PL

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

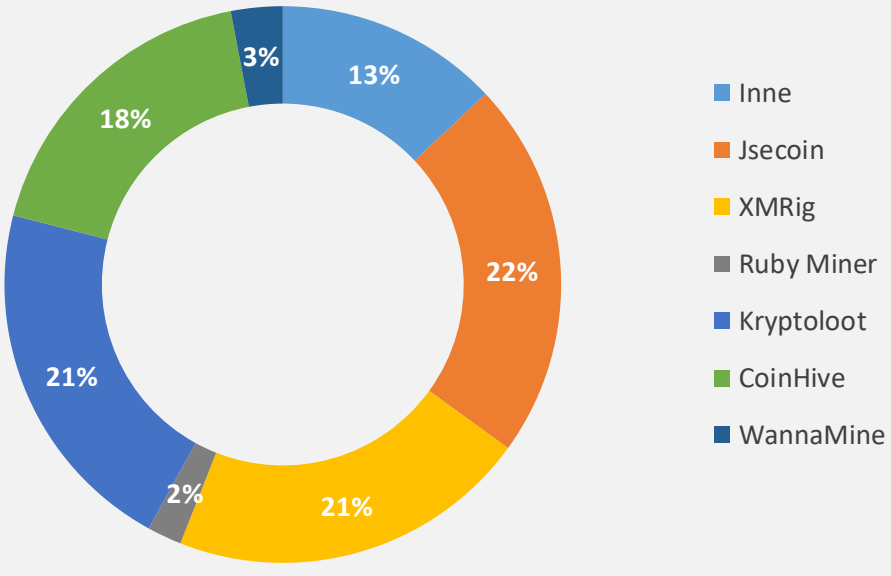
Od stycznia 2019 r. do kwietnia 2020 r.

Crypto-jacking

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

Informacje ogólne

Cryptojacking (znany również jako cryptomining) to niedozwolone wykorzystanie zasobów urządzenia do wydobywania kryptowalut. Celami ataków są wszelkie urządzenia podłączone do internetu, takie jak komputery i telefony komórkowe; jednak cyberprzestępcy coraz częściej atakują infrastrukturę chmury[1]. Tego rodzaju ataki nie są obiektem wielkiego zainteresowania organów ścigania, a ich przypadki są rzadko zgłaszane[2], głównie ze względu na stosunkowo niewiele negatywnych konsekwencji. Niemniej jednak organizacje mogą zauważyć wyższe koszty IT, degradację elementów komputerów, zwiększone zużycie energii elektrycznej i zmniejszoną produktywność pracowników, spowodowaną wolniejszym działaniem stacji roboczych[3].



Rysunek 1: Najczęstsze na świecie złośliwe oprogramowanie do wydobywania kryptowalut. Źródło: Check Point[9]

Wnioski

64,1_miliona przypadków cryptojackingu do końca 2019 roku

78%_spadek aktywności cryptojackingu w drugiej połowie 2019 roku w porównaniu z pierwszym półroczem

Działalność wzrosła o 9% w pierwszej połowie 2019 roku w porównaniu do poprzednich 6 miesięcy 2018 roku[4,5].

65%_ze 120 najpopularniejszych giełd w III kwartale 2019 r. miało słabe lub nieszczelne procesy „Poznaj swojego klienta" (know your customer, KYC)

32% giełd obracało walutami zapewniającymi prywatność („privacy coins").[6]

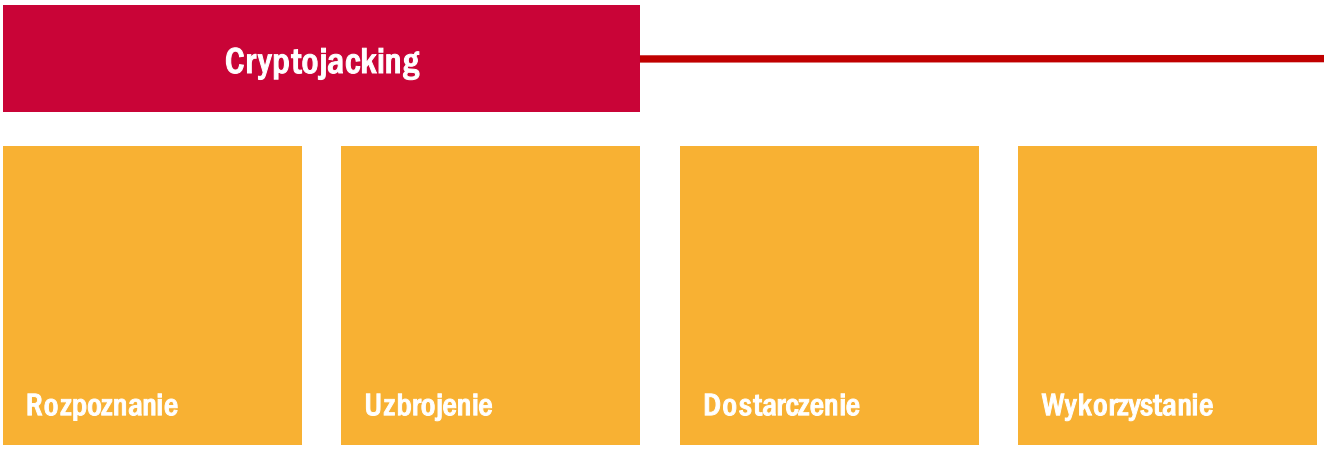
39,3%_infekcji związanych z cryptominingiem w 2019 r. dotyczyło Japonii.

20,8% infekcji związanych z cryptominingiem dotyczyło Indii, a 14,2% Tajwanu. Rysunek 1 przedstawia pięć krajów z najczęściej wykrywanymi próbami infekcji złośliwym oprogramowaniem do cryptominingu w latach 2018 i 2019[7].

13%_incydentów związanych z cryptojackingiem przypisuje się wirusowi trojan.Win32.Miner.bbb

W okresie od listopada 2018 do października 2019 roku następnymi najbardziej aktywnymi „wydobywcami" były Trojan.Win32.Miner.ays (11,35%), Trojan.JS.Miner.m (11,12%).[8]

Kill chain



Proces etapów ataku

Zakres działania

Cryptojacking

Instalacja	Dowodzenie i kontrola	Działania dotyczące celów

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

Trendy

_Popularny serwis cryptominingowy Coinhive został zamknięty

Coinhive wystartował we wrześniu 2017 r. i reklamował się jako alternatywne źródło przychodów dla twórców stron internetowych zamiast banerów reklamowych[24]. Wykorzystywał biblioteki JavaScript, które można było instalować na stronach internetowych, oraz moc obliczeniową odwiedzających je do legalnego wydobywania kryptowaluty. Aż do zamknięcia w marcu 2019 r. był intensywnie nadużywany przez cyberprzestępców, którzy instalowali swój kod na zhakowanych witrynach internetowych, by wydobywać kryptowalutę Monero, czerpiąc z tego zyski. Po jego zamknięciu liczba ataków związanych z cryptojackingiem wykorzystującym witryny internetowe spadła w drugiej połowie 2019 r. o 78%[4]. W wyniku tego spadku cyberprzestępcy zaczęli koncentrować się na celach o większej wartości, takich jak potężne serwery[9] i infrastruktury chmurowe[1]. Miejsce Coinhive w czołówce zajęły od tego czasu[9] Jsecoin (22%), XMRig (21%) i Cryptoloot (21%). Udziały najpopularniejszego na świecie złośliwego oprogramowania do cryptominingu przedstawiono na Rysunku 1.

_Więcej ataków na infrastruktury chmurowe

Trend wzrostowy liczby ataków związanych z wydobywaniem kryptowalut na chmurę był widoczny w pierwszej połowie 2019 roku[15,25]. Środowiska chmurowe zwykle wykorzystują mechanizmy dostosowywania zasobów na żądanie, a zatem są lukratywnymi celami dla uruchamiania oprogramowania „wydobywczego". Odbywa się to jednak kosztem właścicieli witryn, którzy muszą płacić wyższe rachunki za przekroczenie limitów[15]. W pierwszej połowie 2019 r. liczba luk w oprogramowaniu kontenerów chmurowych wzrosła o 46% w porównaniu z tym samym okresem w 2018 roku[26]. Atakujący z powodzeniem wykorzystali interfejsy programowania aplikacji (API) i platformy zarządzania kontenerami w celu instalowania złośliwych obrazów (np. Docker i Kubernetes) oraz wydobywania kryptowalut[25].

Incydenty

Kwiecień 2019_ **Kampania cryptojackingowa nazwana Beapy wykorzystała lukę EternalBlue i dotknęła przedsiębiorstwa w Chinach**[3]

Maj 2019_ **Wydobywające kryptowalutę Monero złośliwe oprogramowanie PCASTLE atakowało głównie systemy w Chinach, wykorzystując bezplikowe techniki dostarczania**[19]

Stwierdzono, że ponad 50000 serwerów należących do firm z sektora ochrony zdrowia, telekomunikacji, mediów i IT zostało zainfekowanych przez szkodliwe oprogramowanie wydobywające kryptowalutę TurtleCoin (TRTL)[20].
Nowa rodzina złośliwego oprogramowania o nazwie BlackSquid wykorzystała osiem znanych exploitów, w tym EternalBlue i DoublePulsar, a następnie rozprzestrzeniła się na serwery internetowe w Tajlandii i Stanach Zjednoczonych, aby dostarczyć skrypty wydobywające Monero[17,21].

Sierpień 2019_ **W 11 repozytoriach języka RubyGem znaleziono złośliwe oprogramowanie cryptojackingowe, narażające tysiące użytkowników na kod służący do cryptominingu**[22]

Trendy

_Przesunięcie w stronę cryptominingu opartego na plikach

W 2019 roku zauważono spadek cryptojackingu opartego na przeglądarkach na rzecz cryptominingu opartego na plikach. Ataki cryptominingowe oparte na plikach[27] rozprzestrzeniają się za pośrednictwem złośliwego oprogramowania i wykorzystują istniejące wcześniej exploity w niezaktualizowanych systemach operacyjnych, takie jak EternalBlue i inne luki wysokiego ryzyka. Do tej zmiany przyczyniło się zamknięcie popularnego serwisu dla witryn cryptominingowych Coinhive[1] oraz spadek wartości kryptowalut[10], a także fakt, że cryptomining oparty na plikach jest bardziej wydajny, niż oparty na witrynach i jest 25-krotnie bardziej opłacalny[3]. Cyberprzestępcy zaopatrzyli swoje złośliwe oprogramowanie w dodatkowe narzędzia, by wydobywać poufne informacje z komputerów ofiar.

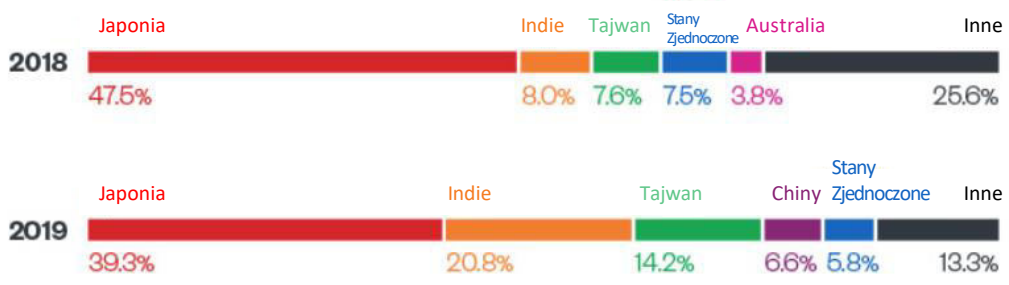
_Liczba ataków typu cryptojacking na całym świecie spada

W roku 2019 zauważono trend spadku[5] liczby ataków cryptojackingowych, głównie ze względu na zamknięcie Coinhive[6], skoordynowane działania organów porządkowych oraz spadek wartości kryptowaluty Monero. Ponieważ jednak intensywność ataków cryptojackingowych zależy od wartości kryptowalut, może pojawić się usługa podobna do Coinhive, powodując nowy skok. Wczesne statystyki za 2020 rok wykazują 30% wzrost rok do roku w marcu.

_Preferowaną kryptowalutą pozostaje Monero

Podobnie jak w przypadku poprzednich trendów, Monero (XMR) było w 2019 roku kryptowalutą preferowaną do działań związanych z cryptojackingiem. Przyczyny są dwie. Po pierwsze, Monero koncentruje się na prywatności i anonimowości, co uniemożliwia śledzenie transakcji. Po drugie, algorytm Proof-of-Work opracowano pod kątem możliwości korzystania ze standardowego procesora, a nie specjalistycznego sprzętu. W trzecim kwartale 2019 r. 32% giełd obracało walutami zapewniającymi prywatność, takimi jak Monero. Jednak spodziewając się nowych przepisów przeciwdziałających praniu pieniędzy, wiele giełd zdecydowało się usunąć waluty chroniące prywatność.

_Najczęściej atakowane kraje



Rysunek 2: Kraje najczęściej atakowane przez cryptojacking. Źródło: Trend Micro[7]

Wektory ataku

_Techniki

Cyberprzestępcy stosowali następujące techniki uruchamiania lub dostarczania kodu wydobywającego kryptowaluty:

- dołączanie funkcji cryptojackingu do istniejącego złośliwego oprogramowania[10];
- atakowanie witryn internetowych[11];
- uporczywe ataki drive-by[12];
- wykorzystanie sieci społecznościowych[13];
- użycie aplikacji mobilnych i sklepów z aplikacjami[14];
- użycie zestawów exploitów[15];
- korzystanie z sieci reklamowych i złośliwych reklam[16];
- użycie nośników wymiennych[17];
- użycie kodu wydobywającego kryptowaluty o charakterze robaka[18].

Rysunek 3: Ile może zarobić botnet do wydobywania kryptowalut w ciągu 30 dni? Źródło: Broadcom[3]

Proponowane działania

- Monitorowanie zużycia energii przez urządzenia użytkowników i, w przypadku podejrzanych skoków wykorzystania procesora, skanowanie pod kątem obecności kodu wydobywającego kryptowaluty opartego na plikach.
- Wdrożenie filtrowania treści, aby usuwać niechciane załączniki, wiadomości e-mail ze złośliwą zawartością i spam.
- Wdrożenie filtrowania protokołu Stratum, używanego przez kod wydobywający kryptowaluty, oraz blokowanie używanych w tym celu adresów IP i domen.
- Ochrona punktów końcowych przez zainstalowanie programów antywirusowych lub wtyczek do przeglądarek blokujących cryptomining.
- Przeprowadzanie regularnych audytów bezpieczeństwa w celu wykrywania anomalii sieciowych.
- Wdrożenie sprawnego zarządzania słabymi punktami i łatkami.
- Użycie białej listy, aby zapobiec uruchamianiu nieznanych plików wykonywalnych na punktach końcowych.
- Inwestowanie w podnoszenie świadomości użytkowników na temat cryptojackingu, zwłaszcza w odniesieniu do bezpiecznego przeglądania internetu.
- Wdrażanie poprawek i aktualizacji przeciwko dobrze znanym exploitom, takim jak EternalBlue, na mniej oczywistych celach, takich jak systemy zarządzania kolejkami, terminale POS, a nawet automaty do sprzedaży.
- Monitorowanie i wciąganie na czarną listę popularnych plików wykonywalnych do wydobywania kryptowalut.

Bibliografia

1. Sergiu Gatlan. „Cryptominers Still Top Threat In March Despite Coinhive Demise" 9 kwietnia 2019 r. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top-threat-in-march-despite-coinhive-demise/

2. „Internet Organised Crime Threat Assessment (IOCTA)". 2019. EUROPOL https://www.europol.europa.eu/iocta-report

3. „Beapy: Cryptojacking Worm Hits Enterprises in China" 24 kwietnia 2019 r. BROADCOM. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

4. Bill Conner. „SONICWALL Cyber Threat Report." 2020. SONICWALL https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. Yessi Bello Perez. „Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019." 24 lipca 2019 r. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-first-half-2019/

6. Ben Noble. „A Third of Cryptocurrency Exchanges Still Host Privacy Coins Despite Fears of Impending FATF Travel Rule." 27 listopada 2019 r. CIPHERTRACE https://ciphertrace.com/ciphertrace-q3-2019-caml-press-release/

7. „Defending Systems Against Cryptocurrency Miner Malware" 28 października 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/be/security/news/cybercrime-and-digital-threats/defending-systems-against-cryptocurrency-miner-malware

8. „Kaspersky Security Bulletin '19 Statistics." 2009. Kaspersky. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf

9. „CYBER SECURITY REPORT" 2020. Check Point Research cp<r>. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

10. Ionut Ilascu. „EternalBlue Exploit Serves Beapy Cryptojacking Campaign." 25 kwietnia 2019 r. Bleeping Computer. https://www.bleepingcomputer.com/news/security/eternalblue-exploit-serves-beapy-cryptojacking-campaign/

11. „New mining worm PsMiner uses multiple high-risk vulnerabilities to spread." 12 marca 2019 r. 360 Total Security. https://blog.360totalsecurity.com/en/new-mining-worm-psminer-uses-multiple-high-risk-vulnerabilities-to-spread/

12. Dan Thorp-Lancaster. „New drive-by cryptocurrency mining scheme persists after you exit your browser window" 9 listopada 2017 r. Windows Central. https://www.windowscentral.com/new-drive-cryptocurrency-mining-scheme-persists-even-after-you-exit-your-browser-window

13. Dr Michaeal McGuire. „Social Media Platforms and the Cybercrime Economy" 2019. Bromium. https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

14. Axelle Apvrille. „Abusing cryptocurrencies on Android smartphones" 2019. Fortinet. https://fortinetweb.s3.amazonaws.com/fortiguard/research/currency-insomnihack19.pdf

15. „2019 Midyear Security Roundup Evasive Treats Pervasive Effects" 2019. TrendMicro https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

16. Margi Murphy. „YouTube shuts down hidden cryptojacking adverts" 29 stycznia 2018 r. The Telegraph https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/

17. Matthew Beedham. „New cryptocurrency mining malware is spreading across Thailand and the US" 4 czerwca 2019 r. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/06/04/security-crypto-jacking-mining-malware/

18. Sean Lyngaas. „BlueKeep is back. For now, attackers are just using it for cryptomining" 4 listopada 2019 r. CyberScoop. https://www.cyberscoop.com/bluekeep-exploited-cryptomining/

19. Janus Agcaoili. „Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques" 5 czerwca 2019 r. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/

20. Marie Huillet. „Researchers Say 50,000 Servers Worldwide Infected With Privacy Coin Cryptojacking Malware" 29 maja 2019 r. Cointelegraph. https://cointelegraph.com/news/researchers-say-50-000-servers-worldwide-infected-with-privacy-coin-cryptojacking-malware

21. Johnlery Triunfante, Mark Vicente. „BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner" 27 sierpnia 2019 r. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/

22. „Malicious cryptojacking code found in 11 Ruby libraries" 2 sierpnia 2019 r., Decrypt. https://decrypt.co/8602/malicious-cryptjacking-code-found-in-11-ruby-libraries

23. Brook Chelmo. „Cryptojacking in 2019: Cryptocurrency Value Keeping Attack Vector in Play" 6 sierpnia 2019 r. SonicWall. https://blog.sonicwall.com/en-us/2019/08/cryptojacking-in-2019-cryptocurrency-value-keeping-attack-vector-in-play/

24. Catalin Cimpanu. „Coinhive cryptojacking service to shut down in March 2019". 27 lutego 2019 r. ZD Net. https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/

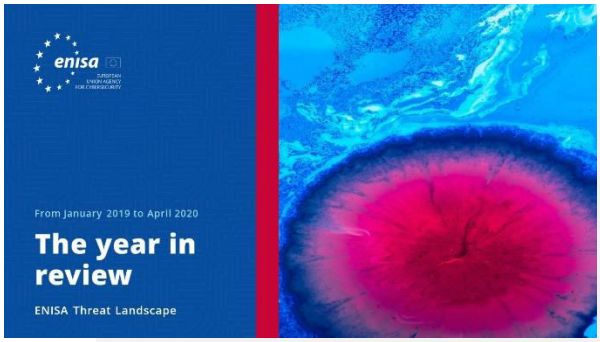
25. Tom Hegel. „Making it Rain - Cryptocurrency Mining Attacks in the Cloud". 14 marca 2019 r. AT&T Business. https://cybersecurity.att.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/

26. „How a Prominent Cryptomining Botnet is Paving the Way for a Lucrative and Illicit Revenue Model". Sierpień 2019 r. Carbon Black. https://www.carbonblack.com/resources/access-mining/

27. „Cryptojacking Attacks: Who's Mining on Your Coin?". 5 kwietnia 2019 r. Security Intelligence. https://securityintelligence.com/cryptojacking-attacks-whos-mining-on-your-coin/

28. „Malware Creates Cryptominer Botnet Using EternalBlue and Mimikatz". 12 kwietnia 2019 r. Bleeping Computer. https://www.bleepingcomputer.com/news/security/malware-creates-cryptominer-botnet-using-eternalblue-and-mimikatz/

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**

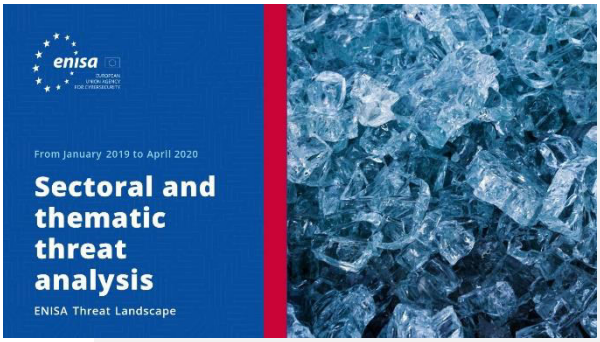
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu