BIAŁA KSIĘGA

Bitdefender

Security

Raport 2020: krajobraz zagrożeń biznesowych.

www.bitdefender.pl

Spis treści

Wstęp 4
- Kluczowe ustalenia 4
- Kluczowe rezultaty analizy telemetrycznej 6

„Nowa normalność": zagrożenia i trendy 6
- Błędna konfiguracja i ryzyko 6
- Internet rzeczy (IoT) 7
  - Ryzyko biznesowe 7
  - Ryzyko związane z pracą zdalną 7
- Podatności 8

Cyberataki „na koronawirusa" 9
- Tematyczny przegląd zagrożeń 9
- Phishing i spear-phishing 11

W szerszej perspektywie. Zmiany w zaawansowanych atakach 12
- Taktyka i techniki ataku 12
  - Scenariusze ataków - studium przypadku WMI 12
  - Techniki i podtechniki MITRE ATT&CK® popularne w 2020 r. 14
- Wzrost popularności APT jako usługi 15
- Zagrożenia sieciowe 16
- Konsekwencje - nowe zagrożenie dla MŚP 17

Regionalna ewolucja tradycyjnych zagrożeń 17

Wnioski 23

*„Z perspektywy 2020 r., **50 procent[1] organizacji było nieprzygotowanych** na scenariusz, w którym musiałyby przenieść całą swoją siłę roboczą do trybu pracy zdalnej. W związku z globalną pandemią SARS-CoV-2[2] ludzie na całym świecie cierpieli z powodu choroby układu oddechowego, jednak wpłynęła ona również na sposób funkcjonowania organizacji i przedsiębiorstw.*

Brak przygotowania na taki scenariusz sprawił, że wiele organizacji było narażonych na potencjalne luki i błędne konfiguracje, które mogły być łatwo wykorzystane przez atakujących w celu włamania się do systemu, kradzieży danych, a nawet czerpania dodatkowych zysków z wyłudzania pieniędzy od zaatakowanych podmiotów.

W ramach nadchodzącego międzynarodowego miesiąca świadomości cyberbezpieczeństwa tym razem Bitdefender udostępnia swój coroczny raport krajobrazu zagrożeń wcześniej, aby pomóc profesjonalistom w planowaniu strategii cyberbezpieczeństwa w 2021 r.

Jesteśmy przekonani, że te obszerne informacje zebrane za pomocą naszych 500 milionów sensorów na całym świecie zapewnią przedsiębiorstwom solidne podstawy do budowania długoterminowej strategii cyberbezpieczeństwa pracy zdalnej."

Bogdan Dumitru, CTO w Bitdefender

1 "Bitdefender 10 IN 10 Study: The Indelible Impact of COVID-19 on Cybersecurity", Bitdefender, https://download.bitdefender.com/resources/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf

2 "Severe acute respiratory syndrome coronavirus 2", Wikipedia, https://en.wikipedia.org/wiki/Severe_acute_respiratory_syndrome_coronavirus_2

Wstęp

Kluczowe ustalenia

PRACA ZDALNA I WPŁYW PANDEMII. Przedsiębiorstwa i organizacje niezależnie od ich wielkości niemal z dnia na dzień przeszły na tryb pracy z domu w wyniku epidemii COVID-19. Mechanizmy kontroli i polityka bezpieczeństwa sieci obowiązujące w sieci firmowej musiały ulec znacznym przeobrażeniom, aby uwzględnić urządzenia pracowników łączące się z infrastrukturą biznesową z niezaufanych sieci. Jednak zdaniem 45%[3] CISO i CIO to urządzenia IoT stanowią największe zagrożenie w domowych sieciach pracowników, ponieważ mogą one zostać łatwo zhakowane przez atakujących i wykorzystane do ataku na urządzenia pracowników, a nawet na całą sieć.

BŁĘDNE KONFIGURACJE. Nowy model pracy zdalnej potencjalnie naraził infrastrukturę biznesową na nowe wektory ataków i zagrożenia, których jeszcze rok wcześniej nie brano by pod uwagę. Ponieważ większość organizacji zmaga się z nagłą koniecznością dostosowania się do pracy zdalnej, nieuchronnie pojawiają się pewne niedopatrzenia i błędy w konfiguracji zabezpieczeń.

Jedną z najczęstszych błędnych konfiguracji, zwłaszcza odkąd praca zdalna stała się standardem, jest włączona i źle skonfigurowana usługa WinRM. Telemetria biznesowa Bitdefender wskazuje, że 9 na 10 punktów końcowych zgłasza to jako główną błędną konfigurację, co oznacza, że jej skuteczne wykorzystanie przez hakera może prowadzić do narażenia punktu końcowego lub innego ryzyka związanego z infrastrukturą biznesową.

INTERNET RZECZY. Ponadto **45%** specjalistów z dziedziny bezpieczeństwa IT uważa, że urządzenia IoT w domowych sieciach pracowników są poważnym wyzwaniem dla bezpieczeństwa, ponieważ mogą być łatwo kontrolowane przez hakerów i zagrażać infrastrukturze biznesowej. Telemetria Bitdefender wykazała, **że liczba podejrzanych incydentów z udziałem IoT w sieciach domowych wzrosła o 46%[4] od stycznia do czerwca. Ataki polegające na skanowaniu portów są przyczyną 55,73%** wszystkich wykrytych incydentów sieciowych, a próby kradzieży haseł przez HTTP stanowią **22,62%** incydentów w sieciach domowych.

BRANŻA. W ujęciu sektorowym specjaliści z dziedziny bezpieczeństwa oszacowali[5], że usługi finansowe (**43%**) i opieka zdrowotna (**34%**) należały do branż, które ucierpiały najbardziej nie tylko z powodu pandemii, ale również w wyniku działań cyberprzestępców szukających zysku, wykorzystując okoliczności, strach, panikę i brak informacji wśród pracowników i organizacji na temat koronawirusa. Służba zdrowia i lekarze odgrywają kluczową rolę w leczeniu i stabilizacji stanu zdrowia pacjentów z koronawirusem, a zakłócenia w infrastrukturze zagrażałyby życiu pacjentów. Dlatego Bitdefender zaoferował organizacjom opieki zdrowotnej wszystkich rozmiarów, od małych gabinetów stomatologicznych i okulistycznych po duże szpitale, bezpłatny[6], dostęp do naszych zabezpieczeń klasy korporacyjnej.

LUKI. Z perspektywy niezałatanych luk w powszechnie instalowanych aplikacjach i systemach operacyjnych, które atakujący wydają się sondować w środowiskach biznesowych, **36,37% wszystkich zgłoszonych niezałatanych luk w pierwszej połowie 2020 r**. obejmuje CVE, które zostały dodane w 2019 r., według telemetrii biznesowej Bitdefender. Spośród nich, **88,39%** dotyczy nienaprawionych luk w **produktach i usługach firmy Microsoft**. Jednak choć większość prób eksploatacji luk dotyczy produktów Microsoftu, atakujący mogą też dążyć do wykorzystania luk w oprogramowaniu klasy korporacyjnej do zarządzania sprzętem, popularnych narzędziach analizy sieciowej stosowanych przez specjalistów z dziedziny IT i bezpieczeństwa, edytorach tekstu i kodu źródłowego, a nawet popularnych aplikacjach multimedialnych.

3 "Bitdefender 10 IN 10 Study: Seven in Ten CISOs Believe Cyberwarfare is an Imminent Threat to Their Organisations", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/368/Bitdefender-10-in-10-Report.pdf

4 "Mid-Year Threat Landscape Report 2020", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

5 "Bitdefender 10 IN 10 Study: The Indelible Impact of COVID-19 on Cybersecurity", Bitdefender, https://download.bitdefender.com/resources/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf

6 "Bitdefender Offers Enterprise-Grade Security at Zero-cost to Healthcare Organizations", Bitdefender, https://www.bitdefender.com/news/bitdefender-offers-enterprise-grade-security-at-zero-cost-to-healthcare-organizations-3815.html

CYBERATAKI „NA KORONAWIRUSA". Zagrożenia wykorzystujące kontekst koronawirusa stały się nową normą, a telemetria Bitdefender wykazała, że atakujący nadają swoim zagrożeniom otoczkę paniki, strachu i manipulacji informacjami. Co ciekawe, cyberataki „na koronawirusa" i rzeczywiste infekcje koronawirusem miały podobną dynamikę rozwoju w marcu i kwietniu - potencjalnie dlatego, że w miarę jak wirus szerzył się w różnych krajach Europy, atakujący opracowywali kampanie ukierunkowane także na te regiony. Telemetria Bitdefendera wykryła, że w tym okresie **4 na 10 e-maili na temat koronawirusa były próbami oszustwa, wyłudzenia lub zawierały malware**.

ROZWÓJ APT JAKO USŁUGI. Nowy krajobraz zagrożeń, przed którym stanęły firmy i organizacje, nie kończył się na oportunizmie atakujących i nagłej zmianie w modelu organizacji pracy. Z ostatnich analiz Bitdefender wynika, że zaawansowane taktyki i techniki, które zwykle przypisuje się grupom APT wspieranym przez niektóre państwa, obecnie są elementem ataków ukierunkowanych na sektory, które wcześniej nie doświadczały ataków APT. Cyberszpiegowski atak APT wymierzony w międzynarodową firmę zajmującą się architekturą i produkcją wideo ujawnił nowy trend, którego małe i średnie firmy nigdy nie uwzględniały w swoich modelach zagrożeń: grupy **APT do wynajęcia**[7]**.**

APT jako usługa wyznacza nowy trend w ewolucji cyberprzestępczości, ponieważ wyspecjalizowani atakujący zazwyczaj mający motywację polityczną[8] lub finansową obecnie przekształcili się w grupy APT do wynajęcia oferując swoje usługi temu, kto da więcej. Macierz zaawansowanych taktyk i technik opracowana przez MITRE[9] jest obecnie tym, co każda organizacja niezależnie od wielkości i obszaru zainteresowań musi uwzględnić aby zarówno zwiększyć swoje szanse na wykrycie zaawansowanych ataków, jak i przeanalizować rozwiązania zabezpieczające pod kątem najbardziej kompleksowego i skutecznego[10] pokrycia łańcucha ataków.

Nie tylko firmy odczuwają skutki nowego trendu, jakim są grupy APT do wynajęcia. Dostawcy usług zarządzanych (MSP) i muszą zmierzyć się z rzeczywistością, że narzędzia i usługi bezpieczeństwa, które oferują klientom, muszą zapewniać to, co najlepsze z obu światów: bezpieczeństwo i wykrywalność zagrożeń w całej infrastrukturze.

Aktualny niedobór umiejętności w zakresie cyberbezpieczeństwa i brak neuroróżnorodności wraz z powyższym trendem otworzyły drogę organizacjom, którym trudniej jest powołać własne wyspecjalizowane zespoły IT i bezpieczeństwa, do skorzystania z zarządzanych usług wykrywania i reagowania (MDR). Te wysoko wyszkolone i wykwalifikowane zespoły cyberbezpieczeństwa mogą zapewnić takie same możliwości w zakresie bezpieczeństwa, jakie daje własne centrum operacji bezpieczeństwa (SOC), lecz za ułamek kosztów i bez ryzyka niedoboru wykwalifikowanych pracowników.

Z punktu widzenia przedsiębiorstw krajobraz zagrożeń w pierwszej połowie 2020 r. znacznie się zmienił pod względem zakresu ataku, zagrożeń i wyzwań, jakie przyniosła światowa pandemia koronawirusa. Organizacje, które rozumiejąc nowe trendy dostosują się do nich, będą miały szansę zarówno zwiększyć swoją odporność na cyberataki, jak i lepiej zabezpieczyć ciągłość funkcjonowania.

TAKTYKI I TECHNIKI MITRE ATT&CK. Jednym z największych wyzwań dla CIO i CISO jest przekazywanie członkom zarządu informacji bez użycia skomplikowanego żargonu technicznego, a jednocześnie na tyle elokwentnie i precyzyjnie, aby decydenci biznesowi zrozumieli ryzyko. Ponad **55%**[11] CISO i CIO – z których wielu uczestniczy w podejmowaniu decyzji na najwyższym szczeblu w swoich organizacjach – uważa, że komunikacja musi ulec zmianie.

Model MITRE ATT&CK™ to kompleksowa matryca taktyk i technik używanych przez łowców zagrożeń zarówno do klasyfikowania ataków i oceny ryzyka organizacji, jak i do identyfikowania i eliminacji potencjalnych zagrożeń w ich infrastrukturze bezpieczeństwa. Model MITRE tworzy wspólny język, którym posługują się wszyscy fachowcy z zakresu

7 "APT Hackers for Hire Used for Industrial Espionage", Bitdefender, https://labs.bitdefender.com/2020/08/apt-hackers-for-hire-used-for-industrial-espionage/

8 "StrongPity APT – Revealing Trojanized Tools, Working Hours and Infrastructure", Bitdefender, https://labs.bitdefender.com/2020/06/strongpity-apt-revealing-trojanized-tools-working-hours-and-infrastructure/

9 MITRE, https://attack.mitre.org/

10 "MITRE ATT&CK Evaluation - Bitdefender a Stellar EDR Vendor For Midsized Organizations & MSPs", Bitdefender, https://businessinsights.bitdefender.com/mitre-attack-evaluation-results

11 "Bitdefender 10 IN 10 Study: The Indelible Impact of COVID-19 on Cybersecurity", Bitdefender, https://download.bitdefender.com/resources/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf

bezpieczeństwa IT, ułatwiając badanie i ocenę zagrożeń. Dlatego też, badanie i mapowanie zagrożeń w całym cyklu życia ataku opiera się na tej samej taksonomii we wszystkich sektorach i organizacjach. W sytuacji, gdy praca zdalna zmienia sposób projektowania infrastruktury biznesowej, MITRE ATT&CK™ może zarówno pomóc w wykrywaniu, mapowaniu i rozumieniu zagrożeń, jak i dostarczyć organizacjom kluczowych i praktycznych informacji, które mogą być użyte do usprawnienia ich zabezpieczeń.

Kluczowe rezultaty analizy telemetrycznej

- 93,10% czynników ryzyka ludzkiego dotyczy używania przez pracowników starych haseł do kont.
- 87,31% wszystkich błędnych konfiguracji dotyczy włączonej usługi WinRM.
- 46,84% wszystkich zgłoszonych ataków na poziomie sieci dotyczy exploitów SMB.
- 41,63% wszystkich zgłoszonych ataków na poziomie sieci to próby ataku typu bruteforce na RDP i FTP.
- 46-procentowy wzrost liczby podejrzanych incydentów IoT w sieciach domowych w I połowie 2020 r.
- 4 na 10 wiadomości e-mail dotyczących koronawirusa było próbami oszustwa, wyłudzenia lub zawierało malware.
- 63,63 procent wszystkich zgłoszonych niezałatanych luk w zabezpieczeniach dotyczy CVE starszych niż 2018 r. (włącznie)
- 42,52% poleceń etapu wykonywania i podtechnik interpretera skryptów wiąże się z wykorzystaniem poleceń i skryptów PowerShell.

„Nowa normalność”: zagrożenia i trendy

W pierwszej połowie 2020 r. organizacje musiały szybko przystosować się do nowego sposobu zarządzania pracownikami, a także poradzić sobie z nowymi i niespodziewanymi zagrożeniami i wyzwaniami. Pandemia koronawirusa zmusiła specjalistów IT i specjalistów ds. bezpieczeństwa do pracy na długie zmiany, aby umożliwić pracownikom pracę zdalną w pełnym wymiarze godzin, a jednocześnie opracować nowe procedury i polityki bezpieczeństwa firmy, które mają ograniczyć zakres ataku.

Pandemia spowodowała, że infrastruktura firmowa została przemodelowana i wspiera bezterminową pracę zdalną, ale zmiany wprowadzone z dnia na dzień w politykach i konfiguracjach prawdopodobnie otworzyły nowe wektory ataków, które na dłuższą metę mogą wykorzystać atakujący. Podczas gdy w 2019 r. średni czas wykrycia i opanowania naruszenia danych szacowano na około 209 dni[12], prawdopodobnie czas ten będzie znacznie dłuższy pod koniec 2020 r., ze względu na wszystkie zmiany i błędne konfiguracje, które wprowadzono w infrastrukturze w wyniku pandemii.

Chociaż niektóre organizacje radzą sobie lepiej niż inne, nie zmienia to faktu, że **72%**[13] CIO i CISO uważa, że w obszarze cyberbezpieczeństwa potrzeba bardziej zróżnicowanego zestawu umiejętności. Jak wynika z tego samego badania, 71% specjalistów z dziedziny bezpieczeństwa uważa, że cyberwojna może stanowić zagrożenie dla ich organizacji. Przekonanie to podzielają również CIO i CISO, jednak tylko 63% z nich zgadza się z tym stwierdzeniem.

To właśnie strach przed byciem poszkodowanym w wyniku incydentu związanego z cyberwojną spędza sen z powiek specjalistom ds. bezpieczeństwa, a mimo to **27%** organizacji nie posiada żadnej strategii obrony przed tego typu zagrożeniami.

Błędna konfiguracja i ryzyko

Szacunkowy średni czas opanowania naruszenia ochrony danych[14] w 2019 r. wyniósł 206 dni, a w 2020 r. prawdopodobnie znacznie się wydłużył ze względu na przeoczone błędne konfiguracje lub z powodu braku narzędzi zapewniających lepszą widoczność [zagrożeń], które ułatwiałyby identyfikację potencjalnych nowych martwych punktów wynikających z nowej rekonfiguracji infrastruktury.

12 “IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years”, IBM, https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

13 “Bitdefender 10 IN 10 Study: Seven in Ten CISOs Believe Cyberwarfare is an Imminent Threat to Their Organisations”, Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/368/Bitdefender-10-in-10-Report.pdf

14 “Cost of a Data Breach Report 2019”, IBM, https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

Według telemetrii biznesowej Bitdefender do najczęściej występujących błędnych konfiguracji punktów końcowych przedsiębiorstw należy **włączona usługa WinRM[15] (87,31%)**. Usługa ta pozwala zespołom IT i bezpieczeństwa na zdalne zarządzanie punktami końcowymi i uruchamianie skryptów na maszynach pracowników. Jest to szczególnie przydatne przy automatyzacji zadań i polityk, ale może też być wykorzystane przez atakujących, jeśli usługa jest źle skonfigurowana.

W połączeniu z czynnikami ryzyka ludzkiego, jakimi są praca poza siedzibą firmy i ewentualne łączenie się z infrastrukturą firmową poprzez niezabezpieczone sieci lub nawet niezarządzane systemy, powoduje to dodatkowe obciążenie dla zespołów bezpieczeństwa, których zadaniem jest przeformułowanie polityk bezpieczeństwa i infrastruktury w celu dostosowania się do nowej sytuacji. Ponadto jedno z największych ryzyk ludzkich dotyczących pracowników wiąże się z **ponownym użyciem starych haseł (93,10%)**, jak wynika z telemetrii biznesowej Bitdefender.

Internet rzeczy (IoT)

Podczas gdy to samo badanie wskazuje, że **75%** CIO i CISO uważa, że częstsze korzystanie z urządzeń IoT zwiększyło wiedzę ich organizacji o sposobach ich ochrony, 20% CIO i CISO uważa, że urządzenia IoT będą nadal upowszechniać się szybciej niż będzie można je zabezpieczyć.

Oznacza to, że choć w ciągu ostatnich kilku lat organizacje zdobyły pewne doświadczenie w zakresie integracji urządzeń IoT, a nawet dostosowały do nich wewnętrzne polityki bezpieczeństwa, stałe upowszechnianie się urządzeń, które w niewielkim stopniu uwzględniają standardy lub ramy bezpieczeństwa, może nadal powodować poważne problemy.

Ryzyko biznesowe

Wykorzystując technologię deception Bitdefender obserwuje trendy ataków na IoT poprzez specjalnie skonfigurowane, umieszczone w sieci aplikacje i usługi, aby zrozumieć sposób działania hakerów i stosowane przez nich sposoby forsowania zabezpieczeń tego typu urządzeń. Sieć przynęt Bitdefender symuluje protokoły takie, jak Telnet lub SSH, aby umożliwić uruchamianie exploitów sieciowych na różnych platformach lub posługuje się pełnowymiarowymi podatnymi na atak maszynami z systemem Windows, eksponując je na działania hakerów w sieci.

W rezultacie nasze sieci pułapek rejestrują średnio **1,5 miliona odsłon co 15 minut,** co świadczy o tym, że atakujący automatyzują znaczną część skanowania podatnych na ataki urządzeń połączonych z internetem. Co **24 godziny** cyberprzestępcy otwierają w naszej sieci pułapek **ponad 8,5 mln sesji przeglądania**. Pokazuje to, że wiele ataków oscyluje wokół manipulacji identyfikatorami sesji i plikami cookie, aż po ataki typu directory traversal na podatne usługi w sieci.

Odnotowująca prawie 8000 sesji SSH i 4500 sesji Telnet co 24 godziny technologia deception umożliwia Bitdefender zebranie około 200 plików na godzinę, zwykle porzucanych przez hakerów i atakujących. Oprócz malware'u pliki te zawierają narzędzia, skrypty, a nawet exploity przeznaczone do przejęcia pełnej kontroli nad urządzeniem lub przemieszczania się po infrastrukturze.

Wszystkie te dane telemetryczne jeszcze bardziej utwierdzają CIO i CISO w przekonaniu, że upowszechnianie się urządzeń IoT wyprzedza standardy i praktyki bezpieczeństwa, które mają je chronić. Niezależnie od tego, czy urządzenia IoT należą do sieci domowych czy korporacyjnych, wiele funkcji i wykorzystywanych usług oraz protokołów komunikacji jest podobnych. Oznacza to, że większość IoT jest obarczona tym samym ryzykiem bez względu na to, do jakiej sieci są podłączone.

Ryzyko związane z pracą zdalną

Podczas gdy **zwykle 61,56% wszystkich urządzeń połączonych z internetem** w sieciach domowych stanowią smartfony, komputery, tablety, laptopy, konsole i routery, według danych telemetrycznych Bitdefender pozostałą część stanowią urządzenia IoT. Bardziej egzotyczne przykłady urządzeń połączonych z internetem obejmują inteligentne żarówki, inteligentne odkurzacze, oczyszczacze powietrza, panele słoneczne, elektroniczne nianie, roboty kuchenne, czujniki ruchu i wiele innych.

Telemetria Bitdefender wskazuje, że liczba podejrzanych incydentów IoT w sieciach domowych wzrosła o 46% od stycznia do czerwca. Ataki skanowania portów były przyczyną 55,73% wszystkich rozpoznanych incydentów sieciowych, natomiast próby kradzieży haseł przez HTTP stanowiły 22,62% wszystkich incydentów sieciowych w sieciach domowych.

15 "Windows Remote Management", Wikipedia, https://en.wikipedia.org/wiki/Windows_Remote_Management

Co ciekawe, ostatnie badania[16] ujawniają, że wiele routerów wykorzystywanych w sieciach domowych/biznesowych nie było aktualizowanych od ponad roku, zawiera setki luk w zabezpieczeniach i działa na przestarzałych systemach operacyjnych i jądrach Linuksa.

Badacze Bitdefender zbadali[17] przypadek, w którym atak na domowe routery doprowadził do zmiany ustawień DNS i przekierowania ofiar na strony serwujące malware. Choć taktyki tej użyto wówczas w celu przekonania ofiar do pobrania i zainstalowania złośliwego oprogramowania w ramach oszustwa „na koronawirusa", może ona stanowić zagrożenie również dla zdalnych pracowników, ponieważ ten sam atak może potencjalnie przekierować ich na stronę phishingową zbierającą korporacyjne dane logowania i inne dane. Tym samym skuteczny atak na domowy router może potencjalnie zagrozić nie tylko danym pracowników zdalnych, ale także firmom.

Podatności

Naprawa luk pozostaje jednym z największych wyzwań w organizacjach. Niezałatane luki są jednym z głównych powodów włamań do systemów organizacji, jak twierdzi 60%[18] poszkodowanych w wyniku naruszeń bezpieczeństwa w 2019 r., a brak widoczności niezałatanych luk zazwyczaj prowadzi do włamań. Jak wynika z tego samego badania, 62% organizacji nie wiedziało nawet, że są podatne na atak dopóki do niego nie doszło, a 52% ma procedurę ręcznej, nie zautomatyzowanej naprawy podatności.

Telemetria biznesowa Bitdefender wskazuje, że **63,63% wszystkich odnotowanych niezałatanych luk w pierwszej połowie 2020 r. dotyczy CVE starszych niż z 2018 r. (włącznie)**. Oznacza to, że podczas gdy **36,37 procent wszystkich zgłoszonych niezałatanych luk w pierwszej połowie 2020 roku, dotyczy CVE zgłoszonych w 2019 roku**, zdecydowana większość organizacji nadal posiada niezałatane luki, które zostały zidentyfikowane w dowolnym miejscu pomiędzy 2002 a 2018 .

Spośród podatności zgłoszonych w 2019 r. Aż 88,39% dotyczy niezałatanych luk w aplikacjach Mozilli, a 7,91% - luk w produktach i usługach Microsoftu.

Przenoszenie CVE poprzez niezałatane luki	
2019	**36,37%**
2018	**31,27%**
2017	**19,37%**
2016	**4,76%**
Inne	**8,23%**

W większości środowisk biznesowych zazwyczaj wykorzystywana jest szeroka gama wersji produktów Microsoftu i Mozilli, co tłumaczy, dlaczego atakujący mogą skupić się na tych konkretnych producentach, ale telemetria biznesowa Bitdefendera wykryła również niezałatane luki w oprogramowaniu Oracle Virtual Box (1,77%), VLC Media Player (1,11%), a nawet Notepad++ (0,24%).

Jednakże, o ile aplikacje te są dość rozpowszechnione w wielu firmach, znaleźliśmy również niezałatane luki w oprogramowaniu klasy korporacyjnej zwykle używanym do zarządzania zasobami, platformami zarządzania tożsamością (IAM), a nawet w popularnych archiwizatorach i narzędziach analizy sieciowej powszechnie używanych przez zespoły IT i bezpieczeństwa. **HPE Intelligent Management Center (IMC), PuTTY, QUEMU i Squid, Atlassian, Extenua SilverSHielD, Wireshark i MongoDB** - to tylko garstka popularnych aplikacji biznesowych, które mają nienaprawione podatności według telemetrii biznesowej Bitdefender. Podczas gdy liczba odnotowanych prób wykorzystania niezałatanych luk w powyższych rozwiązaniach klasy korporacyjnej jest stosunkowo niewielka w porównaniu do Mozilli czy Microsoftu, pokazuje to, że atakujący mogą być również zainteresowani wykorzystaniem luk w konkretnym oprogramowaniu biznesowym.

16 "Home Router Security Report 2020", Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

17 "New Router DNS Hijacking Attacks Abuse Bitbucket to Host Infostealer", Bitdefender, https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/

18 "Costs and Consequences of Gaps in Vulnerability Response", Ponemon Institute & ServiceNow, https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

Przykładowo w maju 2020 r. najczęściej zgłaszaną niezałataną luką o wysokim stopniu zagrożenia w produktach Mozilli była luka CVE-2019-11746[19]. Ta konkretna podatność może zostać wykorzystana w kontekstach typowych dla przeglądarki i dotyczy manipulacji elementami wideo, która może wywołać możliwy do wykorzystania błąd.

W tym samym okresie najczęściej zgłaszaną niezałataną luką o wysokim stopniu zagrożenia w produktach firmy Microsoft w 2019 r. była luka CVE-2019-0541[20]. Luka dotyczy szerokiej gamy produktów Microsoft, od Microsoft Office po Internet Explorer i Office 365 ProPlus. Może ona umożliwić atakującemu przejęcie kontroli nad systemem, jeśli zalogowany użytkownik ma uprawnienia administratora.

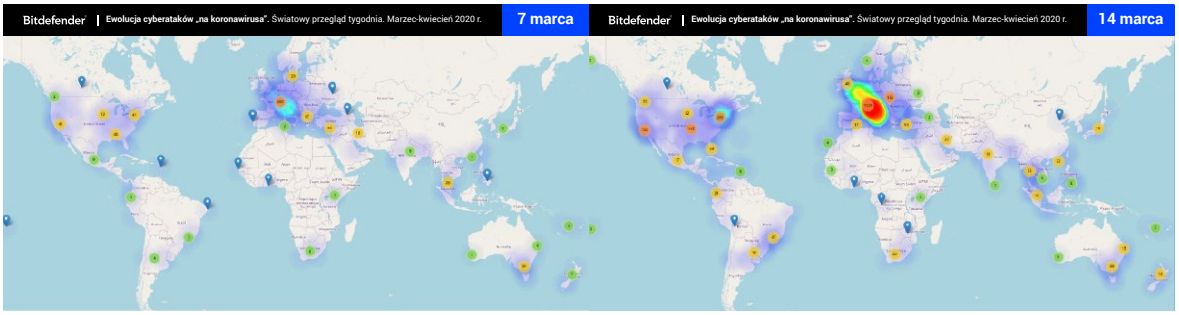
Dane telemetryczne uzyskane dzięki technologii Bitdefender zarządzania aktualizacjami pokazują, że organizacje nadal mierzą się z wyzwaniami, jakimi są aktywne i terminowe wdrażanie poprawek i aktualizacji bezpieczeństwa w systemach operacyjnych i aplikacjach. Czy to z powodu problemów ze wsteczną kompatybilnością, czy też w wyniku braku planowania i wykonywania testów kompatybilności z istniejącą infrastrukturą, niezałatane luki mogą zwiększyć ryzyko naruszenia danych, szczególnie w przypadku pracy z domu, gdzie punkty końcowe pracowników nie są chronione przez urządzenia sprzętowe klasy korporacyjnej przeznaczone do ochrony przed exploitami w warstwie sieciowej.

W czasach, gdy większość kadry pracuje zdalnie, ustanawianie i wdrażanie polityk naprawy luk jeszcze nigdy nie było tak istotne. **Sześć na 10 organizacji** ma komputery z niezałatanymi lukami sprzed 2018 r., co oznacza, że ryzyko wykorzystania tych podatności jest wyższe niż kiedykolwiek wcześniej. Spójna polityka wdrażania poprawek na komputerach wszystkich pracowników może znacząco zmniejszyć ryzyko naruszenia bezpieczeństwa danych wynikające z niezaktualizowanej aplikacji.

Cyberataki „na koronawirusa”

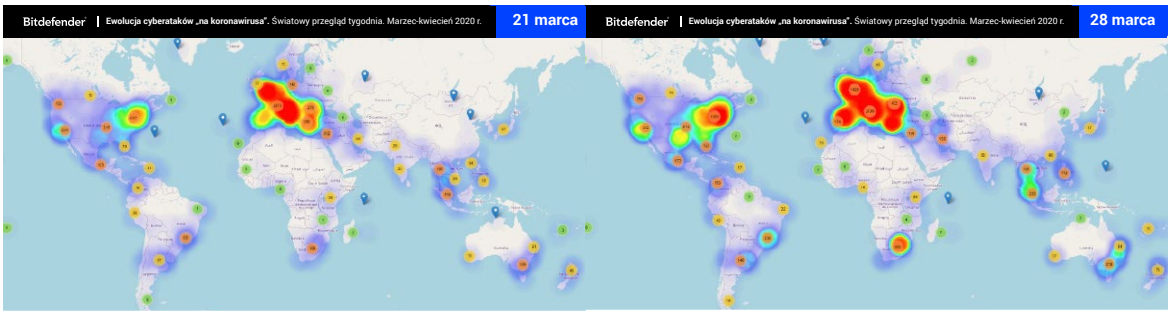
Tematyczny przegląd zagrożeń

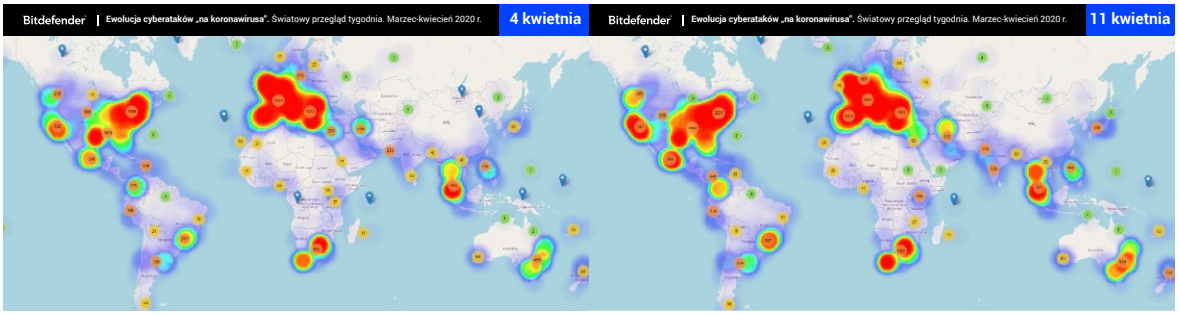
W ciągu 7 tygodni, począwszy od 7 marca, dane telemetryczne Bitdefender dotyczące cyberataków „na koronawirusa” pokazują, że atakujący obrali za cel kraje, w których koronawirus przerodził się w lokalną pandemię. Kraje takie jak Hiszpania, Wielka Brytania, Włochy i Niemcy były szczególnie dotknięte zarówno zagrożeniem biologicznym, jak i wykorzystującym jego kontekst złośliwym oprogramowaniem.

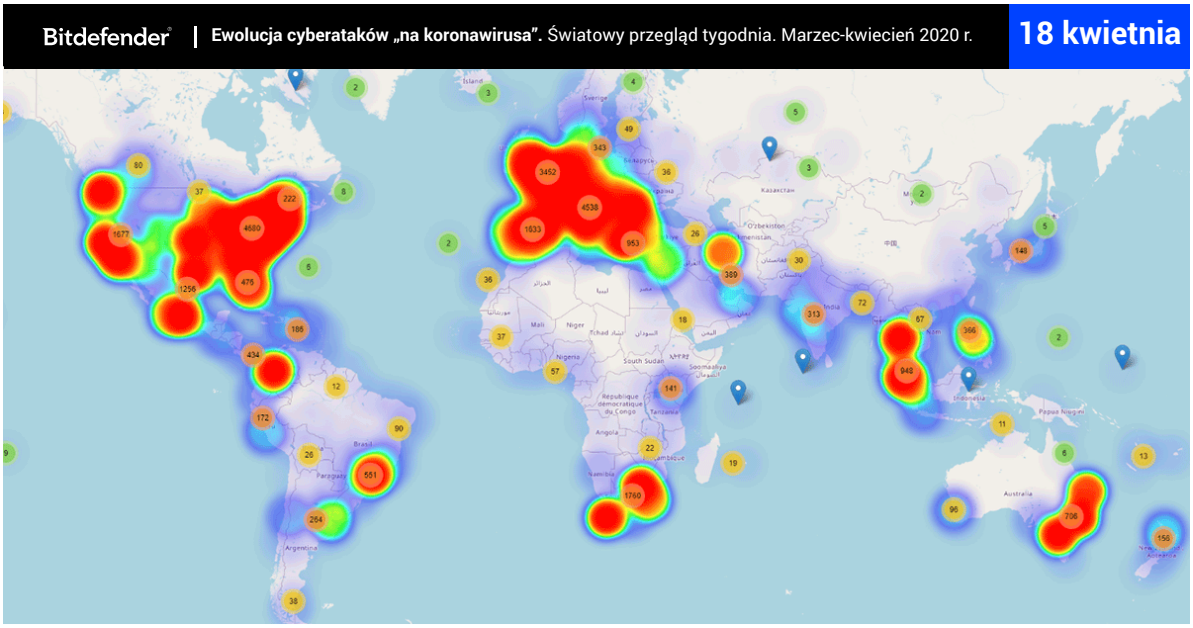


19 CVE-2019-11746, National Institute of Standards and Technology (NIST), https://nvd.nist.gov/vuln/detail/CVE-2019-11746

20 CVE-2019-0541, National Institute of Standards and Technology (NIST), https://nvd.nist.gov/vuln/detail/CVE-2019-0541







Wygląda na to, że pandemia koronawirusa była katalizatorem nasilenia aktywności atakujących i szybkiego tworzenia oportunistycznych kampanii z użyciem spamu, oszustw i malware'u, obliczonych na zmylenie ofiar w celu włamania do ich systemów. Z powyższych map cieplnych wynika, że hakerzy nieustannie śledzili lokalne wiadomości i raporty dotyczące rozwoju pandemii w poszczególnych krajach, dostosowując swoje komunikaty w taki sposób, aby wykorzystać strach i panikę wywołane przez wybuch pandemii.

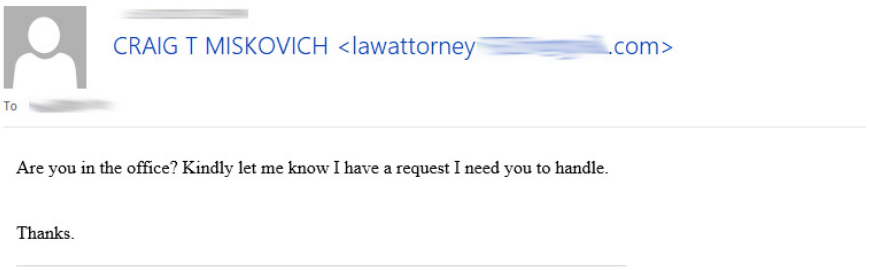
Tradycyjnie, większość spamu, phishingu i oszustw e-mailowych miała postać prostych wiadomości, których głównym celem było nakłonienie odbiorcy do otwarcia podejrzanego załącznika lub linku. Uległo to jednak zmianie, gdy wiadomości zaczęły być starannie konstruowane i formułowane tak, aby wydawały się wiarygodne, prawdziwe i istotne. Skupiając się bardziej na warstwie socjotechnicznej i budowaniu wiarygodności, zagrożenia i wiadomości wykorzystujące kontekst koronawirusa były wymierzone w firmy we wszystkich sektorach, żerując na ogólnym braku informacji wywołanym pandemią.

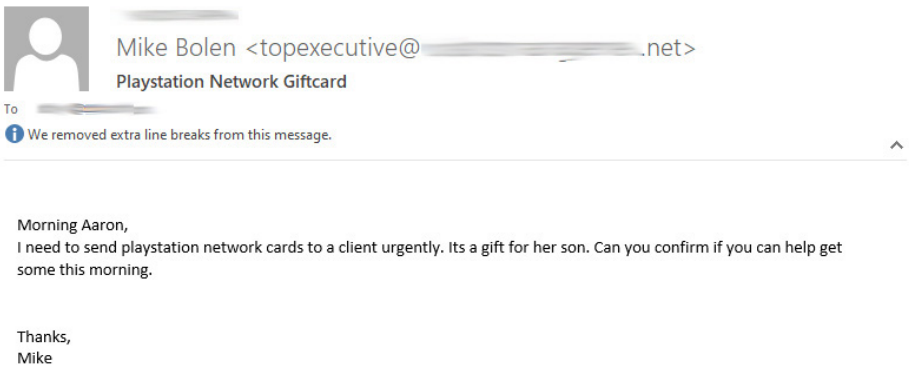
Phishing i spear-phishing

Prawdopodobnie jednym z największych wyzwań dla pracowników w kontekście pracy zdalnej jest uleganie atakom phishingowym i spear-phishingowym. Przed pandemią każdy podejrzany e-mail otrzymany od osoby podającej się za współpracownika byłby łatwo zweryfikowany przy biurku potencjalnego nadawcy. Praca zdalna pozbawiła pracowników fizycznej możliwości potwierdzenia pozornie autentycznych e-maili służbowych, potencjalnie narażając firmy na liczniejsze próby oszustw BEC (ang. Business Email Compromise) niż kiedykolwiek wcześniej.

Pandemia okazała się być silnym katalizatorem oportunistycznego spamu e-mailowego „na koronawirusa", który znacznie nasilił się w pierwszej połowie 2020 r. Telemetria Bitdefender pokazuje[21], że **cztery na 10 e-maili na temat koronawirusa identyfikowano jako spam, phishing lub malware**, co wskazuje, że pracownicy zdalni i przeciętni użytkownicy byli stale narażeni na ryzyko otwarcia szkodliwych e-maili. Zagrożone było bezpieczeństwo punktów końcowych i danych pracowników, podobnie jak infrastruktura korporacyjna, która mogła ucierpieć w wyniku złośliwej zawartości wiadomości e-mail lub adresów URL, co mogło doprowadzić do nasilenia się zagrożenia i podniesienia współczynnika ryzyka organizacji.

Cyberprzestępcy nie są nikim innym, jak tylko oportunistami, a oszustwa BEC zaczęły wykorzystywać ten sam żargon i podejście, które pracownicy biurowi stosowali od czasu wybuchu pandemii. Większość e-maili BEC jest krótka, osobista i zawsze sformułowana tak, aby odbiorca wykonał szybko działanie lub zrobił przysługę współpracownikowi.





21 "Mid-Year Threat Landscape Report 2020", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

Inne mają bardziej ogólny charakter i naśladują styl używany przez wewnętrzny zespół IT lub zautomatyzowane platformy wewnętrzne. Finalnym celem jest nakłonienie pracownika do odpowiedzi na e-mail i zaangażowania go w rozmowę w czasie rzeczywistym z atakującym lub po prostu narażenie punktu końcowego poprzez pobranie złośliwego oprogramowania lub podanie danych uwierzytelniających na stronach kontrolowanych przez atakujących.

W ciągu ostatnich kilku lat oszustwa BEC (ang. business e-mail compromise) ewoluowały[22] pod względem tematycznym od zestawień płac i podatków w 2016 r. do spraw kadrowych i kart podarunkowych w 2018 r. O ile w 2019 r. tematyka BEC oscylowała głównie wokół zmian w zakresie usług medycznych i płac, według HHS w 2020 r. tematem przewodnim wydaje się być COVID-19 i opieka zdrowotna.

Oszustwa BEC odgrywają niszową rolę w ogólnej skali phishingu, ale szacuje się, że wywołują największe szkody, a według FBI straty szacowane są średnio na prawie 75 000 USD[23] w przeliczeniu na skargę w 2019 r., a łącznie na 1,7 mld USD. Ponieważ w 2020 roku pandemia była zjawiskiem globalnym, prawdopodobnie straty finansowe BEC znacznie przekroczą te z 2019 r.

W szerszej perspektywie. Zmiany w zaawansowanych atakach.

Taktyka i techniki ataku

Komunikacja jest kluczem do omawiania ryzyka cybernetycznego i aż **55%[24] CIO i CISO uważa, że musi ona ulec radykalnej zmianie**, jeśli celem ma być zwiększenie inwestycji. Model taktyk i technik **MITRE ATT&CK** opracowany przez **MITRE** Corporation stał się standardem w dziedzinie bezpieczeństwa, do którego wszystkie organizacje mapują incydenty bezpieczeństwa. Ponieważ zawiera on wyczerpującą listę taktyk i technik powszechnie stosowanych w atakach, może pomóc w odwzorowywania incydentów bezpieczeństwa od źródła naruszenia, poprzez penetrację sieci, ustanowienie trwałego dostępu i eksfiltracji (kradzieży) danych.

Raporty dotyczące incydentów bezpieczeństwa oparte na tych ramach stały się nową normą, ponieważ pozwalają specjalistom z dziedziny bezpieczeństwa używać tego samego języka podczas opisywania incydentów. Jednakże, większość funkcji potrzebnych do odwzorowania wszystkich taktyk jest zazwyczaj dostępna w rozwiązaniach z zakresu wykrywania i reagowania w punktach końcowych **(EDR)**, dających zespołom śledczym i zespołom bezpieczeństwa pełny obraz zdarzeń przed i po włamaniu.

Znaczące pokrycie łańcucha ataków jest ostatecznym celem organizacji, ponieważ może pomóc w ustaleniu ich martwych punktów i sposobów ich eliminacji, a także we wzmocnieniu stanu zabezpieczeń dzięki lepszej widoczności całego łańcucha ataków umożliwiającej blokowanie ataków zanim osiągną swój ostateczny cel. Organizacje dążą do minimalizacji ryzyka, a ramy **MITRE** mogą w tym pomóc.

Scenariusze ataków - studium przypadku WMI

Nierzadko zdarza się, że do realizacji wrogich działań wykorzystywane są narzędzia i aplikacje będące częścią systemu operacyjnego. Przykładowo do najpopularniejszych narzędzi, którymi często posługują się atakujących należą PowerShell, a nawet Instrumentacja zarządzania Windows (Windows Management Instrumentation, WMI).

Jeśli mielibyśmy przeanalizować sam sposób, w jaki atakujący i malware posługują się WMI, zauważymy, że model MITRE ATT&CK® obejmuje wiele scenariuszy, w których WMI może być wykorzystane na każdym etapie cyklu życia cyberataku, począwszy od wykonania i uzyskania trwałego dostępu, aż po omijanie zabezpieczeń, rozpoznanie środowiska, penetrację sieci, zdalną kontrolę, a nawet kradzież danych.

22 "Business Email Compromise in the Health Sector", U.S. Department of Health and Human Services (HHS), https://www.hhs.gov/sites/default/files/business-email-compromise-in-the-health-sector.pdf

23 "2019 Internet Crime Report", Federal Bureau of Investigation (FBI), https://pdf.ic3.gov/2019_IC3Report.pdf

24 "Bitdefender 10 IN 10 Study: Seven in Ten CISOs Believe Cyberwarfare is an Imminent Threat to Their Organisations", Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/368/Bitdefender-10-in-10-Report.pdf

Jednym z najbardziej znanych przykładów, w których WMI odegrało kluczową rolę, był wykryty w 2010 r. **Stuxnet**. Jego celem były instalacje nuklearne w Natanz w Iranie, a WMI posłużył do zliczania użytkowników i rozprzestrzenienia się na dostępne udziały sieciowe.

Po odwzorowaniu **wykorzystania WMI przez Stuxnet według modelu MITRE** mamy co następuje:

Trwały dostęp *(Persistence)*:

- Technika T1084 – wywołanie subskrypcji zdarzeń Instrumentacji zarządzania Windows (*Windows Management Instrumentation Event Subscription)*

Rozpoznanie środowiska *(Discovery)*:

- Technika T1087 – rozpoznanie kont (*Account Discovery)*
- Technika T1135 – rozpoznanie udziałów sieciowych *(Network Share Discovery)*

Ruch boczny w sieci *(Lateral Movement)*

- Technika T1105 – zdalne kopiowanie plików *(Remote File Copy)*

Od tamtego czasu większość złośliwego oprogramowania i zagrożeń, niezależnie od stopnia ich złożoności, wykorzystuje możliwości WMI na różnych etapach łańcucha ataku.

Przykładowo **złośliwe oprogramowanie typu cryptominer o nazwie Kingminer** wykorzystuje mechanizm subskrypcji zdarzeń usługi WMI w fazie wykonania: jedna część złośliwego skryptu rejestruje aktywnego odbiorcę skryptu w celu cyklicznego wykonywania. Odbiorca zdarzeń usługi WMI umożliwia stałe działanie skryptu przy użyciu metody **T1546.003, wykonanie na podstawie zdarzenia: subskrypcja zdarzeń Instrumentacji zarządzania Windows** *(Event Triggered Execution: Windows Management Instrumentation Event Subscription).*

Oprogramowanie **ransomware Maze**[25] stało się jedną z najpopularniejszych rodzin ransomware, będąc następcą nieistniejącej już rodziny ransomware GandCrab. Autorzy Maze zaimplementowali mechanizm eksfiltracji, aby wyłudzić okup i wykorzystać błąd operacyjny w celu przechwycenia danych. Korzystając z WMI, Maze niszczy wszelkie kopie zapasowe systemu Windows, takie jak kopie w tle *(Volume Shadow Copy)*. **Poprzez zapytanie o klasę Win32_ShadowCopy WMI**, znajduje kopie w tle, które są usuwane w następnej fazie, znanej również jako **technika T1490, blokada przywracania systemu** (*Inhibit System Recovery*).

Emotet, znany również jako Geodo lub Mealybug, został po raz pierwszy wykryty w 2014 r. i od tego czasu jest nadal aktywny. Najczęstszym wektorem ataku Emotet są spear-phishingowe załączniki do wiadomości e-mail, znane również jako technika T1566.001, phishing: załącznik spear-phishingowy. Jednak pod względem taktyk i technik, nowe wersje często **wykorzystują usługę WMI, aby uniknąć wykrycia**. W tym celu stosują głównie **technikę T1202, pośrednie wykonywanie poleceń** (*Indirect Command Execution*), przy użyciu klasy WMI Win32_Process zamiast bezpośredniego wywołania PowerShell, co pozwala im czasem pozostać niewykrytymi.

Znając sposób działania usługi WMI oraz sposoby jej wykorzystania przez atakujących i malware, firmy mogą ustanowić i wdrożyć polityki używania WMI, które zmniejszą ryzyko nadużyć.

Chociaż istnieją inne przykłady złośliwego oprogramowania wykorzystującego WMI w całym cyklu życia ataku, model **MITRE** zapewnia wspólny język i terminologię używaną do opisania każdej fazy ataku i przyporządkowania jej do taktyki lub techniki. Choć w ciągu ostatniej dekady nastąpił znaczący rozwój złośliwego oprogramowania, atakujących i ogólnie pojętych zagrożeń, model **MITRE** może być doskonałym narzędziem analizy i interpretacji sposobu działania zagrożeń. A to z kolei może pomóc organizacjom wzmocnić poziom bezpieczeństwa.

25 "A Malware Researcher's Guide to Reversing Maze Ransomware", Bitdefender, https://labs.bitdefender.com/2020/03/a-malware-researchers-guide-to-reversing-maze/

Techniki i podtechniki MITRE ATT&CK® popularne w 2020 r.

Telemetria biznesowa Bitdefender wykazała, że wśród taktyk i technik ataku powszechnie używanych przez zaawansowanych hakerów jedną z najczęściej odnotowywanych taktyk stosowanych w celu uzyskania dostępu *(initial access)* jest phishing.

Jedna z taktyk wykorzystywanych najczęściej na etapie **wykonania** *(Execution)* jest określana jako **„Interpreter poleceń i skryptów"** *(Command and Scripting Interpreter, T1059)* w macierzy **MITRE ATT&CK®** Enterprise Matrix i stanowi 21,37% wszystkich taktyk odnotowanych przez telemetrię Bitdefender. Jedna z najpopularniejszych podtechnik (T1059.001) dla tej taktyki polega na wykorzystaniu komend i skryptów PowerShell i stanowi **42,52% wszystkich odnotowanych podtechnik T1059**. Taktyka ta jest popularna wśród hakerów, ponieważ PowerShell może być wykorzystywany do automatyzacji zadań i jest dostępny na komputerze ofiary. Ponadto wykonywanie poleceń i skryptów PowerShell nie wymaga uruchamiania pliku binarnego „powershell.exe", lecz jedynie użycia interfejsów służących do obsługi jego podstawowych komponentów, dostępnych za pośrednictwem interfejsu wiersza poleceń (CLI) systemu Windows.

Jedną z najczęściej odnotowywanych technik uzyskania **trwałego dostępu** *(Persistence)* jest **T1546 - wykonanie inicjowane zdarzeniem** *(Event Triggered Execution)*, do której zmapowany jest szereg zdarzeń systemowych mogących wskazywać na zewnętrzną próbę ingerowania w rejestr systemowy lub w działania umożliwiające hakerom uzyskanie trwałego dostępu do komputera. Najczęściej wychwytywanym przez telemetrię biznesową Bitdefender przykładem podtechniki wykonania inicjowanego zdarzeniem jest T1546.001 - zmiana domyślnego skojarzenia plików *(Change Default File Association)*, która stanowi **31,54% wszystkich raportowanych podtechnik T1546**. Atakujący chętnie korzystają z tej techniki, ponieważ umożliwia ona zmianę skojarzeń plików w rejestrze, a następnie wykonanie poleceń ustawionych jako klucze podrzędne względem tych kluczy powłoki. Zmiana domyślnego programu może umożliwić hakerom wykorzystanie systemu do wykonywania poleceń lub otwierania spreparowanych dokumentów.

W ramach łańcucha ataków hakerzy stosują również techniki **eskalacji uprawnień** *(Privilege Escalation)* w celu uzyskania wyższego poziomu uprawnień na komputerze lub w infrastrukturze ofiary, a jedną z odnotowywanych technik tego typu jest T1134 - manipulacja tokenem dostępu *(Access Token Manipulation)*. Natomiast jedną z najczęściej raportowanych podtechnik jest **T1134.002 - tworzenie procesu za pomocą tokena** *(Create Process with Token)*. Atakujący duplikują token dostępu użytkownika – zwykle takiego, który posiada uprawnienia administratora – i używają go do utworzenia nowego procesu uruchamianego w kontekście zhakowanego użytkownika. Tę technikę ataku można łatwo wyeliminować ograniczając uprawnienia użytkownikom i grupom użytkowników, aby uniemożliwić tworzenie tokenów dostępu, a także poprzez zbadanie aktywności wiersza poleceń obejmującej podnoszenie uprawnień.

Z kolei spośród technik **omijania zabezpieczeń** najczęściej wykorzystywaną techniką jest T1562 – naruszenie obrony (*Impair Defenses)*, jak pokazują dane telemetryczne Bitdefender. Podtechniką szczególnie popularną wśród atakujących jest **T1562.006 - blokowanie sygnalizowania zdarzeń** *(Indicator Blocking*), polegająca na wyłączaniu sensorów bezpieczeństwa odpowiadających za zbieranie i analizowanie danych.

Pozyskanie danych logowania *(Credential Access)* jest również dość popularną techniką, jako że atakujący często próbują uzyskać dane uwierzytelniające przechowywane w niezabezpieczony sposób. Natomiast jedną z najczęściej raportowanych podtechnik jest **T1552.002 - poświadczenia w rejestrze** *(Credentials in Registry)* **stanowiąca 20,27% przypadków raportowanych w ramach T1552 - niezabezpieczone poświadczenia** *(Unsecured Credentials)*. To pokazuje, że hakerzy przeszukują klucze rejestru przy użyciu narzędzi do zrzucania poświadczeń *(ang. credential dumpers)* lub przeszukują klucze rejestru odnoszące się do popularnych klientów SSH i Telnet w celu znalezienia niezabezpieczonych poświadczeń, które mogą wykorzystać. Niektóre grupy APT znane są z wykorzystywania tego mechanizmu, jak również różnych trojanów takich, jak TrickBot.

Etap łańcucha ataku związany z **rozpoznaniem środowiska** *(Discovery)* jest również istotny w procesie rekonesansu, ponieważ pozwala na identyfikację potencjalnych celów o wysokiej wartości, takich jak konta administratorów. Jedną z technik rozpoznawczych odnotowanych przez telemetrię biznesową Bitdefender jest technika T1087 - rozpoznanie kont *(Account Discovery)*. Jednak najczęściej raportowaną podtechniką, wskazywaną w **66,58% przypadków, jest T1087.002 - konto domeny** *(Domain Account)*. Pokazuje to, że atakujący najczęściej chcą uzyskać listę kont użytkowników danej domeny, prawdopodobnie w celu ustalenia, którzy z nich mają prawa administratora. Prostym rozwiązaniem tego problemu jest wprowadzenie polityki, która uniemożliwiłaby pobranie listy kont administratorów.

Inną kwestią mogącą budzić obawy są techniki **ruchu bocznego** *(Lateral Movement)*, gdyż atakujący często próbują badać sieć w poszukiwaniu innych wartościowych celów używając usług SSH lub VNC. Natomiast, w ramach techniki **T1021 - usługi zdalne** *(Remote Services)*, najczęściej raportowaną techniką jest **T1021.002 - udziały administratora SMB/Windows** *(SMB/Windows Admin Shares)*, co sugeruje, że atakujący mogą próbować wchodzić w interakcje ze zdalnymi udziałami sieciowymi przy użyciu *Server Message Block* (SMB). Udziały SMB mogą być bardzo cenne dla zaawansowanych hakerów, gdyż mogą być wykorzystywane do przechowywania plików i ich kradzieży.

Pod względem **technik zdalnej kontroli** *(Command and Control)*, T1071 - protokół warstwy aplikacji *(Application Layer Protocol)* był najczęściej raportowany przez telemetrię biznesową Bitdefender, przy czym najbardziej popularne były dwie podtechniki: **T1071.002 - protokoły transferu plików** *(File Transfer Protocols)* i **T1071.003 - protokoły poczty e-mail** *(Mail Protocols)*. To oznacza, że hakerzy nieustannie komunikują się z infrastrukturą zdalnej kontroli poprzez protokoły transferu plików takie jak FTP, FTPS i TFPT lub poprzez protokoły poczty e-mail takie jak SMTP/S, POP3/S i IMAP. Protokoły te są bardzo rozpowszechnione w organizacjach i zwykle są pomijane przez rozwiązania zabezpieczające opracowane z myślą o wykrywaniu podejrzanych protokołów komunikacyjnych.

Na etapie wpływu *(Impact)*, będącym ostatnim elementem łańcucha ataku, jedną z najczęściej odnotowywanych technik jest T1565 - manipulacja danymi *(Data Manipulation)*. Natomiast podtechnika **T1565.003 - manipulacja danymi podczas uruchamiania programu** *(Runtime Data Manipulation)* **stanowi 72,91%** ogółu raportowanych podtechnik manipulacji danymi. Oznacza to, że atakujący często usiłują manipulować danymi w celu dokonania zmian podczas uruchamiania lub modyfikacji danych wyjściowych konkretnej aplikacji.

Wzrost popularności APT jako usługi

W pierwszej połowie 2020 r. badacze Bitdefender przeanalizowali serię ataków APT, które rzuciły nowe światło na to, jak ewoluowały grupy APT. Zazwyczaj grupy APT były albo sponsorowane przez niektóre państwa, albo nastawione głównie na zysk, ukierunkowując swoje działania zwykle na instytucje państwowe w oparciu o agendę polityczną lub też na instytucje finansowe.

Śledztwo przeprowadzone na początku 2020 r. ujawniło atak irańskiej grupy APT znanej jako Chafer[26] wymierzony w transport lotniczy oraz instytucje państwowe w Kuwejcie i Arabii Saudyjskiej. Niektóre z taktyk i technik ataku stosowanych przez tę grupę nie są rzadkością w przypadku APT: począwszy od wykorzystywania spear-phishingu jako początkowego wektora ataku, poprzez tworzenie własnych kont użytkowników w celu zapewnienia trwałej obecności, a nawet ruchu bocznego przy użyciu niestandardowych narzędzi. Szczególnie interesującym aspektem grupy APT Chafer jest to, że oba ataki prawdopodobnie skupiały się na kradzieży danych, a aktywność napastników miała miejsce w weekendy.

Późniejsze dochodzenie w sprawie innej grupy APT zwanej BitterAPT[27] również wykazało, że grupa ta ma pewne powiązania polityczne. Biorąc pod uwagę regiony docelowe i profile ofiar ujawnione w przeszłości przez badaczy bezpieczeństwa, BitterAPT był znany z tego, że atakował cele w Pakistanie, Chinach, Indiach i innych krajach Azji Południowej, a także Arabii Saudyjskiej. Badanie Bitdefender wykryło nieznane wcześniej aplikacje na Androida, które prawdopodobnie były wymierzone w grupy religijne, imitując aplikacje pokrewne do True Islam lub Saima Eid, jak również warianty ogólne, naśladujące aplikacje takie, jak poczta głosowa, czat, przeglądarki obrazów i aktywatory WhatsApp.

Ciekawostką jest, że dowody pozostawione przez znaczniki czasu (od poniedziałku do piątku między 9 rano a 5 po południu) w analizowanych próbkach sugerują, że grupa ta jest również sponsorowana przez państwo. Te same znaczniki czasu wskazują na to, że grupa ma siedzibę w kraju południowoazjatyckim.

Zagłębiając się w ich poprzednie operacje, wydaje się, że zarówno kampanie z 2014, jak i 2019 r. korzystały z aplikacji imitujących lokalne agregatory wiadomości dla Kaszmiru. Biorąc pod uwagę, że zarówno 2014, jak i 2019 r. były latami wyborczymi w tym regionie, istnieje duże prawdopodobieństwo, że BitterAPT może być sponsorowany przez państwo.

26 "Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia", Bitdefender, https://labs.bitdefender.com/2020/05/iranian-chafer-apt-targeted-air-transportation-and-government-in-kuwait-and-saudi-arabia

27 "BitterAPT Revisited: the Untold Evolution of an Android Espionage Tool", Bitdefender, https://labs.bitdefender.com/2020/06/bitterapt-revisited-the-untold-evolution-of-an-android-espionage-tool/

Być może jednym z najbardziej interesujących wydarzeń w zachowaniu grup APT było zbadanie przez badaczy Bitdefender grupy APT o nazwie StrongPity[28], atakującej cele w Turcji i Syrii, wykorzystującej taktykę „watering hole" do selektywnego infekowania celów. Podczas gdy grupa była znana z działań ukierunkowanych na cele w Belgii i Włoszech, ten konkretny atak skupiony na społeczności kurdyjskiej w Turcji i Syrii wydaje się zbiegać w czasie z turecką operacją wojskową. 1 października 2019 r. był datą zarówno rozpoczęcia operacji wojskowej, jak i znacznikiem czasu na próbkach APT StrongPity.

Zaawansowane taktyki, narzędzia i infrastruktura wykorzystywane przez grupę APT StrongPity wskazują, że dysponuje ona zarówno umiejętnościami jak i potencjalnie jest finansowana przez państwo. Jednak od 2016 r., kiedy to po raz pierwszy pojawiły się informacje o istnieniu tej grupy, była ona nieuchwytna.

W jednym z ostatnich dochodzeń prowadzonych przez badaczy Bitdefender zdołaliśmy przyjrzeć się z bliska procesowi ewolucji grup APT. Podczas gdy tradycyjne złośliwe oprogramowanie ewoluowało w kierunku usługi oferowanej w modelu biznesowym, za którym prawdopodobnie wkrótce podąży ransomware, grupy APT najwyraźniej uległy tej samej zmianie.

Atak cyberszpiegowski wymierzony w międzynarodową firmę architektoniczną i zajmującą się produkcją wideo pokazał, że działania grup APT mogą nie być już motywowane politycznie. Zamiast tego mogą one oferować swoje usługi temu, kto da więcej. Jednym z głównych ustaleń śledztwa było to, że początkowym wektorem ataku na firmę architektoniczną była luka zero-day w popularnym oprogramowaniu do grafiki komputerowej 3D (Autodesk 3ds Max) używanym w firmie.

Wspomniana firma architektoniczna jest znana z tego, że współpracowała przy wartych miliardy dolarów projektach nieruchomości w Nowym Jorku, Londynie, Australii i Omanie. Na podstawie taktyk i technik zastosowanych przez grupę APT w celu ataku, można przypuszczać, że potencjalnie była to grupa APT do wynajęcia zajmująca się cyberszpiegostwem przemysłowym.

Szpiegostwo przemysłowe nie jest niczym nowym i ponieważ w branży nieruchomości panuje duża konkurencja, a kontrakty są wyceniane na miliardy dolarów, stawka w przypadku wygrywania kontraktów na luksusowe projekty jest wysoka. Zdaniem niektórych może to być powodem zwracania się do najemnych grup APT w celu uzyskania przewagi negocjacyjnej.

Zagrożenia sieciowe

Infrastrukturę biznesową stanowią zarówno aplikacje, jak i sieci. Podczas gdy niezałatane luki w aplikacjach i systemach operacyjnych mogą narazić komputery na kontakt z szerokim spektrum złośliwego oprogramowania i cyberprzestępców, zagrożenia sieciowe mogą umożliwić atakującym sondowanie i mapowanie infrastruktury firmy oraz przechwycenie istotnych danych.

Przykładowo w ciągu ostatnich kilku lat hakerzy wykorzystujący ransomware przestawili się z chaotycznego podejścia do dokonywania ataków, czyli stosowania tradycyjnych wektorów, takich jak spear-phishing, na podejście bardziej ukierunkowane. Nadużywanie protokołu zdalnego pulpitu, wykorzystywanie niezałatanych luk w protokole SMB, a nawet łamanie haseł za pomocą metody brute-force podczas sesji FTP lub RDP to najczęstsze taktyki ataków na środowiska biznesowe.

Technologia Bitdefender obrony przed atakami sieciowymi wykryła, że 46,84% wszystkich ataków sieciowych polega na wykorzystaniu luki w protokole SMB. Spośród nich, implant backdoora DoublePulsar[29] stanowi 90,74% wykorzystywanych exploitów SMB. Chociaż może to sugerować, że niektóre organizacje są nadal podatne na ten exploit, jest również prawdopodobne, że DoubelPulsar stał się narzędziem wykorzystywanym przez cyberprzestępców, którzy szukają luk w infrastrukturze.

Struktura ataków sieciowych	
Exploity SMB	46,84%
Ataki typu brute force (FTP, RDP)	41,63%
Inne	11,53%

28 "StrongPity APT – Revealing Trojanized Tools, Working Hours and Infrastructure", Bitdefender, https://labs.bitdefender.com/2020/06/strongpity-apt-revealing-trojanized-tools-working-hours-and-infrastructure/

29 DoublePulsar, Wikipedia, https://en.wikipedia.org/wiki/DoublePulsar

Luki w SMB, takie jak EternalBlue[30], EternalDarkness, EternalChampion, a nawet EternalRomance należą do najpopularniejszych exploitów SMB wykorzystywanych w atakach na sieci firmowe. Jest jednak prawdopodobne, że są one łączone w pakiety z różnymi narzędziami ataku sieciowego i używane kaskadowo do momentu, gdy jednemu z nich uda się wedrzeć do nieuaktualnionego systemu.

Ta sama telemetria ujawniła również, że **ataki typu brute force na usługi RDP i FTP stanowią 41,63% wszystkich ataków sieciowych w infrastrukturze biznesowej**. Skuteczne uzyskanie dostępu do tych usług oznacza, że atakujący mogą przejąć zdalnie kontrolę nad komputerami i punktami końcowymi przedsiębiorstwa, a nawet uzyskać dostęp do wewnętrznych udziałów FTP, gdzie zwykle są przechowywane poufne dane. Jeśli jednak przyjrzymy się aktualnemu krajobrazowi zagrożeń biznesowych, wiele ataków na wspomniane usługi polega na tym, że hakerzy wykorzystujący ransomware starają się zdobyć przyczółek w organizacji wyszukują cenne dane, a następnie przy użyciu niestandardowego pliku ręcznie uruchamiają ransomware z żądaniem wysokiego okupu.

Konsekwencje - nowe zagrożenie dla MŚP

Grupy APT do wynajęcia mogą zmienić sposób, w jaki małe i średnie firmy tworzą swoje modele zagrożeń. Jedną z największych obaw wśród osób decyzyjnych w obszarze IT i bezpieczeństwa jest to, że ich firma może stać się celem ataków grup APT. O ile w przeszłości większość ataków APT na małe i średnie przedsiębiorstwa była częścią ataków na łańcuch dostaw, działalność najemnych grup APT oferujących usługi temu, kto da więcej, może oznaczać, że ataki na małe i średnie przedsiębiorstwa będą coraz częstsze.

Małe i średnie firmy zwykle polegały tylko na modelach ryzyka, które dotyczyły aktualnego krajobrazu zagrożeń lub ewentualnie ryzyka związanego z pracownikami, ale najemnicy APT całkowicie zmieniają założenia polityki bezpieczeństwa takich firm. Modele zagrożeń uwzględniające hakerów finansowanych przez państwo, jak i tych o zaawansowanych umiejętnościach, dotyczyły głównie dużych firm i infrastruktury rządowej. Upowszechnienie się najemnych grup hakerskich APT oznacza, że każda firma niezależnie od jej wielkości lub branży może być narażona na złożone ataki o charakterze szpiegostwa przemysłowego finansowane przez niektóre państwa.

Małe i średnie firmy powinny skupić się na rozszerzeniu swojego arsenału zabezpieczeń nie tylko o oprogramowanie wykrywające malware, lecz także o narzędzia zwiększające widoczność zagrożeń zarówno w warstwie punktów końcowych, jak i sieci. Przykładowo zautomatyzowane narzędzia do wykrywania i reagowania w punktach końcowych wychwytujące taktyki lub techniki powszechnie stosowane przez grupy APT umożliwiają łatwe znalezienie potencjalnego intruza. Ponadto brak wykwalifikowanej kadry bezpieczeństwa IT może być zrekompensowany poprzez skorzystanie z usług zarządzanych zespołów wykrywania i reagowania, które analizują infrastrukturę firmy i proponują narzędzia zabezpieczające i wzmacniające ochronę, a także pełnią rolę wyspecjalizowanych zespołów łowców zagrożeń, które tropią podejrzane zdarzenia. Zarówno EDR jak i MDR stały się dostępne dla małych i średnich firm, oferując za ułamek kosztów ochronę zbliżoną do SOC, na którą zazwyczaj mogły sobie pozwolić tylko duże organizacje.

Regionalna ewolucja tradycyjnych zagrożeń

Podczas gdy krajobraz zagrożeń biznesowych stale się zmienia, a organizacje regularnie inwestują w technologie bezpieczeństwa i budują nowe strategie wykrywania i ograniczania ryzyka, zagrożenia czyhające na ich infrastrukturę nigdy nie ustają.

Dane telemetryczne firmy Bitdefender dotyczące tradycyjnych zagrożeń takich, jak ransomware, oprogramowanie kopiące kryptowaluty, zagrożenia bezplikowe, a nawet potencjalnie niechciane aplikacje (PUA) pokazały, że nadal zagrażają one organizacjom.

Mimo że rynek ransomware dzieli się na szeroką gamę rodzin tegoż oprogramowania, z których każda jest oferowana jako usługa przez posługujących się nim hakerów, liczba skarg[31] zarejestrowanych przez FBI w 2019 r. osiągnęła poziom 2047 i szacunkową wartość strat w wysokości 8,9 mln USD. Jednak dotyczy to tylko firm, które faktycznie zgłosiły incydent ransomware do władz w Stanach Zjednoczonych. W rzeczywistości ransomware od dawna stanowi lukratywny biznes generujący miliardowe zyski w formie okupu płaconego cyberprzestępcom.

30 EternalBlue, Wikipedia, https://en.wikipedia.org/wiki/EternalBlue

31 "2019 Internet Crime Report", Federal Bureau of Investigation (FBI), https://pdf.ic3.gov/2019_IC3Report.pdf

Jednym z najnowszych trendów w dziedzinie ransomware jest dodanie komponentu wymuszania okupu. Po przejęciu kontroli nad organizacją operatorzy ransomware często odnajdują i wyprowadzają poufne dane z firmy zanim uruchomią ransomware. Tym sposobem jeśli firma odmówi poddania się żądaniom okupu, operatorzy ransomware mogą zagrozić opublikowaniem skradzionych danych, zmuszając firmę do poniesienia kary z tytułu naruszenia przepisów RODO, która potencjalnie może przewyższyć wysokość żądanego okupu. Nigdy nie zaleca się ulegania żądaniom okupu, gdyż działa to jak zachęta i pożywka dla operatorów ransomware, a incydent radzi się traktować jako awarię sprzętu.

Patrząc na globalną ewolucję odnotowanych przypadków ransomware na podstawie naszej telemetrii biznesowej, można śmiało powiedzieć, że to zagrożenie nie zniknie. W mediach pojawiło się wystarczająco dużo doniesień o przestojach spowodowanych potencjalnymi incydentami ransomware, które dotyczyły wszystkich - od szpitali po instytucje rządowe. Chociaż wygląda na to, że liczba przypadków ransomware zgłaszanych na całym świecie zmniejsza się od kwietnia 2020 r., sytuacja związana z pracą z domu prawdopodobnie stworzyła nowe możliwości dla cyberprzestępców w zakresie wymuszeń i potencjalnego wyprowadzania danych.

I półrocze 2020 r.	Ransomware
Sty	19,50%
Lut	19,33%
Mar	17,85%
Kwi	14,02%
Maj	15,01%
Cze	14,29%

Światowe raporty generowane przez naszą telemetrię biznesową dotyczące złośliwego oprogramowania typu coin miner wskazują, że kopanie kryptowalut nadal jest przedmiotem zainteresowania cyberprzestępców. Zagrożenie to jest nadal obecne w środowiskach biznesowych, gdzie wykorzystuje moc obliczeniową chmury organizacji po skutecznym ataku na jej systemy lub infekuje różne aplikacje w celu uruchomienia oprogramowania typu coin miner. Chociaż większość przypadków tego rodzaju zagrożeń odnotowano w I kwartale 2020 r., to w IV kwartale poziom wykrytych infekcji stanowił 38,91% ogółu wykryć z I półrocza 2020 r.

I półrocze 2020 r.	Coin miner
Sty	20,63%
Lut	21,77%
Mar	19,10%
Kwi	12,94%
Maj	12,94%
Cze	13,03%

Globalne raporty z naszej telemetrii biznesowej dotyczące zagrożeń bezplikowych wykazały również, że cyberprzestępcy nadal wykorzystują dostępne narzędzia do żerowania na atakowanych środowiskach biznesowych. Niezależnie od tego, czy chodzi o podstępne nakłanianie pracowników do uruchamiania spreparowanych załączników, czy o wykorzystywanie niezałatanych luk w zabezpieczeniach do uruchamiania ataku bezplikowego, przedsiębiorstwa stale potrzebują technologii i polityk opracowanych w celu wykrywania i blokowania tych zagrożeń.

I półrocze 2020 r.	Ataki bezplikowe
Sty	25,25%
Lut	24,26%
Mar	16,83%
Kwi	10,89%
Maj	8,42%
Cze	14,36%

Potencjalnie niechciane aplikacje (PUA) mogą się pojawiać w środowiskach biznesowych, jeśli polityka bezpieczeństwa IT bywa zbyt liberalna wobec pracowników, umożliwiając im instalowanie i używanie oprogramowania bez nadzoru zespołów IT i bezpieczeństwa. Chociaż PUA nie są tak niebezpieczne jak złośliwe oprogramowanie, mogą one instalować dodatkowe komponenty, umożliwiać implantowanie backdoorów lub mogą zwyczajnie utrudniać pracę wyświetlając reklamy i wyskakujące okienka oraz czynić korzystanie z aplikacji uciążliwym. Co ciekawe, nasza telemetria biznesowa wskazuje, że spośród PUA raportowanych w I półroczu 2020 r. szczyt wystąpił tylko w marcu (18,22% ogółu PUA odnotowanych w I półroczu 2020 r.), a na przestrzeni roku zaobserwowano względnie stały poziom wykryć.

I półrocze 2020 r.	PUA
Sty	15,72%
Lut	16,74%
Mar	18,22%
Kwi	15,74%
Maj	16,87%
Cze	16,72%

Stany Zjednoczone

I półrocze 2020 r.	Ransomware
Sty	20,34%
Lut	16,96%
Mar	17,26%
Kwi	15,19%
Maj	16,36%
Cze	13,89%

I półrocze 2020 r.	Coin Miner
Sty	15,98%
Lut	17,96%
Mar	20,13%
Kwi	15,81%
Maj	15,81%
Cze	14,31%

I półrocze 2020 r.	Ataki bezplikowe
Sty	33,33%
Lut	11,11%
Mar	11,11%
Kwi	33,33%
Maj	0,00%
Cze	11,11%

I półrocze 2020 r.	PUA
Sty	15,69%
Lut	15,84%
Mar	17,17%
Kwi	16,41%
Maj	17,78%
Cze	17,11%

Wielka Brytania

I półrocze 2020 r.	Ransomware
Sty	16,64%
Lut	17,96%
Mar	18,26%
Kwi	18,50%
Maj	14,23%
Cze	14,41%

I półrocze 2020 r.	Coin Miner
Sty	18,18%
Lut	24,56%
Mar	18,32%
Kwi	13,36%
Maj	13,36%
Cze	12,08%

I półrocze 2020 r.	PUA
Sty	15,58%
Lut	16,10%
Mar	17,85%
Kwi	16,38%
Maj	17,07%
Cze	17,01%

Szwecja

I półrocze 2020 r.	Ransomware
Sty	20,55%
Lut	17,81%
Mar	23,29%
Kwi	20,55%
Maj	9,59%
Cze	8,22%

I półrocze 2020 r.	Coin Miner
Sty	18,75%
Lut	25,00%
Mar	21,05%
Kwi	12,50%
Maj	12,50%
Cze	8,55%

I półrocze 2020 r.	PUA
Sty	15,27%
Lut	15,63%
Mar	16,72%
Kwi	18,54%
Maj	17,85%
Cze	15,99%

Rumunia

I półrocze 2020 r.	Ransomware
Sty	14,66%
Lut	13,91%
Mar	11,52%
Kwi	12,12%
Maj	24,23%
Cze	23,56%

I półrocze 2020 r.	Coin Miner
Sty	22,88%
Lut	22,39%
Mar	18,65%
Kwi	14,09%
Maj	14,09%
Cze	10,71%

I półrocze 2020 r.	PUA
Sty	13,07%
Lut	14,17%
Mar	18,44%
Kwi	16,05%
Maj	19,15%
Cze	19,12%

Włochy

I półrocze 2020 r.	Ransomware
Sty	19,01%
Lut	17,27%
Mar	17,55%
Kwi	15,32%
Maj	15,81%
Cze	15,04%

I półrocze 2020 r.	Coin Miner
Sty	16,41%
Lut	26,79%
Mar	16,67%
Kwi	13,08%
Maj	13,46%
Cze	13,59%

I półrocze 2020 r.	PUA
Sty	16,14%
Lut	15,80%
Mar	17,91%
Kwi	15,79%
Maj	17,80%
Cze	16,55%

Francja

I półrocze 2020 r.	Ransomware
Sty	19,48%
Lut	19,85%
Mar	19,73%
Kwi	12,45%
Maj	14,55%
Cze	13,93%

I półrocze 2020 r.	Coin Miner
Sty	21,15%
Lut	22,94%
Mar	21,23%
Kwi	15,11%
Maj	10,98%
Cze	8,60%

I półrocze 2020 r.	PUA
Sty	15,38%
Lut	15,78%
Mar	18,73%
Kwi	16,31%
Maj	17,16%
Cze	16,63%

Hiszpania

I półrocze 2020 r.	Ransomware
Sty	20,56%
Lut	16,70%
Mar	14,59%
Kwi	13,36%
Maj	18,80%
Cze	15,99%

I półrocze 2020 r.	Coin Miner
Sty	16,80%
Lut	28,74%
Mar	17,99%
Kwi	11,78%
Maj	11,39%
Cze	13,30%

I półrocze 2020 r.	PUA
Sty	17,77%
Lut	17,80%
Mar	18,13%
Kwi	14,71%
Maj	15,57%
Cze	16,03%

Dania

I półrocze 2020 r.	Ransomware
Sty	23,66%
Lut	14,52%
Mar	19,35%
Kwi	16,67%
Maj	15,05%
Cze	10,75%

I półrocze 2020 r.	Coin Miner
Sty	15,53%
Lut	26,89%
Mar	17,05%
Kwi	12,88%
Maj	14,77%
Cze	12,88%

I półrocze 2020 r.	PUA
Sty	16,04%
Lut	15,00%
Mar	17,06%
Kwi	16,42%
Maj	18,11%
Cze	17,38%

Niemcy

I półrocze 2020 r.	Ransomware
Sty	23,01%
Lut	18,25%
Mar	21,12%
Kwi	14,20%
Maj	12,97%
Cze	10,46%

I półrocze 2020 r.	Coin Miner
Sty	21,07%
Lut	20,05%
Mar	19,04%
Kwi	15,48%
Maj	12,06%
Cze	12,31%

I półrocze 2020 r.	PUA
Sty	14,89%
Lut	15,57%
Mar	18,58%
Kwi	17,01%
Maj	17,50%
Cze	16,46%

Australia

I półrocze 2020 r.	Ransomware
Sty	9,51%
Lut	14,17%
Mar	18,41%
Kwi	15,90%
Maj	22,47%
Cze	19,53%

I półrocze 2020 r.	Coin Miner
Sty	13,96%
Lut	23,72%
Mar	18,39%
Kwi	15,32%
Maj	14,64%
Cze	13,96%

I półrocze 2020 r.	PUA
Sty	11,31%
Lut	15,25%
Mar	19,22%
Kwi	18,51%
Maj	18,35%
Cze	17,36%

Niderlandy

I półrocze 2020 r.	Ransomware
Sty	17,52%
Lut	17,08%
Mar	16,35%
Kwi	17,37%
Maj	14,60%
Cze	17,08%

I półrocze 2020 r.	Coin Miner
Sty	19,71%
Lut	23,22%
Mar	17,44%
Kwi	13,93%
Maj	13,48%
Cze	12,23%

I półrocze 2020 r.	PUA
Sty	14,59%
Lut	15,45%
Mar	18,87%
Kwi	17,55%
Maj	17,82%
Cze	15,73%

Wnioski

Krajobraz zagrożeń biznesowych rozwinął się do tego stopnia, że wszystkie organizacje niezależnie od wielkości czy branży stają w obliczu tych samych zagrożeń. Obecna globalna pandemia stała się katalizatorem dla nowej fali ataków BEC (Business Email Compromise), zmuszając firmy do uaktualnienia stosowanych przez nie programów szkoleń i podnoszenia świadomości.

Z punktu widzenia firm nową normalnością jest praca zdalna, co oznacza, że zakres oddziaływania hakerów rozszerzył się na infrastrukturę i usługi internetowe, które do niedawna były chronione, a także na punkty końcowe firmy znajdujące się z dala od sieci firmowej. Luki, błędne konfiguracje i ogólny niedobór umiejętności w zakresie cyberbezpieczeństwa oznaczają dla firm nowe wyzwania i ryzyko, których większość z nich jeszcze kilkanaście miesięcy temu nie brała pod uwagę.

Działalność najemnych grup APT zmusiła małe i średnie przedsiębiorstwa do zmiany podejścia do kwestii bezpieczeństwa i uwzględnienia nowego zagrożenia w ich modelach ryzyka. Zaniechanie tych zmian, jak również brak odpowiedniego zabezpieczenia infrastruktury mogłyby narazić firmy na straty lub jeszcze poważniejsze konsekwencje. Usługi zarządzanego wykrywania i reagowania (MDR) oraz technologie wykrywania i reagowania w punktach końcowych (EDR) mogą pomóc organizacjom sprostać nowym wyzwaniom i stawić czoła nowym zagrożeniom bez obciążania budżetu przeznaczonego na bezpieczeństwo IT.

Po tym, jak pierwsza połowa 2020 r. upłynęła pod znakiem szybkich zmian w zakresie infrastruktury biznesowej, przesunięć kadrowych i nowych zagrożeń, większość firm stanęła przed jednym z największych wyzwań, jakie kiedykolwiek napotkała na swojej drodze.

Dlaczego Bitdefender

Z dumą służymy naszym klientom

Bitdefender dostarcza rozwiązań i usług dla małych i średnich przedsiębiorstw, dostawców usług i integratorów technologii. Jesteśmy dumni z zaufania, jakim obdarzyły nas takie przedsiębiorstwa jak **Mentor, Honeywell, Yamaha, Speedway, Esurance oraz Safe Systems**.

Lider według raportu Forrester's inaugural Wave™ for Cloud Workload Security
"Rekomendowany" przez NSS Labs w rezultacie testu NSS Labs AEP Group Test
Nagroda Innowatora Branży w dziedzinie technologii Hypervisor Introspection przyznana przez SC Media drugi rok z rzędu
Przedstawiciel firmy Gartner®, dostawca platform do ochrony obciążeń w chmurze

+20 000 partnerów handlowych na świecie

Będąc dostawcą działającym w wyspecjalizowanym kanale dystrybucji, Bitdefender z dumą dzieli sukces z dziesiątkami tysięcy dystrybtorów na całym świecie.

Partner CRN odznaczony 5 gwiazdkami czwarty rok z rzędu. Na liście Security 100 portalu CRN. Partner CRN Cloud drugi rok z rzędu.
Więcej rozwiązań dla integracji z MSP niż u innych dostawców z branży bezpieczeństwa.
3 programy partnerskie Bitdefender umożliwiają wszystkim naszym partnerom – dystrybutorom, dostawcom usług i partnerom w modelu hybrydowym – skupienie się na sprzedaży rozwiązań Bitdefender, które odpowiadają ich własnej specjalizacji.

Autorytet w dziedzinie bezpieczeństwa

Bitdefender jest dumnym partnerem sojuszu technologicznego dla głównych dostawców wirtualizacji, bezpośrednio przyczyniając się do rozwoju bezpiecznych ekosystemów razem z **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS i Pivotal**.
Dzięki pracy wybitnego zespołu śledczego Bitdefender jest również aktywnie zaangażowany w zwalczanie międzynarodowej cyberprzestępczości we współpracy z największymi organami wymiaru sprawiedliwości, takimi jak FBI i Europol, w ramach takich inicjatyw, jak NoMoreRansom i TechAccord. Uczestniczymy także w inicjatywach takich, jak Hansa, których celem jest ograniczenie czarnego rynku. Od 2019 r. Bitdefender jest również dumnym posiadaczem statusu CVE Numbering Authority, nadanego przez organizację non-profit MITRE Corporation.

NAGRODZONY PRZEZ WIODĄCYCH ANALITYKÓW I NIEZALEŻNE ORGANIZACJE BADAWCZE

SOJUSZ TECHNOLOGICZNY

Bitdefender®

Założony w 2001 r. w Rumunii
Liczba pracowników: 1800+

Centrala
Siedziba przedsiębiorstwa – Santa Clara, California, Stany Zjednoczone
Centrala technologiczna – Bukareszt, Rumunia

Przedstawiciel marki Bitdefender w Polsce
Marken Systemy Antywirusowe
Tel: 58 667 49 49
E-mail: kontakt@marken.com.pl
www.bitdefender.pl

OCHRONA SPOD ZNAKU WILKA

Bezpieczeństwo danych, będące dziedziną genialnych innowacji, a zarazem branżą, w której kluczem do skutecznego stawiania czoła wyzwaniom jest najwyższy poziom spostrzegawczości, inteligencji i wnikliwości - to gra z zerowym marginesem błędu. Naszym zadaniem jest zwyciężać za każdym razem, tysiąc razy na tysiąc i milion razy na milion.

To właśnie robimy. Jesteśmy liderami branży nie tylko dzięki spostrzegawczości, inteligencji i wnikliwości naszych specjalistów, ale także dzięki temu, że jesteśmy o krok przed wszystkimi, zarówno tzw. "czarnymi kapeluszami", jak i ekspertami w dziedzinie bezpieczeństwa. Błyskotliwe dzieło pracy naszego zespołu ekspertów jest po Twojej stronie niczym legendarny ałunowy "Dacki smok", napędzany inżynierską intuicją, stworzony by chronić Cię przed wszelkimi niebezpieczeństwami kryjącymi się w tajemnych zawiłościach cyfrowego królestwa.