych konieczne jest wykonanie dodatkowych kontroli bezpieczeństwa, zanim zostanie przywrócone działanie systemów. Należy także ustalić, czy najlepszym sposobem działania będzie odtworzenie całej maszyny wirtualnej, czy też skuteczniejsze okaże się odtwarzanie na poziomie plików. Proces odtwarzania również musi być zrealizowany w bezpieczny sposób, tj. należy uruchomić pełne skanowanie antywirusowe i funkcje poszukiwania szkodliwego oprogramowania oraz wymusić zmianę haseł użytkowników po przywróceniu systemów.

Zagrożenie atakami typu ransomware jest całkiem realne, jednak dzięki odpowiedniemu przygotowaniu przedsiębiorstwa są w stanie zwiększyć odporność na incydenty i ograniczyć ryzyko utraty danych, strat finansowych i uszczerbku na reputacji. Kluczowe jest zastosowanie podejścia wielowarstwowego. Warto przeszkolić personel informatyczny i pozostałych pracowników, aby zminimalizować ryzyko i zwiększyć skuteczność działań prewencyjnych. Należy jednak również wdrożyć rozwiązania, które zapewnią bezpieczeństwo danych i ułatwią tworzenie kopii zapasowych. Trzeba także przygotować się na działania naprawcze w systemach przetwarzania danych podejmowane wówczas, gdy mechanizmy zabezpieczeń stosowane na pierwszych liniach obrony okażą się niewystarczające. Działania takie można zrealizować dzięki funkcjom tworzenia i odtwarzania pełnych kopii zapasowych oraz odzyskiwania po awarii.

[1] *https://www.statista.com/chart/9399/wannacry-cyber-attack-in-numbers/*
[2] *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019*
[3] *https://getgophish.com/*
[4] *https://www.knowbe4.com/*

Praca hybrydowa i wyzwania dla cyberbezpieczeństwa

W 2020 roku wiele firm musiało wprowadzić w trybie nagłym zmiany w swoim modelu działania, zaś dla wielu normą stała się praca zdalna. Kiedy pandemia COVID-19 ustąpi, niektórzy pracownicy wrócą do biur, ale część będzie kontynuować wykonywanie służbowych obowiązków z domu. Praca jest bowiem coraz częściej postrzegana jako czynność, a nie miejsce, do którego trzeba codzienne dojeżdżać.

Praca hybrydowa pozostanie z nami na dłużej

Zespół w hybrydowym środowisku pracy tworzą pracownicy wykonujący obowiązki w siedzibie firmy, zdalni, a także ci, którzy praktykują obie opcje. Ze względu na pandemię COVID-19 liczba zespołów składających się z osób pracujących także zdalnie znacząco się zwiększyła. Mimo że w wielu przypadkach była to nieplanowana zmiana, pracownicy oraz pracodawcy szybko zauważyli płynące z niej korzyści. Ci pierwsi cenią sobie elastyczność, a drudzy widzą sposoby na zwiększenie wydajności, przy jednoczesnym zmniejszeniu kosztów utrzymywania biura.

Można spodziewać się, że popularność pracy hybrydowej będzie trwała także po ustąpieniu pandemii. W niedawnym badaniu[1] przeprowadzonym w Polsce przez Fortinet co piąty ankietowany zapowiedział utrzymanie pracy zdalnej w przyszłości. Dlatego tak istotne jest nabycie umiejętności zarządzania systemami chroniącymi firmowe zasoby IT w nowych realiach i zrozumienie konsekwencji zachodzących zmian dla ich bezpieczeństwa.

Bezpieczeństwo w chmurze

Praca hybrydowa wymaga, aby zespół miał dostęp do potrzebnych aplikacji i danych zarówno wewnątrz tradycyjnej sieci firmowej, jak i poza nią. Przyjęcie rozwiązań wielochmurowych rozszerzyło nasze wyobrażenie na temat tego, gdzie kończą się granice firmy. Niektóre przedsiębiorstwa odkrywają, że architektura bazująca na chmurze, szczególnie przy pracy hybrydowej, wymaga nowej strategii. Pandemia wymusiła także przyspieszony harmonogram przygotowywania infrastruktury do pracy zdalnej. Efektem było ryzyko powstania luk w zabezpieczeniach na rzecz szybkiego umożliwienia pracy.

Tymczasem, aby stworzyć stabilny i bezpieczny model hybrydowy na przyszłość, kluczowe jest właściwe rozwiązanie problemów bezpieczeństwa w środowisku chmurowym. Trzeba przede wszystkim zrozumieć, jak zmieniła się sytuacja od początków istnienia tej techniki. Nie ma już miejsca na model, w którym cały ruch sieciowy przechodzi

przez jedno główne centrum danych. Aby cyfrowa transformacja zadziałała, rozwiązania zapewniające wydajność sieci, zabezpieczeń oraz aplikacji muszą być ujęte w jedno kompleksowe rozwiązanie.

Zmiany w wydatkach na IT

Budżety IT w firmach, które przechodzą na model pracy hybrydowej, znacząco się zmieniają. Firmy zaczynają zauważać, że ich potrzeby w zakresie zabezpieczeń stają się coraz bardziej złożone. Przeznaczane wcześniej na modernizację sieci fundusze są obecnie wykorzystywane do wdrażania chmury, usprawniania współpracy i zabezpieczania punktów końcowych.

Eksperci z firmy Fortinet wskazują m.in., że przedsiębiorstwa stawiające na taki rozproszony model powinny z większym przekonaniem realizować podejście Zero Trust, w którym pracownik otrzymuje dostęp tylko do tych zasobów sieci, które rzeczywiście są mu potrzebne. Firmy będą też musiały na nowo odnaleźć równowagę pomiędzy funkcjonowaniem sieci, jej bezpieczeństwem i potrzebami obliczeniowymi, zwłaszcza w kontekście podziału odpowiedzialności za infrastrukturę, platformę i oprogramowanie.

Czynnik ludzki w cyberbezpieczeństwie

Pracownicy od zawsze przyczyniają się do powstawania jednej z najważniejszych luk w zabezpieczeniach firm, a realia pracy hybrydowej tylko pogłębiły ten stan rzeczy. Obecnie są oni bardziej narażeni na ataki phishingowe i inne zagrożenia. Należy pamiętać, że osoby dopiero rozpoczynające pracę zdalną będą najprawdopodobniej znacznie częściej kontaktować się z działem IT, a potrzeba pobierania licznych plików, uruchamiania nowych aplikacji oraz wykonania określonych procedur zwiększa ryzyko, że atak phishingowy prześlizgnie się przez luki w systemach ochronnych.

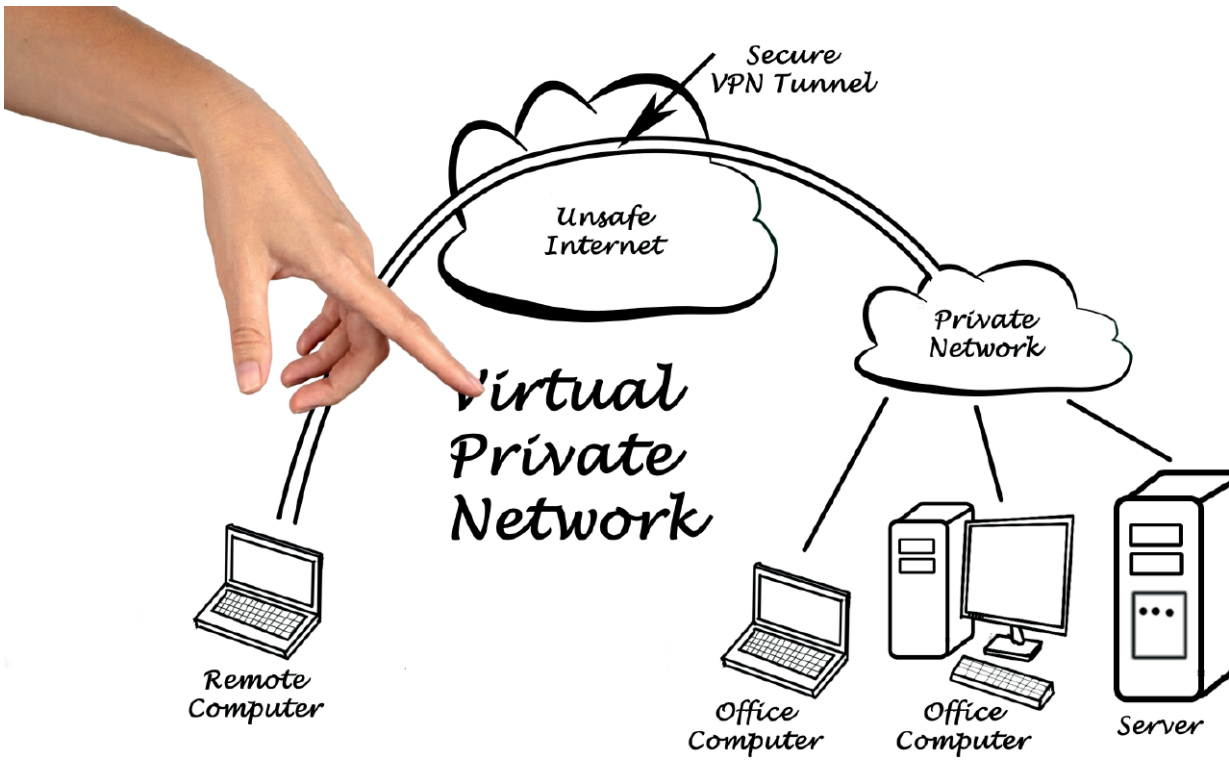
Kluczem do zwalczania ludzkich błędów jest edukacja. Im bardziej personel będzie przeszkolony, tym lepsze będą efekty. Firmy powinny zainteresować się ofertami szkoleń dla pracowników, które ułatwią rozpoznawanie cyberzagrożeń poprzez zrozumienie, kto może stać za atakami, z jakich metod korzysta, jakie działania ochronne należy podjąć i jaką warto znać terminologię. Jedną ze skutecznych i ciekawych metod edukacyjnych jest symulacja ataku phishingowego.

Narzędzia zabezpieczające pracę hybrydową

Chociaż praca hybrydowa wiąże się z nowymi wyzwaniami w zakresie bezpieczeństwa, istnieje wiele narzędzi zapewniających ochronę dla stale rozwijającej się infrastruktury IT. Są to między innymi rozwiązania SD-WAN, które umożliwiają szybkie działanie aplikacji na brzegu i wewnątrz rozległej sieci korporacyjnej, obejmującej liczne urządzenia w domu, w biurze lub w podróży.

Należy także zadbać o dynamiczne zabezpieczenia w chmurze, które ochronią aplikacje i procesy biznesowe o znaczeniu krytycznym – zarówno w chmurowej infrastrukturze publicznej, prywatnej, jak i hybrydowej.

[1] *Badanie przeprowadzone przez agencję ARC Rynek i Opinia na zlecenie Fortinet, w którym udział wzięło 151 pracowników działających w Polsce przedsiębiorstw, październik 2020 roku*



Problemy z zasobami specjalistów w dziedzinie cyberbezpieczeństwa – 4 sposoby na stawienie im czoła

Lucy Kerner, specjalistka ds. bezpieczeństwa i strategii w firmie Red Hat

W obszarze cyberbezpieczeństwa dostępność odpowiednich specjalistów zawsze stanowiła pewien problem. Traktowanie zabezpieczeń tak, jak to często ma miejsce w przypadku szybkiego tworzenia nowych aplikacji biznesowych, nie zawsze uchodzi firmom na sucho. Efektem jest zwykle nadmierne obciążenie specjalistów ds. bezpieczeństwa, których i tak jest zbyt mało. Jednocześnie pracownicy specjalizujący się w cyberbezpieczeństwie są bardzo poszukiwani na rynku pracy, a na zajmowanych przez nich stanowiskach widać dużą rotację.

W przypadku cyberbezpieczeństwa braki personalne mogą być większym zagrożeniem niż sami przestępcy, którzy obiorą sobie za cel kradzież danych, pieniędzy i czasu oraz zniszczenie reputacji firmy. I chociaż problem ten jest znany od dawna, pandemia COVID-19 pogłębiła ten niedobór kadrowy, przez co bezpieczeństwo nierzadko jest zaniedbywane.

Ogólnie trudno jest znaleźć specjalistów w dziedzinie cyberbezpieczeństwa. Pozyskanie takiej osoby jest kosztowne, a często trudno jest zatrzymać ją w firmie na dłużej. Pandemia zaostrzyła niedobór specjalistów w zakresie cyberbezpieczeństwa, ponieważ przedsiębiorstwa skupiły się na podtrzymywaniu – lub budowaniu od podstaw – narzędzi do pracy z domu i właśnie do tych zadań przesunęły swój personel. W wielu firmach proaktywne zabezpieczenia zeszły na dalszy plan, przez co w zespołach ds. cyberbezpieczeństwa pojawiły się olbrzymie luki.

W badaniu przeprowadzonym przed pandemią[1] przez ISC (międzynarodowe stowarzyszenie non-profit zrzeszające menedżerów odpowiedzialnych za bezpieczeństwo informacji) niedobór specjalistów w dziedzinie cyberbezpieczeństwa w Stanach Zjednoczonych oszacowano na prawie 500 000 pracowników. Stowarzyszenie doszło do wniosku, że aby zaspokoić aktualne potrzeby amerykańskich firm, liczba pracowników wyspecjalizowanych w cyberbezpieczeństwie musi wzrosnąć o 62%. W 11 gospodarkach objętych analizą stowarzyszenia liczba pracowników tego segmentu sięga szacunkowo 2,8 miliona osób, a ich globalny niedobór to według szacunków 4,07 miliona. Oznacza to, że na całym świecie kadry wyspecjalizowane w cyberbezpieczeństwie musiałyby być liczniejsze o 145%.

Respondenci stwierdzili, że brak doświadczonych specjalistów w zakresie cyberbezpieczeństwa to jeden z ich największych problemów i czynnik średniego lub nawet ekstremalnego ryzyka dla ich firm. Mimo że badania na potrzeby przeprowadzonego przez Ponemon Institute raportu pt. „Cost of a Data Breach Report[2]" rozpoczęły się kilka miesięcy przed pandemią COVID-19, pytania dodatkowe związane z potencjalnym wpływem pracy zdalnej w trakcie pandemii wykazały, że 76% przedsiębiorstw spodziewa się utrudnionego reagowania na potencjalne naruszenia ochrony danych.

W badaniu przeprowadzonym przez Ponemon Institute oszacowano, że łączny koszt naruszenia ochrony danych wynosi przeciętnie 3,86 mln dol., a zatem zapobieganie incydentom w zakresie cyberbezpieczeństwa ma kluczowe znaczenie. Problemu z brakiem specjalistów ds. cyberbezpieczeństwa nie można rozwiązać błyskawicznie, ale przedsiębiorstwa mogą podjąć pewne działania wykraczające poza próby zatrudnienia nowych pracowników. Oto sposoby na zwiększenie cyberbezpieczeństwa firmy.

1. Wewnętrzne programy szkoleń i certyfikacji w dziedzinie bezpieczeństwa

Perspektywicznie myślące firmy zdają sobie sprawę z faktu, że prawdziwe cyberbezpieczeństwo wymaga zmiany kulturowej. Na pewnym poziomie musi być ono po prostu obowiązkiem każdego pracownika. Nie chodzi tu oczywiście o to, aby dyrektor działu marketingu stanął na pierwszej linii walki z cyberprzestępcami, lecz o to, aby każdy pracownik uczestniczył w programach edukacyjnych i certyfikacyjnych w tym obszarze. Nie wystarczy stworzyć prezentację w programie PowerPoint, zmusić pracowników do zapoznania się z nią i uznać, że problem jest raz na zawsze rozwiązany. Chodzi raczej o opracowanie odpowiednich, dostosowanych do sytuacji programów, które zainteresu-

ją pracowników i pomogą im zrozumieć cyberzagrożenia oraz własną rolę w ich powstrzymywaniu. W tym celu można wykorzystać na przykład szkolenia prowadzone podczas lunchu, symulacje naruszeń bezpieczeństwa, a nawet zabawy typu escape room.

2. Rozpowszechnianie zabezpieczeń

Skoro bezpieczeństwo należy do obowiązków każdego pracownika, personel specjalizujący się w zabezpieczeniach nie powinien pracować wyłącznie w dziale informatycznym. Warto zastanowić się, jak rozpowszechnić zabezpieczenia w całej firmie. Ze względu na wzrost popularności modelu DevSecOps zabezpieczenia w coraz większym stopniu przenikają do procesów programowania, jednak powinny one zostać zintegrowane również z innymi obszarami. Nie tylko pozwoli to zaznajomić cały personel przedsiębiorstwa z kwestiami dotyczącymi bezpieczeństwa, lecz także zachęci do współpracy i będzie szansą na włączenie zabezpieczeń w procesy, produkty i usługi od samego początku.

3. Dokładna analiza posiadanych narzędzi zabezpieczających

Wiele przedsiębiorstw dysponuje narzędziami, których tak naprawdę nie potrzebuje lub które są przestarzałe i nie obsługują nowych technologii, takich jak chmura, kontenery czy oprogramowanie Kubernetes. To strata czasu i pieniędzy. Dużo firm korzysta na przykład z przestarzałych zabezpieczeń stworzonych z myślą o ochronie nieużywanych już systemów.

Przedsiębiorstwa często mają również zbyt wiele narzędzi, nad którymi nie potrafią zapanować, co prowadzi do zduplikowanych rozwiązań i trudności z zarządzaniem rosnącą liczbą produktów. Wiele firm nie wykorzystuje też w pełni funkcji, które są wbudowane w istniejące systemy, takie jak system operacyjny, platforma kontenerowa czy zabezpieczenia udostępniane przez dostawcę chmury. Szczegółowy przegląd istniejących narzędzi wykaże, co jest potrzebne, a co nie, aby można było stawić czoła aktualnym problemom w dziedzinie bezpieczeństwa.

4. Spójna strategia automatyzacji

Przy tak licznych zmiennych nikt nie będzie w stanie załatać każdej luki w zabezpieczeniach. Środowiska informatyczne i świat wokół nas stają się coraz bardziej złożone, podobnie jak incydenty związane z bezpieczeństwem, z którymi zmagają się działy IT. Spójna strategia automatyzacji pozwala firmom skuteczniej niwelować ryzyko przez zmniejszenie liczby błędów ludzkich, jak również rozwiązywać problemy, szybko reagować na alerty bezpieczeństwa oraz tworzyć powtarzalne przepływy pracy w zakresie bezpieczeństwa i zgodności z przepisami.

Warto jednak zauważyć, że automatyzacja nie jest jednym produktem ani nawet zbiorem produktów. Przedsiębiorstwa powinny szukać rozwiązania, które umożliwia zastosowanie spójnej strategii automatyzacji do tworzenia aplikacji, infrastruktury, zabezpieczeń itd. W opracowanym przez Ponemon Institute dokumencie zatytułowanym „Cost of Data Breach Report" stwierdzono, że firmy, które wdrożyły automatyzację na pełną skalę, odnotowują o 3,58 mln dol. niższe całkowite koszty przypadające średnio na naruszenie ochrony danych niż przedsiębiorstwa bez wdrożonej automatyzacji.

Czy problem z niedoborem specjalistów w dziedzinie cyberbezpieczeństwa jest niemożliwy do rozwiązania?

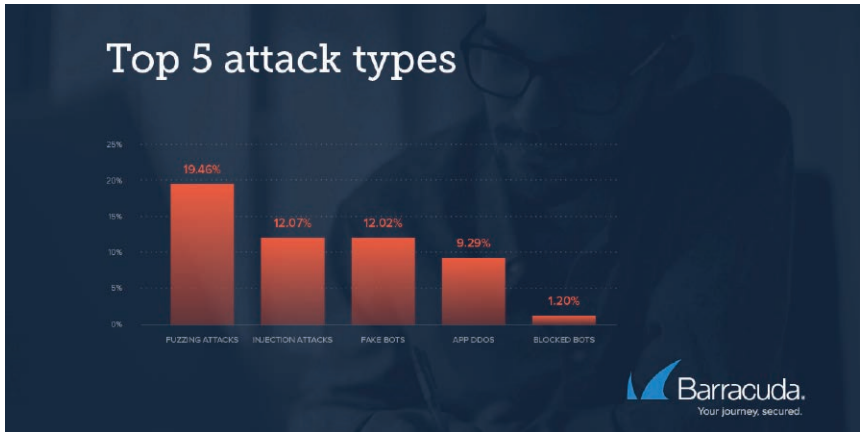
Patrząc realnie, problemu braku pracowników nie można wyeliminować całkowicie. Można mu jednak skutecznie stawić czoła przez proaktywne planowanie, implementację strategicznych technologii oraz realizowane w całej firmie, ciągłe, atrakcyjne szkolenia i wspólne projekty zwiększające świadomość w zakresie bezpieczeństwa.

[1] *https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=18270845 08A24DD75C60655E-243EAC59ECDD4482*

[2] *https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pl*

Informacje o zagrożeniach:
zautomatyzowane ataki na aplikacje internetowe

Cyberprzestępczość stała się wielkim biznesem, a oszuści coraz częściej sięgają po boty i automatyzację, aby ich ataki były wydajniejsze, skuteczniejsze i trudniejsze do wykrycia. W grudniu 2020 r. analitycy firmy Barracuda przeanalizowali próbkę danych z ataków przeprowadzonych w ciągu dwóch miesięcy na aplikacje internetowe, zablokowanych przez systemy Barracuda. Ogromną liczbę stanowiły ataki zautomatyzowane. W pięciu najpopularniejszych atakach stosowane były narzędzia automatyzujące.



Rys. 5 najpopularniejszych typów ataków

Prawie 20% wykrytych ataków stanowiły ataki fuzzingowe, które są realizowane automatycznie w celu wykrycia przypadków, w których aplikacje załamują się, i wykorzystania wykrytych w ten sposób luk do przeprowadzenia ataku. Kolejnych ok. 12 proc. ataków polegało na wstrzyknięciu kodu, przy czym większość atakujących używała do tego zautomatyzowanych narzędzi, takich jak sqlmap. W wielu przypadkach nie następowało wcześniejsze rozpoznanie, które pozwoliłby je zoptymalizować.

Na trzecim miejscu znalazły się boty podszywające się pod roboty indeksujące Google lub innych wyszukiwarek, również stanowiąc nieco ponad 12% ataków. Zaskakująco powszechne (ponad 9% analizowanej przez analityków z firmy Barracuda próbki) były też ataki typu DDoS, czyli rozproszonej blokady dostępu – które były stosowane we wszystkich obszarach geograficznych. Natomiast boty zablokowane przez administratorów strony miały znaczenie marginalne (stanowiły poniżej 2% ataków).

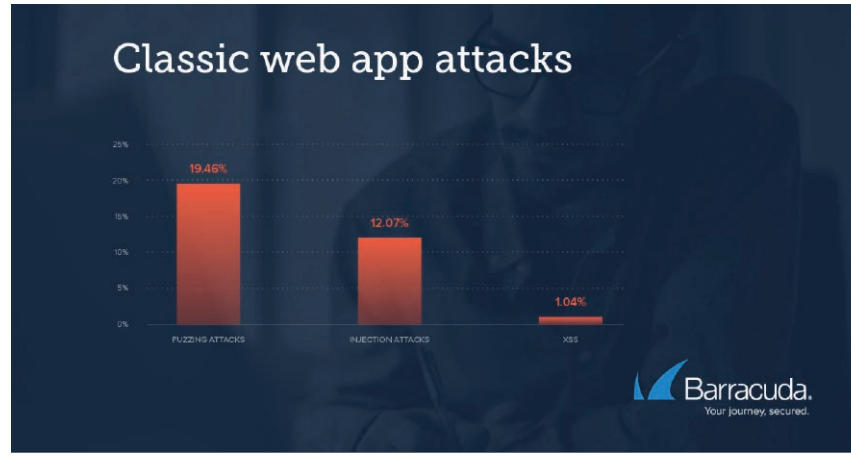
A oto trendy wykryte przez analityków w atakach na aplikacje internetowe oraz sposoby wykorzystywania ataków zautomatyzowanych przez cyberprzestępców.

Wyróżnione zagrożenia

Ataki zautomatyzowane – w atakach zautomatyzowanych stosowane są boty, które próbują wykorzystywać luki i podatności w aplikacjach internetowych. Obejmują one szerokie spektrum zagrożeń: od botów udających szperacze Google w celu uniknięcia wykrycia po ataki DDoS, które przeciążając aplikację, usiłują doprowadzić do awarii witryny.

Chociaż ruch botów to coraz większy problem, nie oznacza to, że cyberprzestępcy porzucają starsze metody ataków. Duża część incydentów przeanalizowanych przez analityków z firmy Barracuda to ataki klasyczne, takie jak wstrzykiwanie kodu (12%) i cross-site scripting (XSS) (1%). Jednak większość ruchu związanego z atakami pochodziła z narzędzi stosowanych do prowadzenia rekonesansu lub wspomnianego narzędzia fuzzing do sondowania aplikacji.

Wstrzykiwanie kodu otwiera najnowszą listę dziesięciu najpoważniejszych zagrożeń, przygotowywaną przez fundację Open Web Application Security Project (OWASP Top 10). Od początku istnienia tej listy są one obecne w każdej kolejnej jej edycji. Są one relatywnie łatwe w wykonaniu i potencjalnie zapewniają cyberprzestępcom duże korzyści, a więc zapewne szybko z nich nie zrezygnują. Dość częste były również ataki typu cross-site scripting (XSS) – trzeci najczęściej stosowany atak w tej grupie.

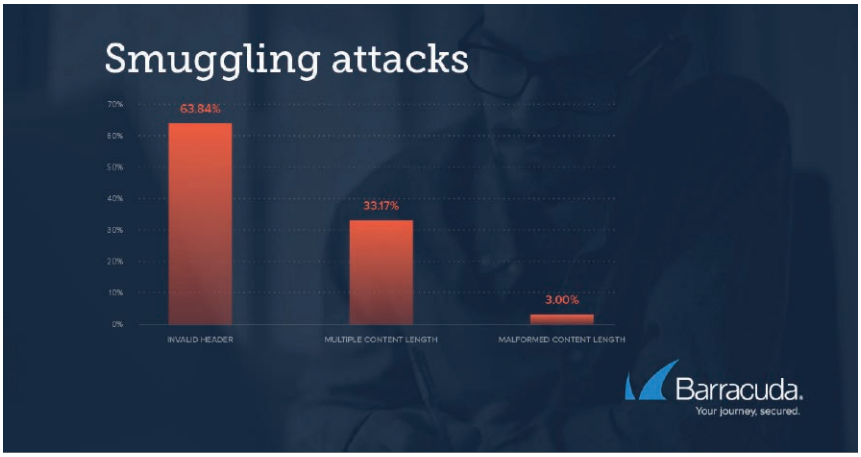


Rys. Klasyczne ataki na aplikacje internetowe

Szczegóły

Znaczna część analizowanego ruchu związanego z atakami miała na celu wykorzystanie podatności aplikacji WordPress (popularny CMS wykorzystywany przez twórców stron internetowych) lub PHP (zwykle były to strony phpMyAdmin stosowane do zarządzania bazą danych MySQL) – odsetek ataków wynosił odpowiednio 6,1% oraz 1,05%. Spora część z nich została przeprowadzona przeciwko stronom niewykorzystującym PHP lub WordPressa, a więc stały za nimi osoby, które korzystają z gotowych, dostępnych w internecie narzędzi hakerskich, lecz nie mają pojęcia na temat ich działania (osoby takie nazywa się script kiddies). Niewykluczone jednak, że wkrótce nauczą się one przeprowadzać rekonesans przed przeprowadzeniem ataku.

Atakiem, którego popularność spadła do pomijalnego poziomu, ale który po ujawnieniu ataku HTTP Desync[1] powraca na skalę masową, jest przemycanie zapytań http (HTTP Request Smuggling). Według badania przeprowadzonego przez firmę Barracuda ponad 60% tego typu ataków wykorzystywało nieprawidłowy nagłówek protokołu http, jedna trzecia wykorzystywała zwielokrotnianie wartości w polu Content-Length, a 3% miało źle sformatowaną wartość w tym polu.



Rys. Ataki polegające na przemycaniu zapytań

Większość zaobserwowanych ataków przeciwko API JSON polegała na testowaniu warunków brzegowych, czyli w gruncie rzeczy były to próby zmylenia tego interfejsu. W 95% tego typu ataków przekraczano dopuszczalną wielkość liczb (Max Number), a w prawie 4% – dopuszczalną długość napisów (Max Value Length). Zaobserwowano również inne próby ataków – ataki XSS i SQL Injection – ale ich liczba w próbce była pomijalna. Analitycy spodziewają się jednak, że w ciągu najbliższego roku może się to zmienić.

Próby wycieku danych dotyczyły głównie ujawnienia wrażliwych danych, takich jak numery kart kredytowych, ubezpieczenia społecznego (używanych w wielu krajach do potwierdzania tożsamości, analogicznie jak polski PESEL) itp. Dominowały próby eksfiltracji numerów kart kredytowych. Głównym celem była Visa, przeciwko której zanotowano ponad trzy czwarte wszystkich ataków tego typu. Daleko w tyle była firma JCB (ponad 20% ataków), natomiast Mastercard, Diners i American Express były atakowane znacznie rzadziej.

Rys. Próby wycieku danych

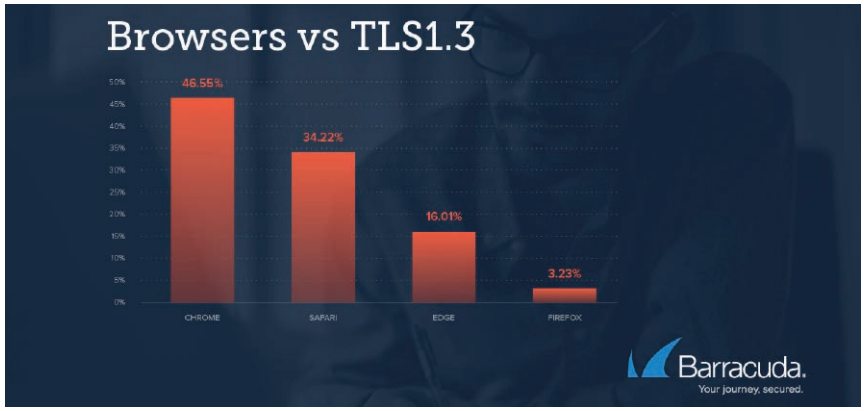
Szyfrowanie

Analitycy firmy Barracuda przeanalizowali również szyfrowanie ruchu, które zapobiega różnym atakom oraz stanowi warstwę ochronną podczas odwiedzania stron internetowych.

Prawie 92% ruchu, który naukowcy z firmy Barracuda analizowali w okresie od października do grudnia 2020 r., stanowił szyfrowany ruch https. Nieszyfrowany protokół http był odpowiedzialny za mniej niż 10% ruchu. To obiecujący postęp i dobra wiadomość dla bezpieczeństwa aplikacji internetowych.

Preferowanym protokołem stosowanym w przeglądarkach jest obecnie TLS1.3, co zwiększa bezpieczeństwo użytkowników. Starszy protokół SSLv3 był rzadko stosowany, ponieważ nie jest on zbyt skuteczny. Nawet wśród organizacji, które korzystają z tego protokołu, ruch SSLv3 był niewielki. To samo dotyczy protokołów TLS1.0 i TLS1.1, których popularność gwałtownie spada – a z których każdy odpowiada za mniej niż 1% analizowanego ruchu.

Najbezpieczniejszy obecnie protokół TLS1.3 stanowił 65% całego analizowanego ruchu https. Około jednej trzeciej stanowił starszy protokół TLS1.2, ale jego popularność powoli spada.



Rys. Analiza przeglądarek korzystających z protokołu TLS1.3

Analiza przeglądarek korzystających z TLS1.3 (w oparciu o informacje zgłaszane przez same przeglądarki w nagłówkach User Agent) ujawniła, że najpopularniejszą przeglądarką (odpowiedzialną za 47% ruchu zaszyfrowanego tym protokołem) był Chrome. Na drugim miejscu znalazło się Safari, które odpowiadało za 34% ruchu TLS1.3. Co zaskakujące, Edge wyprzedził Firefoksa i znalazł się na podium z 16% ruchu, natomiast Firefox wygenerował zaledwie 3% ruchu. Firefox przegrywa z Edge prawdopodobnie z dwóch powodów:

- dominacja przeglądarki Chrome,
- systemy korporacyjne, które dotychczas preferowały przeglądarkę Internet Explorer, obecnie przechodzą na Edge.

Analiza ruchu TLS1.2 przyniosła bardziej zaskakujące wyniki. W protokole tym Internet Explorer generuje większy ruch niż Chrome – odpowiadając za ponad połowę ruchu – natomiast Chrome ma nieco poniżej 40%. Dla porównania, Safari generuje poniżej 10% ruchu, a Firefox – jeszcze mniej.

Analitycy z firmy Barracuda odkryli, że dość często stosowane są automatyczne aktualizacje przeglądarek Chrome i Firefox. Większość tych przeglądarek to najnowsza lub jedna z dwóch najnowszych wersji.

Z Internet Explorera nadal korzysta wiele osób, przy czym zdecydowanie najpopularniejsza była wersja IE11, co pokazuje poprawny trend w kierunku używania bardziej aktualnych i bezpiecznych przeglądarek.

Dla kontrastu, ruch generowany automatycznie rzadko wykorzystuje TLS1.3 – zwykle jest to TLS1.2. Obejmuje to monitory witryn, boty i narzędzia, takie jak curl.

Jak się chronić przed atakami zautomatyzowanymi

W obszarze ochrony przed najnowszymi atakami, takimi jak boty czy ataki przeciwko API, liczba wymaganych rozwiązań może przytłaczać. Na szczęście są one łączone w takich produktach jak WAF (także w postaci usługi, WAF-as-a-Service[2]), które służą również do ochrony aplikacji webowych i ochrony API (WAAP).

Jak można przeczytać w raporcie WAF Magic Quadrant 2020[3]:

„Gartner[4] definiuje usługi WAAP jako ewolucję usług WAF w chmurze. Usługi WAAP obejmują usługi WAF, ochronę przed botami, ochronę przed DDoS i ochronę API, dostarczane w chmurze w modelu subskrypcyjnym".

Organizacje powinny więc poszukać rozwiązania WAF-as-a-Service lub WAAP[5], które obejmuje ochronę przed botami[6], ochronę przed DDoS[7], ochronę API i ochronę przed zapychaniem poświadczeniami[8] – oraz upewnić się, że zostało ono odpowiednio skonfigurowane.

Należy też być na bieżąco z aktualnymi zagrożeniami i śledzić ich zmiany. Według firmy Barracuda do trzech najważniejszych typów ataków w tym roku będą należeć: zautomatyzowane ataki botów[9], ataki na interfejsy API[10] i ataki na procesy tworzenia oprogramowania. Ochrona przed tymi rodzajami ataków jest słabsza, więc zwykle są one skuteczne.

Rys. Analiza przeglądarek korzystających z protokołu TLS1.2

[1] *https://blog.barracuda.com/2020/11/17/http-desync-attacks-a-variant-of-request-smuggling-attacks/*
[2] *https://www.barracuda.com/waf-as-a-service*
[3] *https://www.barracuda.com/waf-mq*
[4] *https://www.gartner.com/en/documents/3903064/defining-cloud-web-application-and-api-protection-servic*
[5] *https://www.barracuda.com/cap*
[6] *https://www.barracuda.com/products/advanced-bot-protection*
[7] *https://www.barracuda.com/glossary/ddos*
[8] *https://blog.barracuda.com/2020/09/21/fbi-sees-spike-in-credential-stuffing-attacks/*
[9] *https://blog.barracuda.com/2021/01/20/appsec-predictions-2021-bots-get-bigger-and-smarter/*
[10] *https://blog.barracuda.com/2021/01/26/appsec-predictions-2021-attackers-increasingly-pivot-to-apis/*

Jak zmienił się krajobraz cyberzagrożeń podczas pandemii?

W minionym roku cyberprzestępcy wykazywali się wyjątkową aktywnością. Miało to oczywiście w dużym stopniu związek z masowym przejściem pracowników biurowych na tryb pracy zdalnej. Atakujący często wykorzystywali gorzej zabezpieczonych użytkowników i ich urządzenia do prowadzenia szeroko zakrojonych kampanii cyberprzestępczych. Zdaniem ekspertów z firmy Cisco trudno oczekiwać, że w 2021 r. prób ataków będzie mniej. Wzrośnie również skala cyberincydentów o bardziej złożonym charakterze.

W najnowszym raporcie Cisco[1] możemy przeczytać o tym, w jakich obszarach cyberprzestępcy byli szczególnie aktywni w 2020 r.

Ataki na zdalne pulpity

Pandemia sprawiła, że znacznie wzrosła popularność zdalnych pulpitów (ang. Remote Desktop Protocol, RDP), czyli technologii, która pozwala na dostęp do komputera (np. biurowego) z lokalizacji zdalnej. Bez wątpienia stanowi to wygodne rozwiązanie w sytuacji masowego przejścia na pracę zdalną, ale jednocześnie wzbudza wiele obaw w kontekście cyberbezpieczeństwa.

Obawy te dotyczą kradzieży danych uwierzytelniających, ataków typu man-in-the-middle (cyberatak, w którym atakujący umieszcza się na linii komunikacji między dwiema stronami) czy zdalnego wykonania kodu (luka w zabezpieczeniach, którą atakujący może wykorzystać do uruchomienia własnego kodu na komputerze lub serwerze). Każde rozwiązanie RDP, jeśli zostanie przejęte, umożliwia atakującemu dostęp do cyfrowych zasobów organizacji.

Według ekspertów Cisco firmy korzystające z wirtualnych pulpitów powinny wdrożyć specjalne środki bezpieczeństwa:

- Unikać podłączania zdalnych pulpitów bezpośrednio do sieci. Zamiast tego można zapewnić pracownikom dostęp do wszystkich niezbędnych zasobów za pomocą usługi VPN.
- Wdrożyć system uwierzytelniania wielopoziomowego – dodatkową warstwę bezpieczeństwa, umożliwiającą potwierdzenie tożsamości użytkowników.
- Blokować użytkowników, którzy podjęli wiele nieudanych prób logowania.

Ransomware i podwójne wymuszenie

W minionym roku ataki typu ransomware przybrały nowe formy. Przykładowo, pojawiły się liczniki odliczające czas, który ma użytkownik na wpłacenie okupu. Eksperci z firmy Cisco zajmujący się cyberbezpieczeństwem zaobserwowali, że coraz częściej zaatakowani użytkownicy otrzymują groźby nie tyle zaszyfrowania, co trwałego usunięcia danych.

Zmieniła się również skala ransomware, a ataki na poszczególne urządzenia często są jedynie narzędziem, które pozwala uzyskać dostęp do sieci organizacji. Gdy to już nastąpi, atak ransomware jest uruchamiany dopiero po tym, gdy atakujący wejdą w posiadanie danych firmy, w tym własności intelektualnej czy poufnych informacji handlowych. Według ekspertów z Cisco często mamy wówczas do czynienia ze zjawiskiem podwójnego wymuszenia – z jednej strony atakujący przejmują dane, które mogą wykorzystać i dalej monetyzować, z drugiej wymuszają okup za ich odszyfrowanie czy niewykasowanie, co ma na celu maksymalizację szkód ofiar i zysków atakujących.

Kwitnie również czarny rynek, na którym sprzedawane są np. dostępy do sieci firmowych. Nieuczciwi użytkownicy mogą zatem lepiej przygotować się do ataku i w jednym momencie rozesłać złośliwe oprogramowanie do większej liczby organizacji.

Co może zrobić biznes, żeby ustrzec się przed nowymi formami ransomware? Eksperci z firmy Cisco podkreślają, że najważniejsze jest kompleksowe podejście do kwestii cyberbezpieczeństwa, na które składa się zapobieganie, lokalizowanie zagrożeń i reagowanie na nie. Ekosystem cyberbezpieczeństwa powinien obejmować m.in.:

- bezpieczeństwo poczty e-mail,
- zarządzanie aktualizacjami i łatami,
- monitoring systemów i sieci,
- segmentację sieci,
- kopie zapasowe i przywracanie systemu po awarii,
- polityki i procedury,
- szkolenia.

Wykradane danych logowania

Kradzież danych umożliwiających logowanie stanowi drugą najczęstszą aktywność cyberprzestępców, jeśli chodzi o włamania do firmowych systemów bezpieczeństwa. Posługując się wykradzionym loginem i hasłem, mogą oni pozostać niezauważeni w sieci danej organizacji. Podobnie jak w przypadku ransomware, również kradzież danych do logowania służy za punkt wyjścia do dalszych ataków i wykradania kolejnych danych do logowania. Cyberprzestępcy nie poprzestają na uzyskaniu dostępu do jednego urządzenia; często z jego poziomu chcą wejść w posiadanie haseł do innych elementów firmowej infrastruktury IT, przeszukując różne obszary systemów, gdzie tego typu informacje są przechowywane. Jak się zabezpieczyć przed tym procederem? Eksperci z firmy Cisco radzą, aby:

- monitorować dostęp do baz danych LSASS (Local Security Authority Subsystem Service) i SAM (Storage Area Management),
- monitorować logi w celu wyszukiwania nieplanowych, podejrzanych aktywności w kontrolerach domen,
- wyszukiwać nieoczekiwane i nieprzydzielone połączenia z adresów IP do kontrolerów domen.

Więcej o tym, jak działali cyberprzestępcy w 2020 roku, można przeczytać w najnowszym raporcie Cisco pt. „Defending Against Critical Threats: A 12 month roundup".

[1] *https://www.cisco.com/c/dam/en/us/products/collateral/security/threats-year-report.pdf*

Cisco prezentuje 5 trendów sieciowych wpływających na zwiększenie elastyczności i odporności biznesu w niepewnych czasach

Pandemia COVID-19 sprawiła, że niemal z dnia na dzień całe zespoły musiały przejść na tryb pracy zdalnej. Firmy zintensyfikowały sprzedaż produktów i usług online, a te, które nie posiadały potrzebnej do tego infrastruktury, stanęły przed wyzwaniem szybkiego dostosowania się do prowadzenia biznesu w Sieci. Inne organizacje z branż takich jak logistyka czy produkcja musiały wprowadzić zmiany w łańcuchach dostaw, niekiedy zmieniając dostawców, aby zapewnić ciągłość działania.

Pandemia stanowiła dzwonek alarmowy dla niemal każdej organizacji, co nie oznacza, że biznes nie doświadczał problemów wcześniej. Jak wynika z raportu PWC pt. „Global Crisis Survey 2019", 7 na 10 organizacji doświadczyło przynajmniej jednego poważnego kryzysu w ciągu ostatnich 5 lat, a 95% jest przekonanych, że nie był on ostatnim[1].

Skuteczne zarządzanie biznesem w sytuacji kryzysu wymaga od liderów IT zmiany sposobu myślenia. Obecnie ważniejsze od narzucanych z góry norm i podejścia reaktywnego, które stanowią fundament tradycyjnego sposobu planowania ciągłości biznesu, jest skoncentrowanie się na zwinności w zakresie IT, która pozwala uodpornić organizację na kryzysy, również te nieoczekiwane.

Sieć: 5 trendów, które zwiększą odporność biznesu

Kluczowe procesy biznesowe są zależne od coraz bardziej złożonego ekosystemu technologii cyfrowych, które w wielu przypadkach stanowią główne narzędzie umożliwiające zapewnienie ciągłości działania, co szczególnie mocno uwidoczniła pandemia COVID-19. Sieć jest platformą, która łączy, zabezpiecza i umożliwia kontakt pomiędzy rozproszonymi użytkownikami, urządzeniami i aplikacjami.

Dobra sieć to coś więcej niż narzędzie umożliwiające nawiązywanie połączeń bez opóźnień. Biznes potrzebuje platform sieciowych, które pozwalają reagować szybko na zmienne okoliczności, wdrażać nowe usługi i modele operacyjne, integrować je z procesami IT, a także zabezpieczać użytkowników, klientów oraz całą firmę.

Najnowszy raport pt. „Cisco 2021 Global Networking Trends" prezentuje pięć trendów, które liderzy IT powinni uwzględnić w swoich inicjatywach mających na celu zwiększenie odporności biznesu.

1. Objęcie systemem bezpieczeństwa pracowników zdalnych

Obecnie, średnio 4,7 razy więcej pracowników wykonuje swoje obowiązki z domu niż przed pandemią[2]. Pracownicy zdalni korzystający z urządzeń osobistych i sieci domowej w celu uzyskania dostępu do firmowych danych oraz aplikacji są szczególnie narażeni na cyberataki. Niekiedy omijają oni VPN i łączą się bezpośrednio z usługą lub aplikacją w chmurze publicznej, która stanowi najtrudniejsze środowisko do zabezpieczenia.

Chcąc zapewnić bezpieczeństwo osób pracujących z domu na szeroką skalę, zespoły IT powinny wdrożyć poniższe praktyki:

- **VPN dla pracowników zdalnych**. VPN wciąż stanowi jeden z najbardziej efektywnych i szybkich sposobów rozszerzenia kontroli i bezpieczeństwa na poziomie korporacyjnym na pracowników zdalnych.
- **Autoryzacja wieloskładnikowa do ochrony aplikacji.** Jest ona kluczowym narzędziem zapewniającym bezpieczeństwo biznesu; pozwala zweryfikować tożsamość każdego użytkownika, zanim otrzyma on dostęp do sieci lub kluczowych aplikacji i danych.
- **Architektura Secure Access Services Edge (SASE), która zapewnia bezpieczeństwo środowiska wielochmurowego.** Bezpieczeństwo w chmurze i SASE pozwalają ochronić biznes przed zagrożeniami pochodzącymi z internetu, niezależnie od rodzaju połączenia, urządzenia, z którego korzysta użytkownik, czy środowiska chmurowego.

2. Zapewnienie bezpiecznego powrotu do biur

Mimo że wiele pytań dotyczących przyszłości pracy wciąż pozostaje bez odpowiedzi, oczywiste jest, że przestrzeń i warunki, w których pracujemy, zmienią się na skutek pandemii. Biznes wykorzystuje potencjał narzędzi telekonferencyjnych i bezprzewodowych technologii sieciowych. Niektóre firmy wdrażają nowe usługi mające na celu zapewnienie bezpieczeństwa, np. systemy monitorujące, czy jest zachowywany dystans społeczny. Potrzeba ograniczenia skupisk ludzi w miejscach pracy przyczynia się również do coraz powszechniejszego wykorzystywania rozwiązań z zakresu automatyzacji oraz robotów, które przyczyniają się zwiększenia produktywności.

Nowoczesna i elastyczna sieć to kluczowy element, który ułatwia bezpieczny i bezproblemowy powrót pracowników do miejsc pracy.

- **Testuj sieć.** Pandemia sprawiła, że użytkownicy nie korzystali z sieci biurowej przez całe tygodnie. Odpowiednia przepustowość nie jest dana raz na zawsze i nie należy brać jej za pewnik. Warto przeprowadzać testy sieci, które pozwolą sprawdzić, czy radzi sobie ona z obecnymi obciążeniami.
- **Automatyzuj procesy udzielania dostępu na podstawie weryfikacji tożsamości.** Organizacje muszą mieć możliwość ciągłego zarządzania, zabezpieczania i segmentacji użytkowników i urządzeń (zarówno nowych, jak i tych znanych), próbujących uzyskać dostęp do usług i zasobów z siedziby firmy, domu czy miejsc publicznych (korzystając z publicznej sieci Wi-Fi).
- **Zwiększ bezpieczeństwo pracowników i klientów na podstawie analizy położenia.** Wdróż monitoring przestrzeni pracy i system alertów oraz zapewnij niezbędne informacje, aby pomóc zagwarantować bezpieczeństwo, a także zadbać o zdrowie pracowników, partnerów, gości i klientów. Wykorzystaj biurową sieć Wi-Fi w połączeniu z takimi rozwiązaniami jak Cisco DNA Spaces, które w czasie rzeczywistym dostarcza informacje o aktualnym zagęszczeniu w pomieszczeniach w biurze i pozwala zareagować, zanim będzie ono zbyt duże.

3. Ułatwienie zarządzania środowiskiem wielochmurowym dla większej odporności

Liderzy IT wykorzystują usługi w chmurze jako sposób na poprawę odporności biznesu w obliczu globalnej pandemii. Zagadnienie to obejmuje m.in. zwiększoną adopcję modelu wielochmurowego – dystrybucję aplikacji, obciążeń i danych w centrach danych działających lokalnie w firmach i u publicznych dostawców usług w chmurze. Ma to na celu nie tylko obniżenie kosztów czy zwiększenie elastyczności, ale także ochronę przed katastrofalnymi awariami i rozproszenie ryzyka ich wystąpienia.

Skuteczne strategie sieciowe w środowisku wielochmurowym[3] opierają się na trzech głównych filarach:

- **Obciążenia w centrum danych.** Przyjęcie modelu operacyjnego w chmurze pomoże w uproszczeniu regulacji, poprawie bezpieczeństwa i zarządzania obciążeniem pracą i usługami w centrach danych znajdujących się w firmach, wielu różnych chmurach i innych środowiskach przetwarzania danych i wykorzystywania mocy obliczeniowej[4].
- **Dostęp**. Wykorzystanie architektur SD-WAN[5] i SASE[6] pozwoli zapewnić użytkownikom i urządzeniom w sieci korporacyjnej i publicznej stały, bezpieczny dostęp do usług wielochmurowych (w tym SaaS[7]) w siedzibie lub oddziale firmy, ale także w domu lub w podróży.
- **Bezpieczeństwo.** Strategia wielochmurowa pozwala na zmniejszenie ryzyka związanego z użytkownikami, urządzeniami i aplikacjami rozproszonymi w wielu chmurach i innych środowiskach obliczeniowych.

4. Automatyzacja operacji dla szybszego powrotu do sprawnego działania

Nagły wzrost liczby rozproszonych pracowników zdalnych nie jest jedyną rzeczą, która wyjątkowo obciąża dzisiejsze zespoły NetOps. Pandemia spowodowała również bezprecedensowy poziom gwałtownych wahań liczby klientów, wzorców ruchu w aplikacjach oraz przypadków nowych zastosowań, takich jak np. e-learning, wideokonferencje, wydarzenia wirtualne, zdalna opieka medyczna, automatyzacja procesów i inne usługi zależne od sieci.

Nie jest więc dużym zaskoczeniem, że obecnie 50% specjalistów z branży sieciowej uznaje automatyzację sieci za krytyczny warunek zapewnienia ciągłości usług i wydajności w czasie zakłóceń[8], a 35% planuje, że do 2022 r. ich sieci we wszystkich domenach będą intuicyjne,

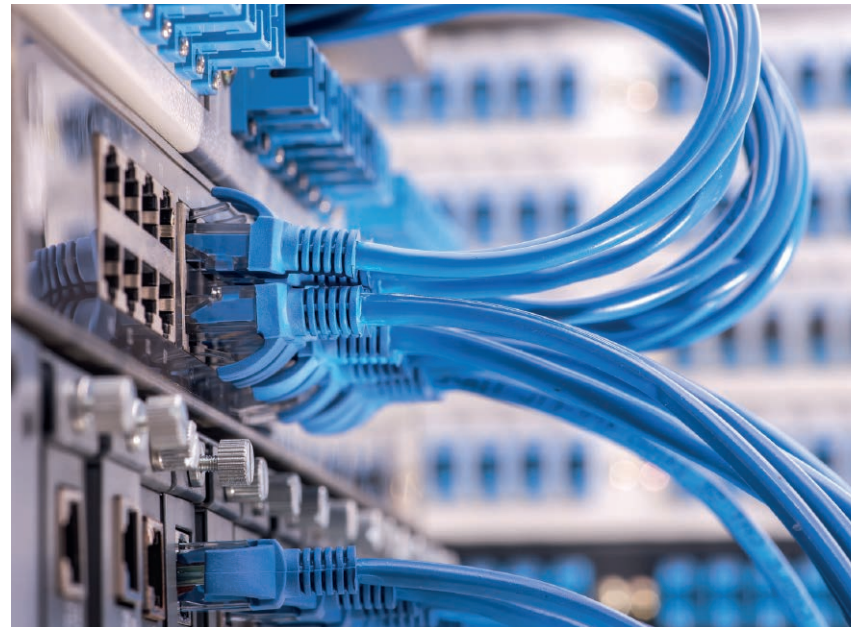
w porównaniu z zaledwie 4% w 2019 r. [9]

Zespoły NetOps mogą ciągle się doskonalić i szybko reagować na rosnące zakłócenia i zagrożenia, stopniowo automatyzując sieć w kolejnych obszarach. Dotyczy to m.in.

- Powtarzalnych zadań „administracyjnych", takich jak tworzenie, konfiguracja i zarządzanie siecią, w celu zmniejszenia obciążeń administracyjnych i poprawy zgodności z regulacjami w każdej dziedzinie.
- Dostępu do sieci, dołączania i segmentacji w celu ochrony grup rozproszonych użytkowników i procesów oraz ograniczenia rozprzestrzeniania się ataków.
- Polityki sieciowej w korporacyjnym centrum danych z segmentacją zorientowaną na aplikacje, która zapewnia ochronę im i danym oraz śledzi obciążenie pracą.
- Polityki sieciowej poza korporacyjnym centrum danych z modelem operacyjnym obejmującym chmurę, który zapewni spójną politykę aplikacji w środowisku lokalnym i hybrydowym środowisku chmurowym.
- Pełnej segmentacji multidomenowej opartej na politykach bezpieczeństwa w celu ustanowienia spójnego modelu dostępu ograniczonego zaufania (zero trust), od użytkowników i procesów po obciążenie pracą.

5. Wykorzystywanie analizy sieci wspieranej sztuczną inteligencją w celu uzyskania lepszych wniosków

Zarządzanie złożonością i skalą działania nowoczesnych sieci oraz wynikającą z tego lawiną zdarzeń i problemów bombardujących wiele różnych platform monitorowania może być zarówno przytłaczające, jak i nieefektywne, zwłaszcza w przypadku wystąpienia zakłóceń. Według danych telemetrycznych zgromadzonych przez rozwiązanie Cisco DNA Center, w sieci bezprzewodowej przedsiębiorstwa odbywa się średnio ok. 4 400 incydentów miesięcznie. Dzięki zastosowaniu analizy sieci z wykorzystaniem sztucznej inteligencji oraz uczenia maszynowego zespoły NetOps otrzymują znacznie łatwiejszy w zarządzaniu zbiór



alertów, na które mogą lepiej reagować.

Aby nadać sens „lawinie zdarzeń", zespoły NetOps powinny wdrożyć systemy analizy sieci oparte o uczenie maszynowe, dzięki czemu mogą liczyć m.in. na:

- Dokładniejsze wykrywanie nieprawidłowości: poprawę dokładności automatycznego wykrywania problemów i anomalii w domenach sieciowych i pomiędzy nimi.
- Szybszą naprawę: korelację zdarzeń w celu wykrycia i wyraźnego opisania najbardziej prawdopodobnej pierwotnej przyczyny problemów i anomalii.
- Zautomatyzowane zarządzanie polityką: określanie urządzeń, aplikacji i trendów oraz proponowanie zalecanych aktualizacji polityk bezpieczeństwa.
- Mniej przypadków degradacji: identyfikację wzorców i trendów oraz dostarczanie informacji kontekstowych, które przyspieszają działania proaktywne, korygujące i zapobiegawcze.
- Wzajemne informowanie: dostarczanie informacji i analiz, które pomogą administratorom sieci porównać wydajność ich sieci z globalnymi, branżowymi lub regionalnymi wzorcami.

Efekt: poprawa odporności biznesu dzięki zaawansowanej platformie sieciowej

Niestety możemy być pewni tego, że wydarzenia mącące spokój będą się pojawiały i będą stanowiły wyzwanie dla wszystkich firm i ich sieci przez najbliższe lata. Nadszedł więc czas, aby na nowo przemyśleć, w jaki sposób strategia sieciowa umożliwia osiągnięcie odporności biznesowej i nadać priorytety nowym projektom sieciowym, które są najbardziej potrzebne już teraz. W epoce „nowej normalności" chodzi o to, aby mieć do dyspozycji sieć, którą będzie można przystosować do tego, co przyniesie przyszłość. Myśląc o strategii odporności biznesowej, należy zastanowić się, w jaki sposób sieć może być jej kluczowym czynnikiem.

Cały raport pt. „Cisco Global Networking Trends 2021" jest dostępny tutaj[10].

[1] *PwC, „Global Crisis Survey 2019"*
[2] *Freeform Dynamics, „A New Perspective on the Modern Workplace", raport sponsorowany przez firmę Cisco, lipiec 2020r.*
[3] *https://www.cisco.com/c/en/us/solutions/cloud/what-is-cloud-networking.html*
[4] *https://www.cisco.com/c/en/us/solutions/cloud/what-is-cloud-computing.html*
[5] *https://www.cisco.com/c/en_uk/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html*
[6] *https://www.cisco.com/c/en/us/products/security/what-is-sase-secure-access-service-edge.html*
[7] *https://www.cisco.com/c/en/us/products/software/what-is-software-as-a-service-saas.html*
[8] *2020 Cisco Business Resilience Networking Survey*
[9] *Cisco, 2020 Global Networking Trends Report*
[10] *https://www.cisco.com/c/en_uk/solutions/enterprise-networks/networking-report.html*

Ochrona na pstryknięcie palcami

Ochrona przed cyberzagrożeniami nie musi być skomplikowana i droga. Może być atrakcyjna cenowo, łatwa w instalacji, a jednocześnie skuteczna i wydajna. Dlatego z myślą firmach, które nie dysponują rozbudowanymi działami IT, zaprojektowaliśmy rozwiązanie Kaspersky Endpoint Security Cloud.

www.kaspersky.pl

Kaspersky
Endpoint Security
Cloud

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.