Numer 3/2021 (38)
ISSN 2720-0604

DLP expert

Data Leak Prevention

www.dlp-expert.pl

Czy firmy powinny płacić okup cyberprzestępcom?

W jaki sposób uczenie maszynowe chroni przed phishingiem, zagrożeniami mobilnymi oraz awariami zakładów produkcyjnych

Pięć trendów, jakie powinny uwzględnić firmy, planując wydatki na cyberbezpieczeństwo w 2022 r

Od szkodliwego e-maila do milionowego okupu – phishing wciąż na fali

Ekspert Fortinet o ochronie infrastruktury sieci 5G

Mija rok Chmury, nadchodzi nowy, niemniej chmurny

Jest taki periodyk, zwany z rosyjska xakep, pisany cyrylicą, jako że rodem on z Federacji Rosyjskiej. Parę lat temu istniał w kraju nad Wisłą podobny periodyk zwany także Haker. Jak wiele pożytecznych bytów i on nie przeżył w warunkach rozwiniętego, acz miłościwie nam panującego czegoś, czego nazwać nie bardzo da się. Takie „ni to pies ni wydra…" by zacytować tu pewnego towarzysza.

W owym periodyku (https://xakep.ru/), opublikowany został artykuł o magazynach danych, bujających w obłokach, zatytułowany „To już nie są twoje dokumenty. Jak „chmurowe" magazyny danych widzi haker". Artykuł jest dość obszerny, i chociaż napisany został w lutym roku minionego, analiza i wnioski ani trochę nie straciły swej aktualności. Autor, Kolchanoff, opisuje swoje najazdy na magazyny Dropbox i Megaupload za pomocą zakupionych w „darkinternetach" danych, skradzionych i otwarcie oferowanych przez rozmaitych łobuzów. Najazdy niektóre, dzięki owym danym, okazały się skuteczne na tyle, że warte były opisania. Autor dokonał rozpoznania cen owych danych i przytoczył średnie, według niego koszty nabycia owoców pracy łobuzów i wnioskuje, że „skórka warta wyprawki" jest.

I tak, średnie notowania:

- (300… 350)$ za 1 milion kombinacji login-hasło lub poczta-hasło, ogólnie,
- (400… 500)$ kosztuje 1 milion kombinacji korporacyjnych skrzynek pocztowych wraz z hasłami do nich. Te dane są kąskiem łakomym dla łobuzów wtórnych.
- Za marne 250$ można natomiast nabyć 1 milion kombinacji w mieszanych bazach, gdzie mogą być dowolne, przypadkowe domeny.

Rynek danych pozyskanych w mniej lub bardziej (nie)legalny sposób jak i narzędzi do „brania sprawy w swoje ręce" przez mniej uzdolnionych adeptów sztuk złodziejskich, prosperuje znakomicie.

Taki złodziej danych jak, dość prymitywny NoF1L3 i jego kolejne mutacje, sprzedawany był po 15$ (NoF1L3; .NET) lub po 45$ (NoF1L3v2; C#) na rozmaitych witrynach typu forum. Kod źródłowy natomiast, kosztował $600. NoF1L3 rabował ciasteczka skrzętnie gromadzone przez przeglądarki (Chrome, Opera, Yandex, Torch, Amiga, Cometa i Orbitum), dane auto uzupełniania (dla l eniwych) formularzy no i, jakże inaczej, hasła. Jeśli ofiara gromadzi kryptowaluty w rodzaju BTC, BCN, DSH, ETH, LTC, XMR czy ZEC to i owe skarbonki podlegały akwizycji. Potem przyszli ludzie poważni i zamknęli „boutique".

Obecnie zaś nabiera rozmachu względnie nowa (utworzona w roku 2018) platforma egzystująca w „ekosystemie" darknet, 2easy, na której, wedle kompanii KELA, (https://ke-la.com/2easy-logs-marketplace-on-the-rise/) oferowane są tzw. logi, czyli masywy danych, skradzionych z przeglądarek zasobów WWW i dziurawych programów przez zastępy „botów" wysyłających do boju żołnierzy w postaci „malware". KELA szacuje iż na 2easy oferowane są obecnie zbiory zgromadzone przez ok. 600000 „botów".

Kluczem do „sukcesu" 2easy, wg KELA, jest żywotność i rozwój platformy oraz stabilna jakość oferowanego „towaru". Jak widać wojna armaty i pancerza w piaskownicy dla dzieci trwa w najlepsze. Poważni ludzie natomiast, mają swoje zabawki i poligony bo zajmują się sprawami poważnymi.

Redakcja DLP

DLP Expert
kwartalnik
numer 3/2021 (38)
październik 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

Tatsuno, światowy producent sprzętu dla branży paliwowej, chroni swoje dystrybutory paliwa przy pomocy rozwiązania firmy Kaspersky

2.07.2021 r. - Tatsuno Corporation, japoński producent dystrybutorów paliwa oraz innych rozwiązań dla klientów działających na globalnym rynku sprzedaży detalicznej paliwa, wybrał rozwiązanie Kaspersky Embedded Systems Security w celu zapewnienia ochrony systemom terminali płatniczych zainstalowanych w swoich dystrybutorach paliwa. Kluczowe korzyści oferowane przez to rozwiązanie obejmują: obsługę systemu Windows XP, wysoki poziom bezpieczeństwa przez długi okres oraz kompatybilność ze sprzętem charakteryzującym się mniejszą wydajnością.

Systemy terminali płatniczych wbudowane w dystrybutory paliwa wytwarzane i sprzedawane przez Tatsuno Corporation przyjmują płatności kartowe. Zagwarantowanie ochrony operacji płatniczych wymaga zastosowania kilku niezawodnych środków i procesów bezpieczeństwa. Obejmują one odpowiednią ochronę zarówno wyspecjalizowanych punktów końcowych (takich jak terminale płatnicze dystrybutorów), jak i sieci, do których są one podłączone, ochronę danych właścicieli kart, mechanizmy kontroli luk w zabezpieczeniach oprogramowania oraz stosowanie metod bezpiecznego dostępu. Niezbędne są również wygodne narzędzia konfiguracji i egzekwowania rygorystycznych zasad bezpieczeństwa oraz okresowe audyty i testy sieci.

Wstępne testy przeprowadzone w Tatsuno wykazały, że Kaspersky Embedded Systems Security, wielopoziomowe rozwiązanie do ochrony wbudowanych urządzeń opartych na systemie

Windows, spełnia wymagania, optymalizując niektóre aspekty dla personelu bezpieczeństwa IT. Ponadto rozwiązanie to działa bezproblemowo na sprzęcie firmy, który posiada ograniczoną pamięć i przestrzeń na dysku. Kaspersky Embedded Systems Security obsługuje system Windows XP i jest odpowiedni dla długiego cyklu życia dystrybutorów paliwa. Pracując z inżynierami z firmy Kaspersky, Tatsuno szybko i sprawnie ukończył testowanie produktu. Rozwiązanie zostało zainstalowane w systemie terminali płatniczych wbudowanym w dystrybutory paliwa Tatsuno w kwietniu 2020 r. i obecnie działa bez zarzutu. Tatsuno planuje również zainstalować je w innych systemach w celu zapewnienia im większego bezpieczeństwa.

Więcej informacji na temat wdrożenia znajduje się na stronie https://r.kaspersky.pl/ApsqY.

Ransomware Qlocker wciąż niebezpieczny – możesz stracić swoje pliki!

5.07.2021 r. - Brak dostępu do firmowych dokumentów, rodzinnych zdjęć i filmów zapisanych na serwerze NAS, a zamiast nich dysk wypełniony spakowanymi plikami 7zip i dokument tekstowy z żądaniem okupu – to oznaki ataku ransomwarem Qlocker. Niestety opcji ratunku jest niewiele. Okup sięga kilku tysięcy złotych, a samodzielne próby rozwiązania problemu mogą jedynie pogorszyć sytuację. W ostatnim czasie eksperci ESET otrzymali kolejne zgłoszenie, tym razem od mieszkańca Poznania, który padł ofiarą ataku.

Problem, z jakim zmierzyła się ofiara wspomnianego zagrożenia szyfrującego, ujawniła potrzeba skorzystania z archiwalnych plików, które znajdowały się na domowym serwerze NAS QNAP. Niestety nie było to możliwe - wszystkie prywatne zdjęcia, filmy, jak i dokumenty firmowe zostały zablokowane. Właściciel serwera nie mógł w żaden sposób dotrzeć do swoich danych, które zostały zaszyfrowane za pomocą archiwizatora 7zip, takiego samego z którego korzysta wielu internautów. Jedynym dostępnym plikiem był dokument tekstowy o nazwie !!!READ_ME.

Jak się okazało cyberprzestępcy wykorzystali dziurę w zabezpieczeniach serwera i zainstalowali ransomware Qlocker, który zaszyfrował wszystkie dane znajdujące się na serwerze. Tego typu sytuacje były nagminne w kwietniu i maju tego roku, natomiast w dalszym ciągu występują. Pomimo, że producent serwerów QNAP przygotował 16 kwietnia 2021 aktualizację, łatającą lukę w zabezpieczeniach, wielu właścicieli serwerów QNAP nadal jej nie zainstalowało.

Chcesz odzyskać pliki, zapłać okup

Po kliknięciu w dokument tekstowy o nazwie !!!READ_ME, wyświetlana jest wiadomość twórców zagrożenia, którzy informują o możliwości przywrócenia zaszyfrowanych plików pod warunkiem zapłacenia okupu w kryptowalucie. Dokument tekstowy zawiera szczegółową instrukcję, w której zawarte są unikalne klucze oraz witryny internetowe umożliwiające zrealizowanie płatności. Atakujący żądają od ofiar kwot sięgających równowartości kilku tysięcy złotych. Eksperci z ESET rekomendują, by okupu nie płacić. Zamiast tego warto skorzystać z porad producenta serwera. Można próbować odzyskać dane na własną rękę, jednak szansa na pomyślność takich działań nie jest duża, a skutkiem nieudanych prób może być uszkodzenie plików i bezpowrotne

ich utracenie. Zamiast tego lepiej poszukać pomocy wśród firm zajmujących się odzyskiwaniem danych. Niestety koszt takiej usługi nierzadko przekracza kwotę okupu.

W opisywanym przypadku na szczęście inne, podłączone do tej samej sieci co serwer, urządzenia nie zostały zainfekowane. Jednocześnie ofiara ataku potwierdziła, że w ostatnim czasie nie otrzymała żadnej podejrzanej wiadomości, a wszelkie inne konta, w tym mailowe, są odpowiednio chronione.

Ransomware REvil: Kaspersky wykrył ponad 5 000 prób ataków w ramach kampanii przeprowadzonej w 22 krajach

6.07.2021 r. - Na początku lipca stało się jasne, że gang ransomware REvil przeprowadził duży atak na dostawców usług zarządzanych (MSP) oraz ich klientów na całym świecie. W rezultacie tysiące firm potencjalnie padło ofiarą oprogramowania ransomware. Badacze z firmy Kaspersky zaobserwowali jak dotąd ponad 5 000 prób infekcji w Europie oraz Ameryce Północnej i Południowej.

Cybergang REvil (znany również jako Sodinokibi) to jedno z „najpłodniejszych" ugrupowań stosujących model ransomware jako usługa (RaaS). Pojawiło się ono w 2019 roku, natomiast rozgłos zyskało w ostatnich kilku miesiącach ze względu na atakowane cele oraz rekordowe zarobki osiągane w wyniku żądania okupu. W ostatnim ataku gang REvil zainfekował dostawcę oprogramowania do zarządzania usługami IT przeznaczonego dla dostawców usług zarządzanych, a jego skutki odczuło wiele firm na całym świecie. Cyberprzestępcy zainstalowali szkodliwą funkcję poprzez skrypt PowerShell, który z kolei został prawdopodobnie wykonany za pośrednictwem oprogramowania dostawcy usług zarządzanych.

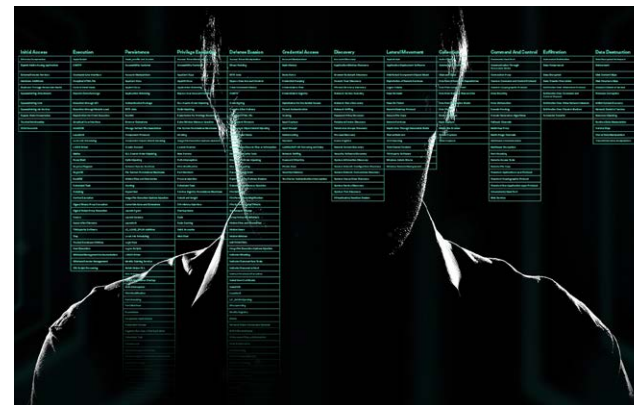
Skrypt wyłączył funkcje ochrony narzędzia Microsoft Defender for Endpoint, a następnie zdekodował szkodliwy plik wykonywalny, który zawierał legalny plik binarny firmy Microsoft, starszą wersję rozwiązania Microsoft Defender oraz szkodliwą bibliotekę zawierającą ransomware REvil. Przy pomocy tej kombinacji komponentów w module ładującym atakujący zdołali wykorzystać technikę ładowania pośredniego biblioteki DLL oraz zaatakować wiele organizacji.

Przy pomocy swojej usługi Threat Intelligence Service firma Kaspersky zaobserwowała ponad 5 000 prób ataków w 22 państwach, najwięcej we Włoszech (45,2% odnotowanych prób ataków), Stanach Zjednoczonych (25,91%), Kolumbii (14,83%), Niemczech (3,21%) oraz Meksyku (2,21%).

Szczegóły techniczne dotyczące najnowszych ataku cybergangu REvil są dostępne na stronie https://r.kaspersky.pl/VcHjl.

Wieloplatformowe szkodliwe oprogramowanie ugrupowania WildPressure atakuje systemy macOS na Bliskim Wschodzie

7.07.2021 r. - Od sierpnia 2019 roku badacze z firmy Kaspersky obserwują Milum – trojana wykorzystywanego przez zaawansowany cybergang WildPressure działający na Bliskim Wschodzie. Badając jeden z najnowszych ataków wymierzony w sektor przemysłowy, eksperci odkryli nowsze wersje szkodnika Milum, napisane w innych językach programowania. Jedna z nich potrafi infekować i uruchamiać się zarówno w systemach Windows, jak i macOS.



Wiele odkryć dokonywanych podczas wyszukiwania zagrożeń zaczyna się od drobnego tropu – tak było również w przypadku opisywanej kampanii. Po zainfekowaniu urządzenia trojan często wysyła do serwerów cyberprzestępców sygnał nawigacyjny, który zawiera informacje o urządzeniu, ustawieniach sieci, nazwie użytkownika oraz inne istotne dane. Dzięki temu atakujący mogą stwierdzić, czy są zainteresowani zainfekowanym urządzeniem. Milum przesyłał dodatkowo informacje dotyczące języka programowania, w którym został napisany. Dlatego analizując tę kampanię po raz pierwszy w 2020 roku, badacze z firmy Kaspersky podejrzewali, że istnieją różne wersje tego trojana napisane w różnych wersjach językowych. Teraz ta teoria okazała się słuszna.

Wiosną 2021 roku firma Kaspersky zidentyfikowała nowy atak cybergangu WildPressure, przeprowadzony przy użyciu zestawu nowszych wersji szkodliwego oprogramowania Milum. Wykryte pliki zawierały trojana napisanego w języku C++ oraz odpowiadający mu wariant w języku Visual Basic Script (VBScript). Dalsze dochodzenie ujawniło kolejną wersję szkodnika w języku Python, która została przygotowana zarówno dla systemu operacyjnego Windows, jak i macOS. Wszystkie trzy wersje trojana potrafiły pobierać i wykonywać polecenia operatora, gromadzić informacje oraz aktualizować się do nowszej wersji.

Wieloplatformowe szkodliwe oprogramowanie potrafiące infekować urządzenia działające w systemie macOS należy do rzadkości. Po zainfekowaniu urządzenia szkodnik uruchamia kod zależny od systemu operacyjnego w celu przetrwania w atakowanej maszynie oraz gromadzenia danych. Trojan potrafi również sprawdzić, czy na urządzeniu działają rozwiązania bezpieczeństwa.

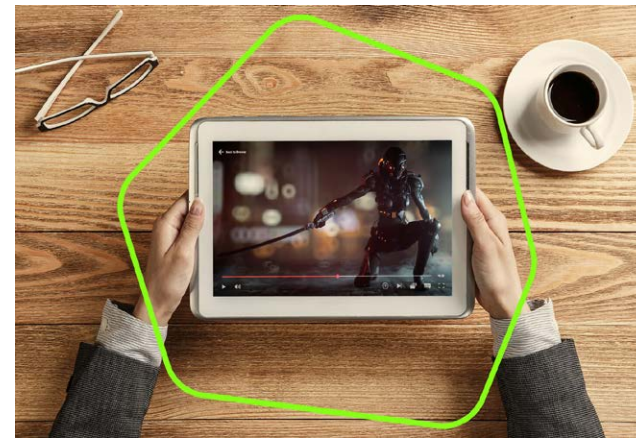
„W kręgu zainteresowania ugrupowania WildPressure pozostaje ten sam obszar geograficzny. Twórcy szkodliwego oprogramowania rozwijają podobne narzędzia w wielu językach prawdopodobnie w celu utrudnienia wykrycia ich. Strategia ta nie jest unikatowa wśród zaawansowanych cybergangów, jednak rzadko obserwujemy szkodliwe oprogramowanie dostosowane do działania w dwóch systemach jednocześnie. Inna ciekawostka to fakt, że jednym z atakowanych systemów operacyjnych jest macOS, co może być zaskakujące, biorąc pod uwagę geograficzny obszar zainteresowania tego ugrupowania" – powiedział **Denis Legezo**, starszy badacz ds. cyberbezpieczeństwa z Globalnego Zespołu ds. Badań i Analiz (GReAT) firmy Kaspersky.

Szczegóły techniczne dotyczące nowych próbek szkodliwego oprogramowania ugrupowania WildPressure są dostępne na stronie https://r.kaspersky.pl/Xc6ZQ.

Jakiś czas temu Denis Legezo poprowadził warsztat online, w którym zaprezentował, w jaki sposób można przeprowadzić inżynierię wsteczną próbek szkodliwego oprogramowania ugrupowania WildPressure. Zapis warsztatu można obejrzeć na stronie https://r.kaspersky.pl/uWBTx.

Wzrasta oszukańcza aktywność tuż przed premierą długo oczekiwanego filmu o superbohaterce

8.07.2021 r. - Po kilkukrotnej zmianie daty premiery z powodu pandemii świat w końcu będzie mógł obejrzeć długo oczekiwany film pt. „Czarna Wdowa". W obliczu restrykcji nałożonych w związku z koronawirusem organizatorzy zdecydowali się na istotny krok – premiera Czarnej Wdowy odbędzie się jednocześnie w kinach oraz serwisach streamingowych. Badacze z firmy Kaspersky informują, że przeniesienie premiery do internetu wzmogło zainteresowanie tym filmem nie tylko wśród kinomaniaków, ale również oszustów.



Aby dowiedzieć się, w jaki sposób cyberprzestępcy próbują zarobić na fanach kina superbohaterskiego, eksperci z firmy Kaspersky przeanalizowali szkodliwe pliki podszywające się pod film Czarna Wdowa, jak również związane z filmem strony phishingowe przygotowane w celu kradzieży danych uwierzytelniających użytkowników.

W efekcie eksperci zauważyli nagłe wzrosty liczby prób cyberataków zbiegające się z ogłaszanymi kolejno datami premiery filmu, a mianowicie: 1 maja 2020 r., 7 maja, 9 maja 2021 r. oraz w czerwcu i lipcu 2021 r.

Eksperci z firmy Kaspersky wykryli również wiele stron phishingowych przygotowanych przez cyberprzestępców w celu kradzieży danych uwierzytelniających widzów. Chcąc obejrzeć długo oczekiwany film, użytkownicy odwiedzali stronę internetową, na której mogli zobaczyć kilka pierwszych minut produkcji, po czym, aby kontynuować oglądanie, musieli się zarejestrować. Podczas rejestracji proszono ich o podanie szczegółów dotyczących karty płatniczej w celu potwierdzenia miejsca zamieszkania. Po upływie pewnego czasu z karty były pobierane pieniądze, jednak – jak można się spodziewać – filmu nie można było obejrzeć. Tego rodzaju phishing jest szeroko rozpowszechniony i uznawany za jeden z najpopularniejszych wśród oszustów.

Cyberprzestępcy coraz bardziej interesują się grami wideo

9.07.2021 r. - W 2020 roku, gdy państwa na całym świecie zmuszone były wprowadzić lockdown, gwałtownie wzrosła liczba graczy, co naturalnie przyciągnęło uwagę cyberprzestępców, którzy szukali sposobów wykorzystania tego trendu dla osobistych korzyści. Badacze z firmy Kaspersky przyjrzeli się ewolucji tych zagrożeń na przestrzeni półtora roku.

Wiosną ubiegłego roku badacze z firmy Kaspersky zidentyfikowali znaczący wzrost liczby wykrytych przez technologię ochrony WWW stron internetowych, których nazwy nawiązywały do popularnych gier i platform: w kwietniu 2020 r. liczba zablokowanych w ciągu jednego dnia przekierowań zwiększyła się o 54% w stosunku do stycznia 2020 r.

Liczba ataków wykorzystujących temat gier nadal rosła mimo złagodzenia obostrzeń wiosną, osiągając w listopadzie 2020 r. rekordową wartość niemal 2 500 000. Po odnotowanym na po-

czątku 2021 r. spadku liczba ataków zwiększyła się po raz kolejny, osiągając w kwietniu 2021 r. wartość 1 125 010, co stanowi wzrost o 34% w porównaniu z marcem tego roku.

Podobnie jak w ubiegłym roku, najpopularniejszą grą wykorzystywaną jako przynęta jest Minecraft, chociaż powoli wyprzedza ją Counter Strike: Global Offensive. Znaczący wzrost pod względem występowania w roli wabika odnotowała latem 2020 r. gra Dota. Najpowszechniejszymi zagrożeniami rozpowszechnianymi poprzez szkodliwe odnośniki wykorzystujące temat gier były rozmaite trojany, czyli szkodliwe programy, które pozwalają cyberprzestępcom wykonywać wszelkie czynności, od kasowania i blokowania danych po zakłócanie działania komputera, przy czym szkodniki podszywały się pod darmowe wersje, aktualizacje lub rozszerzenia popularnych gier, jak również tzw. cheaty pozwalające modyfikować gry, by były mniej wymagające.

Szczegóły techniczne dotyczące cyberataków związanych z grami znajduje się na stronie https://r.kaspersky.pl/R8A8w.

Phishing w komunikatorach internetowych

13.07.2021 r. - Badacze z firmy Kaspersky przyjrzeli się atakom phishingowym przeprowadzanym z użyciem komunikatorów na urządzeniach z Androidem. Najwięcej szkodliwych odsyłaczy wykrytych w okresie od grudnia 2020 r. do maja 2021 r. wysłano za pośrednictwem aplikacji WhatsApp (89,6%) oraz Telegram (5,6%). Na trzecim miejscu znalazł się Viber (z udziałem 4,7%) oraz Hangouts (z udziałem poniżej jednego procenta). Wśród państw z najwyższą liczbą ataków phishingowych znalazła się Rosja (46%), Brazylia (15%) oraz Indie (7%). Na całym świecie odnotowywano 480 prób ataków dziennie.

Według badań[1] w 2020 r. komunikatory internetowe wyprzedziły portale społecznościowe o 20%, stanowiąc najpopularniejsze narzędzie komunikacji. Liczba użytkowników komunikatorów na całym świecie wynosiła 2,7 miliarda[2] i – według prognoz – do końca 2023 r. zwiększy się do 3,1 miliarda. Stanowi to niemal 40% ludności na świecie.

Niedawno rozwiązanie Kaspersky Internet Security for Android zostało wzbogacone o nową funkcję „Bezpieczna komunikacja", która chroni użytkowników przed otwarciem szkodliwych odsyłaczy otrzymanych za pośrednictwem komunikatorów internetowych (WhatsApp, Viber, Telegram, Hangouts) oraz wiadomości SMS. Dzięki temu firma Kaspersky mogła przeanalizować zanonimizowane kliknięcia odsyłaczy phishingowych w różnych komunikatorach internetowych i stwierdzić, że w okresie od grudnia 2020 r. do maja 2021 r. na całym świecie zarejestrowano 91 242 wykryć tego rodzaju zagrożeń.

Według statystyk rozwiązanie Kaspersky Internet Security for Android wykryło najwięcej szkodliwych odsyłaczy w komunikatorze WhatsApp, częściowo dlatego, że stanowi on najpopularniejszy[3] komunikator na świecie. Największy odsetek takich wiadomości wykryto w Rosji (42%), Brazylii (17%) oraz Indiach (7%).

Wśród użytkowników aplikacji Kaspersky Internet Security for Android najmniej kliknięć odsyłaczy phishingowych odnotował Telegram, ale pod względem rozkładu geograficznego przypominał WhatsAppa. Najwięcej szkodliwych odsyłaczy wykryto w Rosji (56%), Indiach (6%) oraz Turcji (4%). Z danych statystycznych wynika, że komunikatory Viber i Hangouts odnotowały mniej wykryć. Główna różnica między nimi dotyczy ich rozkładu geograficznego. Najwięcej wykryć w komunikatorze Viber odnotowano w Rosji (89%) oraz krajach Wspólnoty Niepodległych Państw – Ukrainie (5%) oraz Białorusi (2%), podczas gdy większość wykrytych linków w komunikatorze Hangouts pochodziło ze Stanów Zjednoczonych (39%) oraz Francji (39%).

Pod względem liczby ataków phishingowych na jednego użytkownika w komunikatorze WhatsApp na prowadzeniu znalazła się Brazylia (177) oraz Indie (158). Jednocześnie użytkownicy rosyjscy przodowali pod względem liczby wykryć takich zagrożeń na komunikatorze Viber (305) oraz Telegram (79).

[1] *https://spectrm.io/insights/blog/messaging-app-statistics-most-popular-communication-method-2020/*

[2] *https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/*

[3] *https://backlinko.com/whatsapp-users*

Cyberprzestępcy przejmują konta i wyłudzają pieniądze – na celowniku użytkownicy Facebooka i Instagrama

14.07.2021 r. - Twój znajomy publikuje w mediach społecznościowych emocjonalny post nt. wypadku czy choroby bliskich i prosi Cię o wsparcie finansowe lub szybki przelew BLIKIEM? Uważaj, bo jego konto mogło zostało przejęte, a Ty masz do czynienia z cyberprzestępcami. W ostatnim czasie badacze ESET dostrzegli nowe przypadki oszustw, które wykorzystują skradzione konta do wyłudzania pieniędzy. Jak informują eksperci ds. cyberbezpieczeństwa, większość ofiar mogłaby uniknąć zagrożenia, gdyby używała uwierzytelniania wieloskładnikowego.

Od lat sukcesywnie przybywa kont na Instagramie i Facebooku. Z pierwszej platformy korzysta ponad miliard użytkowników, a z drugiej blisko 3 miliardy. To skala, która powoduje, że media społecznościowe niezmiennie pozostają obiektem zainteresowania cyberprzestępców. Wśród ostatnich obserwacji, badań i analiz ekspertów ESET szczególną uwagę zwrócił przypadek pewnego użytkownika Instagrama ze Stanów Zjednoczonych, którego konto zostało skradzione, a następnie wykorzystane w celu wyłudzenia pieniędzy od obserwujących go osób. Uwagę nieświadomego użytkownika zwróciły telefony oraz wiadomości zaniepokojonych znajomych, którzy dopytywali o nowy wpis na Instagramie. Jak się wkrótce okazało, na profilu ofiary pojawił się post informujący o wypadku samochodowym, w którym rzekomo ucierpiała jego mama. Oszuści, podszywając się pod użytkownika, prosili o pieniądze, które pomogą sfinansować kosztowną operację. Chociaż o kradzieży konta dowiedział się bardzo szybko, to niestety na jakiekolwiek działania prowadzące do odzyskania profilu było już za późno, ponieważ wszelkie hasła zostały zmienione przez hakerów. Jak się później okazało, konto zostało również powiązane z innym adresem mailowym, co skutecznie uniemożliwiło ofierze odzyskanie profilu.

Coraz śmielsze metody oszustów

To co wyróżnia ten przypadek, to silny aspekt psychologiczny bazujący bez skrupułów na emocjach użytkowników mediów społecznościowych. Umieszczony przez oszustów film w Instastories przedstawiał oddział intensywnej terapii z płaczącym kobiecym głosem w tle. Na nagraniu nie było widać żadnych osób i nie można było w żaden sposób zidentyfikować szpitala, ale wielu obserwujących profil uważało, że na nagraniu słychać głos ich znajomego - co najmniej dwóch z nich wysłało pieniądze oszustom na wskazany w poście rachunek bankowy. Ponadto przestępcy odpowiadali w imieniu użytkownika w wiadomościach bezpośrednich. Jedna z osób obserwujących profil ofiary, która przekazała oszustom 30 dolarów, otrzymała odpowiedź: „Przepraszam, że nalegam, ale czy możesz mi pożyczyć jeszcze 40 dolarów do jutra?" – dopiero w tym momencie, znajoma ofiary uznała, że ma do czynienia z oszustwem.

Znajomy na Facebooku prosi o kod BLIK?

W ostatnim czasie, także polscy użytkownicy Facebooka mogli otrzymać wiadomość od znajomego, który zwraca się z prośbą o szybką pożyczkę za pomocą BLIK-a. W tym przypadku oszuści posługują się przejętymi kontami na Facebooku i wysyłają wiadomości do znajomych ofiary – prośba najczęściej dotyczy zagubionego portfela i związanej z tym potrzeby pożyczenia pieniędzy. Niestety dzięki tej metodzie, w momencie przekazania kodu BLIK, ofiara ma bardzo nikłe szanse na odzyskanie pieniędzy. Oszust może w bardzo szybki sposób pobrać pieniądze z bankomatu i po prostu zniknąć. Jak podaje śląska Policja, takich przypadków w Polsce jest sporo, dlatego tym bardziej należy zwracać uwagę na poziom zabezpieczeń swoich kont na portalach społecznościowych.

Wyciekła lista 50 000 ofiar Pegasusa

18.07.2021 r. - W lipcu tego roku dziennikarze 17 redakcji rozpoczęli publikację serii artykułów opisujących wspólne śledztwo dotyczące Pegasusa[4] — narzędzia do inwigilacji smartfonów, sprzedawanego przez izraelską firmę NSO agencjom rządowym różnych krajów, w tym polskiemu CBA[5]. Reporterzy pozyskali listę 50 000 numerów telefonów osób, które były na celowniku Pegasusa.

Najpełniejszy raport techniczny dotyczący tego, na czym polegały różne warianty ataków, opublikowała Amnesty International[6]. Poniżej prezentujemy aspekty wybrane przez redaktorów Niebezpiecznika.

Pegasus korzysta z nieznanych producentom smartfonów i aplikacji błędów i jest w stanie przejąć kontrolę zarówno nad najnowszymi iPhonami (iOS 14.6), jak i smartfonami z Androidem. Nie zawsze ofiara musi kliknąć link — czasem wystarczy, że po prostu odbierze wiadomość w konkretnej aplikacji (np. WhatsApp, iMessage, a nawet w... Apple Music!). Co więcej, kolejny raz udowodniono, że nie jest prawdą, iż to narzędzie jest wykorzystywane tylko do walki z terrorystami i „poważnymi" przestępcami. Na liście celów znaleźli się niewygodni dla poszczególnych krajów dziennikarze, aktywiści, a nawet prawnicy.

Listę 50 000 numerów telefonów osób, które były na celowniku Pegasusa, pozyskali dziennikarze pracujący dla Forbidden Stories i Amnesty International. Podzielili się nią z wybranymi mediami na całym świecie i rozpoczęli publikację serii artykułów obnażających hipokryzję zarówno NSO, producenta Pegasusa, jak i kłamstwa poszczególnych jego klientów, czyli rządów ok. 40 krajów.

Do tej pory nie ujawniono pełnej listy numerów. Jednak jeśli czyjś numer się na niej znajduje, to nie oznacza to, że został faktycznie zainfekowany Pegasusem i w istocie był inwigilowany,

ale z dużym prawdopodobieństwem próbowano go zainfekować. Nie wiadomo, kto przekazał dziennikarzom tę listę ani jak zebrał numery. Niektórzy sugerują, że lista pochodzi z logów usługi HLR, którą wykorzystywało oprogramowanie NSO.

Dziennikarze sprawdzili smartfony 67 celów; na urządzeniach ponad połowy z tych osób znaleźli ślady Pegasusa. Infekcję potwierdzono na 23 urządzeniach, a próby infekcji na 14 kolejnych. Jak podkreślają redaktorzy Niebezpiecznika, infekcję łatwiej jest wykryć na urządzeniach Apple, ponieważ Android nie loguje wszystkiego. Ponad 1000 numerów celów należy do osób z Europy[7]. Aż 180 celów to dziennikarze takich redakcji jak New York Times, Wall Street Journal, Bloomberg, Al Jazeera, Radio Free Europe, El Pais, Le Monde, Reuters, Associated Press, Economist czy France 24.

Część zainfekowanych Pegasusem dziennikarzy została zamordowana. Poza dziennikarzami na liście celów były numery biznesmenów, przywódców duchowych, pracowników naukowych, działaczy sektora NGO, związkowców, urzędników państwowych (w tym premierów i ministrów), a także rodziny przywódcy jednego z państw.

[4] *https://niebezpiecznik.pl/post/pegasus-infekcja-telefonia-komorkowa/*

[5] *https://niebezpiecznik.pl/post/jak-wyglada-rzadowy-trojan-pegasus-od-srodka/*

[6] *https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/*

[7] *https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus*

Co dziesiąty incydent naruszenia cyberbezpieczeństwa w firmach jest uznawany za poważny

kaspersky **21.07.2021 r. - Ze zanonimizowanych metadanych dostarczonych dobrowolnie przez klientów usługi Kaspersky MDR wynika, że jeden na dziesięć (9%) możliwych do uniknięcia incydentów naruszenia cyberbezpieczeństwa może spowodować poważne zakłócenia lub nieautoryzowany dostęp do zasobów klienta. Przeważająca większość incydentów (72%) miała średni poziom krytyczności. To oznacza, że zagrożenia te, gdyby nie zostały wykryte przez technologie bezpieczeństwa, wpłynęłyby na wydajność zasobów lub mogłyby doprowadzić do nadużycia danych.**

Cyberataki stają się coraz bardziej złożone i wykorzystują techniki pozwalające uniknąć wykrycia przez podstawowe rozwiązania bezpieczeństwa. Wykrywanie takich zagrożeń i zapobieganie im to zadanie dla zaawansowanych specjalistów zajmujących się wyszukiwaniem zagrożeń, którzy potrafią dostrzec podejrzane działania, zanim wyrządzą szkodę firmie. Firma Kaspersky przeanalizowała zanonimizowane incydenty zidentyfikowane przy pomocy usługi Kaspersky MDR w IV kwartale 2020 r. w celu ustalenia, jak szeroko rozpowszechnione oraz krytyczne były wykryte incydenty.

Badanie wykazało, że niemal każda branża, z wyjątkiem mediów oraz transportu, odnotowała w analizowanym okresie krytyczne incydenty. Najczęściej dotyczyły one organizacji z sektora publicznego (41% wszystkich wykrytych krytycznych incydentów dotyczyło tej branży), branży IT (15%) oraz finansowej (13%).

Niemal jedną trzecią (30%) takich krytycznych incydentów stanowiły ataki ukierunkowane wykorzystujące czynnik ludzki. Prawie jedną czwartą (23%) – infekcje przy użyciu newralgicznego szkodliwego oprogramowania, w tym ransomware. W 9% przypadków cyberprzestępcy zdobyli dostęp do firmowej infrastruktury IT przy użyciu socjotechniki, wykorzystując braki wiedzy personelu atakowanych firm w zakresie podstawowych zasad cyberhigieny.

Eksperci z firmy Kaspersky zauważyli również, że aktualne zaawansowane ataki APT są zwykle wykrywane wraz z pozostałościami po wcześniejszych skomplikowanych działaniach cyberprzestępców. To sugeruje, że jeśli organizacja reaguje na atak, często pada ofiarą ponownych szkodliwych działań, prowadzonych najprawdopodobniej przez tego samego sprawcę. Ponadto w organizacjach, które doświadczyły ataków APT, eksperci często identyfikowali ślady symulacji zachowania antagonistycznego, takiego jak atakowanie własnej organizacji w celu wykrycia jej słabości oraz podatności czy ocena operacyjnych możliwości zabezpieczeń firmy poprzez symulację wyrafinowanych ataków.

Pełny raport wykorzystany w tej informacji prasowej jest dostępny na stronie https://r.kaspersky.pl/u85fv.

Piąte urodziny inicjatywy No More Ransom pomagającej w walce z ransomware

kaspersky **28.07.2021 r. - Mija pięć lat od powstania inicjatywy „No More Ransom", która została uruchomiona w 2016 r. przez organy ścigania oraz firmy z branży bezpieczeństwa IT, m.in. Kaspersky, aby pomóc ofiarom oprogramowania ransomware odzyskać swoje dane. Efekty inicjatywy można podsumować następującymi liczbami: ponad 900 milionów dolarów udaremnionych nielegalnych zysków oraz ponad 6 milionów osób, które pobrały bezpłatne narzędzia deszyfrujące.**

Ransomware to rodzaj szkodliwego oprogramowania, które blokuje dostęp do cennych danych użytkowników (zwykle przy użyciu szyfrowania) i pozwala sprawcom zażądać okupu od ofiary w zamian za odzyskanie dostępu do zablokowanych informacji. W ostatnich latach oprogramowanie ransomware rozpowszechniło się bardzo szeroko, wyrządzając ogromne szkody zarówno użytkownikom prywatnym, jak i organizacjom na całym świecie.

W 2016 roku jednostka holenderskiej policji krajowej zajmująca się zwalczaniem przestępczości związanej z technologią zaawan-

sowaną, Europejskie Centrum ds. Walki z Cyberprzestępczością w ramach Europolu oraz firmy Kaspersky i McAfee postanowiły wspólnie stworzyć serwis internetowy, aby wesprzeć ludzi i organizacje w walce z oprogramowaniem ransomware. Zasób ten miał pomóc ofiarom ataków ransomware odzyskać zaszyfrowane dane bez płacenia okupu przestępcom. W tym celu uczestnicy inicjatywy publikują bezpłatne narzędzia do deszyfracji, które mogą pomóc ofiarom określonych rodzin oprogramowania ransomware odzyskać swoje dane bez spełniania żądań okupu. Ponadto strona zawiera porady dotyczące zapobiegania temu zagrożeniu oraz instrukcje dotyczące zgłaszania cyberprzestępstwa w danym kraju.

Od momentu uruchomienia inicjatywy liczba jej partnerów zwiększyła się z czterech do ponad 170, a użytkownikom udostępniono 121 narzędzi deszyfrujących. Pomagają one w walce ze 150 rodzinami oprogramowania ransomware i w ciągu ostatnich pięciu lat zostały pobrane przez około sześć milionów osób. Według danych No More Ransom uczestnicy tej inicjatywy przeszkodzili cyberprzestępcom w zdobyciu ponad 900 milionów dolarów nielegalnych zysków.

Firma Kaspersky – jako jeden z założycieli inicjatywy – dostarczyła pięć narzędzi deszyfrujących, które pomogły odzyskać dane zaszyfrowane przez 32 rodziny oprogramowania ransomware. Począwszy od 2016 r. narzędzia te zostały pobrane ponad 150 000 razy.

Informacje przydatne w walce z oprogramowaniem ransomware oraz dalsze szczegóły dotyczące inicjatywy No More Ransom są dostępne na stronie https://www.nomoreransom.org/pl/index.html.

Ataki DDoS w II kwartale 2021 r.: Polska po raz pierwszy w pierwszej trójce atakowanych krajów

29.07.2021 r. - W drugim kwartale 2021 r. łączna liczba ataków DDoS zmniejszyła się o 38,8% w porównaniu z analogicznym okresem 2020 r. oraz o 6,5% w stosunku do pierwszych trzech miesięcy bieżącego roku. Chiny znalazły się na pierwszym miejscu zestawienia krajów z największą liczbą serwerów, z których przeprowadzano ataki na urządzenia Internetu Rzeczy. Pierwsze miejsce na liście najczęściej atakowanych krajów zajęły Stany Zjednoczone, przed Chinami i – po raz pierwszy w historii – Polską. Najdłuższy atak DDoS w drugim kwartale 2021 r. trwał aż 776 godzin (ponad 32 dni).

W ostatnim czasie cyberprzestępcy szukali różnych sposobów na wzmocnienie ataków DDoS. Widocznym trendem jest także wykorzystywanie luk w zabezpieczeniach w celu atakowania serwerów DNS. Prowadziło to w szczególności do zakłócenia działania usług Xbox Live, Microsoft Teams, OneDrive oraz innych rozwiązań chmurowych firmy Microsoft. Ofiarą ataków DDoS padli również dostawcy usług internetowych.

II kwartał można ogólnie określić jako stosunkowo spokojny. Średnia liczba ataków DDoS wynosiła od 500 do 800 dziennie. W najspokojniejszym dniu odnotowano 60 ataków, z kolei w najbardziej intensywnym — 1164.

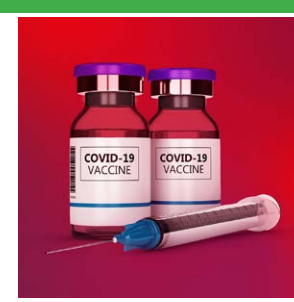
Zmiany nastąpiły w rozkładzie geograficznym ataków DDoS. Liderem pod względem liczby ataków DDoS zostały po raz kolejny Stany Zjednoczone (36%). Z kolei Chiny (10,2%), które do tego roku regularnie zajmowały pierwsze miejsce, nadal tracą przewagę – ich udział w liczbie ataków zmniejszył się o 6,3%. Na trzecim miejscu znalazła się Polska (6,3%) – nowość w rankingu – której udział w liczbie ataków zwiększył się z 2,01% do 6,34%. Na czwartej pozycji uplasowała się Brazylia, której udział zwiększył się niemal dwukrotnie i wynosił 6%. Kanada (5,2%), która wcześniej zamknęła pierwszą trójkę, spadła na piątą pozycję.

Eksperci z firmy Kaspersky zbadali również, gdzie znajdowały się boty i szkodliwe serwery atakujące urządzenia Internetu Rzeczy w celu rozszerzenia sieci zainfekowanych urządzeń (tzw. botnetów). Stwierdzono, że większość urządzeń przeprowadzających ataki znajdowała się w Chinach (31,8%), na drugim miejscu uplasowały się Stany Zjednoczone (12,5%), z kolei na trzecim Niemcy (5,9%).

Pełny raport firmy Kaspersky poświęcony ewolucji ataków DDoS w II kwartale 2021 r. jest dostępny na stronie https://r.kaspersky.pl/N7q2J.

Od wybuchu pandemii badacze z firmy Kaspersky zidentyfikowali ponad 5 000 stron phishingowych związanych z COVID-19

2.08.2021 r. - Aby lepiej zrozumieć, w jaki sposób oszuści wykorzystują obecne wyzwanie epidemiologiczne, eksperci z firmy Kaspersky przeanalizowali wiadomości spamowe związane z pandemią oraz strony phishingowe przygotowane przez cyberprzestępców w celu kradzieży danych uwierzytelniających użytkowników. Od marca 2020 r. do lipca 2021 r. technologie firmy Kaspersky udaremniły ponad milion prób odwiedzenia takich stron przez użytkowników.



Do najczęstszych oszustw stosowanych przez cyberprzestępców należą fałszywe oferty płatności oraz testy na COVID-19 oferowane po niższej cenie. Ostatnio popularne stały się phishingowe reklamy sfałszowanych kodów QR mających udawać certyfikaty szczepień.

Aktywność oszustów związana z pandemią osiągnęła punkt szczytowy w marcu 2021 r. W czerwcu badacze z firmy Kaspersky zaobserwowali niewielki spadek, jednak niedługo potem cyberprzestępcy zintensyfikowali swoje wysiłki. W tym miesiącu produkty firmy Kaspersky wykryły i zablokowały o 14% więcej stron phishingowych związanych z pandemią niż w maju.

Spam i phishing w II kwartale 2021 r.: fałszywe powiadomienia od kurierów i spam na Whatsappie

5.08.2021 r. - Badacze z firmy Kaspersky przyjrzeli się ewolucji spamu i phishingu w drugim kwartale bieżącego roku. Od ponad roku oszuści intensywnie wykorzystują chaos związany z przesyłkami[8], aby skłonić użytkowników do otwarcia odnośników w phishingowych wiadomościach e-mail. W minionym kwartale trend ten utrzymał się. Co więcej, cyberprzestępcy stali się bieglejsi w tłumaczeniu swoich treści spamowych na różne języki. Wzrosła liczba fałszywych faktur, które były wystawiane na całym świecie i dotyczyły wszelkich płatności, od cła po koszty wysyłki. W przypadku takich wiadomości ofiary były często przekierowywane na fałszywą stronę internetową, gdzie mogły nie tylko stracić pieniądze, ale również ujawnić swoje dane dotyczące karty kredytowej.

Cyberprzestępcy uruchamiali również strony internetowe oferujące możliwość kupienia przesyłek, które nie dotarły do odbiorcy. Użytkownicy nie wiedzieli, co znajduje się w danej przesyłce. Licytowali na podstawie ciężaru paczki. Jednak po zapłaceniu zwycięskiej stawki nigdy nie otrzymali swojej „wygranej".

Inna nowa sztuczka stosowana przez oszustów w minionym kwartale dotyczyła spamu wysyłanego do użytkowników komunikatora WhatsApp z żądaniem niewielkiej kwoty. Stosowano kilka różnych scenariuszy. W jednym z nich użytkowników proszono o wzięcie udziału w ankiecie dotyczącej aplikacji WhatsApp oraz wysłanie wiadomości do kilku kontaktów w celu otrzymania nagrody. W innym scenariuszu użytkownicy dowiadywali się, że wygrali pokaźną nagrodę – musieli jedynie zapłacić niewielką kwotę, aby ją odebrać.

W jeszcze innym oszustwie wykorzystano debatę wokół nowej polityki prywatności aplikacji WhatsApp, która zezwala na wymianę informacji z Facebookiem. Cyberprzestępcy tworzyli fałszywe strony internetowe, na których zapraszali użytkowników do czatu na WhatsAppie z „pięknymi nieznajomymi". W rzeczywistości po kliknięciu odsyłacza prowadzącego do czatu ofiara trafiała na fałszywą stronę logowania do Facebooka – potencjalnie ujawniając na niej swoje informacje osobowe. Użytkownicy otrzymywali również odsyłacze do fałszywych aplikacji podszywających się pod WhatsAppa, co wiązało się z ryzykiem pobrania szkodliwego oprogramowania.

Pełny raport firmy Kaspersky poświęcony ewolucji spamu i phishingu w II kwartale 2021 r. jest dostępny na stronie https://r.kaspersky.pl/SkJXp.

[8] *https://plblog.kaspersky.com/covid-fake-delivery-service-spam-phishing/13393/*

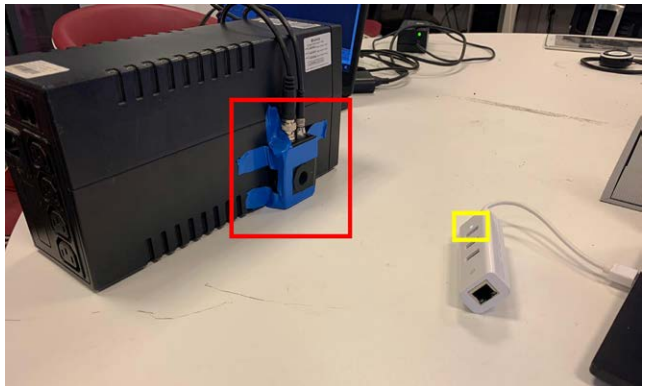
Podsłuchiwanie przez diodę zasilania

10.08.2021 r - Podsłuchiwanie dźwięku poprzez analizę wizualną to dość popularny temat akademickich badań nad bezpieczeństwem. Badacze z Centrum Cyberbezpieczeństwa Uniwersytetu Ben-Guriona donoszą o kolejnym osiągnięciu określanym jako „Glowworm attack". Nazwa łączy w sobie angielskie wyrazy oznaczające robaka i świecenie, co w tym przypadku jest bardzo trafne. O sprawie szerzej napisał portal Niebezpiecznik.

Metoda ataku opiera się na fakcie, że zmiany w poborze energii powodują nieznaczne (niewidoczne gołym okiem) zmiany w intensywności świecenia diod zasilania. Uchwycenie i analiza tych fluktuacji pozwala na rekonstrukcję dźwięku odtwarzanego z urządzenia, jednak nagranie zwykłą kamerą tu nie wystarczy — do ataku należy użyć teleskopu z zamontowanym czujnikiem elektrooptycznym oraz systemu odzyskiwania dźwięku składającego się z przetwornika analogowo-cyfrowego i laptopa z oprogramowaniem do modyfikacji sygnału. Warto podkreślić, że Glowworm nie wymaga wcześniej przygotowanego słownika, modeli matematycznych ani sieci neuronowych.

Zanim naukowcy dokonali testowych ataków, uważnie sprawdzili, czy fluktuacje diod zasilania naprawdę odpowiadają odtwarzanym dźwiękom (mogły na nie wpływać np. zakłócenia elektromagnetyczne z pobliskich urządzeń). Na tym etapie jeszcze nie używano teleskopów, a jedynie sensora skierowanego na badane urządzenie. Testowano m.in. głośniki JBL i Creative, rozdzielacze USB i Raspberry Pi.

Następnie przeprowadzono inne testy, np. w całkowitej ciszy, ze sygnałami świergotowymi, ludzką mową itd. Eksperymenty pozwoliły zauważyć m.in., że na niektórych urządzeniach tylko część częstotliwości uwidacznia się w sygnale optycznym. Badaczom udało się ustalić, jaki jest związek między fluktuacjami diod a głośnością odtwarzania. Opracowano metody poprawiania otrzymanego sygnału poprzez filtrowanie niektórych częstotliwości, obniżanie wysokości dźwięku (zidentyfikowano problem z jej zawyżaniem), wzmacnianie częstotliwości typowych dla ludzkiej mowy, odszumianie itd. Atak Glowworm nie wymaga użycia sieci neuronowych, a naukowcy nie wykluczają opracowania specjalnego sprzętu, który mógłby bez udziału laptopa prze-



twarzać sygnały z diod na dźwięk w czasie rzeczywistym z minimalnym opóźnieniem.

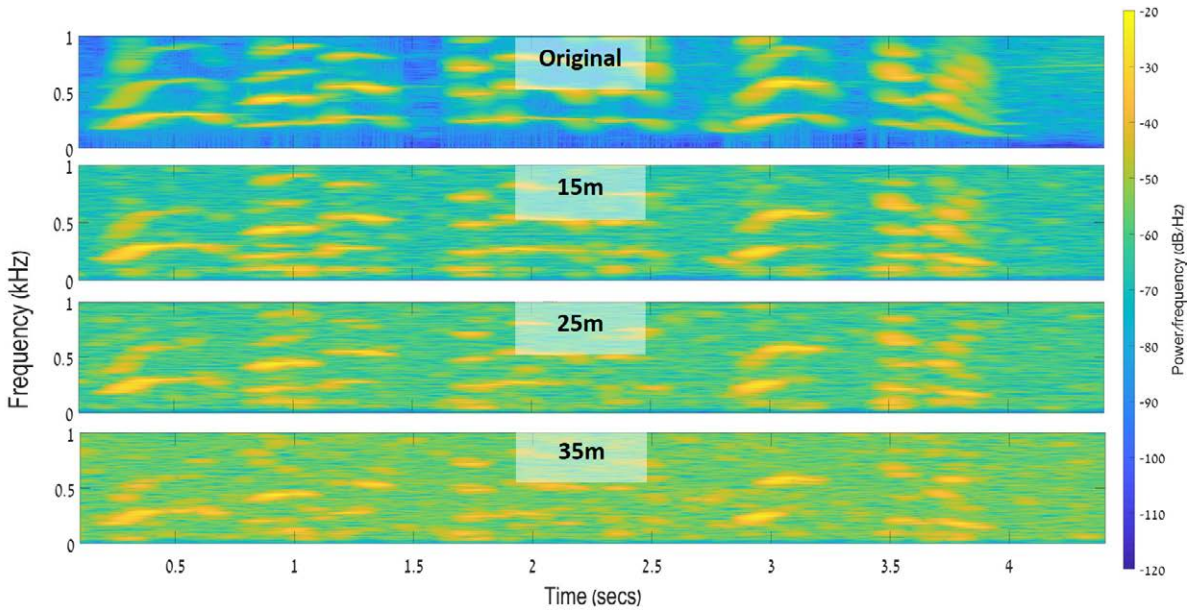
Badacze przeprowadzili atak testowy. Na tym etapie użyli teleskopu i symulowali atak przez szybę, aby móc go porównać z atakami Visual Microphone i Lamphone. Eksperyment powtarzano na różnych dystansach – 15, 25 i 35 metrów od celu.

Poniższe spektrogramy pokazują efekty. Odległość ma wyraźny wpływ na jakość nagrań, ale efekty widoczne przy 35 metrach mogą wystarczyć do pomyślnego szpiegowania.

Z punktu widzenia atakującego opisana metoda ma wiele zalet. Przede wszystkim naprawdę wiele urządzeń jest podatnych na atak i właściwie nic nie wiadomo o tym, aby jakiś producent stosował środki zaradcze. Jak podkreślają redaktorzy Niebezpiecznika, w samym ataku Glowworm tkwi więcej niewykorzystanego potencjału: można użyć np. lepszych teleskopów i sensorów optycznych oraz lepiej dostrojonych urządzeń do przetwarzania sygnału. Mimo że metoda ta nie wymaga użycia sieci neuronowych, ich użycie mogłoby poprawić jakość uzyskiwanego dźwięku.

Mamy tu do czynienia z atakiem TEMPEST, w którym wykorzystywane są cechy układów elektrycznych w atakowanych urządzeniach. Podczas gdy „wizualne mikrofony" pozwalały podsłuchiwać dowolne dźwięki w pomieszczaniu, w przypadku Glowworma możemy podsłuchać to, co z urządzenia się odtwarza czy odsłuchuje (a w czasie pandemii więcej rozmów przechodzi przez głośniki).

Efekty ataku Glowworm w dużej mierze zależą od urządzenia, którego użyto do testów (lepsze wyniki uzyskuje się na głośnikach niż na rozdzielaczach USB), a ponadto na precyzję wyników wpływa także odległość oraz ustawienie przedmiotów w pomieszczeniu. Odporność na atak daje np. zaklejenie czarną taśmą diod urządzenia, jednak obecnie odkrycie to ma charakter akademicki i wymaga użycia specyficznego sprzętu. Producenci sprzętu, zwłaszcza tego używanego w miejscach przetwarzania informacji poufnych, powinni rozważyć zredukowanie fluktuacji diody LED na przykład poprzez dodanie kondensatora, który zadziała niczym filtr dolnoprzepustowy. Rozwiązanie to byłoby stosunkowo niedrogie. Prędzej czy później ktoś prawdopodobnie wykorzysta ustalenia badaczy z Uniwersytetu Ben-Guriona, aby metodę ulepszyć, uczynić tańszą lub stworzyć na jej podstawie gotowy produkt przeznaczony tylko do wybranych odbiorców na specjalnym rynku. Wtedy problem wyda się poważniejszy.



Podsłuchiwanie dźwięku poprzez analizę wizualną to dość popularny temat akademickich badań nad bezpieczeństwem.

Ransomware głównym cyberzagrożeniem w drugim kwartale 2021 r.

11.08.2021 r. - Grupa ekspertów ds. bezpieczeństwa z zespołu Cisco Talos Incident Response (CTIR) wskazuje na ransomware jako główne cyberzagrożenie w drugim kwartale 2021 r. Ten rodzaj ataków odpowiadał za niemal połowę wszystkich cyberincydentów. Przypadki ransomware występowały trzy razy częściej niż kolejny typ zagrożeń ujęty w zestawieniu. Ich ofiarą padały organizacje z niemal każdej branży: transportowej, telekomunikacyjnej, maszynowej, chemicznej, produkcyjnej, technologicznej, nieruchomości, rolnictwa, usług komunalnych, służby zdrowia, a także instytucje rządowe i placówki edukacyjne.

Trzeci kwartał z rzędu najczęstszymi obiektami ataków były organizacje służby zdrowia, na drugim miejscu znalazły się instytucje rządowe. Ma to oczywiście związek z pandemią COVID-19, która sprawiła, że zaatakowane jednostki były bardziej skłonne do zapłacenia okupu w zamian za jak najszybsze przywrócenie dostępu do usług i zasobów. Części cyberincydentów udało się zapobiec, zanim nastąpiło szyfrowanie danych, dzięki rozwiązaniom z rodziny Cisco Secure.

Cyberprzestępcy dokonujący ataków typu ransomware korzystali z rozwiązań open-source i komercyjnych narzędzi, takich jak Cobalt Strike czy aplikacji zainstalowanych na urządzeniu ofiary. Inne zaobserwowane rodzaje ataków obejmowały wykorzystywanie znanych podatności, mocy obliczeniowej urządzeń ofiary do kopania kryptowalut czy danych do logowania. Eksperci Cisco Talos odnotowali również kilka przypadków naruszeń cyberbezpieczeństwa z użyciem urządzeń USB zainfekowanych trojanami, czego nie byliśmy świadkami od wielu lat.

Zdaniem specjalistów Cisco Talos brak uwierzytelniania wieloskładnikowego stanowi jedną z największych przeszkód na drodze do stworzenia skutecznego systemu cyberbezpieczeństwa w biznesie. Zespół CTIR zaobserwował ataki typu ransomware, którym można było zapobiec, gdyby wdrożono rozwiązania klasy MFA (ang. Multi Factor Authentication) w kluczowych usługach.

Więcej informacji na blogu Cisco Talos Intelligence[9].

[9] *https://blog.talosintelligence.com/2021/08/talos-incident-response-quarterly.html*

Policja aresztowała osobę włamującą się na Profile Zaufane

13.08.2021 r - W sierpniu tego roku policja poinformowała[10] o zatrzymaniu i aresztowaniu na dwa miesiące 27-latka, który bez uprawnienia wszedł na konta 239 osób oraz udostępnił innym pozyskane dane do logowań. Jak informuje serwis Niebezpiecznik.pl, mężczyzna:

- **utrzymywał, że działa w celu poprawy bezpieczeństwa Polaków,**
- **przyznał się do ataku na Profil Zaufany,**
- **nikogo nie szantażował.**

27-latek sprawdzał, czy hasła Polaków znajdujące się w różnych wyciekach pasują też do ich Profilu Zaufanego. Taki atak nazywa się „zapychaniem poświadczeniami" (ang. credential stuffing) i polega na sprawdzeniu, czy pary „login + hasło" pochodzące z różnych wycieków i wykradzionych baz danych pasują do jakiegoś serwisu — w tym przypadku do Profilu Zaufanego.

Masowe próby logowania są widoczne dla administratorów, a jeśli analizują oni logi, powinni zauważyć, że ktoś próbuje zgadywać hasła. Najwyraźniej dostrzegli oni działania atakującego, gdyż w serwisie wdrożona została funkcja powiadamiania właścicieli kont o nieudanej próbie logowania.

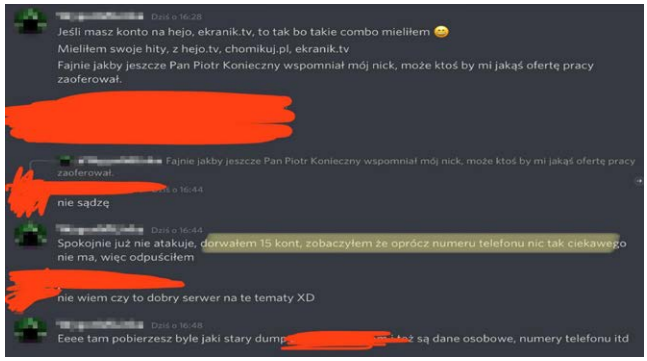
W lipcu 27-latek zaatakował 27 ofiar, a podczas analizy zabezpieczonego komputera policjanci odkryli, że w sierpniu mężczyzna dodatkowo zhakował 212 kont.

W trakcie dokładnego sprawdzenia komputera funkcjonariusze ujawnili liczne bazy danych loginów i haseł oraz oprogramowanie służące jako tzw. narzędzie hakerskie. (...) Grozi mu kara do 8 lat pozbawienia wolności.

Kara do 8 lat sugeruje, że mężczyzna ma zarzut z Art. 269. § 1:

Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

Jak zauważają redaktorzy Niebezpiecznika, sprawdzanie danych z różnych wycieków pod kątem własnego serwisu warto robić, bo jest niemalże pewne, że prędzej czy później zrobi to za nas ktoś obcy. Niestety polskie prawo nie jest do końca jasne



w tej materii, dlatego jeśli ktoś nie chce podejmować ryzyka, powinien wymusić na użytkownikach włączenie uwierzytelnienia dwuetapowego. Nawet w najsłabszym wariancie chroni to przed problemem recyklingu haseł, który jest wykorzystywany w atakach zapychania poświadczeniami.

Jednak wygląda na to, że aresztowany 27-latek nie tylko to miał na sumieniu. Policja wspomina w swojej notatce o „udostępnianiu danych innym osobom" i „ujawnieniu narzędzi hakerskich".

Samo przeprowadzenie testów penetracyjnych (czyli w zasadzie ataku) nie jest jeszcze przestępstwem, o ile realizowane jest zgodnie z zasadami ujętymi w art. 269c lub art. 269b §1a. A zgodnie z nimi:

- trzeba działać wyłącznie w celu zabezpieczenia systemu albo opracowania takiej metody,
- trzeba niezwłocznie powiadomić dysponenta systemu o ujawnionych zagrożeniach,
- „atak" nie może naruszyć interesu publicznego lub prywatnego ani wyrządzić szkody.

To nie oznacza jednak, że każda firma, w której systemach ktoś znajdzie podatności, nie zgłosi sprawy organom ścigania. Ryzyko tłumaczenia się w sądach wciąż istnieje, nawet jeśli błąd zostanie zgłoszony odpowiedzialnie i etycznie, a autor takich badań nie będzie stosować jakiegokolwiek szantażu.

[10] *https://www.policja.pl/pol/aktualnosci/207010,Atak-hakerski-na-konto-uzytkownikow-Profilu-Zaufanego.html*

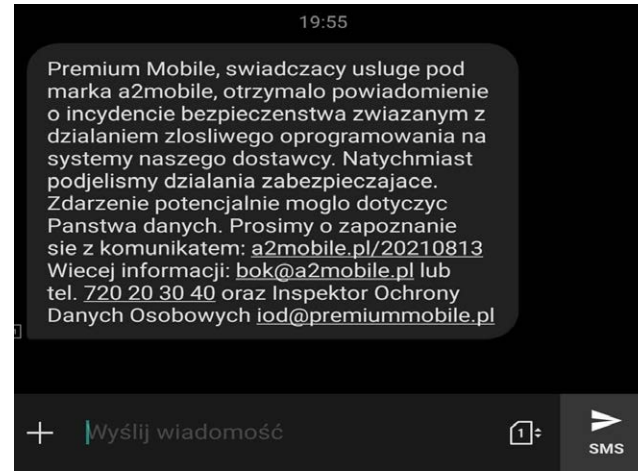
Dane klientów operatorów komórkowych były powszechnie dostępne

16.08.2021 r. - W sierpniu tego roku trzech operatorów wirtualnych działających na infrastrukturze sieci Plus (a2mobile, Premium Mobile i NAU Mobile) poinformowało klientów o „możliwości naruszenia danych osobowych". Komunikat był następstwem ataku ransomware w firmie, która jest dostawcą systemu zarządzania klientami dla tych operatorów.

Jak opisuje serwis Niebezpiecznik.pl, problemy związane z atakiem zaczęły być odczuwalne już 8 sierpnia. Niektórzy z klientów dowiadywali się, że przeniesienie numeru do sieci nie jest obecnie możliwe. Jak można wyczytać z oświadczenia[11] operatora Premium Mobile i oświadczenia a2mobile, spółki o incydencie dowiedziały się już następnego dnia, jednakże dopiero 11 sierpnia otrzymały potwierdzenie, że „incydent bezpieczeństwa" może stanowić ryzyko dla klientów. Co ciekawe, NAU Mobile w swoim oświadczeniu twierdzi[12], że o sprawie dowiedział się dwa dni później, 13 sierpnia.

Ujawnione zostały następujące dane:

- seria i numer dokumentu tożsamości (w przypadku niektórych klientów),
- PESEL (w przypadku niektórych klientów),
- numer telefonu,
- adres zamieszkania,
- adres e-mail,
- imię i nazwisko,



- numer rachunku bankowego (w przypadku niektórych klientów).

Co ciekawe, z tej samej firmy zewnętrznej, z której korzystały a2mobile, Premium Mobile i NAU Mobile, miał korzystać jeszcze jeden operator wirtualny, jednak jego serwery prawdopodobnie nie zostały zaszyfrowane, bo nie poinformował klientów o incydencie.

Jeśli ktoś przekazał operatorowi swoje dane z dokumentu tożsamości, powinien zastrzec ten dokument tożsamości — w banku lub online, za darmo, przez Profil Zaufany[13]. Jego ponowne

wyrobienie jest darmowe. Poza wymianą dowodu warto też zmienić adres e-mail i numer telefonu.

[11] *https://premiummobile.pl/20210813-2/*

[12] *https://naumobile.pl/wp-content/uploads/2021/08/Informacja-dla-klientow-NAU-Mobile.pdf?fbclid=IwAR3img fYHYl59AoU9wdKoTmoudcdFoaPSZZNLGk-7XjHpBnlfmKlgQbWhI4*

[13] *https://www.gov.pl/web/gov/zglos-utrate-lub-uszkodzenie-swojego-dowodu-osobistego-uniewaznij-dowod*

Rozbicie gangu Emotet: Kaspersky publikuje nowy film dokumentalny o likwidacji największej na świecie działalności cyberprzestępczej

17.08.2021 r. - Tomorrow Unlocked, wytwórnia filmów dokumentalnych firmy Kaspersky, zapowiada kolejny odcinek z serii hacker:HUNTER zatytułowany „Emotet vs The World Police". Film ujawnia szczegóły międzynarodowej operacji, która doprowadziła do rozbicia gangu Emotet, stojącego za jednym z najniebezpieczniejszych botnetów oraz jednymi z najniebezpieczniejszych usług cyberprzestępczych minionej dekady. Premiera wspomnianego dokumentu odbyła się 18 sierpnia na kanale YouTube[14] Tomorrow Unlocked. Jest to piąty odcinek z serii hacker:HUNTER[15].

Ukazany z perspektywy prokuratorów oraz policjantów z Niemiec, Holandii oraz Ukrainy film opowiada o tym, jak międzynarodowa współpraca służb policyjnych doprowadziła do zlikwidowania jedynej w swoim rodzaju działalności cyberprzestępczej. Ponadto cieszący się międzynarodowym uznaniem badacze cyberbezpieczeństwa ukazują szerszy kontekst sprawy i próbują przewidzieć, czego możemy spodziewać się w przyszłości. Policja zdołała powstrzymać przestępców, ponieważ zaczęła myśleć jak oni – tak jeden z badaczy podsumował w filmie całą operację.

Emotet stał na czele komercjalizacji dostępu do Sieci, wspomagając poprzez swoje działania „w tle" cyberprzestępstwa na całym świecie. Pod pewnymi względami Emotet przypominał zorganizowany gang XX wieku – oferował środki umożliwiające popełnianie przestępczości, a w późniejszych latach swojej działalności sam nigdy nie przeprowadzał ataków, co utrudniało zidentyfikowanie stojących za nim osób. Emotet otworzył drzwi ugrupowaniom cyberprzestępczym postępującym bez skrupułów i atakującym istotne jednostki oraz organizacje, takie jak szpitale.

Od momentu wykrycia w 2014 r. Emotet nieustannie ewoluował – utrzymywał i sprzedawał narzędzia oraz dostęp do setek tysięcy urządzeń na całym świecie, które mogły być następnie infekowane różnego rodzaju szkodliwym oprogramowaniem, takim jak ransomware czy trojany bankowe. Botnet, czyli sieć zainfekowanych urządzeń, rozrastał się poprzez wykorzystywanie szkodliwych załączników w wiadomościach spamowych – po otwarciu takiego załącznika urządzenie było infekowane szkodliwym oprogramowaniem, a tym samym stawało się podatne na inne zagrożenia. Emotet stosował to skądinąd dość powszechne podejście na ogromną skalę, co wyróżniało go spośród innych cyberprzestępców.

Dzięki ogromnej, zdecentralizowanej infrastrukturze rozmieszczonej w różnych państwach gang ten był niezwykle skuteczny, a rozbicie go wydawało się prawie niemożliwe. Tak było do stycznia 2021 r., gdy Europol ogłosił zlikwidowanie jego operacji oraz aresztowanie kluczowych członków. Cała akcja została zatwierdzona przez Europol i przeprowadzona dzięki ścisłej współpracy rządów różnych państw z Europy i spoza kontynentu, co było niezbędnym elementem powodzenia tej operacji.

Nowy film z serii Hacker:Hunter pokazuje, jak wyglądały „interesy" gangu Emotet, oraz przedstawia operację, która doprowadziła do jego upadku. Widzowie będą mogli zajrzeć za kurtynę oraz poznać relację osób, które prowadziły dochodzenie.

Reżyserką filmu jest Jessica Benhamou, a jego producentami Max Peltz oraz Stephen Robert Morse. Twórcą serii hacker:HUNTER jest Hugo Berkeley, który wyreżyserował także dwa pierwsze filmy dokumentalne z tej serii – o ugrupowaniu Carbanak oraz ataku ransomware WannaCry. Pełną listę osób zaangażowanych w realizację filmu można znaleźć tutaj[16].

„Cyberprzestępczość rozwija się, a cyberprzestępcy łączą siły, dlatego rządy muszą odpowiednio reagować i podejmować współpracę, aby móc zwalczać zagrożenia i stojące za nimi osoby. Myślę, że ludzie często nie zdają sobie sprawy, ile wysiłku wymaga rozbicie cybergangu. Cieszę się, że mogliśmy pokazać, jak wiele osób – pełnych pasji i poświęcenia – współpracowało ze sobą, aby do tego doprowadzić" – powiedziała **Jessica Benhamou**, reżyserka filmu.

Premiera filmu dokumentalnego odbyła się 18 sierpnia 2021 r. W premierze wzięli udział Marco Preuss, dyrektor europejskiego zespołu GReAT firmy Kaspersky, **Jessica Benhamou**, reżyserka najnowszego odcinka z serii hacker:HUNTER, oraz **Rainer Bock**, producent wykonawczy hacker:HUNTER.

Zwiastun filmu jest dostępny tutaj[17]. Wszystkie odcinki serii hacker:HUNTER są dostępne na stronie https://tomorrowunlocked.com/guardians/hacker_hunter[18].

Informacje na temat Tomorrow Unlocked

Tomorrow Unlocked[19] to magazyn online poświęcony kulturze technologicznej oraz wytwórnia filmowa firmy Kaspersky. Serwis koncentruje się na historiach pokazujących, w jaki sposób technologia pomaga tworzyć lepszą przyszłość, oferując materiały do czytania, filmy dokumentalne oraz podstawowe informacje. Więcej szczegółów znajduje się na stronie tomorrowunlocked.com

[14] *https://www.youtube.com/tomorrow_unlocked*

[15] *https://www.tomorrowunlocked.com/guardians/hacker_hunter/*

[16] *https://www.imdb.com/title/tt15159010/fullcredits/*

[17] *https://www.youtube.com/watch?v=I7_lLpxWiYw*

[18] *https://www.tomorrowunlocked.com/guardians/hacker_hunter/*

[19] *https://www.tomorrowunlocked.com/*

FMWhasapp: szkodliwy kod rozprzestrzenia się za pośrednictwem nieoficjalnej modyfikacji popularnego komunikatora internetowego

24 sierpnia 2021 r. - Badacze z firmy Kaspersky wykryli FMWhasapp – szkodliwą wersję popularnej, nieoficjalnej modyfikacji dla komunikatora WhatsApp. Rozprzestrzenia ona trojana mobilnego Triada, który pobiera inne szkodliwe narzędzia, wyświetla uciążliwe reklamy, dodaje użytkowników do płatnych subskrypcji i przechwytuje wiadomości SMS.

WhatsApp jest jednym z najpopularniejszych komunikatorów internetowych, jednak nie wszyscy są zadowoleni z dostępnych w nim funkcji. Dlatego w pogoni za najbardziej optymalną wersją użytkownicy decydują się czasami na zainstalowanie tzw. modów, które oferują więcej opcji w porównaniu z wersją oficjalną, jak np. wybór dynamicznych szablonów czy możliwość czytania usuniętych wiadomości.

Twórcy takich modyfikacji często umieszczają w nich różne reklamy, aby czerpać zyski ze swojej pracy. Niestety znajdują się wśród nich również oszuści, którzy poprzez reklamy rozprzestrzeniają szkodliwy kod. Przykładem jest modyfikacja FMWhasapp w wersji 16.80.0, która zawiera mobilnego trojana Triada[20] oraz bibliotekę reklam.

W niebezpiecznej wersji moda FMWhatsapp trojan Triada stanowi pośrednika. Najpierw zbiera dane dotyczące urządzenia mobilnego, a następnie, na polecenie swojego właściciela, pobiera na telefon dalsze trojany. Mogą one samodzielnie uruchamiać reklamy, zapisywać ofiarę do płatnych usług subskrypcyjnych, a nawet logować się na konto WhatsAppa, przechwytując wiadomość SMS w celu potwierdzenia logowania. Tym samym urządzenie może zostać wykorzystane do nielegalnej aktywności.

Rozwiązania firmy Kaspersky wykrywają szkodliwą modyfikację FMWhatsapp jako Trojan.AndroidOS.Triada.ef.

Szczegóły techniczne dotyczące omawianego zagrożenia są dostępne na stronie https://r.kaspersky.pl/Ey7VY

[20] *https://www.kaspersky.pl/o-nas/informacje-prasowe/2570*

Album Donda Kanye'ego Westa – premiera muzyczna wyczekiwana nie tylko przez fanów, ale również cyberoszustów

26.08.2021 r. - W ostatnich miesiącach fani Kanye'ego Westa śledzili postępy w produkcji jego najnowszego albumu – Donda. Najpierw artysta wynajął cały stadion i zamknął się w nim, by dokończyć pracę nad płytą. Następnie urządził prawdziwe show, podczas którego nie zabrakło efektów specjalnych oraz lewitacji pod dachem stadionu. Cały ten szum wokół mającego niebawem ukazać się krążka skłonił firmę Kaspersky do zbadania, czy cyberprzestępcy wykorzystują to wydarzenie do rozprzestrzeniania szkodliwych plików oraz ataków phishingowych.

Chociaż w okresie od lipca do sierpnia 2021 r. eksperci nie zauważyli dużego zainteresowania ze strony oszustów, znaleźli kilka przykładów niebezpiecznych programów oraz fałszywych odsyłaczy żerujących na wspomnianym albumie.

W szczególności badacze zidentyfikowali dwa pliki podszywające się pod nowy utwór, które pobierają narzędzia reklamowe (adware) i potencjalnie inne szkodliwe programy:

- Download-File-KanyeWestDONDA320.zip_88481.msi
- Kanye West _ DONDA (Explicit) (2021) Mp3 320kbps [PMEDIA] __ - Downloader.exe

Inne przykłady to różne rodzaje oszustw. W pierwszym przypadku użytkownicy otrzymują link do pobrania „albumu" i zostają poproszeni o wzięcie udziału w ankiecie oraz potwierdzenie, że nie są robotami. Ankieta zawiera szereg pytań, takich jak: „Ile zarabiasz?" oraz „Czy chcesz być bogaty?". Po wypełnieniu ankiety użytkownik jest kierowany na fałszywą stronę internetową, na której będzie mógł rzekomo zarabiać na bitcoinach. Naturalnie, o albumie nie ma już mowy, a jeśli skuszony ofertą użytkownik zapragnie zostać bitcoinowym milionerem i poda swoje dane

osobowe, może stracić pieniądze.

Inny powszechny przypadek – użytkownik znajduje odsyłacz do archiwum z albumem. W rzeczywistości jest ono zainfekowane szkodliwym oprogramowaniem. Po rozpakowaniu urządzenie użytkownika zostaje zainfekowane.

Placówki oświatowe najczęstszym celem ataków ransomware – badanie Sophos

1.09.2021 r. – Prawie połowa instytucji edukacyjnych została w ostatnim roku zaatakowana przez ransomware – wynika z badania firmy Sophos. Placówki oświatowe ponoszą najwyższe ze wszystkich branży koszty zniwelowania skutków ataku, średnio to aż 2,73 mln dolarów. Aż 35% decyduje się na zapłacenie przestępcom okupu, jednak tylko co dziesiąta odzyskuje wszystkie dane. Największe problemy stanowi przestarzała infrastruktura IT oraz braki kadrowe.

Zdalne nauczanie okazją dla cyberprzestępców

Rok 2020 był trudny dla instytucji edukacyjnych – aż 44% z nich doświadczyło ataku ransomware, co stanowi największy odsetek spośród wszystkich branż. Szybkie przejście na zdalny tryb nauczania przyniosło zespołom IT z placówek oświatowych dodatkowe wyzwania: musiały zabezpieczyć nowe platformy i urządzenia, a także zapewnić szkolenia. Prawie trzy czwarte wskazuje, że w ubiegłym roku wzrosło obciążenie pracą związaną z cyberbezpieczeństwem. Prawie dwie trzecie (65%) stwierdziło zaś, że wydłużył się czas ich reakcji.

Placówki oświatowe za ataki płacą najwięcej

Aby odzyskać zaszyfrowane dane, 35% instytucji zapłaciło okup – średnio 112 tys. dolarów. Większą skłonność do płacenia przestępcom wykazały jedynie branża energetyki i usług komunalnych oraz samorządy lokalne. Tylko co dziesiąta placówka edukacyjna po spełnieniu żądań atakujących odzyskała wszystkie informacje. Co trzecia odzyskała połowę lub mniej danych.

Jak wynika z badania Sophos, oświata ponosi największe straty z powodu ransomware'u. Średnio to aż 2,73 mln dolarów, o połowę więcej niż światowa średnia. Na tę kwotę składają się koszty zapłacenia okupu, ale też odzyskania danych, załatania luk w zabezpieczeniach i usuwania skutków ataku. Wysokie straty mogą wynikać w dużej mierze z przestarzałej i rozproszonej infrastruktury IT. Po ataku instytucje często muszą odbudowywać i zabezpieczać swoje systemy od podstaw.

Szkoły nieprzygotowane na ataki

33% placówek edukacyjnych nie doświadczyło ataku ransomware w ubiegłym roku, ale obawia się, że nastąpi to w przyszłości, zaś 22% uważa, że nie zostaną zaatakowane. Aż 6 na 10 respondentów, którzy nie spodziewają się ataku, polega przy tym na rozwiązaniach, które nie chronią przed ransomware.

O badaniu

Badanie Sophos „State of Ransomware in Education 2021" przeprowadzono w styczniu i lutym 2021 roku, na próbie 5,4 tys. menedżerów z obszaru IT, w tym 499 z branży edukacyjnej. Respondentów wybrano z 30 krajów w Europie (w tym także w Polsce), Ameryce Północnej i Południowej, Azji-Pacyfiku i Azji Środkowej, na Bliskim Wschodzie i w Afryce.

Trzy najczęstsze scenariusze ataków na firmowe skrzynki e-mail

1.09.2021 r. - Badacze z firmy Kaspersky obserwują coraz więcej ataków na biznesowe skrzynki e-mail (ang. Business E-mail Compromise, BEC). W okresie od maja do lipca 2021 r. rozwiązania firmy zablokowały ponad 9,5 tysiąca takich niebezpiecznych działań cyberprzestępców, łącznie z atakami na firmy z branży transportowej, przemysłowej, detalicznej, IT czy dostawczej. Ataki BEC wymagają od cyberprzestępców znacznych zasobów i przygotowań, które mogą trwać od kilku tygodni do miesięcy. Jeden udany atak może doprowadzić do milionowych strat.

W ramach przygotowań do ataku BEC cyberprzestępcy zwykle inicjują korespondencję e-mail z pracownikiem ofiary w celu zdobycia jego zaufania i nakłonienia do wykonania działań, które mogą być potencjalnie niebezpieczne dla firmy lub jej klientów. W tym celu atakujący korzystają ze skradzionych wcześniej skrzynek e-mail innych pracowników lub z adresów, które wizualnie przypominają oficjalne domeny danej firmy. Czasami prze-

stępcy kradną dane logowania jednego z pracowników niższego szczebla, by przeprowadzić atak na kogoś z kadry menedżerskiej lub zarządzającej. W większości przypadków celem ataków są pieniądze firmy, jednak zdarzają się także działania zmierzające do kradzieży informacji poufnych, takich jak baza danych klientów czy wewnętrzne dokumenty związane z rozwojem biznesu.

Eksperci z firmy Kaspersky wyłonili trzy najpopularniejsze scenariusze stosowane przez cyberprzestępców w ramach ataków BEC.

Oszustwo „na pracownika wyższego szczebla"

W takim scenariuszu pracownik otrzymuje fałszywą wiadomość e-mail, pochodzącą rzekomo od kogoś z kadry menedżerskiej lub zarządzającej. Atakujący mogą w ten sposób próbować nakłonić pracownika do przesłania poufnych informacji np. do „radcy prawnego", którego adres należy oczywiście do cyberprzestępców. Korzystając z tej metody, atakujący mogą ukraść wrażliwe informacje firmy, które nigdy nie powinny wydostać się poza jej sieć.

Oszustwo „na zmianę numeru konta"

W ramach ataku dział finansowy firmy może otrzymać fałszywą wiadomość e-mail od rzekomego pracownika, który prosi o zmianę numeru konta do wypłaty wynagrodzenia. Jeżeli ktoś z działu finansowego dokona takiej zmiany, wynagrodzenie należne pracownikowi trafi prosto w ręce cyberprzestępców.

Oszustwo „na fałszywą fakturę"

Ataki tego typu również są wycelowane w działy finansowe, jednak tym razem fałszywa wiadomość pochodzi rzekomo od dostawcy lub innego kontrahenta atakowanej firmy. Treść może informować o opóźnieniu w płatności za usługę lub po prostu zawierać zupełnie nową fakturę do opłacenia. Jeżeli atakowany pracownik dokona przelewu na wskazany numer konta, pieniądze trafią do oszustów.

„Przygotowując się do ataku BEC, cyberprzestępcy cierpliwie gromadzą informacje o swojej ofierze i wykorzystują je do zdobycia zaufania. Niektóre z takich działań są możliwe, ponieważ atakujący mogą łatwo znaleźć ogólnodostępne nazwiska i stanowiska pracowników oraz inne informacje dostępne np. na stronach internetowych firm. Podczas realizowania ataków oszuści zwykle korzystają z szeregu metod socjotechniki, co umożliwia im przekonanie ofiar, że są tym, za kogo się podają. Z tego powodu firmy nie powinny lekceważyć konieczności regularnego szkolenia swojego personelu w zakresie cyberbezpieczeństwa" – powiedział **Aleksiej Marczenko**, szef działu rozwoju technologii filtrowania zawartości w firmie Kaspersky.

Aby zminimalizować szansę udanego ataku na biznesowe skrzynki e-mail, firmy powinny korzystać ze skutecznych rozwiązań bezpieczeństwa wyposażonych w zaawansowane technologie antyphishingowe i antyspamowe.

W celu zwiększenia świadomości personelu w zakresie cyberzagrożeń firmy mogą korzystać ze zautomatyzowanej platformy szkoleniowej, takiej jak Kaspersky Automated Security Awareness Platform (ASAP)[21].

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

Eksperci Cisco Talos ostrzegają przed nowym rodzajem ataków: cyberprzestępcy mogą monetyzować przepustowość sieci bez wiedzy użytkowników

2.09.2021 r. - Cyberprzestępcy znajdują nowe sposoby, aby zarabiać na atakach. Jak podaje Cisco Talos, coraz częściej robią to w oparciu o platformy umożliwiające dzielenie się ruchem sieciowym zwane „proxyware", takie jak Honeygain, IPRoyal Pawns, Nanowire, Peer2Profit czy PacketStream. W niepowołanych rękach umożliwiają one wykorzystanie przepustowości sieci użytkowników bez ich wiedzy, działając w tle na zainfekowanym urządzeniu. W niektórych przypadkach cyberprzestępcy wyłączają alerty bezpieczeństwa, które mogłyby ostrzec zaatakowanego użytkownika.

Platformy „proxyware" umożliwiają udostępnienie części przepustowości sieci innym użytkownikom. Oczywiście za opłatą. Z tego rozwiązania korzystają m.in. firmy marketingowe testujące kampanie online w różnych regionach geograficznych. Z kolei użytkownicy prywatni mogą w ten sposób obejść ograniczenia wynikające z braku dostępu np. do serwisów streamingowych czy platform gamingowych w określonym kraju. Wykorzystują oni sieć z miejsca, gdzie usługa działa, nie ruszając się z fotela. Wraz ze wzrostem popularności tego rozwiązania, zainteresowali się nim również cyberprzestępcy, którzy zaczęli wykorzystywać je w kampaniach malware. Najbardziej oczywistym rodzajem ataku jest przejęcie przepustowości bez wiedzy użytkownika np. na potrzeby kopania kryptowalut.

Skala zjawiska jakim jest nielegalne wykorzystanie „proxyware" staje się coraz większa. Ma to związek ze wzrostem popularności samego narzędzia. Potwierdzają to niedawno opublikowano dane dotyczące Honeygain, jednej z najpopularniejszych platform proxyware, pochodzące z „2021 User Experience and Awareness Survey". W tegorocznej edycji badania wzięło udział, aż 250 tys. użytkowników narzędzia. To ponad 16 razy więcej niż w 2020 r.

Nowy rodzaj ataków to nowe wyzwania dla zespołów IT

Wykorzystanie „proxyware" to nowy trend, ale jak podkreślają specjaliści Cisco Talos, o ogromnym potencjale rozwoju. Uzyskany nielegalnie dostęp do sieci pozwala cyberprzestępcom zatrzeć ślady prowadzące do źródeł ataków. Wszelkie działania prowadzone z wykorzystaniem skradzionej przepustowości są ukryte pod adresem IP ofiary. Dzięki temu wydaje się, że pochodzą one z sieci godnych zaufania, co usypia czujność specjalistów ds. cyberbezpieczeństwa i utrudnia dostosowanie konwencjonalnych systemów bezpieczeństwa, które analizują m.in. listę zablokowanych adresów IP.

Nowe formy ataków wiążą się z nowymi wyzwaniami dla specjalistów ds. bezpieczeństwa, w szczególności w tych organizacjach gdzie dostęp do Internetu jest ograniczony lub sieć jest oznaczona jako „domowa". Eksperci Cisco podkreślają, że istnieją także platformy, które umożliwiają dzielenie się ruchem sieciowym wprost z centrum danych. Dlatego warto, aby organizacje rozważyły wprowadzenie zakazu korzystania z platform typu „proxyware" w pracy. Punkty końcowe nie powinny nawiązywać połączenia z sieciami za ich pośrednictwem. Specjaliści Cisco Talos rekomendują wdrożenie kompleksowych mechanizmów zapewniających bezpieczne logowanie i dystrybuujących alerty, aby zapewnić efektywne lokalizowanie i odpowiadanie na przypadki prób połączenia z „proxyware", gdyż może to świadczyć o tym, że doszło do ataku.

Więcej informacji na blogu Cisco Talos: https://blog.talosintelligence.com/2021/08/proxyware-abuse.html

Bankowy trojan QakBot w natarciu – liczba ataków rośnie

2.09.2021 r. - Liczba użytkowników atakowanych trojanem bankowym QakBot wzrosła w pierwszych siedmiu miesiącach 2021 r. o 65% (do niemal 17,5 tysiąca) w porównaniu z analogicznym okresem w ubiegłym roku. Ten wzrost aktywności skłonił badaczy z firmy Kaspersky do przeanalizowania zmian w nowych wersjach tego szkodliwego programu.

Po udanym zainfekowaniu urządzenia trojany bankowe pozwalają cyberprzestępcom kraść pieniądze z kont i e-portfeli ofiary i z tego powodu są uważane za jedne z najniebezpieczniejszych szkodliwych programów. QakBot został wykryty już w 2007 r. jako jeden z wielu trojanów bankowych, które się wówczas pojawiły. Jednak od tego czasu twórcy QakBota zainwestowali wiele zasobów w jego rozwój, czyniąc go jednym z najpotężniejszych i najniebezpieczniejszych szkodliwych narzędzi tego typu.

Poza funkcjami typowymi dla trojanów bankowych, takich jak przechwytywanie znaków wprowadzanych z klawiatury, kradzież ciasteczek z przeglądarek czy przechwytywanie loginów i haseł, nowe wersje QakBota zostały wyposażone m.in. w technologie pozwalające na wykrywanie, czy został on uruchomiony w środowisku wirtualnym. Tego typu środowiska są często wykorzystywane przez specjalistów ds. rozwiązań bezpieczeństwa i badaczy cyberzagrożeń w celu identyfikowania niebezpiecznych programów na podstawie ich zachowania. Jeżeli nowa wersja QakBota wykryje, że została uruchomiona w środowisku wirtualnym, może wyłączyć szkodliwe funkcje lub całkowicie wstrzymać swoje działanie. Ponadto QakBot stosuje także inne techniki chroniące go przed wykryciem i analizą.

Badacze z firmy Kaspersky wykryli jeszcze jedną nową, nietypową dla trojanów bankowych, funkcję QakBota – może on kraść e-maile z zainfekowanych maszyn. Skradzione wiadomości są następnie wykorzystywane w działaniach socjotechnicznych wycelowanych w osoby z listy kontaktów ofiary.

Produkty firmy Kaspersky wykrywają i neutralizują wszystkie znane wersje trojana QakBot.

Szczegóły techniczne dotyczące omawianego zagrożenia są dostępne na stronie https://r.kaspersky.pl/zLJwu.

Konsultant informuje Cię o konieczności odbioru notebooka lub ekspresu do kawy? Uważaj, to kolejne ataki vishingowe mające na celu wyłudzenie danych!

3.09.2021 r. - W ostatnim czasie badacze ESET otrzymali kolejne zgłoszenie dotyczące oszustw telefonicznych, mających na celu wyłudzenie danych. Tym razem zamiast atrakcyjnych ofert kredytowych lub propozycji dofinansowania do instalacji fotowoltaicznej, ofiary otrzymują informację o konieczności odebrania notebooka, ekspresu do kawy lub innego sprzętu RTV. - To już kolejny przypadek vishingu, który został zarejestrowany w tym roku. Coraz częściej cyberprzestępcy korzystają też z konsultantów-robotów, którzy coraz sprawniej zachowują się w zetknięciu z ofiarą ataku – ostrzegają eksperci ds. bezpieczeństwa ESET.

Ataków vishingowych jest coraz więcej. W ostatnim czasie mogli się o tym przekonać ci, którzy otrzymywali telefony od rzekomych pracowników banku ING lub firmy Tauron. Coraz częściej jednak po drugiej stronie słuchawki znajduje się komputer, który wykorzystuje nagrane kwestie, aby móc manipulować ofiarami w celu wyłudzenia danych osobowych.

Do odebrania notebook

W najnowszej kampanii vishingowej cyberprzestępcy podają się za rzekomą firmę ze sprzętem RTV z siedzibą w Płocku, która oferuje sprzęty informatyczne oraz gospodarstwa domowego – brak jednak jakichkolwiek informacji, aby taka firma faktycznie istniała i świadczyła tego rodzaju usługi. Zgodnie z relacją ofiary ataku rzekomy konsultant poinformował ją o konieczności odbioru notebooka. Jednak, aby odebrać sprzęt, należy w pierwszej kolejności podać telefonicznie dane osobowe, które są wymagane w procesie weryfikacji. W tym przypadku oszuści natrafili jednak na numer służbowy, o czym właściciel telefonu poinformował konsultanta dodając, że nie jest zainteresowany ofertą. Jak mówi ofiara ataku, po dłuższej ciszy konsultant poprosił ją ponownie o udostępnienie danych osobowych w celu weryfikacji i ustalenia właściciela numeru telefonu. To sprawiło, że ofiara

zorientowała się, że ma do czynienia robotem, który odtwarza nagrane kwestie.

- „Roboty wykorzystywane do vishingu mają określoną pulę komunikatów, które są wykorzystywane w rozmowie z ofiarą. W tym przypadku na informację, że ofiara nie jest zainteresowana, robot ponowił prośbę o podanie danych osobowych w celu rzekomej weryfikacji numeru telefonu. Powtórzony, identyczny komunikat zwrócił uwagę ofiary i automatycznie zdemaskował oszustów" – powiedział **Kamil Sadkowski**, starszy specjalista ds. cyberbezpieczeństwa ESET.

Jak rozpoznać robota?

Chociaż w wielu przypadkach jakość nagrań i responsywność robotów mogą wzbudzić naszą czujność już w pierwszych sekundach rozmowy, to ta metoda ataku jest stale udoskonalana i wkrótce może stać się poważnym zagrożeniem, w szczególności dla osób starszych, które łatwiej ulegają tego rodzaju manipulacjom. Jak relacjonuje ofiara ataku, konsultant wydawał się podejrzany już od początku rozmowy. Przerywał wypowiedzi ofiary a pomiędzy wypowiadanymi zdaniami pojawiały się bardzo długie pauzy. Podejrzana była również intonacja konsultanta, która nie była adekwatna do prowadzonej aktualnie rozmowy.

- „Ograniczona liczba nagranych zdań sprawia, że w przypadku, gdy ofiara zadaje dużo pytań lub ponawia swoje pytanie wiele razy, robot jest zmuszony powtarzać swoje kwestie, a to może w bardzo szybkim tempie wskazać, czy mamy do czynienia z próbą oszustwa. Warto również zwrócić uwagę na logiczność wypowiadanych zdań. W wielu przypadkach taki robot wyłapuje jedynie słowo kluczowe i przygotowuje na nie odpowiedź, która może nie nawiązywać do kontekstu rozmowy" – powiedział **Kamil Sadkowski**.

Zagrożenia dla przemysłowych systemów sterowania: więcej spyware i szkodliwych skryptów w pierwszej połowie 2021 r.

kaspersky

9.09.2021 r. - Według zespołu ICS CERT firmy Kaspersky niemal jeden na trzy komputery przemysłowe stanowił cel szkodliwej aktywności w pierwszej połowie 2021 r. W okresie tym cyberprzestępcy intensywnie wykorzystywali różne rodzaje oprogramowania spyware oraz szkodliwych skryptów podczas przeprowadzania swoich ataków. Tego rodzaju zagrożenia stanowią duże wyzwanie dla przemysłowych systemów sterowania.

Ataki na organizacje przemysłowe są szczególnie niebezpieczne, ponieważ mogą prowadzić do kradzieży danych oraz pieniędzy, jak również zakłóceń w ustalonym systemie produkcji. Wraz ze wzrostem zróżnicowania zagrożeń dla takich sieci wzrasta zainteresowanie nimi ze strony cyberprzestępców, a tym samym potrzeba zapewnienia niezawodnej ochrony przed nimi.

Z raportu przygotowanego przez zespół Kaspersky ICS CERT wynika, że w pierwszej połowie 2021 r. rozwiązania bezpieczeństwa firmy zablokowały ponad 20 000 wariantów szkodliwego oprogramowania. Aby dowiedzieć się, jak w badanym okresie zmienił się krajobraz zagrożeń dla systemów przemysłowych, badacze przeanalizowali różne rodzaje szkodliwego oprogramowania wykorzystywanego w cyberatakach. Okazało się, że odsetek oprogramowania spyware oraz szkodliwych skryptów wykorzystywanych w atakach na systemy przemysłowe nieustannie wzrastał na przestrzeni minionych sześciu miesięcy.

O 0,4 punktu procentowego wzrosła liczba programów spyware (trojany szpiegujące, backdoory oraz keyloggery), które wykorzystywane są głównie do kradzieży pieniędzy. Jednocześnie o 0,7 punktu procentowego zwiększyła się liczba szkodliwych skryptów. Cyberprzestępcy stosują takie narzędzia na różnych stronach internetowych z nielegalnie skopiowaną zawartością w celu przekierowania użytkowników do zasobów rozprzestrzeniających spyware lub szkodliwe oprogramowanie, którego celem jest kopanie kryptowaluty bez wiedzy użytkownika.

Więcej informacji na temat krajobrazu zagrożeń dla systemów przemysłowych w pierwszej połowie 2021 r. znajduje się na stronie https://r.kaspersky.pl/y2MPy.

Zarządzanie łatami w połączeniu z dobrymi praktykami dot. haseł zmniejsza ryzyko cyberataków na firmy nawet o 60%

kaspersky

14.09.2021 r. - W sześciu na dziesięć (63%) cyberatakach badanych przez zespół Kaspersky Global Emergency Response sprawcy wykorzystali ataki siłowe i słownikowe na hasła oraz luki w zabezpieczeniach jako początkowe wektory wniknięcia do środowiska organizacji. Nowy raport[22] firmy Kaspersky pokazuje, że samo wdrożenie odpowiedniej polityki zarządzania łatami zmniejsza ryzyko incydentów o 30%, natomiast zastosowanie dobrych praktyk dotyczących haseł zmniejsza prawdopodobieństwo powodzenia cyberataku o 60%.

Chociaż o znaczeniu regularnego łatania i aktualizacji, jak również stosowania silnych haseł, zdaje sobie sprawę każdy, kto choć w niewielkim stopniu orientuje się w kwestiach dotyczących cyberbezpieczeństwa, aspekty te nadal stanowią słabe punkty w wielu organizacjach i umożliwiają cyberprzestępcom wtargnięcie do systemów atakowanych firm.

Z analizy zanonimizowanych danych pochodzących z przypadków reagowania na incydenty[23] wynika, że atak siłowy i/lub słownikowy stanowi najpowszechniej wykorzystywany początkowy wektor wniknięcia do sieci firmy. W porównaniu z poprzednim

rokiem udział ataków siłowych zwiększył się z 13% do 31,6%, być może z powodu pandemii oraz rozpowszechnienia pracy zdalnej. Drugim najczęściej spotykanym wektorem jest wykorzystywanie luk w zabezpieczeniach (31,5%). Badanie pokazało, że te, które zostały wykryte w 2020 r., wykorzystano jedynie w kilku incydentach. W pozostałych przypadkach sprawcy atakowali z użyciem starszych niezałatanych podatności, takich jak CVE-2019-11510, CVE-2018-8453 oraz CVE-2017-0144.

Ponad połowa wszystkich ataków, które rozpoczęły się od szkodliwych e-maili, ataków siłowych oraz wykorzystania zewnętrznych aplikacji, została wykryta w przeciągu godzin (18%) lub dni (55%). Niektóre z tych ataków trwały znacznie dłużej – średnio do 90,4 dni. Z raportu wynika, że przypadki wykorzystania ataku siłowego jako wektora początkowego są teoretycznie łatwe do wykrycia, jednak w praktyce jedynie część z nich zostanie zidentyfikowana, zanim dojdzie do wyrządzenia konkretnych szkód.

Chociaż zapobieganie atakom siłowym oraz instalowanie w porę aktualizacji nie wydaje się stanowić problemu dla profesjonalnego zespołu ds. cyberbezpieczeństwa, w praktyce całkowite wyeliminowanie tych problemów jest w zasadzie niemożliwe.

[22] https://securelist.com/incident-response-analyst-report-2020/104080/

[23] Kaspersky Incident Response to rozwiązanie, które pomaga zmniejszyć negatywny wpływ incydentu naruszenia bezpieczeństwa lub ataku na środowisko IT firmy. Obejmuje cały cykl badania incydentu, od zebrania dowodów „na miejscu" po identyfikację dodatkowych oznak naruszenia bezpieczeństwa, przygotowanie planu korygującego oraz wyeliminowanie zagrożenia. Raport Incident Response Analyst zawiera analizę usług badania incydentów zrealizowanych przez firmę Kaspersky w okresie styczeń–grudzień 2020 r. w Ameryce Południowej i Północnej, Europie, Afryce, na Bliskim Wschodzie, w Azji, jak również Rosji oraz w krajach Wspólnoty Niepodległych Państw.

Raport FortiGuard Labs: Ataki z użyciem ransomware'u zdarzają się dziesięć razy częściej niż rok temu

16.09.2021 r. - Fortinet, globalny lider w dziedzinie zintegrowanych i zautomatyzowanych rozwiązań cyberochronnych, przedstawił najnowszą edycję raportu Global Threat Landscape, opracowanego przez analityków FortiGuard Labs. Dane dotyczące zagrożeń zaobserwowanych w pierwszej połowie 2021 r. wskazują na znaczny wzrost liczby i poziomu wyrafinowania ataków skierowanych przeciwko osobom prywatnym, przedsiębiorstwom oraz krytycznej infrastrukturze. Na celowniku cyberprzestępców nadal znajduje się rosnąca liczba osób pracujących i uczących się zdalnie. Podjęta w odpowiednim czasie współpraca pomiędzy organami ścigania, a także podmiotami z sektora publicznego i prywatnego daje szansę na zakłócenie działań cyberprzestępców w drugiej połowie 2021 roku.

Oto najważniejsze informacje z raportu za pierwsze półrocze 2021 r:

1. W cyberatakach typu ransomware chodzi o coś więcej niż pieniądze

Dane FortiGuard Labs wskazują, że aktywność oprogramowania ransomware w czerwcu 2021 r. była ponad dziesięć razy wyższa niż rok temu. Świadczy to o konsekwentnym i stałym wzroście popularności tego narzędzia. Incydenty z użyciem ransomware'u sparaliżowały łańcuchy dostaw wielu przedsiębiorstw, szczególnie w branżach o krytycznym znaczeniu. Bardziej niż kiedykolwiek wpłynęły na życie codzienne, handel, produktywność pracowników itd.

Cyberprzestępcy najczęściej atakowali przedsiębiorstwa z sektora publicznego, branży telekomunikacyjnej, motoryzacyjnej, produkcyjnej oraz dostawców zarządzanych usług bezpieczeństwa (MSSP). Niektórzy jednak zmienili swoją strategię i odchodzą od inicjowania ataku poprzez wiadomości e-mail. Obecnie szczególne znaczenie ma dla nich zdobywanie danych zapewniających dostęp do sieci korporacyjnych i sprzedawanie ich, co przekłada się na rozwój modelu usługowego Ransomware-as-a-Service (RaaS).

Kluczowy wniosek jest taki, że ransomware pozostaje oczywistym i aktualnym zagrożeniem dla wszystkich firm, niezależnie od ich branży i wielkości. Muszą one przyjąć zatem proaktywne podejście do bezpieczeństwa stosować rozwiązania do ochrony urządzeń końcowych w czasie rzeczywistym, wykrywania incydentów i automatycznego reagowania na nie, wraz z podejściem Zero Trust Access, segmentacją sieci i szyfrowaniem.

2. Jedna na cztery firmy wykryła malvertising

W ubiegłym półroczu cyberprzestępcy najchętniej wykorzystywali techniki scareware oraz malvertising. Bazujące na nich ataki dotknęły ponad 25% firm. W tym kontekście należy zwrócić uwagę zwłaszcza na rodzinę trojanów Cryxos, które na zainfekowanych lub złośliwych stronach wyświetlały oszukańcze powiadomienia. Chociaż duża część wykrytych przypadków jest prawdopodobnie połączona z innymi podobnymi kampaniami wykorzystującymi JavaScript, to uznaje się je za malvertising.

Cyberprzestępcy próbują tym samym zareagować na popularność powszechnie praktykowanego hybrydowego trybu pracy i nauki, co przekłada się na zmianę trendów w ich taktyce. Teraz dążą już nie tylko do przestraszenia ofiary, ale też do wymuszenia na niej spełnienia swoich żądań. Ważne jest zatem edukowanie użytkowników sieci i zwiększenie ich świadomości na temat cyberbezpieczeństwa, aby zapobiec atakom typu scareware i malvertising.

3. Trendy dotyczące botnetów wskazują, że cyberprzestępcy atakują brzeg sieci

Gwałtowne nasilenie aktywności odnotowano z kolei w przypadku botnetów. W ciągu pół roku odsetek podmiotów, które wykryły je w swojej sieci, wzrósł z 35% do 51%. Związane jest to z wykorzystywaniem przez cyberprzestępców złośliwego kodu o nazwie

TrickBot. Pierwotnie był to trojan bankowy, ale został rozwinięty do postaci wyrafinowanego zestawu narzędzi do przeprowadzania wieloetapowych ataków.

Wprowadzenie zdalnego trybu pracy i nauki, a wraz z tym zmiana codziennych nawyków, dla cyberprzestępców wciąż stanowią okazję do działania. Z tego powodu najbardziej rozpowszechnionym botnetem był Mirai atakujący urządzenia Internetu rzeczy (IoT) używane przez osoby pracujące lub uczące się w domu. W 2020 roku wyprzedził botneta zdalnego dostępu Ghost i utrzymuje pozycję lidera także w 2021 roku. Ghost natomiast stanowi nadal poważne zagrożenie – umożliwia on przejęcie pełnej kontroli nad zainfekowanym systemem, przechwytywanie na żywo obrazu z kamery internetowej i mikrofonu oraz pobieranie plików. Dlatego, aby chronić sieci i aplikacje, potrzebne jest stosowanie podejścia Zero Trust Access. Znaczne ograniczenie uprawnień dostępu zabezpiecza rozwiązania IoT i inne urządzenia podłączone do sieci.

4. Zaburzenie funkcjonowania środowisk cyberprzestępczych przekłada się na zmniejszenie liczby zagrożeń

Chociaż cyberprzestępcy stają się coraz bardziej skuteczni, w 2021 r. walka z nimi przyniosła pewne sukcesy. W czerwcu twórca TrickBota został postawiony w stan oskarżenia pod wieloma zarzutami. Udało się również wyeliminować Emotet, jeden z najbardziej złośliwych programów w historii. Znaczącym krokiem było także podjęcie działań, które mają na celu przerwanie operacji związanych z należącym do kategorii ransomware oprogramowaniem Egregor, NetWalker i Cl0p. Stanowi to znaczący impuls do dalszej walki z cyberprzestępczością, głownie dla rządów z całego świata i organów ścigania.

Ponadto, duży rozgłos, który towarzyszył niektórym atakom, spowodował wycofanie się z działalności kilku operatorów ransomware. Dane FortiGuard Labs wykazały spowolnienie aktywności cyberprzestępców po wyłączeniu Emoteta. Ataki związane z wariantami TrickBot i Ryuk jeszcze się zdarzały, jednak ich skala była mniejsza. Świadczy to o tym, jak trudno jest natychmiast wyeliminować cyberzagrożenia lub wykorzystywane przez nie łańcuchy dostaw w całości, jednakże wspomniane wydarzenia stanowią ważne osiągnięcia.

5. Cyberprzestępcy preferują techniki unikania oraz eskalację uprawnień

Skrupulatna analiza danych dotyczących cyberzagrożeń pozwala na wyciągnięcie wniosków na temat tego, jak obecnie ewoluują techniki ataków. FortiGuard Labs badało specyficzne funkcje wykrytego złośliwego oprogramowania poprzez uruchomienie jego próbek, aby przyjrzeć się zaimplementowanym przez cyberprzestępców mechanizmom zachowania. W efekcie sporządzono listę negatywnych rezultatów, które złośliwe oprogramowanie mogłoby spowodować, gdyby zostało uruchomione w docelowych środowiskach IT.

Z tego eksperymentu wynika, że przestępcy dążyli między innymi do eskalacji uprawnień, unikania mechanizmów ochronnych, przemieszczania się pobocznymi wobec wewnętrznych systemów ścieżkami oraz wykradania danych. Aż 55% zaobserwowanych funkcji eskalacji uprawnień wykorzystało technikę przechwytywania wywołań systemowych (hooking), zaś w 40% przypadków obecne były mechanizmy wstrzykiwania procesów.

Przykłady te pokazują, że w działalności cyberprzestępców istnieje oczywisty nacisk na stosowanie taktyki unikania obrony i eskalacji przywilejów. Dzięki tym obserwacjom, chociaż techniki te nie są nowe, zespoły ds. cyberbezpieczeństwa będą lepiej przygotowane do obrony przed przyszłymi atakami. Zintegrowane i korzystające z mechanizmów na sztucznej inteligencji (AI) platformowe podejście do bezpieczeństwa, bazujące na informacjach o zagrożeniach, jest niezbędne wobec zmieniającej się sytuacji, przed którą stoją dziś przedsiębiorstwa.

Skuteczność działania zapewni tylko partnerstwo, szkolenia, a także bazująca na sztucznej inteligencji prewencja oraz wykrywanie incydentów i reagowanie na nie

Chociaż instytucje rządowe i organy ścigania podejmowały wspólne akcje przeciw cyberprzestępczości w przeszłości, pierwsza połowa 2021 roku może być przełomowa pod względem tempa działań. Służby współpracują z dostawcami branżowymi, podmiotami zajmującymi się badaniem cyberzagrożeń oraz innymi globalnymi instytucjami partnerskimi. Jest to efekt przyjętej strategii, polegającej na połączeniu zasobów i informacji o cyberzagrożeniach w celu podjęcia bezpośrednich działań przeciwko przestępcom.

Niezależnie od tego, zastosowanie mechanizmów zautomatyzowanego wykrywania zagrożeń i sztucznej inteligencji (AI) pozostaje niezbędne, aby można było reagować na ataki w czasie rzeczywistym, łagodzić ich skutki z odpowiednią szybkością oraz we właściwej skali na każdym brzegu sieci. Ponadto, niezwykle ważne są szkolenia użytkowników w zakresie cyberbezpieczeństwa, ponieważ każdy może stać się ofiarą przestępstwa w sieci. Aby zapewnić ochronę poszczególnym pracownikom i całej firmie, potrzebny jest regularny instruktaż na temat najlepszych praktyk.

„Obserwujemy wzrost liczby skutecznych i niszczycielskich cyfrowych ataków, dotykających tysiące przedsiębiorstw w ramach jednej kampanii, co stanowi ważny punkt zwrotny w wojnie z cyberprzestępczością. Teraz, bardziej niż kiedykolwiek, każda osoba ma do odegrania ważną rolę we wzmocnieniu łańcucha działań mających na celu zneutralizowanie ataków. Połączenie sił dzięki współpracy musi być priorytetem w celu przerwania łańcuchów dostaw cyberprzestępców. Dzielenie się danymi oraz partnerskie relacje umożliwią skuteczniejsze reagowanie i lepsze przewidywanie stosowanych w przyszłości technik w celu powstrzymania działań przeciwników. Ciągłe szkolenia w zakresie świadomości cyberbezpieczeństwa, jak również bazujące na sztucznej inteligencji mechanizmy zapobiegania zagrożeniom, wykrywania ich i reagowania na nie, zintegrowane w urządzeniach końcowych, sieciach i chmurze, pozostaną kluczowe w walce z cyberprzestępcami". Powiedział **Derek Manky**, szef działu Security Insights i Global Threat Alliances, FortiGuard Labs.

Informacje o raporcie

Najnowszy raport Global Threat Landscape Report zawiera zbiorczą analizę opracowaną przez FortiGuard Labs, sporządzoną na podstawie danych z pierwszej połowy 2021 roku, pochodzących z należącej do Fortinetu rozległej sieci czujników, gromadzących miliardy informacji o zagrożeniach obserwowanych na całym świecie. W podobny sposób, jak ramy MITRE ATT&CK klasyfikują taktykę i techniki działania cyberprzestępców w trzech grupach obejmujących rozpoznanie, zarządzanie zasobami i próbę uzyskania dostępu, tak FortiGuard Labs wykorzystuje ten model do opisania w dokumencie Global Threat Landscape Report w jaki sposób hakerzy znajdują luki, budują złośliwą infrastrukturę i eksplorują środowisko ofiary. Raport uwzględnia również perspektywę globalną i regionalną.

BloodyStealer: nowy zaawansowany trojan wycelowany w konta popularnych platform gier online

27.09.2021 r. - Badacze z firmy Kaspersky odkryli zaawansowanego trojana BloodyStealer, sprzedawanego na forach darknetu i wykorzystywanego do kradzieży kont graczy na popularnych platformach do gier, takich jak Steam, Epic Games Store czy EA Origin. Wyposażony w funkcje, które utrudniają wykrycie oraz analizowanie go, jak również w kilka interesujących możliwości, a do tego oferowany w niskiej cenie subskrypcyjnej, BloodyStealer to doskonały przykład zagrożeń, z jakimi stykają się gracze online. Informacje o nim, jak również przegląd produktów związanych z grami kradzionymi i sprzedawanymi w darknecie można znaleźć w najnowszym raporcie[24] firmy Kaspersky dot. zagrożeń związanych z grami.

Jak wynika z najnowszego badania firmy Kaspersky, w darknecie istnieje zapotrzebowanie na przedmioty oraz konta w grach. Loginy do gier wraz z hasłami do popularnych platform, takich jak Steam, Origin, Ubisoft czy EpicGames, można kupić już za około 55 zł za tysiąc kont w sprzedaży hurtowej oraz za 1-30% wartości konta w sprzedaży detalicznej. Skradzione konta nie pochodzą z przypadkowych wycieków danych, ale są raczej wynikiem celowych kampanii cyberprzestępczych z wykorzystaniem szkodliwego oprogramowania, takiego jak BloodyStealer.

BloodyStealer to trojan kradnący informacje, który gromadzi i potajemnie wyprowadza różne rodzaje danych, takich jak np. pliki cookie, hasła, formularze, karty bankowe, z przeglądarek, zrzutów ekranu, pamięci logowania czy sesji z różnych aplikacji. Obejmują one sesje gier, w szczególności na platformach EpicGames, Origin oraz Steam

Badacze z firmy Kaspersky po raz pierwszy zauważyli omawianego trojana w marcu 2021 r., gdy reklamowano jego możliwości unikania wykrycia oraz ochrony przed inżynierią wsteczną oraz ogólnie analizą szkodliwego oprogramowania. Szkodnik jest sprzedawany na forach czarnorynkowych w atrakcyjnej cenie – niecałe 40 zł za miesięczną subskrypcję lub około 150 zł za dożywotnią subskrypcję.

Szkodnik zwrócił uwagę badaczy ze względu na wykorzystywanie kilku metod służących skomplikowaniu analizy oraz inżynierii wstecznej, łącznie z użyciem kompresji oraz technik zapobiegających debugowaniu. Trojan jest sprzedawany na czarnym rynku, a klienci mogą zabezpieczyć go za pomocą wybranego przez siebie mechanizmu kompresji lub wykorzystywać w ramach innego wieloetapowego łańcucha infekcji. Eksperci z firmy Kaspersky wykryli ataki wykorzystujące trojana BloodyStealer w Europie, w Ameryce Łacińskiej oraz rejonie Azji i Pacyfiku.

O ile BloodyStealer nie został stworzony wyłącznie w celu kradzieży informacji dotyczących gier, atakowane przez niego platformy wyraźnie wskazują na zapotrzebowanie na tego rodzaju dane wśród cyberprzestępców. Dane logowania, konta, przedmioty w grach – wszystkie te „produkty" związane z grami są sprzedawane hurtowo bądź indywidualnie w darknecie w atrakcyjnej cenie.

[24] *https://securelist.com/bloodystealer-and-gaming-assets-for-sale/104319/*

NetActuate otwiera nowe data center w Warszawie i zapowiada rozwój oferty IaaS w Europie

28.09.2021 r. - NetActuate, dostawca brzegowej mocy obliczeniowej w modelu IaaS, otworzył nowe centrum danych w Warszawie. Oznacza to uruchomienie wszystkich usług operatora jednej z pięciu największych (pod względem liczby węzłów) sieci IPv4 i IPv6 na świecie – w tym anycast, maszyn wirtualnych, bare metal i kolokacji – z Warszawy.

„Nasze nowe wdrożenie w Polsce umożliwia nam oferowanie solidnego zestawu globalnych usług infrastruktury brzegowej zlokalizowanych w Europie Środkowej" — powiedział **Mark Mahle**, dyrektor generalny i główny architekt technologiczny firmy NetActuate. „Strategiczna lokalizacja Warszawy zwiększa wydajność i niezawodność naszej sieci dla użytkowników końcowych zarówno na rynkach Europy Wschodniej, jak i Zachodniej".

Warszawskie data center NetActuate zlokalizowane jest w ścisłym centrum biznesowym stolicy. W tej lokalizacji klienci mogą wybierać z szerokiej gamy usług sieciowych, a także mogą łączyć się bezpośrednio z klientami i partnerami w swoim cyfrowym łańcuchu dostaw. Placówka ta zapewnia również bezpośredni dostęp do Equinix Internet Exchange™ Poland (dawniej PLIX), który jest największym punktem wymiany ruchu internetowego w Polsce. Warszawska lokalizacja NetActuate oferuje najno-

wocześniejsze standardy bezpieczeństwa i posiada certyfikaty zgodności z normami ISO 22301, ISO 27001, ISO 9001:2015 i PCI DSS.

Uruchomienie usług w Polsce jest częścią większego planu rozwoju NetActuate w Europie.

„W najbliższym czasie planujemy uruchomienie nowej platformy IaaS pod nazwą vmgen. Dzięki vmgen użytkownicy będą mogli korzystać z globalnej infrastruktury brzegowej w niezwykle prosty i szybki sposób" - powiedział **Kacper Dąbrowski**, Dyrektor ds. Projektów Europejskich w NetActuate i Dyrektor Generalny vmgen. „Nowy projekt jest dedykowany na rynki Europejskie, a pracuje nad nim ciągle rozwijany zespół programistów w Polsce".

Dostawcy usług cyfrowych mogą łatwo wdrożyć i rozszerzać swoją globalną obecność na platformie Anycast NetActuate, stworzonej z myślą o zapewnieniu niskich opóźnień i wysokiej niezawodności. W ramach globalnego zasięgu NetActuate klienci mogą wdrażać swoje środowiska hybrydowe w Polsce oraz w ponad 30 innych lokalizacjach na całym świecie, bez konieczności zarządzania wieloma dostawcami ich infrastruktury i usług sieciowych.

Spyware FinFisher wraca z rozbudowanym arsenałem

kaspersky

29.09.2021 r. - Badacze z firmy Kaspersky opublikowali wyniki szczegółowego badania dotyczącego wszystkich nowości, o jakie wzbogacone zostało niedawno oprogramowanie spyware FinSpy dla systemu Windows, macOS oraz Linux. Prowadzona przez osiem miesięcy analiza ujawniła stosowane przez twórców tego szkodnika zaawansowane metody zaciemniania kodu oraz inne mechanizmy przeciwdziałania analizie, jak również użycie modułu infekującego UEFI w maszynach ofiar. Wyniki badania sugerują duży nacisk na obchodzenie mechanizmów ochrony przez szkodnika, które sprawia, że FinFisher to jak dotąd jedno z najtrudniejszych do wykrycia narzędzi spyware.

FinFisher, znany również jako FinSpy lub Wingbird, to narzędzie do monitoringu, które firma Kaspersky obserwuje od 2011 r. Potrafi gromadzić różne dane uwierzytelniające, wykazy plików oraz różne dokumenty, a ponadto przesyłać strumieniowo lub rejestrować dane oraz uzyskiwać dostęp do kamery internetowej i mikrofonu. Jego implanty dla systemu Windows były wielokrotnie badane do 2018 r., gdy wydawało się, że FinFisher zniknął ze sceny.

Później jednak rozwiązania firmy Kaspersky wykryły podejrzane instalatory legalnych aplikacji, takich jak TeamViewer, VLC Media Player oraz WinRAR, zawierające niebezpieczny kod, którego nie dało się powiązać z żadnym znanym szkodliwym oprogramowaniem. Tak było do czasu wykrycia strony internetowej w języku birmańskim zawierającej zainfekowane instalatory oraz próbki FinFishera dla systemu Android. Odkrycie to skłoniło badaczy z firmy Kaspersky do kontynuowania badań.

W przeciwieństwie do wcześniejszych wersji szkodnika, które od razu zawierały trojana w zainfekowanej aplikacji, nowe próbki są chronione przez dwa komponenty. Pierwszy przeprowadza kilka testów bezpieczeństwa, aby sprawdzić, czy infekowane urządzenie nie należy do badacza bezpieczeństwa. Jeśli tak nie jest, serwer dostarcza drugi komponent, który ma potwierdzić, że infekowana ofiara jest zamierzonym celem. Dopiero wtedy serwer wydaje polecenie zainstalowania pełnoprawnego trojana.

FinFisher został poddany zaciemnianiu przy pomocy czterech złożonych, niestandardowych narzędzi. Głównym celem tego procesu jest spowolnienie analizy. Ponadto trojan stosuje nietypowe sposoby gromadzenia informacji. Na przykład wykorzystuje tryb programisty w przeglądarkach w celu przechwytywania ruchu chronionego przy użyciu protokołu HTTPS.

Badacze wykryli również próbkę szkodnika FinFisher, która zastępowała menedżera rozruchu Windows UEFI – komponent, który uruchamia system operacyjny po starcie oprogramowania układowego wraz ze szkodnikiem. W ten sposób atakujący mogą zainstalować szkodliwy kod bez konieczności obchodzenia zabezpieczeń oprogramowania układowego. Infekcje UEFI są niezwykle rzadkie i ogólnie trudne do przeprowadzenia. Wyróżniają się tym, że umożliwiają długotrwałe utrzymywanie się szkodnika w systemie. Chociaż w omawianym przypadku cyberprzestępcy nie infekują samego oprogramowania układowego UEFI, a jedynie etap rozruchu, atak ten cechował się wyjątkową ukradkowością, ponieważ szkodliwy moduł został zainstalowany na oddzielnej partycji i mógł kontrolować proces uruchamiania zainfekowanego urządzenia.

Szczegóły techniczne dotyczące trojana FinFisher są dostępne na stronie https://r.kaspersky.pl/elfFI.

Trojan Tomiris może wskazywać na wznowioną aktywność cybergangu stojącego za atakiem Sunburst

kaspersky

30.09.2021 r. - nalizując nieznane dotąd zaawansowane cyberzagrożenie, badacze z firmy Kaspersky trafili na nowe szkodliwe oprogramowanie posiadające kilka istotnych atrybutów łączących je z DarkHalo – cybergangiem stojącym za atakiem Sunburst[25]. Atak ten należy do najbardziej znaczących incydentów naruszenia bezpieczeństwa łańcucha dostaw ostatnich lat.

O wspomnianym incydencie zrobiło się głośno w grudniu 2020 r. cyberugrupowanie DarkHalo złamało zabezpieczenia dostawcy oprogramowania dla przedsiębiorstw i przez długi czas wyko-

rzystywało jego infrastrukturę do rozprzestrzeniania narzędzia szpiegowskiego pod przykrywką legalnych aktualizacji aplikacji. Wydaje się, że szum medialny wokół ataku oraz zainteresowanie, jakie wzbudził w społeczności związanej z bezpieczeństwem, sprawiły, że wspomniany gang zniknął ze sceny. Jednak z badania przeprowadzonego niedawno przez Globalny Zespół ds. Badań i Analiz (GReAT) firmy Kaspersky wynika, że niekoniecznie tak było.

W czerwcu 2021 r., ponad sześć miesięcy po zniknięciu DarkHalo, badacze z firmy Kaspersky znaleźli ślady udanego ataku przejęcia DNS uderzającego w kilka organizacji rządowych w tym samym państwie. Przejęcie DNS to rodzaj ataku polegający na zmodyfikowaniu nazwy domeny (służącej do tłumaczenia adresu URL strony internetowej na adres IP serwera, na którym dany zasób jest przechowywany) w taki sposób, aby ruch sieciowy był przekierowywany do serwera kontrolowanego przez cyberprzestępców. W przykładzie zidentyfikowanym przez firmę Kaspersky cele ataku próbowały uzyskać dostęp do interfejsu WWW firmowego serwisu e-mail, jednak były przekierowywane do fałszywej kopii tego zasobu, a następnie podstępnie nakłaniane do pobrania zainfekowanej aktualizacji oprogramowania. Podążając tropem atakujących, badacze z firmy Kaspersky zdobyli tę „aktualizację" i odkryli, że instalowała ona nieznanego wcześniej trojana o nazwie Tomiris.

Dalsza analiza wykazała, że głównym celem szkodnika było zagnieżdżenie się w atakowanym systemie oraz pobieranie innych szkodliwych komponentów. Niestety, nie udało się ich zidentyfikować podczas badania. Zauważono natomiast jedną istotną rzecz: Tomiris wykazywał podejrzane podobieństwo do narzędzia Sunshuttle – szkodnika instalowanego w następstwie ataku Sunburst.

Poniższa lista podobieństw nie jest wyczerpująca:

- Podobnie jak Sunshuttle, trojan Tomiris został stworzony w języku programowania Go.
- Każdy z trojanów stosuje jedną metodę szyfrowania/zaciemniania w celu zakodowania zarówno konfiguracji atakowanej maszyny, jak i ruchu sieciowego.
- Oba szkodniki stosują podobne techniki mające na celu długotrwałe utrzymanie się w zainfekowanym systemie.
- Podobieństwa w kodzie wskazują na zastosowanie tych samych technik programistycznych.
- Występowanie błędów językowych w kodzie trojanów może wskazywać na to, że oba szkodliwe programy zostały napisane przez osoby, dla których angielski nie jest językiem ojczystym – powszechnie uznaje się, że cybergang DarkHalo jest rosyjskojęzyczny.
- Trojan Tomiris został wykryty w sieciach, w których inne maszyny były zainfekowane szkodnikiem Kazuar, o którym wiadomo, że jego kod pokrywa się częściowo[26] z kodem trojana Sunshuttle.

„Żadne z powyższych podobieństw, rozpatrywane indywidualnie, nie daje wystarczającej podstawy, by z wystarczającym stopniem pewności powiązać trojana Tomiris ze szkodnikiem Sunshuttle. Przyznajemy, że wiele z tych podobieństw może być przypadkowych, jednak mimo to uważamy, że wszystkie razem mogą sugerować, że szkodniki te zostały stworzone przez te same osoby" – powiedział **Pierre Delcher**, badacz ds. cyberbezpieczeństwa z firmy Kaspersky.

„Jeśli nasze przypuszczenie o istnieniu powiązania między trojanami Tomiris oraz Sunshuttle jest słuszne, rzuca ono nieco światła na sposób, w jaki cyberprzestępcy odbudowują swoje zasoby po tym, jak zostaną „złapani". Zachęcamy społeczność związaną z analizowaniem zagrożeń do odtworzenia naszego badania oraz przedstawienia dodatkowych opinii dotyczących wykrytych przez nas podobieństw między tymi trojanami" – dodał **Iwan Kwiatkowski**, badacz ds. cyberbezpieczeństwa z firmy Kaspersky.

Szczegóły techniczne związane ze związkami pomiędzy trojanem Tomiris a atakiem Sunburst znajdują się na stronie https://r.kaspersky.pl/ZB7c9.

[25] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3353/kaspersky-publikuje-wstepna-analize-szkodliwego-oprogramowania-sunburst-i-udostepnia-dekoder-by-pomoc-w-wyszukiwaniu-potencjalnych-ofiar-cyberataku*

[26] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3357/brakujace-ogniwo-badacze-z-firmy-kaspersky-lacza-atak-na-firme-solarwinds-z-backdoorem-kazuar*

GUS ujawnił e-maile kilkuset Polaków ze Spisu Powszechnego

30.09.2021 r. - Pewien czytelnik serwisu internetowego Niebezpiecznik otrzymał odpowiedź na swoje pytanie, które zadał jakiś czas temu Głównemu Urzędowi Statystycznemu. Wygląda na to, że jego pytanie było podobne do pytań wielu innych Polaków, bo w otrzymanym e-mailu zwrotnym znalazło się ponad pół tysiąca innych adresów e-mail.

Kiedy pracowniczka GUS-u zdała sobie sprawę z pomyłki, próbowała „Odwołać wiadomość". Nie wiedziała jednak, iż ta funkcja powoduje ponowny wyciek danych, bo wysyła do wszystkich kolejną wiadomość, którą klienty pocztowe spoza domeny nadawcy (czyli GUS) ignorują, pokazując jej zabawną treść...

Inny z czytelników, który też został ujęty w odbiorcach wspomnianej wiadomości, poinformował redaktorów Niebezpiecznika, że po pewnym czasie otrzymał przeprosiny z prośbą o skasowanie poprzedniej wiadomości.

Warto dodać, że GUS ujawnił dane tylko osób, które się spisały — w tym ich adresy e-mail. Tymczasem Niebezpiecznik zaprezentował kolejną wiadomość (chociaż ta była przeznaczona dla rachmistrzów), o której powiadomił również jeden z czytelników.

Jak widać, błędy ludzkie się zdarzają, a w takich sytuacjach nie pomogą nawet najlepsze systemy. Jak zauważają redaktorzy Niebezpiecznika, taki incydent uniemożliwiłaby chociażby poprawna konfiguracja serwerów pocztowych GUS-u.

Raport FortiGuard Labs: Ataki z użyciem ransomware'u zdarzają się dziesięć razy częściej niż rok temu

Fortinet, globalny lider w dziedzinie zintegrowanych i zautomatyzowanych rozwiązań cyberochronnych, przedstawił najnowszą edycję raportu pt. „Global Threat Landscape" opracowanego przez analityków FortiGuard Labs. Dane dotyczące zagrożeń zaobserwowanych w pierwszej połowie 2021 r. wskazują na znaczny wzrost liczby i poziomu wyrafinowania ataków skierowanych przeciwko osobom prywatnym, przedsiębiorstwom oraz infrastrukturze krytycznej. Na celowniku cyberprzestępców nadal znajduje się rosnąca liczba osób pracujących i uczących się zdalnie. Podjęta w odpowiednim czasie współpraca pomiędzy organami ścigania, a także podmiotami z sektora publicznego i prywatnego daje szansę na zakłócenie działań cyberprzestępców w drugiej połowie 2021 roku.

Oto najważniejsze informacje z raportu za pierwsze półrocze 2021 r:

1. W cyberatakach typu ransomware chodzi o coś więcej niż pieniądze

Dane FortiGuard Labs wskazują, że aktywność oprogramowania ransomware w czerwcu 2021 r. była ponad dziesięć razy wyższa niż rok temu. Świadczy to o konsekwentnym i stałym wzroście popularności tego narzędzia. Incydenty z użyciem ransomware'u sparaliżowały łańcuchy dostaw wielu przedsiębiorstw, szczególnie w branżach o krytycznym znaczeniu. Bardziej niż kiedykolwiek wpłynęły na życie codzienne, handel, produktywność pracowników itd.

Cyberprzestępcy najczęściej atakowali przedsiębiorstwa z sektora publicznego, branży telekomunikacyjnej, motoryzacyjnej, produkcyjnej oraz dostawców zarządzanych usług bezpieczeństwa (MSSP). Niektórzy jednak zmienili swoją strategię i odchodzą od inicjowania ataku poprzez wiadomości e-mail. Obecnie szczególne znaczenie ma dla nich zdobywanie danych zapewniających dostęp do sieci korporacyjnych i sprzedawanie ich, co przekłada się na rozwój modelu usługowego Ransomware-as-a-Service (RaaS).

Kluczowy wniosek jest taki, że ransomware pozostaje oczywistym i aktualnym zagrożeniem dla wszystkich firm, niezależnie od ich branży i wielkości. Muszą one przyjąć zatem proaktywne podejście do bezpieczeństwa stosować rozwiązania do ochrony urządzeń końcowych w czasie rzeczywistym, wykrywania incydentów i automatycznego reagowania na nie, wraz z podejściem Zero Trust Access, segmentacją sieci i szyfrowaniem.

2. Jedna na cztery firmy wykryła malvertising

W ubiegłym półroczu cyberprzestępcy najchętniej wykorzystywali techniki scareware oraz malvertising. Bazujące na nich ataki dotknęły ponad 25% firm. W tym kontekście należy zwrócić uwagę zwłaszcza na rodzinę trojanów Cryxos, które na zainfekowanych lub szkodliwych stronach wyświetlały oszukańcze powiadomienia. Chociaż duża część wykrytych przypadków jest prawdopodobnie połączona z innymi podobnymi kampaniami wykorzystującymi JavaScript, to uznaje się je za malvertising.

Cyberprzestępcy próbują tym samym zareagować na popularność powszechnie praktykowanego hybrydowego trybu pracy i nauki, co przekłada się na zmianę trendów w ich taktyce. Teraz dążą już nie tylko do przestraszenia ofiary, ale też do wymuszenia na niej spełnienia swoich żądań. Ważne jest zatem edukowanie użytkowników sieci i zwiększenie ich świadomości na temat cyberbezpieczeństwa, aby zapobiec atakom typu scareware i malvertising.

3. Trendy dotyczące botnetów wskazują, że cyberprzestępcy atakują brzeg sieci

Gwałtowne nasilenie aktywności odnotowano z kolei w przypadku botnetów. W ciągu pół roku odsetek podmiotów, które wykryły je w swojej sieci, wzrósł z 35% do 51%. Związane jest to z wykorzystywaniem przez cyberprzestępców szkodliwego kodu o nazwie TrickBot. Pierwotnie był to trojan bankowy, ale został rozwinięty do postaci wyrafinowanego zestawu narzędzi do przeprowadzania wieloetapowych ataków.

Wprowadzenie zdalnego trybu pracy i nauki, a wraz z nim zmiana codziennych nawyków, dla cyberprzestępców wciąż stanowią okazję do działania. Z tego powodu najbardziej rozpowszechnionym botnetem był Mirai atakujący urządzenia internetu rzeczy (IoT) używane przez osoby pracujące lub uczące się w domu. W 2020 roku wyprzedził on botnet zdalnego dostępu Ghost i utrzymuje pozycję lidera także w 2021 roku. Ghost natomiast stanowi nadal poważne zagrożenie – umożliwia on przejęcie pełnej kontroli nad zainfekowanym systemem, przechwytywanie na żywo obrazu z kamery internetowej i mikrofonu oraz pobieranie plików. Dlatego, aby chronić sieci i aplikacje, konieczne jest stosowanie podejścia Zero Trust Access — znaczne ograniczenie uprawnień dostępu zabezpiecza rozwiązania IoT i inne urządzenia podłączone do sieci.

4. Zaburzenie funkcjonowania środowisk cyberprzestępczych przekłada się na zmniejszenie liczby zagrożeń

Chociaż cyberprzestępcy stają się coraz skuteczniejsi, w 2021 r. walka z nimi przyniosła pewne sukcesy. W czerwcu twórca TrickBota został postawiony w stan oskarżenia pod wieloma zarzutami. Udało się również wyeliminować Emotet, jeden

z najbardziej szkodliwych programów w historii. Znaczącym krokiem było także podjęcie działań, które mają na celu przerwanie operacji związanych z należącym do kategorii ransomware oprogramowaniem Egregor, NetWalker i Clop. Stanowi to znaczący impuls do dalszej walki z cyberprzestępczością, głownie dla rządów z całego świata i organów ścigania.

Ponadto duży rozgłos, który towarzyszył niektórym atakom, spowodował wycofanie się z działalności kilku operatorów ransomware. Dane FortiGuard Labs wykazały spowolnienie aktywności cyberprzestępców po wyłączeniu Emoteta. Ataki związane z wariantami TrickBot i Ryuk jeszcze się zdarzały, jednak ich skala była mniejsza. Świadczy to o tym, jak trudno jest natychmiast wyeliminować cyberzagrożenia lub wykorzystywane przez nie łańcuchy dostaw w całości, jednakże wspomniane wydarzenia stanowią ważne osiągnięcia.

5. Cyberprzestępcy preferują techniki unikania oraz eskalację uprawnień

Skrupulatna analiza danych dotyczących cyberzagrożeń pozwala na wyciągnięcie wniosków na temat tego, jak obecnie ewoluują techniki ataków. FortiGuard Labs badało specyficzne funkcje wykrytego szkodliwego oprogramowania poprzez uruchomienie jego próbek, aby przyjrzeć się zaimplementowanym przez cyberprzestępców mechanizmom zachowania. W efekcie sporządzono listę negatywnych rezultatów, które szkodliwe oprogramowanie mogłoby spowodować, gdyby zostało uruchomione w docelowych środowiskach IT.

Z tego eksperymentu wynika, że przestępcy dążyli między innymi do eskalacji uprawnień, unikania mechanizmów ochronnych, przemieszczania się pobocznymi wobec wewnętrznych systemów ścieżkami oraz wykradania danych. Aż 55% zaobserwowanych funkcji eskalacji uprawnień wykorzystało technikę przechwytywania wywołań systemowych (ang. hooking), zaś w 40% przypadków obecne były mechanizmy wstrzykiwania procesów.

Przykłady te pokazują, że w działalności cyberprzestępców istnieje oczywisty nacisk na stosowanie taktyki unikania obrony i eskalacji przywilejów. Chociaż techniki te nie są nowe, dzięki tym obserwacjom zespoły ds. cyberbezpieczeństwa będą lepiej przygotowane do obrony przed przyszłymi atakami. Zintegrowane i korzystające z mechanizmów na sztucznej inteligencji (AI) platformowe podejście do bezpieczeństwa, bazujące na informacjach o zagrożeniach, jest niezbędne wobec zmieniającej się sytuacji, przed którą stoją dziś przedsiębiorstwa.

Skuteczność działania zapewni tylko partnerstwo, szkolenia, a także bazująca na sztucznej inteligencji prewencja oraz wykrywanie incydentów i reagowanie na nie

Chociaż instytucje rządowe i organy ścigania podejmowały wspólne akcje przeciw cyberprzestępczości w przeszłości, pierwsza połowa 2021 roku może być przełomowa pod względem tempa działań. Służby współpracują z dostawcami branżowymi, podmiotami zajmującymi się badaniem cyberzagrożeń oraz innymi globalnymi instytucjami partnerskimi. Jest to efekt przyjętej strategii polegającej na połączeniu zasobów i informacji o cyberzagrożeniach w celu podjęcia bezpośrednich działań przeciwko przestępcom.

Niezależnie od tego, zastosowanie mechanizmów zautomatyzowanego wykrywania zagrożeń i sztucznej inteligencji (AI) pozostaje niezbędne, aby można było reagować na ataki w czasie rzeczywistym, łagodzić ich skutki z odpowiednią szybkością oraz we właściwej skali na każdym brzegu sieci. Ponadto niezwykle ważne są szkolenia użytkowników w zakresie cyberbezpieczeństwa, ponieważ każdy może stać się ofiarą przestępstwa w sieci. Aby zapewnić ochronę poszczególnym pracownikom i całej firmie, potrzebny jest regularny instruktaż na temat najlepszych praktyk.

Derek Manky, szef działu Security Insights i Global Threat Alliances, FortiGuard Labs, powiedział:

„Obserwujemy wzrost liczby skutecznych i niszczycielskich cyfrowych ataków, dotykających tysiące przedsiębiorstw w ramach jednej kampanii, co stanowi ważny punkt zwrotny w wojnie z cyberprzestępczością. Teraz bardziej niż kiedykolwiek wcześniej każda osoba ma do odegrania ważną rolę we wzmocnieniu łańcucha działań mających na celu zneutralizowanie ataków. Połączenie sił dzięki współpracy musi być priorytetem w celu przerwania łańcuchów dostaw cyberprzestępców. Dzielenie się danymi oraz partnerskie relacje umożliwią skuteczniejsze reagowanie i lepsze przewidywanie stosowanych w przyszłości technik w celu powstrzymania działań przeciwników. Ciągłe szkolenia w zakresie świadomości cyberbezpieczeństwa, jak również bazujące na sztucznej inteligencji mechanizmy zapobiegania zagrożeniom, wykrywania ich i reagowania na nie, zintegrowane w urządzeniach końcowych, sieciach i chmurze, pozostaną kluczowe w walce z cyberprzestępcami".

Działania podmiotów z sektora publicznego i prywatnego, mające na celu przerwanie łańcuchów dostaw cyberprzestępczości, nabierają tempa.

Informacje o raporcie

Najnowszy raport zatytułowany „Global Threat Landscape Report" zawiera zbiorczą analizę opracowaną przez FortiGuard Labs, sporządzoną na podstawie danych z pierwszej połowy 2021 roku, pochodzących z ależącej do Fortinetu rozległej sieci czujników, gromadzących miliardy informacji o zagrożeniach obserwowanych na całym świecie. Tak jak ramy MITRE ATT&CK klasyfikują taktykę i techniki działania cyberprzestępców w trzech grupach obejmujących rozpoznanie, zarządzanie zasobami i próbę uzyskania dostępu, tak FortiGuard Labs wykorzystuje ten model do opisania w dokumencie Global Threat Landscape Report, w jaki sposób hakerzy znajdują luki, budują szkodliwą infrastrukturę i eksplorują środowisko ofiary. Raport uwzględnia również perspektywę globalną i regionalną.

Czy firmy powinny płacić okup cyberprzestępcom?

Łukasz Bromirski, ekspert Cisco odpowiedzialny za rozwój produktów z obszaru cyberbezpieczeństwa

Płacić, czy nie płacić – oto jest pytanie... warte nawet miliony złotych. Ransomware to słowo, które spędza sen z powiek setkom szefów działów IT na całym świecie. Ataki za pomocą tzw. oprogramowania wymuszającego okup są coraz częstsze, a ich liczba rośnie z roku na rok.

W tym roku byliśmy już świadkami kilkuset ataków, w tym tych najgłośniejszych i najbardziej zuchwałych: na firmy CD Projekt RED, Kaseya czy Colonial Pipeline w Stanach Zjednoczonych. Warto jednak pamiętać, że większość tego typu zdarzeń nie trafia na pierwsze strony gazet.

Ryzyko zapłaty

„Mamy kontrolę nad wszystkimi twoimi danymi. Zapłać X bitcoinów, a my je odblokujemy".

Nie ma prostej odpowiedzi na tak postawione żądanie – nie mamy tu bowiem do czynienia z sytuacją zero-jedynkową – „nigdy nie płacić okupu" kontra „po prostu zapłacić okup". Jak podkreślają specjaliści, można znaleźć argumenty zarówno „za", jak i „przeciw" płaceniu cyberprzestępcom. Każdy tego typu incydent należy jednak przeanalizować osobno.

Wyobraźmy sobie, że firma X decyduje się na zapłatę. W ten sposób bezpośrednio finansuje nielegalne działania przestępców; pośrednio pokazuje zaś, że ufa tym, którzy właśnie włamali się do jej sieci i uczynili z niej zakładnika. Nie ma przecież gwarancji, że po wpłaceniu okupu intruzi odblokują dane. A nawet jeśli to uczynią, wciąż trzeba będzie stawić czoła kolejnym zagrożeniom. Dzisiaj na zapłatę decydują się w szczególności duże firmy. Na tę sytuację powoli negatywnie zaczynają reagować ubezpieczyciele, którzy podnoszą składki.

Po pierwsze, zapłacenie okupu nie sprawi, że cyberprzestępcy samoistnie znikną z zaatakowanego środowiska.

Płatność nie naprawi również błędów w zabezpieczeniach, a to przecież to przez nie atakującym udało się zdobyć przyczółek w sieci. W większości wypadków cyberprzestępcy nie dzielą się nawet wiedzą, jak udało im się włamać, a nawet jeśli to zrobią – na ile można im ufać, że podzielili się wszystkimi informacjami? Zaatakowana organizacja nie ma pewności, czy faktycznie poznała wszystkie możliwe do wykorzystania furtki . Cyberprzestępcy na pewno skorzystają z kolejnej okazji, jeżeli taka się nadarzy.

Po drugie, biznesowa zasada mówi, że łatwiej jest generować przychody z istniejących klientów, niż szukać nowych. Ta prawidłowość ma zastosowanie również wśród hakerów. Nawet nie mając sprawdzonej ścieżki ataku, wykonali już mapowanie sieci, aplikacji i być może mają znacznie więcej danych i dostępów, niż przyznają. Przykładowo pełną listę kont z uprawnieniami administratora, do których hasła już złamali, albo złamią w ciągu najbliższych godzin czy dni. Mogą chcieć ponownie „spróbować szczęścia" z tą samą organizacją.

Po trzecie, nigdy nie można mieć pewności, że odblokowane dane nie zostały przypadkowo uszkodzone. Zawsze coś może pójść nie tak, nawet jeśli atakujący za pomocą oprogramowania ransomware stara się postępować „zgodnie ze sztuką". Wiele było już przypadków, gdy rzekome oprogramowanie odszyfrowujące lub klucz wpisany do szkodliwego oprogramowania uszkadzał pliki w wyniku zwykłych ludzkich błędów programistycznych.

W efekcie kwota okupu to tak naprawdę tylko jeden z pierwszych kosztów. Zaatakowana firma będzie musiała ponieść też inne nakłady finansowe, począwszy od gruntownego audytu, łatania platform IT w celu usunięcia pierwotnej przyczyny włamania (jeśli jest znana) czy wreszcie zorganizowania szkoleń z zakresu cyberbezpieczeństwa, jeśli wektorem ataku był np. udany phishing. W przeciwnym razie (choć gwarancji nie ma przecież nigdy) firma znowu padnie ofiarą ataku i stanie przed tą samą decyzją: czy płacić okup.

Okup to ostateczność

Zapłacenie okupu powinno być ostatecznością dla każdej ofiary cyberprzestępstwa. Zrozumiałe jest jednak, że niektórzy decydują się na zapłatę, ponieważ w wielu przypadkach stanowi to realnie niewielki procent całkowitych kosztów naprawy sytuacji. Na przykład, w zeszłym roku miasto Atlanta w Stanach Zjednoczonych wydało około 17 milionów dolarów na przywrócenie systemów po ataku ransomware, podczas gdy napastnicy początkowo zażądali okupu w wysokości 52 tys. dolarów.

To oczywiste, że przypadki włamań mających poważne konsekwencje społeczne lub potencjalnie wpływających na bezpieczeństwo ludzi będą stanowiły silniejszy bodziec do zapłaty.

Bycie nieatrakcyjnym to zaleta

Czy to się komuś podoba, czy nie, gdy organizacja pada ofiarą ataku ransomware i zdecyduje się zapłacić, staje się partnerem biznesowym cyberprzestępców — ludzi, których tożsamość pozostaje anonimowa i najprawdopodobniej nie zostaną pociągnięci do odpowiedzialności przez organy ścigania. Gdy doszło do ataku, cyberprzestępcy trzymają w ręku wszystkie karty. Każda firma chciałaby uniknąć powyższego scenariusza, dlatego warto przedsięwziąć kilka kroków zaradczych.

Eksperci Cisco radzą, aby spojrzeć na swoją firmę tak, jak zrobiłby to napastnik. Dzięki temu można łatwiej dostrzec słabe punkty w ramach całej architektury IT. Kolejny krok to ustalenie priorytetów i zniwelowanie podatności na atak. Cyberprzestępców przyciąga łatwy i szybki zarobek – okazując się drogim i trudnym celem, stajemy się nieatrakcyjni. I to się opłaca.

Zdaniem specjalistów Cisco nigdy nie wolno zakładać, że jesteśmy w pełni chronieni przed hakerami. Warto wziąć poprawkę na to, że nawet najlepsza architektura, jeśli zostanie zaatakowana, może nie wytrzymać takiej próby. Wtedy niezbędny okaże się przygotowany wcześniej plan awaryjny obejmujący utrzymanie procesów i odtworzenie kopii zapasowych dotyczących wszystkich najistotniejszych obszarów działania organizacji — takich jak dział prawny, dział kadr i finansów, IT, zespoły produkcyjne czy zarząd. Ponadto warto przeprowadzać testy z realnej skuteczności swoich planów – często okazuje się, że drobne pomyłki czy przeoczenia mogą być opłakane w skutkach, a cały misternie budowany plan runie jak domek z kart.

Grupa do zadań specjalnych

Departament Sprawiedliwości Stanów Zjednoczonych, Europol oraz kilka największych firm technologicznych na świecie, w tym Cisco, utworzyły grupę zadaniową ds. oprogramowania ransomware, aby zwalczać problem u źródła. Inicjatorzy przedsięwzięcia zgodnie uzn ali, że współpraca międzynarodowa i publiczno-prywatna mają kluczowe znaczenie dla osiągnięcia tego celu.

Musimy skierować nasze wysiłki na to, by jak najlepiej zrozumieć, w jaki sposób działają twórcy oprogramowania ransomware. Naszym celem nadrzędnym jest ostateczne rozbicie grup cyberprzestępczych zajmujących się oprogramowaniem służącym do wymuszania okupu oraz odstraszenie ich potencjalnych następców. Oczywiście nie jest to zagadnienie banalne, ale każda działalność podnosząca koszt po stronie atakujących to większa szansa dla obrońców. Rozsądnie zorganizowana architektura bezpieczeństwa to pierwszy krok. Dobrze przygotowany zespół to kolejny etap. Ważne jest również wsparcie specjalistów posiadających szeroką wiedzę o zagrożeniach, która pochodzi z używanych w firmie systemów. Większość atakujących wycofa się po pierwszych niepowodzeniach. Znamy również przypadki firm, w których doszło do włamania, ale dzięki wykorzystaniu najlepszych praktyk bezpieczeństwa (segmentacja sieci, uwierzytelnianie wieloskładnikowe, zasada ograniczonych uprawnień w myśl filozofii „zerowego zaufania") miało ono tak ograniczony zasięg, że atakujący rezygnowali z dalszych prób złamania zabezpieczeń.

Na czym tak naprawdę polega reguła 3-2-1 w tworzeniu kopii zapasowych?

Rick Vanover, dyrektor ds. strategii produktowej w Veeam

3-2-1 to reguła, którą warto pielęgnować. W Veeam propagujemy ją od wielu lat, aby zapewnić organizacjom możliwość odzyskiwania danych wtedy, gdy jest to najbardziej potrzebne. Objaśnię zatem regułę 3-2-1 i pokażę sposób, w jaki można przekształcić ją w bardziej nowoczesny sposób myślenia, który wspiera odporność organizacji.

Co to jest reguła 3-2-1?

Regułę 3-2-1 po raz pierwszy zaproponował amerykański fotograf Peter Krogh. Była to dość istotna innowacja w świecie fotografii, która miała głębokie implikacje również w innych dyscyplinach technologicznych i pozostaje ponadczasowa aż po dziś dzień. Choć, rzecz jasna, reguła 3-2-1 jest elastyczna i ponadczasowa, poprosiłem Petera, aby wyraził swoje zdanie na temat tego, jak można stosować ją w dzisiejszych czasach. Oto odpowiedź, którą otrzymałem:

„Mimo że skupiam się głównie na mediach cyfrowych, reguła 3-2-1 jest dość uniwersalna. W rzeczywistości sama reguła była po prostu streszczeniem praktyk, które poznałem od profesjonalistów z branży IT, gdy pisałem swoją pierwszą książkę. Nadałem jej tylko chwytliwą nazwę.

Przez blisko 20 lat reguła 3-2-1 była doskonałym narzędziem do oceny narażenia na ryzyko związane z danymi. Wszystko zaczęło się w erze dysków twardych o pojemności 30 GB i kopii zapasowych przechowywanych na płytach CD – a teraz reguła ta świetnie skaluje się w świecie dysków o pojemności 18 TB i wszechobecnej pamięci masowej w chmurze. W czasach, w których tak dużą część naszego życia (i środków) przechowujemy w formie cyfrowej, a także w obliczu rosnących zagrożeń ze strony złośliwego oprogramowania, ważne jest, aby każdy dysponował odpowiednimi ramami do oceny podatności na ryzyko".

Peter Krogh

Swoimi słowami mogę opisać regułę 3-2-1 w następujący sposób:

- powinny istnieć 3 kopie danych;
- na 2 różnych nośnikach;
- przy czym 1 kopia będzie przechowywana w innym miejscu.

Mając zarys w postaci tej podstawowej reguły, możemy przenieść ją do środowiska pracy z nowoczesnymi danymi newralgicznymi dla działalności. Nie zapominajmy jednak o ważnych atrybutach tej podstawowej reguły:

- nie zakłada ona żadnych szczególnych wymagań technologicznych ani sprzętowych,
- może sprawdzić się w niemal każdym scenariuszu awarii.

Jak korzystamy z reguły 3-2-1 w firmie Veeam?

W przypadku firmy Veeam i kopii zapasowych danych reguła 3-2-1 stanowi świetny punkt wyjścia. Moim zdaniem taki punkt wyjścia jest konieczny, aby zyskać odporność, której tak bardzo potrzebujemy w dzisiejszych czasach — a nie jest tajem-

nicą, że czasami mogą istnieć więcej niż 3 równoległe kopie zapasowe. W przypadku niektórych danych osobiście zdarzało mi się zarządzać 5 kopiami!

W niektórych najbardziej prymitywnych implementacjach reguła 3-2-1 funkcjonowałaby w następujący sposób:

- dane produkcyjne (kopia 1, nośnik 1),
- kopia zapasowa danych w repozytorium Veeam (kopia 2, nośnik 2),
- odtwarzanie poza siedzibą w przypadku awarii (kopia 3, nośnik 3).

To 3 różne nośniki, więc tak naprawdę przekraczamy minimalne kryteria, choć niektórzy nie postrzegają danych produkcyjnych jako kopii w regule 3-2-1 i warto o tym wspomnieć. Oznacza to, że w przypadku 2 pozostałych kopii konieczne są różne nośniki i wszechstronność, która pozwoli na przywrócenie danych.

W organizacjach, z którymi obecnie prowadzę rozmowy, istnieją nawet 4 kopie najbardziej newralgicznych zbiorów danych, jeśli uwzględnić również dane produkcyjne.

Wiele sposobów na realizację reguły 3-2-1

Jedną z rzeczy, które bardzo lubię w firmie Veeam – jako dostawcy oprogramowania z silnym zapleczem partnerstw – jest możliwość wyboru wielu kombinacji reguły 3-2-1. Obecnie jest to bardzo uniwersalne rozwiązanie i każde z poniższych wdrożeń można zaliczyć do konfiguracji 3-2-1:

- kopie zapasowe na dysku (DAS, SAN, NAS i urządzenia),
- kopie zapasowe na taśmach,
- kopie zapasowe na wymiennych urządzeniach pamięci masowej,
- kopie migawkowe pamięci masowej (na oddzielnych nośnikach niż produkcyjne!),
- kopie zapasowe w obiektowej pamięci masowej, np. w chmurze publicznej z warstwą możliwości repozytorium Scale-out Backup,
- kopie zapasowe w zimnej archiwizacji w chmurze publicznej z warstwą archiwizacji repozytorium Scale-out Backup,
- kopie zapasowe hostowane lub zarządzane przez dostawcę usług, w tym Veeam Cloud Connect,
- replikacja na innym hoście lub w innej lokalizacji za pomocą funkcji replikacji Veeam,
- zadania tworzenia kopii zapasowej w innej lokalizacji pamięci masowej.

W ostatnich latach niektóre organizacje podejmowały ciekawe działania w tym zakresie, np. tworząc wielokrotne kopie zapasowe. Kopia zapasowa maszyn wirtualnych, kopia oparta na agencie, kopia oparta na plikach, a nawet kopia wtyczek aplikacji mogą być stosowane w połączeniu ze sobą. Nie jest to powszechna praktyka, ale w przypadku absolutnie niezbędnych zbiorów danych jest to bardzo atrakcyjna opcja.

Zalety kopii zapasowych z punktu widzenia analityki biznesowej

Rozmawiałem z przedstawicielami wielu organizacji, które wykonywały więcej niż 3 kopie danych w locie w przypadku niektórych z newralgicznych zbiorów danych kopii zapasowych lub infrastruktury odzyskiwania danych po awarii (DR). Jednym z zaskakujących przypadków użycia jest w tym przypadku możliwość dodatkowej analityki danych. Może to być testowanie za pomocą SureBackup lub bardziej szczegółowa analityka biznesowa z wykorzystaniem danych w infrastrukturze kopii zapasowych lub DR. Dodatkowe, podobne przypadki użycia zwiększają wartość samego rozwiązania do tworzenia kopii zapasowych w tego typu organizacjach.

Zmodernizowana reguła 3-2-1: reguła 3-2-1-1-0 w wydaniu firmy Veeam

Reguła 3-2-1 jest niezbędnym punktem wyjścia, jednak reguła 3-2-1-1-0, stosowana przez Veeam, to świetne rozwiązanie na miarę dzisiejszych czasów.

Reguła 3-2-1-1-0 to sposób na rozwój. Zapewnia możliwość odzyskania danych w przypadku wielu rodzajów incydentów, które mogą się wydarzyć. Poniższa grafika zawiera wizualizację naszej reguły 3-2-1-1-0:

Różnica sprowadza się do „1-0" na końcu, tj. do zmiany, którą wprowadziliśmy w firmie Veeam. Dzięki tym dodatkowym krokom zmodernizowana reguła zapewnia niezwykłą wszechstronność. W tym przypadku zasady są następujące:

- powinny istnieć 3 kopie danych,
- na 2 różnych nośnikach,
- przy czym 1 kopia będzie przechowywana w innym miejscu,
- 1 kopia powinna być offline, odizolowana lub niezmienialna,
- 0 błędów to wymóg podczas weryfikacji odzyskiwania SureBackup.

Te dwa dodatkowe punkty są dziś bardzo ważne. Dysponowania kopią zapasową danych, która jest albo offline, albo odizolowana od innych środowisk, albo niezmienialna to niezwykle odporne założenie, które pozwala na odzyskanie danych w przypadku ataku oprogramowania ransomware. Istnieją pewne scenariusze, w których jedna kopia może mieć wiele cech – np. nośnik taśmowy WORM usunięty z urządzenia biblioteki taśmowej będzie kopią offline, niezmienialną i odizolowaną zarazem. Mam w zwyczaju stosować określenie „ultraodporność" w odniesieniu do kopii danych, które są albo offline, albo odizolowane, albo niezmienialne.

Brak niespodzianek na etapie przywracania danych to dziś duża zaleta – ale nie z powodów, które pozornie mogą wydawać się najważniejsze. Weryfikacja odzyskiwania danych za pomocą rozwiązania SureBackup to świetny sposób na upewnienie się, że dane będzie można przywrócić. I nie chodzi tu o to, że kopia zapasowa nie jest „dobra", ale o to, że pewne zachowania są widoczne tylko podczas przywracania lub ponownego uruchamiania systemu, co może uniemożliwić jego przywrócenie zgodnie z planem.

Reguła 3-2-1-1-0 w firmie Veeam

Reguła 3-2-1-1-0 firmy Veeam opisuje sposób, w jaki należy postępować w dzisiejszych czasach. W witrynie firmy Veeam dostępnych jest wiele historii klientów, które są dowodem na to, że dobre serwery, pamięci masowe i dane również są narażone na problemy. Teraz, bardziej niż kiedykolwiek wcześniej, musimy zapewnić sobie kontrolę nad naszymi danymi, aby mieć możliwość ich odzyskania. Reguła 3-2-1 to świetny punkt wyjścia, a dzięki firmie Veeam można przenieść ją na jeszcze wyższy poziom!

W jaki sposób uczenie maszynowe chroni przed phishingiem, zagrożeniami mobilnymi oraz awariami zakładów produkcyjnych

Piotr Kupczyk,
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska

Naukowcy zaczęli aktywnie badać możliwości inteligencji komputerowej już w latach pięćdziesiątych[1]. Na przestrzeni ostatnich siedemdziesięciu lat uczenie maszynowe (ang. Machine Learning – ML) z koncepcji teoretycznej stało się technologią intensywnie wykorzystywaną w praktyce – od mechanizmu rekomendacji filmów i seriali w serwisie Netflix po autonomiczne samochody czy rozpoznawanie mowy w smartfonach. Główną zaletą stosowania ML jest to, że decyzje podejmuje program, co pozwala ograniczyć nakład pracy wykonywanej przez człowieka.

Uczenie maszynowe znajduje również zastosowanie w cyberbezpieczeństwie – między innymi w usprawnieniu oraz automatyzacji wykrywania szkodliwego oprogramowania. W tym tekście skupię się na kilku najbardziej interesujących technikach uczenia maszynowego stosowanych w celu zapewnienia cyberochrony.

Uczenie maszynowe w walce z zaawansowanym phishingiem w wiadomościach e-mail

Przy pomocy pieczołowicie przygotowanej wiadomości phishingowej cyberprzestępcy mogą skutecznie nakłaniać określoną organizację lub użytkownika do działania, które przyniesie im korzyść. W tym celu tworzą wiadomości, w których podszywają się pod znane firmy i instytucje, a także wykorzystują popularne wydarzenia, takie jak pandemia wirusa powodującego COVID-19[2]. W kontekście ataków na firmy przestępcy mogą podszywać się pod kontrahenta, potencjalnego klienta, przełożonego czy współpracownika z danego działu. Takie działania noszą nazwę Business E-mail Compromise (BEC)[3].

Aby ochronić użytkowników przed takimi atakami, rozwiązanie bezpieczeństwa powinno szybko przeanalizować wszystkie parametry wiadomości e-mail, w tym jej treść, załączniki, nagłówki oraz kod HTML, aby zdecydować, czy powinna ona zostać zablokowana, a przynajmniej oznaczona jako potencjalnie niebezpieczna. W tym celu można wykorzystać uczenie maszynowe.

W tym przypadku powinny istnieć dwa modele ML:

- Pierwszy z nich będzie automatycznie analizował parametry techniczne wiadomości e-mail (takie jak nagłówki). Model ten jest trenowany na setkach milionów wpisów metadanych pochodzących z rzeczywistych wiadomości e-mail, aby uczył się rozpoznawać kombinacje śladów technicznych, które świadczą o szkodliwości danej wiadomości. To jednak nie wystarczy do wydania werdyktu.
- Drugi model będzie wykrywać szkodliwy charakter e-maila w oparciu o jego zawartość. W celu osiągnięcia zamierzonego efektu atakujący stosują w tekście język o zabarwieniu emocjonalnym oraz wyraźne wezwanie do działania (np. „Twoja paczka nie mogła zostać dostarczona, uaktualnij swoje dane w tym miejscu", „Abyśmy mogli dostarczyć Twoją przesyłkę, musisz w ciągu 24 godzin uregulować płatność" itp.). Model rozpoznaje tego typu słowa i frazy typowe dla wiadomości phishingowych.

Następnie te dwa modele ML zestawią ze sobą wyniki swojej pracy i wydadzą ostateczny werdykt – np. ta wiadomość to phishing – dzięki czemu użytkownik nie otworzy niebezpiecznego zasobu.

Uczenie maszynowe w walce z zagrożeniami mobilnymi dla systemu Android

W 2020 roku badacze z firmy Kaspersky wykryli łącznie ponad 5 milionów zagrożeń mobilnych – o dwa miliony więcej niż w 2019 r.[4] Jednym z kluczowych zadań ochrony mobilnej jest zapewnienie bezpieczeństwa przed nieznanymi szkodliwymi obiektami, które pojawiły się na wolności niedawno.

Na urządzeniach z systemem iOS zainstalowanie aplikacji przeznaczonych dla szerszego grona użytkowników jest możliwe wyłącznie poprzez oficjalny sklep, który jest ściśle moderowany przez firmę Apple. W przypadku urządzeń z systemem Android aplikacje można zainstalować z wielu różnych źródeł i sklepów z aplikacjami. Niestety, niekiedy wykorzystują to cyberprzestępcy, umieszczając szkodliwe oprogramowanie w aplikacjach podszywających się pod gry, przydatne oprogramowanie, materiały pornograficzne itd. W celu skutecznego i szybkiego wykrycia tych zagrożeń niezbędne jest

uczenie maszynowe.

Znajdujący się na urządzeniu użytkownika agent ML skanuje każdą pobieraną aplikację pod kątem określonych cech, takich jak wymagane uprawnienia dostępu czy liczba i rozmiar struktur wewnętrznych. Metadane są przesyłane do opartego na chmurze modelu uczenia maszynowego, który następnie decyduje, czy na podstawie danego zestawu parametrów aplikację należy zaklasyfikować jako szkodliwą, czy nie. W dalszej kolejności model wysyła odpowiedź określającą bezpieczeństwo danego pliku, a w oparciu o te informacje produkt bezpieczeństwa na urządzeniu decyduje o ewentualnym zablokowaniu pobierania i instalacji aplikacji.

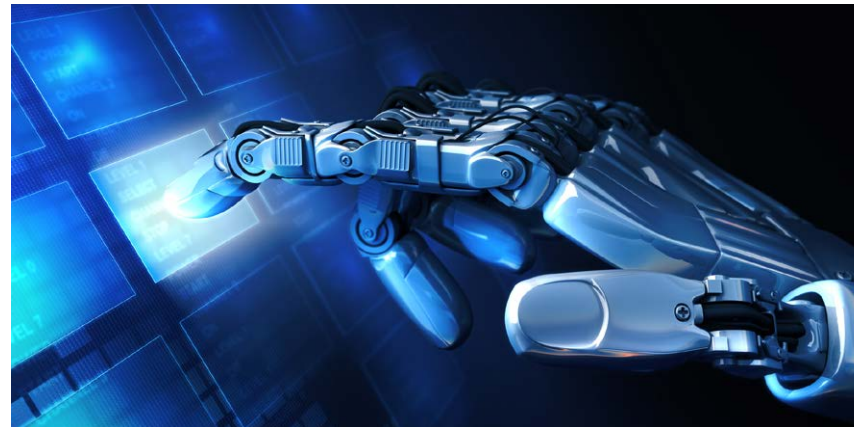
Taka analiza ML wymaga znaczących zasobów komputerowych, znacznie większych niż te dostępne na urządzeniu mobilnym, dlatego cały proces zwykle przebiega w chmurze.

Uczenie maszynowe w zapobieganiu awariom w zakładach produkcyjnych

Usterki w sprzęcie, błędne konfiguracje, błąd ludzki czy ataki hakerskie mogą spowodować awarię maszyn przemysłowych. Jeśli dojdzie do takiego zdarzenia, ważne jest, by jak najszybciej wykryć odchylenie w procesach produkcji. W przeciwnym razie incydent może wymknąć się spod kontroli, prowadząc w najlepszym razie do przestoju, a w najgorszym do poważnych naruszeń bezpieczeństwa.

Problem polega na tym, że wczesne symptomy incydentu są praktycznie niemożliwe do wykrycia poprzez monitorowanie progów czy operatora-człowieka. W sytuacji gdy w każdej sekundzie pojawiają się tysiące odczytów telemetrii, nawet doświadczony operator będzie w stanie skoncentrować się jedynie na kilku, ignorując resztę.

Tutaj z pomocą przychodzi uczenie maszynowe przeznaczone do wykrywania anomalii (ang. Machine Learning Anomaly Detection, MLAD). Sieć neuronowa potrafi przeanalizować ogromną ilość danych telemetrycznych, zrozumieć wszystkie aspekty działania maszyny oraz nauczyć się, jak zachowuje się ona



w normalnych warunkach – np. jak sygnały zmieniają się z czasem i jakie zależności między nimi występują.

Gdy szkolenie modelu ML zostanie zakończone, przechodzi on w tryb wykrywania anomalii. Otrzymuje wówczas dane telemetryczne w czasie rzeczywistym i jeśli rozbieżność między modelem a obserwacją przekroczy pewien próg, zachowanie maszyny zostanie uznane za nietypowe i uruchomiony zostanie alarm. Model wydaje wczesne ostrzeżenie przed atakami, usterkami oraz niewłaściwym zrządzaniem, zanim problem zostanie dostrzeżony przez jakiekolwiek inne narzędzie.

Uczenie maszynowe w walce z zaawansowanymi cyberatakami

W niektórych przypadkach techniki uczenia maszynowego, takie jak usługi zarządzanego wykrywania i reagowania (ang. Managed Detection and Response, MDR), mogą być wykorzystane jako uzupełnienie ludzkiej wiedzy w walce z zaawansowanymi zagrożeniami.

W ramach usługi MDR zewnętrzne centrum operacji bezpieczeństwa pomaga klientom biznesowym reagować na zaawansowane cyberataki. Bada ono alerty otrzymane z punktów końcowych klientów pod kątem śladów ataków, a następnie wysyła klientowi odpowiedni raport wraz z działaniami, które należy podjąć. Eksperci z centrum bezpieczeństwa analizują niektóre próbki zagrożeń ręcznie, jednak biorąc pod uwagę ich skalę, fizycznie nie są w stanie przyjrzeć się każdemu alertowi z osobna.

W tym przypadku uczenie maszynowe może automatycznie odfiltrowywać alerty, którymi nie są zainteresowani analitycy z centrum operacji bezpieczeństwa, ustanawiać poziomy istotności takich komunikatów oraz oferować wskazówki przydatne w procesie analizy. W ten sposób zminimalizowany zostaje średni czas reakcji.

W trybie uczenia model analizuje alerty i przyznaje im ocenę punktową. Im wyższa ocena, tym większe prawdopodobieństwo, że alert musi zostać przeanalizowany przez ekspertów. Alerty z oceną na poziomie powyżej określonego progu są przesyłane do analityków z centrum operacji bezpieczeństwa, którzy ręcznie nadają im etykietkę i wzbogacają dane służące do szkolenia modelu ML.

W trybie zwalczania zagrożeń model analizuje alerty i priorytetyzuje te z nich, które wymagają przetwarzania ręcznego. Taka strategia znacznie skraca średni czas ich przetwarzania.

W firmie Kaspersky uważamy, że obszar zastosowana uczenia maszynowego będzie się nieustannie rozszerzał. Rozwój technik ML w produktach stanowi jeden z priorytetów działu badań i rozwoju firmy, ponieważ dzięki nim cyberochrona może działać inteligentniej, szybciej i skuteczniej.

[1] *https://www.forbes.com/sites/bernardmarr/2016/02/19/a-short-history-of-machine-learning-every-manager-should-read*
[2] *https://www.kaspersky.pl/o-nas/informacje-prasowe/3299*
[3] *https://kas.pr/ga7g*
[4] *https://securelist.com/mobile-malware-evolution-2020/101029*

Pięć trendów, jakie powinny uwzględnić firmy, planując wydatki na cyberbezpieczeństwo w 2022 r

Jewgienija Naumowa,
Wiceprezes wykonawczy, dział rozwiązań korporacyjnych, Kaspersky

Koniec roku oznacza, że w przeciwieństwie do aury na zewnątrz panuje gorący okres oceniania i planowania budżetów na przyszłe dwanaście miesięcy. Chociaż nic nie wskazuje na rychły koniec pandemii, firmy będą musiały uwzględnić jej obecne skutki: praca zdalna do pewnego stopnia utrzyma się, podobnie jak ekonomiczne następstwa kryzysu związanego z COVID-19.

Chcąc pomóc firmom określić priorytety podczas planowania budżetów na przyszły rok, przybliżę kilka obserwacji z naszego ostatniego badania dotyczącego ekonomii cyberbezpieczeństw[1].

1. W ubiegłym roku budżety zostały okrojone, ale nie będzie tak zawsze.

Budżety na cyberbezpieczeństwo na 2021 r. zostały zaplanowane pod koniec 2020 r. – w samym środku pandemii – przez co wiele firm podeszło do wydatków niezwykle ostrożnie. W efekcie, w przypadku małych firm, średni budżet na cyberbezpieczeństwo na 2021 r. praktycznie nie zmienił się i wynosił 267 000 dolarów (w porównaniu z 275 000 dolarów w poprzednim roku). Z kolei duże firmy zmniejszyły swoje wydatki na ten cel – z 14 milionów dolarów w 2020 r. do 11,4 mln dolarów w 2021 r.

Jednak od wiosny 2021 r. analitycy publikują optymistyczne prognozy dotyczące wzrostu rynku IT oraz bezpieczeństwa informacyjnego: Gartner przewiduje[2], że łączne globalne wydatki na IT w 2021 r. zwiększą się o 8,4%. Również IDC prognozuje duży wzrost wydatków na bezpieczeństwo IT w Europie[3] oraz regionie Azji i Pacyfiku[4].

Ciągłe innowacje, cyfryzacja produktów oraz udoskonalone procesy biznesowe – wszystko to sprawia, że organizacje będą musiały priorytetyzować inwestycje w cyberbezpieczeństwo. Jednak ze względu na te i inne czynniki, o których opowiem w dalszej części, wymagania mogą się znacząco zmienić.

2. Koszty finansowe incydentów naruszenia bezpieczeństwa nie zmieniły się znacząco, co nie znaczy, że pokonaliśmy cyberprzestępców.

W 2021 roku koszty finansowe incydentów naruszenia bezpieczeństwa danych nieznacznie wzrosły w przypadku małych i średnich firm, za to zmniejszyły się o 15% w przypadku przedsiębiorstw. Jednak spadek ten nie oznacza wycofywania się cyberprzestępców. Skala wpływu incydentów zależy nie tylko od złożoności ataków, ale również od działań firm.

Incydent naruszenia bezpieczeństwa danych może prowadzić do bezpośrednich strat, w tym strat biznesowych lub kar. Dalszy wpływ finansowy zależy od tego, czy incydent zostanie upubliczniony.

W takim przypadku firma będzie musiała wydać więcej: na dodatkowe wsparcie PR-owe lub z tytułu grzywien, kar oraz odszkodowań. W efekcie średni koszt incydentu naruszenia bezpieczeństwa danych w przypadku przedsiębiorstwa, które nie ujawnia szczegółów na jego temat, wynosi 827 000 dolarów Jeżeli jednak informacja o incydencie wycieknie do mediów, koszt wzrośnie do 1,2 miliona dolarów.

W tym roku dadzą o sobie znać znaczące inwestycje w cyberbezpieczeństwo poczynione w odpowiedzi na wcześniejsze incydenty naruszenia danych – takie jak udoskonalenia w zakresie oprogramowania oraz infrastruktury IT lub szkolenia zorganizowane dla pracowników. Widać to np. w pozytywnej dynamice wykrywania zagrożeń oraz szybkości reagowania na nie. Z naszego badania wynika, że z każdym rokiem organizacje szybciej wykrywają incydenty naruszenia bezpieczeństwa. W 2016 roku jedynie 15% małych i średnich firm oraz 14% dużych posiadało systemy, które ostrzegały przed atakami oraz umożliwiły natychmiastową bądź szybką reakcję na incydent w ciągu kilku godzin. W 2021 roku odsetek ten wynosił 27%.

3. Szersze wdrażanie chmury wymaga wyspecjalizowanej ochrony.

Nasze badanie pokazuje, że po wybuchu pandemii w firmach częściej korzysta się z usług chmury. W 2019 roku 72% z nich wykorzystywało jakiś rodzaj chmury – publiczną, prywatną lub infrastrukturę wirtualnych stacji roboczych (VDI). W latach 2020-2021 odsetek ten zwiększył się do 88%[5].

W efekcie zmieniły się potrzeby w zakresie ochrony infrastruktury chmury. Stworzone w poprzednich latach projekty dotyczące bezpieczeństwa były w znacznej mierze skrojone dla infrastruktury lokalnej, co oznacza, że mogą nie być wystarczające dla organizacji migrujących do chmury. Klienci powinni określać wymagania związane z ochroną w oparciu o swoją obecną infrastrukturę, a to wymaga nowego, wyspecjalizowanego pakietu rozwiązań cyberbezpieczeństwa, uwzględniającego określone obszary, takie jak ochrona kontenerów lub tożsamości w chmurze, jak również narzędzi służących do wykrywania i reagowania na złożone zagrożenia w środowiskach wielochmurowych.

4. Kluczowe znaczenie dla ochrony przed złożonymi zagrożeniami ma widoczność infrastruktury oraz incydentów.

IT oraz bezpieczeństwo IT ma za zadanie nie tylko chronić infrastrukturę przed włamaniami, ale również sprawić, by była efektywna i nie ograniczała się do procesów biznesowych, niezależnie od tego, jak szybko zmienia się firmowa sieć. Praca zdalna, jak również cyfryzacja procesów i produktów firm sprawiły[6], że zabezpieczenie tak złożonej infrastruktury stanowi największe utrapienie firm, zaraz po ochronie danych. Jednym z powodów jest to, że im bardziej złożony system, tym trudniej jest monitorować to, co się dzieje. W przypadku dwóch na pięć firm (41%) stanowi to największy problem w kontekście postępowania z atakami złożonymi.

Dla wielu firm tak skomplikowane środowisko stanowi główny powód dodatkowych inwestycji. Wyrafinowany atak często łączy w sobie wyglądające na legalne oraz trudne do wykrycia taktyki. Kolejny problem polega na tym, że ogromna liczba alertów wygenerowanych przez różne rozwiązania bezpieczeństwa utrudnia analitykom priorytetyzowanie incydentów oraz dostrzeganie korelacji między działaniami przestępców. Niezbędne jest automatyczne wykrywanie i reagowanie, które potrafi nie tylko wykrywać wiele drobnych oznak ataku, ale również korelować je ze sobą oraz z zewnętrznymi danymi dotyczącymi zagrożeń. Umożliwi to efektywne klasyfikowanie alertów oraz ujawnienie rzeczywistego zaawansowanego ataku, który zostanie następnie zgłoszony zespołom ds. reagowania na incydenty.

5. Zapotrzebowanie na wiedzę ekspercką napędza outsourcing oraz zmiany w budżetowaniu.

Chociaż zapotrzebowanie na wykwalifikowanych pracowników oraz wiedzę ekspercką nie jest niczym nowym[7], w tym roku po raz pierwszy stało się ono głównym motywatorem outsourcingu cyberbezpieczeństwa. Szybka adaptacja nowych technologii oraz zmiana modeli pracy, w połączeniu z wykładniczym wzrostem złożoności IT, sprawiają, że co drugie średnie i duże przedsiębiorstwo (odpowiednio 52% i 56%), które powierza zarządzanie bezpieczeństwem dostawcy usług zarządzanych, potrzebuje wysoce wykwalifikowanych profesjonalistów.

Firmy, które przechodzą na korzystanie z usług zlecanych na zewnątrz, powinny odpowiednio dostosować swój proces budżetowania, ponieważ ta część budżetu zmieni pozycję z nakładów kapitałowych (CapEx) na koszty działalności (OpEx): inwestycje w sprzęt co kilka lat zmienią się w miesięczną subskrypcję.

Nie wiemy na pewno, jakie nowe wyzwania przyniesie kolejny rok. Wbrew naturalnej skłonności ludzi do zachowania ostrożności pojawia się również sposobność, by dokonać zmiany i podjąć śmiałe decyzje. Dotyczy to także procesu budżetowania: podejście typu „zróbmy podobnie jak w zeszłym roku" już nie zadziała. Ocena ryzyka oraz modelowanie powinny uwzględniać najnowsze trendy, zmiany w infrastrukturze korporacyjnej oraz procesach biznesowych, jak również – co najistotniejsze – potrzeby biznesowe. Idąc dalej, w celu zabezpieczenia określonych systemów niezbędne jest nowe podejście, w którym ochrona jest uwzględniana na samym początku projektowania. Podejście, które określamy jako „zaprojektowane z myślą o bezpieczeństwie", pomoże firmom uzyskać cyberodporność na większość zagrożeń.

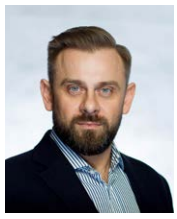
[1] *https://calculator.kaspersky.com/app/report*
[2] *https://www.gartner.com/en/newsroom/press-releases/2021-04-07-gartner-forecasts-worldwide-it-spending-to-reach-4-trillion-in-2021*
[3] *https://www.idc.com/getdoc.jsp?containerId=prEUR248131621*
[4] *https://www.idc.com/getdoc.jsp?containerId=prAP48212321*
[5] *Dane pochodzą z badania przeprowadzonego w okresie maj-czerwiec 2021 r. Przeankietowano 4303 przedstawicieli firm z 31 krajów zatrudniających ponad 50 pracowników.*
[6] *https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever*
[7] *https://www.techrepublic.com/article/the-cybersecurity-skills-gap-persists-for-the-fifth-year-running*

Najbezpieczniejsze metody logowania:

- **35,5 proc. - kod SMS**
- **25,4 proc. - odcisk palca**
- **24,7 proc. - hasło**

1/4 Polaków wierzy w weryfikację tożsamości przy pomocy odcisku palca

Na nowe dowody osobiste z odciskiem palca właściciela jeszcze poczekamy. Tymczasem co czwarty Polak uważa weryfikację linii papilarnych za najbezpieczniejszy sposób potwierdzenia tożsamości. Najbardziej tej metodzie ufają młodzi, z których ponad 1/3 wskazuje ją jako najlepszą. Tak wynika z badania serwisu ChronPESEL.pl i Krajowego Rejestru Długów przeprowadzonego pod patronatem Urzędu Ochrony Danych Osobowych. Nie można jednak zapomnieć o innych zasadach ochrony danych, ponieważ oszuści nie próżnują: tylko w I połowie 2021 r. łączna kwota udaremnionych wyłudzeń kredytów wzrosła o 24 proc. Każdego dnia przestępcy próbowali wyłudzić na skradzione dane prawie 900 tys. zł.

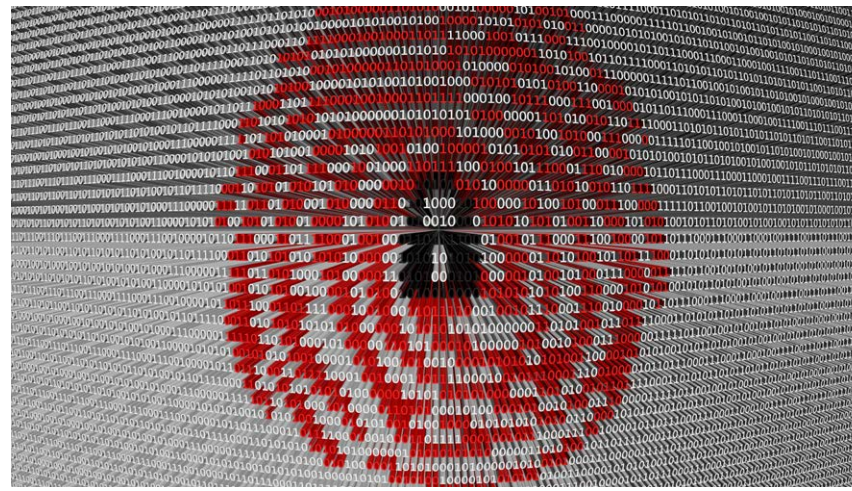


Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl

Na pytanie o bezpieczne metody logowania do portali i bankowości internetowej najwięcej osób (35,5 proc.) wskazało kod SMS. Na drugim miejscu znalazła się jednak weryfikacja linii papilarnych oraz używanie hasła, które preferuje około 25 proc. ankietowanych. Znacznie mniej osób, bo niewiele ponad 9 proc., za najbezpieczniejszy sposób potwierdzenia tożsamości uznało weryfikację twarzy. To potwierdza, że metody wykorzystujące dane biometryczne są obecne w świadomości Polaków, a mimo to wciąż wolą oni korzystać z tradycyjnych rozwiązań.

Tymczasem, jak wynika z przeprowadzonego badania, już 35 proc. respondentów w wieku między 18 a 24 r.ż. uważa weryfikację linii papilarnych za najbezpieczniejszy sposób potwierdzenia tożsamości podczas logowania w banku lub do innych portali internetowych. Może to zwiastować zmianę nastawienia społeczeństwa w niedalekiej przyszłości. Za wyjątkowo pewną metodę uznaje ją także blisko 30 proc. ankietowanych wieku od 55 do 64 lat. Jednak tylko najmłodsza grupa badanych umieściła ją na pierwszym miejscu. Najmniejszym zaufaniem darzą ją osoby mające ponad 65 lat.

W przypadku potwierdzenia weryfikacji twarzą warto zwrócić uwagę na różnice w podejściu między kobietami i mężczyznami. Podczas gdy wśród panów nie cieszy się ona dużym zaufaniem – około 7 proc. wskazało ją jako najbez-



pieczniejszą, to wśród przedstawicielek płci pięknej ten odsetek jest prawie dwa razy wyższy i wynosi blisko 12 proc. Jeszcze bardziej w tę metodę wierzą osoby w średnim wieku (45-54 lata).

Niestety nawet najbardziej złożone sposoby logowania i potwierdzania tożsamości nie wystarczą, jeśli nie będziemy pamiętać o przestrzeganiu podstawowych zasad bezpieczeństwa.

Z jednej strony dużą wagę przykładamy do wyboru złożonego sposobu logowania lub konstruujemy skomplikowane hasło, z drugiej — nie zachowujemy odpowiedniej czujności w sytuacjach znacznie prostszych. Wystarczy bowiem, że nie czytając dokładnie otrzymanego SMS lub e-maila, klikniemy umieszczony tam link i pobierzemy szkodliwe oprogramowanie, które pozwoli przestępcom na dostęp do naszych danych i konta. Uważać musimy też na telefony od rzekomych konsultantów z instytucji bankowych, którzy informują nas o zablokowaniu podejrzanych transakcji i pod pretekstem potwierdzenia naszej tożsamości wyciągają od nas najważniejsze dane.

Warto również zachować czujność i śledzić na bieżąco ostrzeżenia pojawiające się w mediach. W ostatnim czasie mogliśmy się dowiedzieć na przykład o oszustach podszywających się pod aplikację mObywatel, którzy wysyłają fałszywe informacje o rzekomym nowym terminie szczepienia. W komunikatach przestępcy zachęcają do kliknięcia linku, który ma rzekomo pozwolić na zainstalowanie aplikacji. W rzeczywistości powoduje jednak pobranie szkodliwego oprogramowania, które umożliwia im dostęp do naszego telefonu. W ten sposób oszuści mogą wejść w posiadanie naszych haseł do logowania, np. w aplikacji bankowej. W efekcie możemy stracić wszystkie oszczędności i zostać z kilkoma pożyczkami do spłacenia.

Na nowe dowody osobiste poczekamy dłużej

Kolejne dane biometryczne pojawią się również na nowych dowodach osobistych. Dotychczas widniał na nich jedynie wizerunek twarzy; teraz znajdą się tam także dwa odciski palców w formatach cyfrowych. W związku z tym wnioski o wydanie nowego dowodu nie będą mogły być składane online i konieczna będzie wizyta w urzędzie. Według szacunków Ministerstwa Spraw Wewnętrznych i Administracji, w tym roku dowód będzie musiało wymienić ponad 1,5 mln Polaków. Dodatkowo 358 tys. osiągnie pełnoletność.

Przyczyną tej zmiany jest konieczność dostosowania nowych przepisów do rozporządzenia Parlamentu Europejskiego i Rady UE. Regulacje te zobowiązują państwa członkowskie do wprowadzenia do dowodów osobistych drugiej cechy biometrycznej, czyli odcisków palców. Polska musi dodatkowo uzupełnić warstwę graficzną dokumentu tożsamości o podpis posiadacza. Zmiany nie powodują konieczności wymiany dowodów osobistych. Będą one ważne przez okres, na jaki zostały wydane.

Zmiana miała być wprowadzona od początku sierpnia br., jednak z powodu konieczności ponownego przeprowadzenia przetargu na urządzenia do pobierania linii papilarnych wejście w życie przepisów zostało przesunięte. Na razie nie znamy nowego terminu.

Rośnie kwota udaremnionych wyłudzeń kredytów

Jak wynika z danych udostępnionych przez ekspertów bankowych, w I połowie 2021 r. łączna kwota udaremnionych wyłudzeń kredytów wyniosła prawie 160 mln zł. W porównaniu z II półroczem 2020 r. oznacza to wzrost o prawie 24 proc. Z jednej strony świadczy to o postępującym uszczelnianiu systemu; z drugiej — biorąc pod uwagę również fakt, że o ponad 28 proc. wzrosła średnia kwota powstrzymanych prób wyłudzenia (w I poł. 2021 r. to ponad 43 tys. zł) — dowodzi to coraz większej śmiałości przestępców próbujących wykorzystać skradzione dokumenty.

Z tego powodu należy unikać sytuacji, w których zostawiamy komuś nasz dowód osobisty, oraz od razu reagować w momencie, gdy zorientujemy się, że go zgubiliśmy lub został skradziony. Jednak sama ochrona dowodu osobistego nie wystarczy, ponieważ złodzieje danych osobowych szukają dzisiaj swoich ofiar głównie w internecie.

Nie możemy zapominać o tym, że dowód osobisty jest tylko nośnikiem naszych danych osobowych. Przestępcy nie muszą dzisiaj kraść portfeli czy skanować dowodów, aby wejść w ich posiadanie. Oczywiście należy ich pilnować i nie dopuszczać do sytuacji, w których gdzieś go zostawiamy, ale musimy mieć też świadomość, że to nie wystarczy, by zapewnić sobie bezpieczeństwo. Niestety, z uwagi na to, w jak wielu miejscach podajemy nasze dane — na przykład w urzędach, przychodniach, w hotelach, a przede wszystkim w Sieci — takiej pewności nigdy mieć nie będziemy.

O badaniu

Badanie na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych zostało przeprowadzone w I połowie 2021 roku metodą CAWI na reprezentatywnej grupie 1007 respondentów przez IMAS International

Od szkodliwego e-maila do milionowego okupu – phishing wciąż na fali

Monika Sierocinski,
Team Lead CAM
w firmie Sophos

Phishing to wciąż popularna metoda ataków na firmy. Jak wynika z badania Sophos, aż 59% dużych przedsiębiorstw w Polsce zauważyło wzrost liczby tego typu wiadomości trafiających na skrzynki pracowników w ostatnim roku. Nawet jeden e-mail zawierający szkodliwy link może skutkować wielomilionowymi stratami związanymi z kradzieżą i zaszyfrowaniem firmowych danych. Konieczna jest edukacja pracowników, jednak trzeba przy tym pamiętać, że nawet specjaliści IT różnie definiują phishing.

Od fałszywego e-maila do zablokowania systemu

Na całym świecie aż 7 na 10 firm zatrudniających co najmniej 100 pracowników zanotowało wzrost liczby ataków phishingowych w ostatnim roku. Przestępcy szybko wykorzystali możliwości, jakie stworzyła pandemia: gwałtowny wzrost liczby osób pracujących z domu, popularności zakupów online i powszechny niepokój. Podobną skalę ataków zanotowały wszystkie sektory, co wskazuje, że cyber-

przestępcy starają się przede wszystkim dotrzeć do jak największej liczby pracowników.

Phishing pozostaje skuteczną metodą cyberataków od ponad 25 lat. Przestępcy grają na ludzkich emocjach i zaufaniu: wyłudzają dane oraz nakłaniają do kliknięcia szkodliwych linków lub załączników, podszywając się pod znane firmy i instytucje. Firmy często uważają phishing za niewielkie zagrożenie, jednak zazwyczaj to tylko pierwszy etap bardziej złożonego ataku. Kliknięcie szkodliwego linku w e-mailu od rzekomego współpracownikamoże skutkować wielomilionowymi stratami. Przestępcy zyskują wtedy dostęp do komputera ofiary oraz firmowej sieci, mogą pobierać z niej informacje, blokować je, a nawet kraść pieniądze.

Wiele definicji phishingu

Badanie przeprowadzone prze firmę Sophos wykazało, że nawet specjaliści IT różnie rozumieją phishing. W Polsce najczęściej wskazują, że są to e-maile zawierające szkodliwy załącznik (69%), e-maile wysyłane w ramach kampanii ukierunkowanych, poprzedzonych wywiadem środowiskowym (63%), kradzież danych uwierzytelniających przez pocztę elektroniczną (63%) i e-maile zawierające szkodliwe linki (62%). Wiadomości SMS nakłaniające do podania informacji (smishing) za phishing uważa 41%.

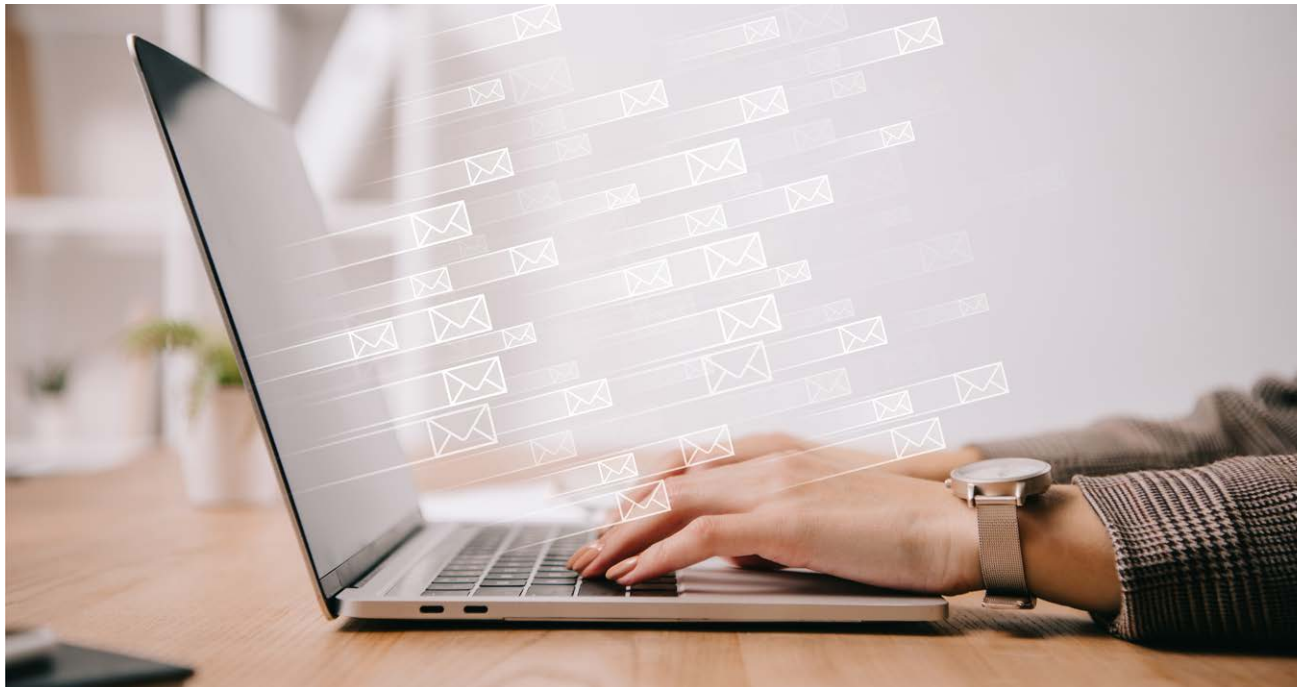
Duże firmy edukują pracowników – czy właściwie?

84% firm w Polsce, zatrudniających co najmniej 100 osób, prowadzi działania edukacyjne, aby przeciwdziałać phishingowi. Głównie są to szkolenia i symulacje ataków. 3 na 4 firmy miały program edukacyjny jeszcze przed wybuchem pandemii, wciąż jednak tylko połowa przedsiębiorstw śledzi współczynnik kliknięć wiadomości phishingowych, a nieco ponad 3/5 liczbę zgłaszanych podejrzanych e-maili. Takie informacje mogłyby pomóc zespołom IT w dopasowywaniu szkoleń do potrzeb pracowników oraz poprawianiu poziomu ochrony.

Najlepiej oczywiście uniemożliwiać docieranie szkodliwych wiadomości do adresatów, z wykorzystaniem zabezpieczeń poczty elektronicznej. Jednak zawsze należy je też uzupełniać zwiększaniem świadomości zagrożeń wśród pracowników. Trzeba przy tym pamiętać, że phishing dla poszczególnych osób nie zawsze znaczy to samo. Aby szkolenia, zwłaszcza kadry nietechnicznej, były skuteczne, ważne jest wyjaśnienie definicji ataków i kanałów, którymi są realizowane, a także upewnienie się, że wszyscy rozumieją je podobnie. Równie istotne jest sprawdzanie, czy pracownicy zgłaszają podejrzane wiadomości i czy wiedzą, czego nie powinni klikać.

O badaniu

Badanie zatytułowane „Phishing Insights, 2021" zostało przeprowadzone przez niezależną agencję Vanson Bourne na zlecenie Sophos. Ankieta objęła 5,4 tys. decydentów IT z firm zatrudniających od 100 do 5 tys. pracowników. Badanie przeprowadzono w styczniu i lutym 2021 roku wśród respondentów z 30 krajów Europy (w tym w Polsce), obu Ameryk, Azji i Pacyfiku, Azji Środkowej, Bliskiego Wschodu i w Afryce.



50 lat historii e-maila

– od wiadomości „QWERTYUIOP” do głównego narzędzia cyberprzestępców

50 lat temu inżynier Ray Tomlinson wysłał pierwszą na świecie wiadomość e-mail. Był to krok milowy dla rozwoju komunikacji cyfrowej, która połączyła cały świat. Ułatwiła ona nie tylko kontakty międzyludzkie, ale także zmieniła sposób działalności wielu firm. Jednak wraz ze wzrostem popularności poczty elektronicznej zwiększyła się także skala wykorzystania jej do cyberataków. Warto wiedzieć zatem, jak zapewnić bezpieczeństwo poczty elektronicznej, zarówno prywatnej, jak i w swoim miejscu pracy.

Od jednej wiadomości do 5 mld skrzynek pocztowych – historia e-maila

Zanim Ray Tomlinson wysłał pierwszego e-maila, koncepcją poczty elektronicznej zajmowały się różne, niezależne ośrodki badawcze. Za prekursorów tej formy komunikacji uznaje się Noela Morrisa i Toma van Vlecka. Ich program umożliwiał przesyłanie informacji o zakończeniu pobierania plików między użytkownikami komputerów typu mainframe. Był on przeznaczony dla systemu Compatible Time-Sharing System (CTSS) w Massachusetts Institute of Technology (MIT). W tym samym czasie opracowano kilka podobnych rozwiązań, zarówno na poziomie rządowym, jak i komercyjnym. Mowa tu o systemie operacyjnym Q32 SDC SDS 940, systemie AUTODN armii amerykańskiej oraz CP/CMS firmy IBM.

Jednak prawdziwy przełom nastąpił w 1971 r. za sprawą Tomlinsona. Efektem jego pracy dla Departamentu Obrony USA było oprogramowanie, które służyło do komunikacji przez rządową sieć ARPANET. Treść pierwszej wiadomości wysłanej z jednego komputera do drugiego była przypadkowa i prawdopodobnie brzmiała „QWERTYUIOP”. Tomlinson wprowadził również symbol @ do adresu skrzynki mailowej. Kolejną ważną datą w historii poczty elektronicznej był rok 2004. Wtedy firma Google uruchomiła pierwszą wersję popularnego dziś Gmaila, do korzystania z którego na początku trzeba było uzyskać zaproszenie od istniejącego użytkownika. Natomiast w 2011 r. Microsoft wprowadził na rynek produkt Office 365. Od tamtej pory pełnoprawne rozwiązania chmurowe stały się powszechnie stosowane w wielu firmach. Zmieniło to sposób

ich działalności i zwiększyło poziom produktywności.

Skala cyberataków wykorzystujących e-mail rośnie

Obecnie poczta elektroniczna cieszy się dużą popularnością i zapewne długo się to nie zmieni, bowiem ułatwia codzienne życie na wielu płaszczyznach. Aktualnie istnieje ponad 5 miliardów adresów e-mail, a wielu użytkowników posiada więcej niż jeden. Używane są one w równym stopniu do komunikacji służbowej i prywatnej.

Szacunkowo, 4,1 miliarda użytkowników na całym świecie wysyła dziennie ok. 320 miliardów wiadomości e-mail. Liczby te świadczą o tym, jak ważnym narzędziem komunikacji jest poczta elektroniczna. Niestety, wiedzą o tym także cyberprzestępcy, dlatego często wybierają tę drogę do przeprowadzania ataków. Według raportu zatytułowanego „Verizon Data Breach Investigations" z 2021 r. zagrożenie szkodliwymi wiadomościami e-mail zwiększyło się znacząco. W ciągu roku odsetek skutecznych ataków phishingowych wzrósł z 25% do 36%[1], natomiast w przypadku ataków ransomware podwoił się – sukcesem kończy się 10% z nich. Raport wskazuje, że pojawiła się także nowa taktyka wymuszania okupu: cyberprzestępcy najpierw pobierają dane i szyfrują pliki na urządzeniu ofiary, a następnie wykorzystują ten fakt do wywierania dodatkowego nacisku, np. szantażują ich opublikowaniem. Żeby włamać się do firmowej sieci, cyberprzestępcy wykorzystują także dane logowania. Z raportu firmy Verizon wynika, że stanowią one ok. 58% zdobytych łupów.

Eksperci Fortinet podkreślają, że poczta elektroniczna jest ściśle powiązana z operacjami biznesowymi, dlatego firmy powinny szczególnie zadbać o jej ochronę. Bezpieczeństwo i prywatność danych ma znaczenie fundamentalne dla ich działalności. Podobną rolę kwestia ta pełni także w dalszym rozwoju komunikacji cyfrowej.

Jak chronić pocztę elektroniczną przed cyberzagrożeniami?

Obecnie obserwujemy wzrost liczby ataków wielowektorowych. Można także zauważyć wczesne oznaki stosowania przez cyberprzestępców bardziej zaawansowanych technik, takich jak sztuczna inteligencja i uczenie maszynowe.

Rozwój metod stosowanych przez cyberprzestępców oznacza, że rozwiązania zapewniające ochronę poczty elektronicznej muszą obejmować także inne obszary infrastruktury bezpieczeństwa. Tylko dostosowanie jej do wdrożonej w firmie platformy lub infrastruktury sieciowej umożliwi wymianę informacji o tzw. wskaźnikach naruszenia (Indicators of Compromise, IoC). Usprawni to jednocześnie reagowanie na incydenty przez zespoły zajmujące się cyberbezpieczeństwem i odciąży je od powtarzalnej pracy.

[1] *https://www.verizon.com/business/resources/reports/dbir/*

Bezpieczeństwo w chmurze w 2021 r.: najnowsze trendy i obserwacje

Ochrona zasobów chmurowych nadal pozostaje jednym z głównych tematów w 2021 roku. Dlatego firmy Fortinet oraz Cybersecurity Insiders postanowiły przeprowadzić badanie wśród specjalistów ds. cyberbezpieczeństwa z całego świata, pracujących we wszystkich branżach. Ich spostrzeżenia zostały zebrane w nowym raporcie pt. „2021 Cloud Security Report[1]", w którym ponad 500 osób – od kierowników technicznych po menedżerów i ekspertów – przedstawia swoje obserwacje dotyczące bezpieczeństwa w chmurze, sposoby wykorzystania tego typu zasobów przez ich firmy oraz najważniejsze najlepsze praktyki.

Zróżnicowany cyfrowy krajobraz oraz rola bezpieczeństwa w chmurze

Przede wszystkim, co zresztą nie jest zaskakujące, przedsiębiorstwa nie ustają we wdrażaniu rozwiązań chmurowych w celu realizacji kluczowych założeń biznesowych. Trend ten w najbliższym czasie nie ulegnie raczej spowolnieniu. Raport wskazuje, że w chmurze ponad połowę swoich zadań obliczeniowych wykonuje 33% firm, a w ciągu najbliższych 12-18 miesięcy odsetek ten wzrośnie do 56%.

Popularne stają się także środowiska wielochmurowe – przedsiębiorstwa obierają je jako element swojej strategii lub po prostu zaczynają korzystać z nich w wyniku naturalnej ewolucji biznesowej. Większość firm realizuje strategię hybrydową lub wielochmurową (71%). Czynią to ze względu na możliwość integracji wielu usług, zapewnienia skalowalności lub ciągłości działalności. 76% podmiotów korzysta z usług dwóch lub więcej dostawców w chmurze. Ale nie oznacza to, że rozwiązania wdrażane w siedzibie przedsiębiorstw odeszły do lamusa – nadal stanowią ponad jedną trzecią wdrożeń. Oznacza to jednak, że firmy działają obecnie w rozszerzonym i zróżnicowanym cyfrowym świecie.

Infrastruktura pełna wyrafinowanych zagrożeń

Uwzględniając rosnącą liczbę źródeł, skąd może nadejść atak, nie jest zaskoczeniem, że bezpieczeństwo pozostaje przedmiotem uwagi. Praktycznie wszyscy respondenci wskazali, że są umiarkowanie zaniepokojeni kwestią ochrony zasobów w chmurach publicznych, a prawie jedna trzecia jest bardzo zaniepokojona. Mimo to na czele listy zagrożeń dla bezpieczeństwa chmury nie znalazła się działalność cyberprzestępców, a błędy popełnione podczas konfigurowania narzędzi ochronnych – tak twierdzi 67% specjalistów. Złożoność zarządzania środowiskami wielochmurowymi wyraźnie zwiększa to, co już stanowi wyzwanie.

78% ankietowanych uznałoby za pomocne lub niezwykle pomocne posiadanie jednej platformy zabezpieczającej zasoby chmurowe, zapewniającej jeden pulpit administracyjny, umożliwiający jednocześnie konfigurowanie reguł polityki w celu zagwarantowania spójnej i kompleksowej ochrony danych w różnych środowiskach chmurowych.

Jednocześnie specjaliści ds. cyberbezpieczeństwa działają w warunkach ograniczonego budżetu, a koszty inwestycji są dla nich podstawowym kryterium przy podejmowaniu decyzji o wyborze rozwiązania ochronnego. Wygląda na to, że zarządy niektórych przedsiębiorstw mogą jeszcze nie rozumieć, iż osiągnięcie celów biznesowych za pomocą chmury jest niemożliwe bez zagwarantowania bezpieczeństwa w tym środowisku.

Złożoność chmury pokonana dzięki strategii ochronnej

Stawienie czoła wyzwaniom przedstawionym w raporcie zatytułowanym „2021 Cloud Security Report" wymaga przyjęcia strategii, której elementem jest przeciwdziałanie złożoności środowisk chmurowych. Firmy bowiem wciąż korzystają z różnorodnych zestawów narzędzi zapewniających zróżnicowany sposób kontroli i poziom zabezpieczenia, specyficzny dla każdej z platform chmurowych.

Portfolio rozwiązań Adaptive Cloud Security firmy Fortinet zapewnia przedsiębiorstwom możliwość wyeliminowania tak dużego poziomu złożoności środowisk chmurowych. Głęboko zintegrowane, natywne rozwiązania ochronne zapewniają spójny wgląd w stan pracy środowiska, zabezpieczają je, a także umożliwiają sprawowanie kontroli zgodnie ze spójnymi regułami polityki w środowiskach wielochmurowych i hybrydowych. Te wspólne ramy nie tylko zapewniają jednolity poziom bezpieczeństwa, ale również upraszczają cyberobronę, raportowanie zgodności z regulacjami i współużytkowanie danych. Zespoły mogą swobodnie korzystać z dowolnej platformy chmurowej, która odpowiada ich konkretnym potrzebom, mając pewność, że ich dane i aplikacje będą bezpieczne, odporne i łatwo dostępne.

Chmura jest obecnie krytycznym elementem cyfrowego środowiska w większości firm, a często także kluczowym czynnikiem umożliwiającym osiągnięcie sukcesu w przyszłości. Dopasowanie strategii bezpieczeństwa do strategii biznesowej jest kluczem do zagwarantowania, że przyszłości nas nie zawiedzie.

[1] *https://www.fortinet.com/resources-campaign/dynamic-cloud-security/2021-cloud-security-report?utm_source=blog&utm_campaign=2021-cloud-security-report*

Ekspert Fortinet o ochronie infrastruktury sieci 5G

Ronen Shpirer,
4G & 5G Solutions Marketing Director, Fortinet

Zintensyfikowany w ubiegłym roku proces modernizacji infrastruktury sieci komórkowej w celu wprowadzenia standardu 5G wzbudził sporo kontrowersji. Zjawisko to stało się przedmiotem publicznej debaty, co wywołało polaryzację społeczeństwa. Mimo to coraz więcej krajów decyduje się na wdrożenie sieci 5G, biorąc pod uwagę korzyści, jakie zapewniają one zarówno użytkownikom indywidualnym, jak i przedsiębiorstwom.

Przepis na unikalność sieci piątej generacji

5G różni się od poprzednich generacji sieci komórkowych w dwóch głównych aspektach. Po pierwsze, rozbudowane możliwości zapewniane przez ten standard nie są wynikiem systematycznej, stopniowej ewolucji, tak jak miało to miejsce przy powstawaniu poprzednich wersji protokołów transmisji danych w urządzeniach mobilnych. Charakterystyczne dotychczas dla sieci komórkowych zamknięte protokoły i interfejsy zostały zastąpione popularnymi w branży IT protokołami, interfejsami API i mechanizmami chmurowymi.

Po drugie, 5G zapewnia wartość dodaną zarówno przedsiębiorstwom w branży przemysłowej, jak i operatorom sieci komórkowych. Dzięki szerokiej funkcjonalności firmy mogą opracowywać nowe produkty i usługi, zwiększać wydajność i wprowadzać mechanizmy automatyzujące, których stosowanie nie było możliwe z zastosowaniem wyłącznie sieci przewodowych lub Wi-Fi.

5G stwarza również szansę rozwoju operatorom sieci komórkowych. W tradycyjnym modelu ich przychody były silnie uzależnione od sprzedaży kart SIM. Dzięki ekosystemowi 5G możliwe jest lepsze zaadresowanie segmentu biznesowego i dostarczanie klientom usług wykraczających poza łączność komórkową.

Wpływ sieci 5G na cyberbezpieczeństwo

Innowacje wprowadzone w sieciach nowej generacji stwarzają nowe zagrożenia dla cyberbezpieczeństwa. Wykorzystanie w infrastrukturze powszechnie stosowanych protokołów IT oraz otwarty i rozproszony charakter sieci 5G sprawia, że staje się ona atrakcyjnym celem dla hakerów. Jej użytkownicy skupiają się głównie na zaletach, takich jak bardzo szeroki zasięg, duża skalowalność, wydajność i elastyczność obsługi – zarówno gdy infrastruktura 5G zostanie wykorzystana w rdzeniu środowiska IT, na jego brzegu, jak i do uzyskiwania zdalnego dostępu. Nie można jednak zapominać o jej odpowiednim zabezpieczeniu. Mechanizmy ochronne muszą być zintegrowane nie tylko z chmurową infrastrukturą wirtualną, ale też z warstwą orkiestracji, aby zapewnić bezpieczeństwo firmowym danym oraz ciągłość biznesową przedsiębiorstwa.

Hiperskalowalność, ultraniskie opóźnienia, obsługa komunikacji w modelu machine-to-machine (M2M), przewidywalność i wysoka precyzja pokrycia sygnałem – to tylko część z możliwości 5G, które wpłyną na popularyzację tego standardu w przemyśle i wśród konsumentów. Dlatego tak ważne jest całościowe podejście do tematu bezpieczeństwa. Automatyzacja działań ochronnych i analiza zagrożeń mają kluczowe znaczenie dla zabezpieczania np. urządzeń internetu rzeczy, przemysłowego internetu rzeczy, sieci publicznych i prywatnych oraz aplikacji.

Bezpieczne 5G – szansa na rozwój

5G to najlepiej zaprojektowana pod kątem bezpieczeństwa generacja sieci komórkowych. Jest to jednak tylko dobry punkt wyjścia, natomiast konieczne pozostaje opracowanie szczegółowych standardów ochrony rozwiązań podłączonych do 5G. W 2020 roku firma Fortinet zorganizowała badanie na temat możliwości zastosowania sieci 5G w przedsiębiorstwach z różnych branż. Wynika z niego, że bezpieczeństwo jest kluczowym aspektem przy podejmowaniu decyzji o wykorzystaniu sieci piątej generacji:

- Prawie 90% respondentów uważa, że kwestie bezpieczeństwa zapewnianego przez operatorów sieci komórkowych są kluczowe lub bardzo ważne dla zastosowania 5G w firmach z różnych branż.
- Ponad 80% badanych stwierdziło, że zapewnione bezpośrednio w standardzie 5G zabezpieczenia są ważne, ale stanowią tylko podstawę potrzebną do pełnej ochrony.
- Według 54% ankietowanych operatorzy powinni oferować model wspólnej odpowiedzialności za bezpieczeństwo wdrożeń wykorzystujących komunikację w sieci 5G. Jednak większość z nich (86%) wyobraża sobie ten model tylko jako alternatywę wobec tradycyjnego podejścia, zakładającego kompleksowe zabezpieczenie środowiska przez operatora.

Nowe podejście

Bezpieczeństwo komunikacji w infrastrukturze mobilnej poprzednich generacji bazowało na ochronie samej sieci – tworzeniu środowiska otoczonego „murem" i zabezpieczaniu wszystkich punktów łączności, takich jak internet, roaming, zdalny dostęp pracowników oraz partnerów zewnętrznych itp. Jednak charakter sieci 5G i jej kluczowa rola w segmencie biznesowym sprawia, że kwestie bezpieczeństwa powinny być traktowane szerzej i obejmować następujące działania:

1. Ochrona infrastruktury 5G przed atakami w celu zapewnienia ciągłości i dostępności usług, podobnie jak w sieciach poprzednich generacji.
2. Ochrona całego ekosystemu 5G, aby możliwe było zapewnienie przedsiębiorstwom z różnych branż korzystania z pełnej funkcjonalności sieci 5G z zachowaniem wymogów bezpieczeństwa oraz możliwości przestrzegania przepisów prawa i innych regulacji.
3. Umożliwianie przedsiębiorstwom zarabianie na świadczeniu szerokiej gamy usług zarządzanych związanych z zapewnianiem bezpieczeństwa przy różnego typu zastosowaniach sieci 5G.

Bezpieczeństwo powinno być istotnym czynnikiem umożliwiającym klientom rozwój dzięki wdrażanym rozwiązaniom 5G, zaś operatorom komórkowym uzyskanie dodatkowych źródeł zysku.

Rzeczywistość związana z oprogramowaniem ransomware jest coraz bardziej brutalna — jak firmy mogą stawić jej czoła?

Dave Russell,
wiceprezes
ds. strategii dla
przedsiębiorstw,
Veeam

Ataki typu ransomware powodują dziurę w budżetach przedsiębiorstw, które muszą płacić okup w wyniku wysoce ukierunkowanych ataków ze strony organizacji przestępczych. Problem ten pogłębił się wraz z pojawieniem się masowej pracy zdalnej. Rozszerzenie granic biura na lokalizacje internetowe i zdalne ujawniło poważne luki w zabezpieczeniach, a przestępcy chętnie je wykorzystują.

Według organizacji CyberSecurity Ventures nowy atak ransomware ma miejsce co 11 sekund[1]. W takiej sytuacji najlepiej jest nie płacić, jednak większość firm i tak godzi się na żądania cyberprzestępców. Wiele z nich czuje ogromną presję, aby ograniczyć szkody związane z przestojami spowodowanymi przez oprogramowanie ransomware, a teoretycznie najszybszym rozwiązaniem jest zapłata.

Fakt, że tak wiele z nich zdecydowało się na taki krok, nie jest zaskoczeniem — obecnie zmagają się one z innymi wyzwaniami i presją, które wynikają z okoliczności pandemii COVID-19. Takie podejście stanowi jednak zachętę dla cyberprzestępców do dalszego wykorzystywania tego lukratywnego, nielegalnego rynku, o czym świadczy 600-procentowy wzrost liczby ataków od czasu pojawienia się COVID-19.

Na szczęście przedsiębiorstwa i rządy uznały, że koniecznie trzeba zatrzymać ten trend. Oprogramowanie ransomware jest obecnie gorącym tematem każdego spotkania zarządu, a nawet stało się przedmiotem dyskusji na szczycie G7, jak również wielu innych rozmów dyplomatycznych pomiędzy światowymi przywódcami. Nadszedł czas, aby pomyśleć o nowoczesnej ochronie danych i jej przyszłości.

Przestępczość zorganizowana

Łatwo jest zapomnieć, że za oprogramowaniem ransomware, które zadomowiło się w systemie firmy, stoi przestępca. Kiedyś uważano, że oprogramowanie ransomware błąka się w internecie i jest szkodliwe tylko wtedy, gdy się je kliknie. Obecnie wiele osób zaczyna dostrzegać jego poważny, złożony i ukierunkowany charakter. Jest to przestępczość zorganizowana, która działa w sposób innowacyjny, aby przeniknąć do firmy i np. łańcucha dostaw. Stanowi ona realne zagrożenie dla całych branż i społeczności.

Jak więc możemy chronić się przed takimi osobami? Wadą naszego połączonego i cyfrowego świata jest to, że napastnik może przebywać w zupełnie innym zakątku ziemi, co utrudnia ściganie przy użyciu tego samego systemu prawnego, któremu podlega konkretna firma. Problem polega na tym, że kontrola na taką skalę będzie wymagać współpracy międzynarodowej i działań rządowych wykraczających poza wszystko, co widzieliśmy w sferze bezpieczeństwa cybernetycznego. Rzecz jasna będzie to również wymagać czasu, którego, jak wiadomo, firmy nie mają w obliczu ciągłych zagrożeń.

Dlatego też podczas gdy my czekamy na to polityczne zaangażowanie, firmy muszą być w pełni przygotowane na nieustające i zmasowane ataki ransomware — zwłaszcza teraz, gdy popularna jest praca zdalna. Dotychczasowe środki cyberbezpieczeństwa nie wystarczą; należy wdrożyć nowoczesne środki ochrony danych.

Myśl jak haker

Podobnie jak detektyw, który musi myśleć jak przestępca, aby rozwiązać zagadkę, jedynym sposobem na skuteczną ochronę firm przed cyberatakami jest myślenie jak hakerzy. Są nieustępliwi, wyjątkowo świadomi i zdyscyplinowani. Pracodawcy i pracownicy muszą działać tak samo, aby nie dopuścić do powstania słabych punktów.

Właściwa higiena cyfrowa musi stać się drugą naturą, a nie czymś, co ćwiczy się przez tydzień po corocznym szkoleniu z zakresu cyberbezpieczeństwa, a następnie zapomina. Brak łatania oprogramowania należy traktować tak samo jak niezamykanie biura na noc, a brak planu odzyskiwania danych po awarii powinien być równoznaczny z rezygnacją z ubezpieczenia majątku firmowego. Nie możemy myśleć wyłącznie o zabezpieczeniu przestrzeni fizycznej — wrogowie działają w przestrzeni cyfrowej.

Innym ważnym aspektem jest myślenie o skali sukcesu hakera. W wielu przypadkach spędzają oni cały dzień na atakowaniu systemów. Poświęcają swój czas na rozwój i wprowadzanie innowacji do swoich ataków, aby pokonać bariery bezpieczeństwa. Rozsądnie jest zakładać, że w końcu będą w stanie to zrobić, nawet jeśli zastosowane zostaną najlepsze zabezpieczenia cybernetyczne. Jak widać na przykładzie liczby firm płacących okup, atak może wyrządzić wystarczająco dużo szkód, aby skłonić firmy do zapłacenia okupu, zamiast obrania alternatywnych dróg.

Firmy bez względu na branżę, w której działają, powinny zainwestować w nowoczesne praktyki ochrony danych, aby zminimalizować skutki ataków ransomware. Postrzeganie ataków jako nieuniknionych jest pierwszym krokiem do stworzenia bezpieczniejszej kultury cybernetycznej, a pracownicy powinni być bardziej wyedukowani i świadomi istnienia i metod atakowania przez oprogramowanie ransomware. Jednocześnie firmy muszą mieć odpowiednie zabezpieczenia, aby minimalizować zakłócenia, w tym oprogramowanie antywirusowe i zapory sieciowe, a także procedury ciągłego tworze nia kopii zapasowych i odzyskiwania danych, aby zapewnić odpowiednie zabezpieczenie przed niszczącymi skutkami oprogramowania ransomware.

[1] *https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021*

Zapewnij swoim pracownikom bezpieczną pracę - niezależnie od miejsca

Dzięki Kaspersky ASAP - platformie edukacyjnej online - możesz zadbać, by Twoi pracownicy byli gotowi na cyberzagrożenia, zarówno gdy pracują w biurze jak i w domu.

Nasza platforma powstała przy udziale czołowych ekspertów ds. cyberbezpieczeństwa, dzięki czemu obejmuje najbardziej aktualne i istotne zagadnienia. Zarządzanie szkoleniami jest zautomatyzowane, a pracownicy biorą udział w praktycznych i angażujących lekcjach, które budują ich świadomość i umiejętności z zakresu cyberbezpieczeństwa.

Wypróbuj wersję testową już teraz: asap.kaspersky.pl

kaspersky AKTYWUJ PRZYSZŁOŚĆ

Kaspersky Automated Security Awareness Platform

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.