PL

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Od stycznia 2019 r. do kwietnia 2020 r.

O programowaniu ransomware

Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Informacje ogólne

Oprogramowanie typu ransomware stało się popularną bronią używaną przez sprawców szkodliwych działań, którzy codziennie próbują szkodzić rządom, firmom i osobom fizycznym. Ofiara ransomware może ponieść straty finansowe w postaci okupu, którego żąda atakujący, albo kosztów odzyskania utraconych danych, jeśli nie spełni jego żądań. W 2019 roku miasto Baltimore w stanie Maryland doświadczyło blokady działalności służb miejskich, a okup za przywrócenie sprawności miał wynosić 18,2 mln USD (ok. 15,4 mln EUR) – jednak miasto odmówiło jego zapłacenia.[1] Wobec rosnącej liczby incydentów jest oczywiste, że zamiast pytania, czy atak nastąpi, należy zadać sobie pytanie, kiedy się to wydarzy. W większości działań krajów w walce z oprogramowaniem typu ransomware rozwiązania wymaga kilka kwestii, takich jak brak koordynacji i współpracy między agencjami i władzami oraz brak przepisów, które jednoznacznie penalizują ataki ransomware.

Choć polisy ubezpieczeniowe obejmujące cyberbezpieczeństwo istnieją od początku 2000 r.[2], właśnie głównie ataki ransomware spowodowały wzrost zainteresowania tego typu ubezpieczeniami w ciągu ostatnich pięciu lat. W przypadku niektórych incydentów w 2019 roku[7] takie umowy pozwalały ofiarom odzyskać koszty okupu lub przywrócenia sprawności systemów. Niestety, jeśli atakujący wiedzą, że potencjalny cel oprogramowania typu ransomware jest ubezpieczony, zakładają, że najprawdopodobniej zapłaci okup. Innym problemem jest to, że ubezpieczyciele płacą okup z góry, aby ograniczyć szkody i zachować dotychczasową reputację ofiary. Jednak rozwiązanie problemu przez płacenie okupu zachęca społeczność hakerów i nie gwarantuje ani przywrócenia sprawności, ani zachowania reputacji.[3]

Wnioski

*10,1 mld EUR*_ to szacowana wysokość okupów w 2019 r.

Kwota zapłaconych okupów była o 3,3 mld euro wyższa niż w 2018 r.

*365%*_ wzrost liczby wykrytych incydentów w przedsiębiorstwach w 2019 r.

Liczba programów typu ransomware wykrytych na komputerach w środowiskach biznesowych wzrosła w porównaniu z pierwszą połową 2018 roku[22].

*66%*_ organizacji ochrony zdrowia doświadczyło ataku

W roku 2019 ataku ransomware doświadczyło ponad 66% organizacji ochrony zdrowia[23].

*45%*_ zaatakowanych organizacji zapłaciło okup

To odsetek organizacji zaatakowanych w 2019 roku, które zapłaciły okup – połowa z nich mimo to utraciła dane[37].

*28%*_ incydentów związanych z bezpieczeństwem przypisano złośliwemu oprogramowaniu

Ransomware było drugim pod względem powszechności zagrożeniem po złośliwym oprogramowaniu C2 i było związane z jedną trzecią (28%) incydentów związanych z bezpieczeństwem[32].

Kill chain

Proces etapów ataku

Zakres działania

Rozwiązanie Cyber Kill Chain® zostało opracowane przez Lockheed Martin na podstawie wojskowej koncepcji związanej ze strukturą ataku. Aby zbadać określony wektor ataku, należy użyć poniższego schematu Cyber Kill Chain w celu stworzenia mapy każdego etapu procesu i określić narzędzia, techniki i procedury, z jakich skorzystał atakujący.

WIĘCEJ INFORMACJI

Opis

_Ransomware mierzy wyżej

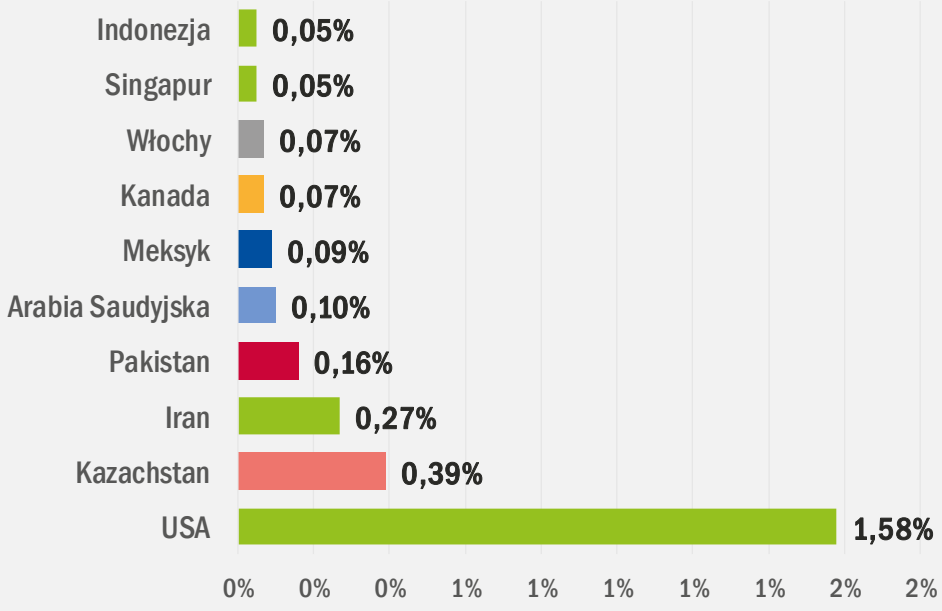
W pierwszym i drugim kwartale 2019 r. ataków oprogramowania typu ransomware było mniej, niż odnotowano w analogicznym okresie poprzednich trzech lat. Jednak skupiały się ona na ważnych celach. W 2018 roku odnotowano ekspansję trojana RAT, umożliwiającego zdalny dostęp do komputera, programów pobierających i backdoorów, ale w tym roku złośliwe oprogramowanie pozostawało bezczynne[9,10]. Obecnie wiadomo, że oprogramowanie to dostarczyło atakującym informacji umożliwiających wskazanie wrażliwych, ważnych celów, skłonnych zapłacić wyższe kwoty okupu. W efekcie w omawianym roku oprogramowanie typu ransomware rozprzestrzeniło się na inne sektory poza branżą ochrony zdrowia, atakując firmy przemysłowe i produkcyjne. Ostatnio oprogramowanie typu ransomware z rodziny LockerGoga wykorzystano do uszkadzania systemów sterujących maszynami w zakładach produkcyjnych[11].

_Ubezpieczenia cybernetyczne bardziej popularne

W 2019 r. wartość rynku polis bezpieczeństwa cybernetycznego w samych Stanach Zjednoczonych wyniosła 8 mld USD (ok. 6,7 mld euro). Chociaż podobne produkty istnieją od czasu „błędu roku 2000" (Y2K lub Millennium Bug), w ostatnich latach zyskały większe zainteresowanie organizacji rządowych, miast, organizacji ochrony zdrowia i innych potencjalnych celów wysokiego ryzyka oprogramowania typu ransomware. Takimi polisami były objęte atak SamSam w Atlancie w stanie Georgia i incydent w Lake City na Florydzie[16]. W związku ze wzrostem liczby wymuszeń okupu, organizacje i firmy coraz bardziej potrzebują polis bezpieczeństwa cybernetycznego. Jednak zdrowy rozsądek podpowiada, że ofiary muszą w miarę możliwości unikać ulegania żądaniom. Zapłacenie okupu zachęca atakującego do powtórzenia czynu, a jednocześnie nie gwarantuje przywrócenia sprawności systemu – w wielu przypadkach atakujący nie dotrzymują swojej części umowy.

_Otwarty protokół RDP (Remote Desktop Protocol) to duże ryzyko

Kilka udanych odmian ransomware, takich jak SamSam, BitPaymer czy CrySiS, bierze na cel serwery RDP w celu zainicjowania ataku[20]. Niestety, wiele organizacji wciąż realizuje zdalny dostęp za pomocą protokołu RDP, zamiast bezpieczniejszej wirtualnej sieci prywatnej (VPN). Problem z RDP polega na tym, że ma on słabe punkty, które można wykorzystać, a usługa RDP może korzystać z serwerów łatwo dostępnych z poziomu internetu. Zgłoszono ponad 800 000 niezaktualizowanych, podatnych na ataki systemów z usługami RDP; wśród nich systemy z zakresu IP centrum danych Microsoft Azure[51]. Chociaż Microsoft zapewnił, że systemy te należą do podmiotu zewnętrznego, pojawia się problem dotyczący bezpieczeństwa dostawców usług w chmurze.



Rysunek 1: 10 krajów o największym udziale użytkowników zaatakowanych przez mobilne trojany ransomware w drugim kwartale 2019 r. Źródło: Kaspersky[34]

Opis

_ Poszukiwani

LOCKERGOGA_ został po raz pierwszy ujawniony w styczniu 2019 r. po ataku na francuską firmę konsultingową Altran Technologies[40]. Przestały działać jej sieci informatyczne i wszystkie aplikacje, co zakłóciło działalność firmy w kilku krajach. LockerGoga jest instalowany i uruchamiany przez narzędzie PsExec, będące lekkim zamiennikiem telnetu, zdolnym do przejścia niektórych kontroli bezpieczeństwa jako częściowo prawidłowe oprogramowanie[11]. Po zainstalowaniu modyfikowane są konta użytkowników w docelowym systemie i następuje siłowe wylogowywanie. Ponadto zmieniane są nazwy plików narzędzi, a pliki przenoszone, w wyniku czego ich znalezienie staje się prawie niemożliwe. W późniejszych wersjach LockerGoga blokada jest tak silna, że ofiary nie mogą nawet zobaczyć komunikatu ransomware ani instrukcji odblokowania, nawet jeśli żądania zostały spełnione. Tylko nieliczne programy antywirusowe i chroniące przed złośliwym oprogramowaniem są w stanie wykryć LockerGoga i bronić przed nim, a deszyfrator nie istnieje[10]. W 2019 r. oprócz Altran Technologies celem LockerGoga był koncern NorskHydro i dwie amerykańskie firmy chemiczne, Hexion i Momentive[41]. Tylko w przypadku ataku na NorskHydro koszt zniszczeń oszacowano na 50 mln USD (ok. 42 mln EUR)[21].

KATYUSHA_ to trojan ransomware użyty po raz pierwszy w październiku 2018 r. Szyfruje pliki ofiary, usuwa kopie zapasowe VSS i dostarcza załączniki pocztą e-mail. Do rozprzestrzeniania się Katiusza wykorzystuje exploity EternalBlue i DoublePulsar[45]. Niestety, nie są jeszcze dostępne żadne deszyfratory ani narzędzia do obrony.

JIGSAW_ nie tylko szyfruje pliki ofiary, ale także usuwa je, jeśli żądania nie zostaną spełnione w podanym, najczęściej 24-godzinnym terminie. Co więcej, jeśli ofiara spróbuje wyłączyć komputer, tempo usuwania plików wzrasta. To nie przypadek, że to ransomware zostało nazwane imieniem postaci z horroru[45]. Jednak firmy zajmujące się bezpieczeństwem regularnie wydają aktualizacje wydajnego deszyfratora Jigsaw[46].

PEWCRYPT_ powstał na początku 2019 roku i, w przeciwieństwie do większości ransomware, jego jedynym celem jest zmuszenie użytkowników do subskrybowania kanału youtubera PewDiePie. PewDiePie konkurował pod względem popularności z indyjskim kanałem Bollywood T-Series i jego fani postanowili zwiększyć jego szanse na wygraną za pomocą PewCrypt. PewCrypt to typowe oprogramowanie typu ransomware, rozprzestrzeniające się za pośrednictwem spamu i złośliwych reklam internetowych. Zostało napisane w języku programowania Java. W marcu 2019 roku autor udostępnił narzędzie deszyfrujące[47].

RYUK_ pojawił się w sierpniu 2018 r. i prawdopodobnie był powiązany z grupami hakerskimi z Korei Północnej. Wkrótce okazało się, że autorzy Ryuka to ta sama grupa, która używała ransomware Hermes i ukradła jego kod. Główne cechy Ryuka to wykorzystanie algorytmów wojskowych i ukierunkowane ataki na duże przedsiębiorstwa. Większość jego ofiar otrzymuje żądania zapłaty okupu w bitcoinach.[45]

DHARMA_ to kryptowirus, który pojawił się w 2016 roku, ale wciąż powstają jego nowe wersje. Dharma nie tylko szyfruje pliki ofiary, ale i usuwa wszelkie kopie zapasowe VSS. W 2019 r. rozprzestrzeniał się przez zakażone pliki z popularnymi, szkodliwymi lub prawidłowymi rozszerzeniami, takimi jak „.gif", „.AUF", „.USA", „.xwx", „.best" i „.heets". We wrześniu 2019 roku analityk bezpieczeństwa udostępnił program Rakhnidecryptor[42], pozwalający ofiarom Dharmy odszyfrować pliki.

GANDCRAB_ został po raz pierwszy użyty w styczniu 2018 r. i w niecały miesiąc zainfekował ponad 50 tys. systemów, stając się jednym z najczęściej występujących programów typu ransomware 2018 roku[43]. Wykorzystuje makra Microsoft Office, VBScript oraz PowerShell i atakuje niezauważenie[45]. GandCrab, oparty na modelu ransomware-as-a service (RaaS), jest podobny do Cerbera i pozwala jego twórcom i przestępcom dzielić się zyskami. Zespołowi utworzonemu przez Europol, rumuńską policję, Prokuraturę Generalną i Bitdefender po zhakowaniu serwerów GandCrab udało się stworzyć narzędzie odszyfrowujące[44]. W drugim kwartale 2019 r. operatorzy GandCrab ogłosili „przejście na emeryturę" po zebraniu z okupów ponad 2 miliardów dolarów. Za następcę GandCrab uważane jest pojawiające się w małych kampaniach ransomware Sodinokibi[10].

Opis

_ Poszukiwani

REVIL lub SODINOKIBI lub SODIN_ po raz pierwszy pojawił się w ataku na włoskie narzędzie WinRAR w czerwcu 2019 roku. Podejrzewa się również, że był użyty w trzech atakach MSP i czwartym na amerykańską firmę PerCSoft, której klienci należą głównie do sektora ochrony zdrowia[48]. Sodinokibi wydaje się być produktem znanej grupy cyberszpiegowskiej FruityArmor, która działa od 2016 roku. Ataki Sodinokibi dotknęły kilku krajów na całym świecie. Najbardziej atakowanym przez Sodinokibi krajem jest Tajwan, który doznał do tej pory 17,56% wszystkich zarejestrowanych ataków. W Europie najczęściej atakowane są Niemcy (8,05%), Włochy (5,12%) i Hiszpania (4,88%). Sodinokibi jest dystrybuowany w modelu RaaS i szyfruje pliki potrzebne do przeprowadzenia ataku inaczej dla każdego systemu. Atakujący osadzają w kodzie „klucz szkieletowy", umożliwiający im zdalne odszyfrowanie plików, niezależnie od użytego szyfrowania[49]. Jeśli jednak komputer ma układ klawiatury rosyjski, armeński, syryjski lub jeden spośród kilku innych, Sodinokibi nie może go zaszyfrować, co prawdopodobnie wskazuje na pochodzenie autorów[50].

SAMSAM_ już piąty rok z rzędu atakuje infrastrukturę krytyczną na całym świecie. Ataki SamSam koncentrują się głównie na szpitalach, firmach z sektora ochrony zdrowia i organizacjach rządowych, co zapewnia szybką zapłatę dużych okupów. Wykorzystuje on słabe punkty protokołu RDP (Remote Desktop Protocol). Do tej pory grupa odpowiedzialna za dystrybucję SamSam zebrała ponad 6 mln USD (ok. 5 mln EUR) okupów i spowodowała u ofiar straty przekraczające 30 mln USD (ok. 25,4 mln EUR)[45]. Tylko w ataku na miasto Atlanta w 2018 r. szkody i koszty przywrócenia sprawności systemów wyniosły 17 mln USD (ok. 14,4 mln EUR)[43].

„Rok 2019 przyniósł wzrost wyrafinowania potencjalnych zagrożeń w związku z używaniem przez wielu cyberprzestępców exploitów, kradzieży poświadczeń i ataków wieloetapowych”.

w: ETL 2020

Opis

_ Atakowane sektory

PAŃSTWA NARODOWE WCIĄŻ W CENTRUM UWAGI_ W 2018 r. oprogramowanie typu ransomware było wykorzystywane do atakowania organizacji państwowych jako narzędzie do zarabiania pieniędzy. Tendencja ta utrzymywała się w 2019 roku, a narody lub grupy narodowe ukrywały swoją tożsamość za pomocą tych samych narzędzi stworzonych przez inne grupy lub podmioty z państw narodowych. Taka manipulacja narzędziami pozwala na ukrycie pochodzenia atakującego i uniknięcie jakichkolwiek konsekwencji dyplomatycznych, zwłaszcza gdy celem jest organizacja rządowa lub państwowa.

W roku 2019 miało miejsce kilka ataków na organizacje rządowe lub państwowe. Na przykład od kalifornijskiego miasta Lodi[4] atakujący zażądali zapłacenia okupu w wysokości 400 tys. USD (ok. 340 tys. euro) za odblokowanie linii telefonicznych policji, linii alarmowej robót publicznych, numerów urzędu miasta oraz danych dotyczących płatności miejskich i systemów finansowych. Miasto odmówiło zapłaty okupu i przywróciło sprawność systemów przy użyciu kopii zapasowych. Departament zasobów informacyjnych stanu Teksas poinformował o skoordynowanym ataku ransomware na 23 małe organizacje rządowe w sierpniu 2019 roku[5]. Koszty dla hrabstwa w stanie Texas oszacowano na 3,25 mln USD (ok. 2,75 mln EUR). Atak RobbinHood na Baltimore spowodował szkody w wysokości 18,2 mln USD (około 15,4 mln EUR), zaś w wyniku ataku Ryuk Lake City na Florydzie poniosło straty w kwocie 460 tys. USD (ok. 389 768 EUR). W lipcu 2019 r. miasto New Bedford w stanie Massachusetts zostało dotknięte atakiem ransomware, którego sprawcy żądali zapłacenia okupu w wysokości 5,3 mln USD (ok. 4,4 mln EUR). Miasto odmówiło zapłacenia okupu, wydając 1 mln USD na likwidację skutków ataku[7].

DO IMPREZY DOŁĄCZAJĄ INSTYTUCJE EDUKACYJNE_ W roku 2019 zaobserwowaliśmy przesunięcie ataków na instytucje edukacyjne. Według raportu opublikowanego przez firmę Emsisoft, ofiarami 62 incydentów związanych z oprogramowaniem typu ransomware padło 1051 szkół i uczelni. W roku 2018 ofiarami incydentów było tylko 11 placówek oświatowych. Z raportu wynika, że amerykańskie szkoły były na drugim miejscu listy atakowanych podmiotów po urzędach miast[8].

SEKTOR OCHRONY ZDROWIA WCIĄŻ NA CELOWNIKU_ Organizacje ochrony zdrowia były ulubionym celem ataków oprogramowania typu ransomware we wszystkich poprzednich latach i trend ten utrzymał się również w 2019 roku. Latem zaatakowany został kalifornijski dostawca usług medycznych Wood Ranch Medical, którego elektroniczna dokumentacja medyczna została całkowicie zniszczona (łącznie z kopiami zapasowymi) po odmowie zapłacenia okupu. Incydent zmusił Wood Ranch Medical do ogłoszenia, że do końca roku zaprzestanie działalności[12]. W kwietniu 2019 roku dokładnie to samo spotkało innego dostawcę usług medycznych, Michigan Brookside ENT and Hearing Center[13], który również został zmuszony do zamknięcia. Ponadto w Australii zaatakowano dwie grupy szpitali: GippslandHealth Alliance oraz South West Alliance of Rural Health. W efekcie szpitale w kilku miastach, w tym Warrnambool, Colac, Geelong, Warragul, Sale i Bairnsdale, nie mogły wykonywać normalnych procedur, ponieważ ich systemy zostały wyłączone w celu ograniczenia ekspozycji na zagrożenia[14]. W tym sektorze utrata danych jest równie dotkliwa, jak strata finansowa. Na przykład w wyniku ataku oprogramowania typu ransomware, przeprowadzonego w czerwcu 2019 roku na grupę Premier Family Medical w stanie Utah, wyciekły poufne informacje dotyczące zdrowia ponad 300 tys. pacjentów[15].

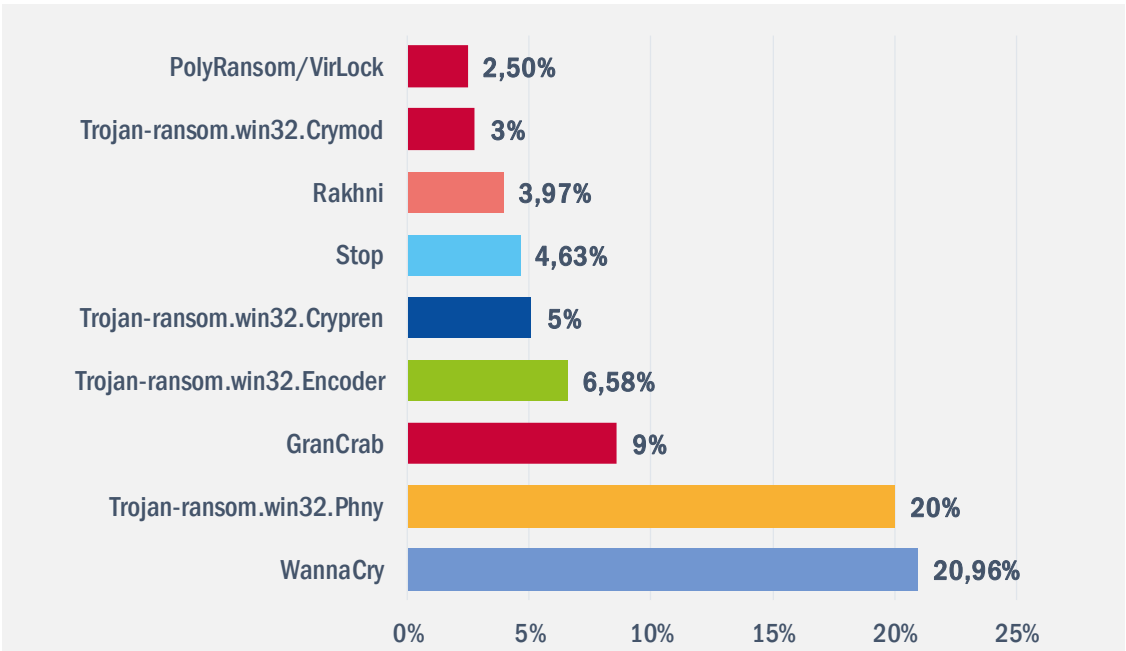
MSP NIE DZIAŁAJĄ_ Wiele branż powierza poufne informacje, mające zasadnicze znaczenie dla ich działalności, dostawcom usług zarządzanych (MSP) i dostawcom usług w chmurze (CSP). Klienci polegają na nich również w zakresie integralności danych i zapobiegania nieuprawnionemu dostępowi do nich[17]. Tymczasem oprogramowanie typu ransomware GandCrab i Sodin wykorzystuje słabe punkty dostawców usług internetowych, które odsłaniają ich infrastrukturę i powierzone dane, i w efekcie narażają na atak ransomware wszystkich klientów MSP. Takie słabe punkty ma Webroot2FA, popularne narzędzie MSP, co zostało wykorzystane w kilku przypadkach w 2019 roku[18]. W tym roku w ciągu zaledwie trzech miesięcy zostało zaatakowanych kilku MSP, takich jak PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. oraz IT By Design[19].

Wektory ataku

_Jak

Nowe oprogramowanie typu ransomware o nazwie Sodinokibi wykorzystuje niedawno ujawniony słaby punkt lukę Oracle WebLogic Server CVE-2019-2725 w celu uzyskania możliwości zdalnego wykonywania kodu. Ofiara zostaje zarażona, jeśli nie podejmie odpowiednich działań. Wydano oficjalne poprawki dla Oracle WebLogic Server w wersjach 10.3.6.0 i 12.1.3.0[51]. Ten sam atak wykorzystuje słaby punkt CVE-2018-8453 w celu uzyskania większych uprawnień użytkownika, kończenia procesów znajdujących się na czarnej liście, usuwania plików z czarnej listy i eksfiltracji informacji o hoście[48].

Inny słaby punkt, CVE-2019-0708, jest również wykorzystywany do instalowania oprogramowania typu ransomware. Umożliwia to nieautoryzowane połączenie za pośrednictwem protokołu RDP firmy Microsoft. W maju 2019 roku Microsoft wydał poprawki dla aktualnych wersji systemu operacyjnego (OS), a także dla wersji, które nie są już obsługiwane[51].



Rysunek 2: Najważniejsze ataki oprogramowania typu ransomware w 2019 r. Źródło: Kaspersky[39]

Incydenty

- Incydent w Baltimore County[1]
- Atak na szpitale w Alabamie[7]
- Incydent w mieście Lodi (Kalifornia)[4]
- Incydent w Teksasie (departament dział zasobów informacyjnych stanu Teksas)[5]
- Atak Ryuk w Lake City (Floryda)[7]
- Incydent w New Belford (Massachusetts)[6]
- Ataki ransomware na ponad 500 szkół i uniwersytetów[8]
- Przypadek Wood Ranch Medical (Kalifornia)[12]
- Przypadek Michigan Brookside ENT and Hearing Centre[13]
- Przypadki GippslandHealth Alliance oraz South West Alliance of Rural Health (Australia)[14]
- Przypadek Premier Family Medical Group (Utah)[15]
- Przypadki MSP PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. oraz IT By Design[19]
- Incydent centrum danych Microsoft Azure[51]
- Atak LockerGoga na Altran Technologies[40]
- Atak LockerGoga na Norsk Hydro[7]
- Ataki LockerGoga na Hexion i Momentive[41]
- Incydent Albany IT[60]
- Incydent w Jackson County (Georgia)[61]
- Incydent w Riviera Beach (Floryda)[62]
- Incydent w Nowym Orleanie[63]
- Atak na duńskiego producenta aparatów słuchowych Demant[64]

Ograniczenie ryzyka

Proponowane działania

- Utrzymywanie niezawodnych kopii zapasowych zgodnych z regułą 3-2-1 (tj. co najmniej trzy kopie w dwóch różnych formatach, w tym jedna z nich w innej lokalizacji)[5].
- Wykupienie polisy ubezpieczeniowej pokrywającej szkody spowodowane atakiem ransomware[21].
- Stosowanie segmentacji sieci, szyfrowania danych, kontroli dostępu i egzekwowanie zasad, by zapewnić minimalną ekspozycję danych.
- Korzystanie z metod takich jak monitorowanie, pozwalających szybko wykrywać infekcje.
- Monitorowanie dostępu do używanej infrastruktury publicznej i jej stanu.
- Utworzenie w każdej organizacji lub firmie centrum bezpieczeństwa (SOC, security operation centre) zatrudniającego wykwalifikowanych specjalistów w dziedzinie bezpieczeństwa.
- Używanie odpowiednich, aktualizowanych na bieżąco narzędzi do zapobiegania atakom ransomware.
- Dokładne zdefiniowanie i wdrożenie minimalnego zestawu praw dostępu użytkowników do danych, by zminimalizować skutki ataków (tj. mniej praw, mniej zaszyfrowanych danych).
- Wdrożenie sprawnego zarządzania słabymi punktami i łatkami.
- Zaimplementowanie filtrowanie treści, by odfiltrować niechciane załączniki, wiadomości e-mail ze złośliwą zawartością, spam i niechciany ruch sieciowy.
- Instalacja ochrony punktów końcowych za pomocą programów antywirusowych, a także blokowania wykonywania plików (np. blokowanie wykonywania plików z folderu Temp).
- Stosowanie zasad kontrolowania urządzeń zewnętrznych i dostępności portów.
- Używanie białych list, by zapobiec uruchamiania nieznanych plików wykonywalnych na punktach końcowych.
- Inwestowanie w podnoszenie świadomości użytkowników na temat oprogramowania typu ransomware, zwłaszcza w odniesieniu do bezpiecznego przeglądania.

_Deszyfratory

Znaczne postępy zostały poczynione przez EUROPOL[7] i 163 partnerów projektu „No more ransom”[7]. W 2019 roku portal dodał 28 narzędzi i obecnie może odszyfrować efekty 140 różnych rodzajów infekcji ransomware[65]. Opracowano kilka programów do odszyfrowywania efektów działania oprogramowania typu ransomware, a wiele innych zostało zaktualizowanych. Przykłady podano poniżej.

RANSOMWARE	DESZYFRATOR
Aurora[52], **Muhstik**[53], **Ryuk**[54]	Emsisoft
Rakhni, Aura, Autoit, Pletor, Rotor, Lamer, Lortok, Democry, TeslaCrypt, Chimera, Crysis, Jaff, Dharma, Cryakl, Yatron, FortuneCrypt,[55,56]	Kaspersky Lab
GandCrab[44]	Europol, rumuńska policja i GPO, Bitdefender
Jigsaw[46]	Avast
Mira[57]	F-Secure
Nemty[58]	Tesorion
PewCrypt[47]	Autor PewCrypt

Bibliografia

1. „Washington idle as ransomware ravages cities big and small" 28 września 2019 r. Politico. https://www.politico.com/news/2019/09/28/ransomware-cities-washington-007376

2. „What you — and your company — should know about cyber insurance", 20 sierpnia 2019 r. Talos. https://blog.talosintelligence.com/2019/08/cyber-insurance-FAQs.html

3. „The State of Ransomware in 2019", 17 czerwca 2019 r. IT Pro Today. https://www.itprotoday.com/threat-management/state-ransomware-2019

4. „California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware". 2 sierpnia 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware

5. „Coordinated Ransomware Attack Cripples Local Government Organizations in Texas", 19 sierpnia 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coordinated-ransomware-attack-cripples-local-government-organizations-in-texas

6. „The State of Ransomware in the US: Report and Statistics 2019". 12 grudnia 2019 r. Blog EMSISOFT. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

7. „Alabama hospitals have been hit by a massive ransomware attack" 3 października 2019 r. https://www.foxnews.com/tech/alabama-hospitals-ransomware-attack

8. „500+ Schools Have Been Affected by Ransomware in 2019", 4 października 2019 r. Campus Safety, https://www.campussafetymagazine.com/safety/500-schools-ransomware-2019/

9. „Latest Quarterly Threat Report - Q1 2019", 2019 r. Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

10. „Proofpoint Q2 2019 Threat Report - Emotet's hiatus, mainstream impostor techniques, and more". 19 września 2019 r. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q2-2019-threat-report-emotets-hiatus-mainstream-impostor-techniques

11. „6 of the Biggest Cybersecurity Crises of 2019 (So Far)" 24 września 2019 r. Blog EC-Council. https://blog.eccouncil.org/6-of-the-biggest-cybersecurity-crises-of-2019-so-far/

12. „Ransomware Attacks Double in 2019: Medical Providers Can't Recover and Shut Down", 3 października 2019 r. https://www.natlawreview.com/article/ransomware-attacks-double-2019-medical-providers-can-t-recover-and-shut-down

13. „Michigan's Brookside ENT and Hearing Center forced to close due to a Ransomware Attack", 23 kwietnia 2019 r. SPAM Fighter. https://www.spamfighter.com/News-22154-Michigans-Brookside-ENT-and-Hearing-Center-forced-to-close-due-to-a-Ransomware-Attack.htm

14. „Victorian hospitals across Gippsland, Geelong and Warrnambool hit by ransomware attack". 1 października 2019 r. https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988?nw=0

15. „Ransomware Attack Affects 300,000 Patients in Utah". 12 września 2019 r. CISO Mag. https://www.cisomag.com/ransomware-attack-affects-300000-patients-in-utah/

16. „The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks". 27 sierpnia 2019 r. ProPublica. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

17. „CYBER THREATSCAPE REPORT". 2019. Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

18. „Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread". 2019. Coveware. https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

19. „Armor Identifies 15 New Ransomware Victims in the Last 2 Weeks, All of them Educational Institutions – Threat Intelligence". 20 września 2019 r. Armor. https://www.armor.com/resources/armor-identifies-10-new-ransomware-victims-in-the-past-9-days/

20. „4 Ransomware Trends to Watch in 2019". 13 lutego 2019 r. https://www.recordedfuture.com/ransomware-trends-2019/

21. „BDO Cyber Threat Insights - 2019 2nd Quarter Report", Lipiec 2019 r. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

22. „BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare". Październik 2019 r. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

23. „Healthcare Cyber Heists in 2019", 3 października 2019 r. VMWare. https://www.carbonblack.com/resources/threat-research/healthcare-cyber-heists-in-2019/

24. „Australia | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/australia-global-threat-report-defender-power-on-the-rise/

25. „France | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/france-global-threat-report-defender-power-on-the-rise/

26. „Italy | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/italy-global-threat-report-defender-power-on-the-rise/

27. „Japan | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/japan-global-threat-report-defender-power-on-the-rise/

28. „Canada | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/canada-global-threat-report-defender-power-on-the-rise/

29. „Singapore | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/singapore-global-threat-report-defender-power-on-the-rise/

30. „UK | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/uk-global-threat-report-defender-power-on-the-rise/

31. „Anticipating the Unknowns". Marzec 2019 r. Cisco. https://ebooks.cisco.com/story/anticipating-unknowns/

32. „2020 Data Breach Investigations Report" 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

33. „IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks". 5 września 2019 r. IBM. https://newsroom.ibm.com/2019-09-05-IBM-Security-Study-Taxpayers-Oppose-Local-Governments-Paying-Hackers-in-Ransomware-Attacks

34. „IT threat evolution Q2 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

35. „IT threat evolution Q1 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

36. „The state of industrial cybersecurity". Lipiec 2019 r. Kaspersky. https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

37. „2019 Cyberthreat Defense Report" Cyber Edge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

38. „Evasive Threats, Pervasive Effects". 27 sierpnia 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

39. „IT threat evolution Q3 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

40. „What You Need to Know About the LockerGoga Ransomware". 20 marca 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/

41. „BDO Cyber Threat Insights - 2019 2nd Quarter Report", Lipiec 2019 r. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

Bibliografia

42. Deszyfratory ransomware, Kaspersky https://noransom.kaspersky.com/

43. „Raport ENISA o krajobrazie zagrożeń" (ENISA Threat Landscape Report 2018). 28 stycznia 2019 r. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

44. „New GandCrab v5.1 Decryptor Available Now", 19 lutego 2019 r. Bitdefender LABS. https://labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/

45. „10 Ransomware Attacks You Should Know About in 2019", 28 kwietnia 2019 r. Allot. https://www.allot.com/blog/10-ransomware-attacks-2019/

46. Deszyfratory ransomware Avast. https://www.avast.com/ransomware-decryption-tools

47. Źródło ransomware PewCrypt. GitHub. https://github.com/000JustMe/PewCrypt

48. „Are the REvil, GranCrab Ransomware Families Related?" 25 września 2019 r. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/revil-gandcrab-related/

49. „Threat Landscape Report", Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2019.pdf

50. „Sodin Ransomware includes exploit for Windows CVE-2018-8453 bug". 4 lipca 2019 r. Security Affairs. https://securityaffairs.co/wordpress/87944/malware/sodin-ransomware-cve-2018-8453.html

51. „Threat Landscape Report" 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q2-2019.pdf

52. „Emsisoft Decryptor for Aurora", 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/aurora

53. „Emsisoft Decryptor for Muhstik", 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/muhstik

54. „Caution! Ryuk Ransomware decryptor damages larger files, even if you pay". 9 grudnia 2019 r. Emsisoft. https://blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/

55. „RakhniDecryptor tool for defending against Trojan-Ransom.Win32.Rakhni ransomware". Kaspersky. https://support.kaspersky.com/10556

56. „Another two bite the dust: Kaspersky updates decryption tool to fight ransomware pair". 27 września 2019 r. The Online Citizen. https://www.theonlinecitizen.com/2019/09/27/another-two-bite-the-dust-kaspersky-updates-decryption-tool-to-fight-ransomware-pair/

57. „Mira Ransomware Decryptor", 1 kwietnia 2019 r. F-Secure. https://blog.f-secure.com/mira-ransomware-decryptor/

58. „Nemty update: decryptors for Nemty 1.5 and 1.6" Tesorion. https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/

59. „McAfee Labs Threats Report", sierpień 2019 r. McAfee, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

60. „The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/2

61. „The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/3

62. „The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/6

63. „The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/7

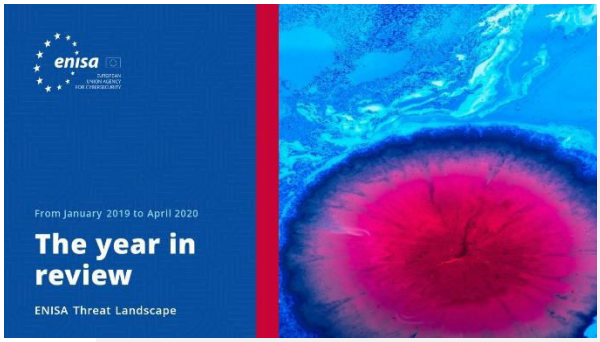
64. „The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/11

65. https://www.nomoreransom.org/

„CTI ma ugruntowaną pozycję w dziedzinie bezpieczeństwa cybernetycznego jako podstawowe narzędzie zwiększania sprawności i skuteczności w obronie przed cyberatakami.”

w: ETL 2020

Powiązany



Raport ENISA o krajobrazie zagrożeń
Przegląd roku

Zestawienie trendów w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

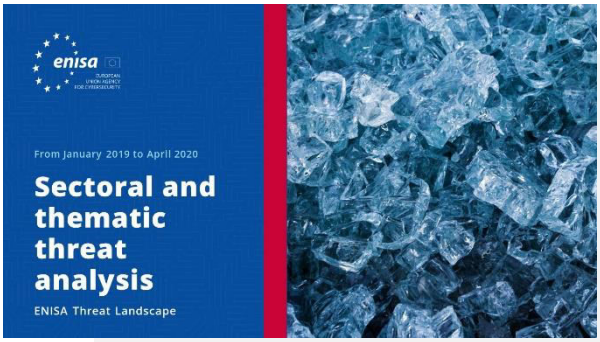
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Tematyka badań

Zalecenia dotyczące tematów badawczych z różnych kwadrantów w dziedzinie cyberbezpieczeństwa i rozpoznawania zagrożeń cybernetycznych.

PRZECZYTAJ RAPORT



Raport ENISA o krajobrazie zagrożeń
Sektorowa i tematyczna analiza zagrożeń

Kontekstualna analiza zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Nowe trendy

Główne trendy w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Omówienie kwestii rozpoznawania cyberzagrożeń

Aktualny stan wywiadu dotyczącego cyberzagrożeń w UE.

PRZECZYTAJ RAPORT

Informacje o agencji

_ Agencja

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. Utworzona w roku 2004 i wzmocniona przez Akt o cyberbezpieczeństwie Agencja Unii Europejskiej ds. Cyberbezpieczeństwa wnosi wkład w politykę cybernetyczną UE; zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa; współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i pogłębianie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz w efekcie, zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Więcej informacji na temat ENISA i jej działalności można znaleźć na stronie www.enisa.europa.eu.

Współautorzy

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) oraz *wszyscy członkowie ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) i Thomas Hemker.

Wydawcy

Marco Barros Lourenço (ENISA) i Louis Marinos (ENISA).

Dane kontaktowe

Zapytania dotyczące tego dokumentu można kierować na adres enisa.threat.information@enisa.europa.eu.

Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

Chcielibyśmy poznać opinie czytelników na temat tego raportu!
Poświęć chwilę, by wypełnić kwestionariusz. Aby uzyskać dostęp do formularza, kliknij tutaj.

Zastrzeżenia prawne

Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja nie musi przedstawiać aktualnego stanu wiedzy i ENISA może ją okresowo aktualizować.

Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

Niniejsza publikacja ma charakter wyłącznie informacyjny. Musi ona być dostępna nieodpłatnie. Ani ENISA, ani żadna osoba działająca w jej imieniu nie ponoszą odpowiedzialności za wykorzystanie informacji zawartych w niniejszym sprawozdaniu.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecja
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

https://www.enisa.europa.eu