enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Złośliwe oprogramowanie

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

Informacje ogólne

Złośliwe oprogramowanie to cyberatak, do którego wykorzystuje się złośliwe oprogramowanie. Wśród odmian złośliwego oprogramowania można wymienić oprogramowanie do wydobywania kryptowalut, wirusy, oprogramowanie ransomware, robaki i programy szpiegujące. Ich wspólne cele to kradzież informacji albo tożsamości, szpiegostwo i dezorganizacja usług[1].

W roku 2019 oprogramowanie do wydobywania kryptowalut stanowiło dominujący gatunek złośliwego oprogramowania w krajobrazie zagrożeń[2], skutkując wysokimi kosztami obsługi informatycznej, zwiększonym zużyciem energii elektrycznej i zmniejszoną wydajnością pracowników[3]. Odnotowano nieco większą liczbę wystąpień oprogramowania ransomware w 2019 r. w porównaniu z 2018 r., lecz nadal plasuje się ono w dolnej części listy złośliwego oprogramowania[2].

Protokoły internetowe i dotyczące poczty e-mail stanowiły najczęstszy początkowy wektor ataku używany do rozprzestrzeniania złośliwego oprogramowania. Niektóre rodziny złośliwego oprogramowania były jednak w stanie bardziej rozpowszechnić się w sieci wskutek stosowania technik ataku siłowego lub wykorzystywania luk w systemie. Choć liczba globalnych przypadków wykrycia ataku utrzymała się na poziomie z poprzedniego roku, dała się zauważyć wyraźna zmiana z celów konsumenckich na biznesowe[4].

Wnioski

400 000 wykrytych przypadków zainstalowanego uprzednio oprogramowania szpiegowskiego i reklamowego na urządzeniach mobilnych[4]

13% wzrost liczby wykrytych przypadków złośliwego oprogramowania dla systemu Windows w biznesowych punktach końcowych na całym świecie[4]

71% organizacji doświadczyło działania złośliwego oprogramowania, które rozprzestrzeniało się od jednego pracownika do drugiego[47]

46,5% wszystkich przypadków złośliwego oprogramowania we wiadomościach e-mail wykryto w plikach typu „.docx”[24]

50% wzrost liczby odnotowanych przypadków oprogramowania stworzonego w celu wykradania danych osobowych lub prześladowania innych użytkowników[15]

67% złośliwego oprogramowania przesłano z użyciem szyfrowanych połączeń HTTPS[48]

Kill chain

Proces etapów ataku

Zakres działania

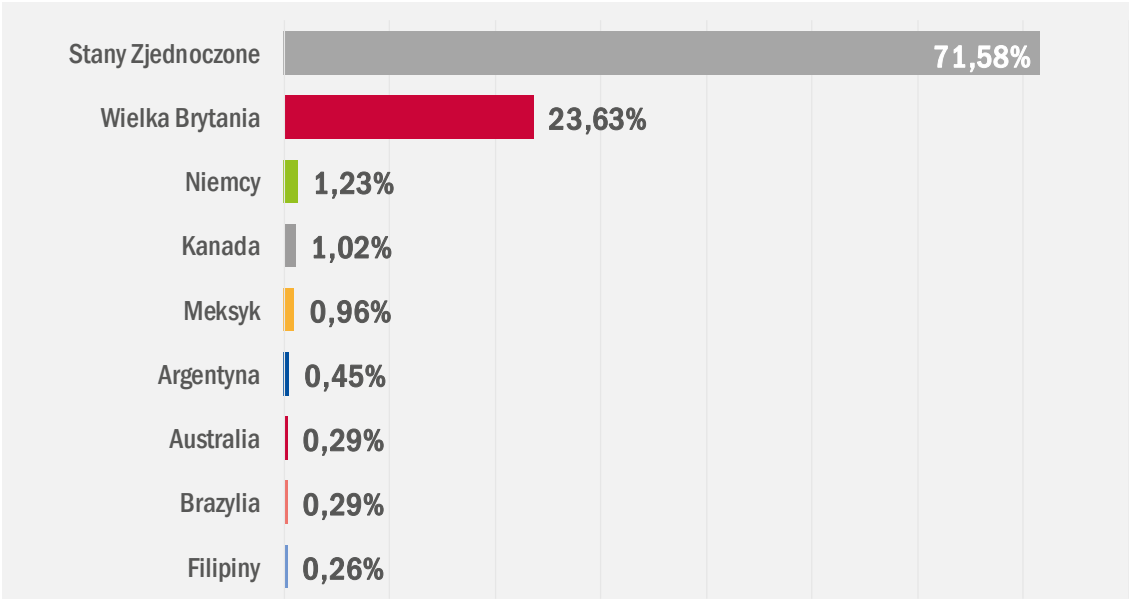
Rozwiązanie Cyber Kill Chain® zostało opracowane przez Lockheed Martin na podstawie wojskowej koncepcji związanej ze strukturą ataku. Aby zbadać określony wektor ataku, należy użyć poniższego schematu Cyber Kill Chain w celu stworzenia mapy każdego etapu procesu i określić narzędzia, techniki i procedury,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

WIĘCEJ INFORMACJI

Najczęściej spotykane rodzaje złośliwego oprogramowania

Najczęściej spotykanym szczepem złośliwego oprogramowania w 2019 r. był Emotet, który w 2020 r. nadal ewoluuje. Emotet to bankowy koń trojański, który po raz pierwszy wykryto w 2014 r. Od tego czasu został on wzbogacony o funkcję zarządzania i kontroli (Command & Control, C2), dodatkowe mechanizmy unikania, jak sprawdzanie, czy pracuje w środowisku piaskownicy oraz możliwość dostarczania niebezpiecznego oprogramowania, jak Trickbot i Ryuk[7]. Powyższa ilustracja przedstawia ranking złośliwego oprogramowania bankowego wykrytego w 2019 r.

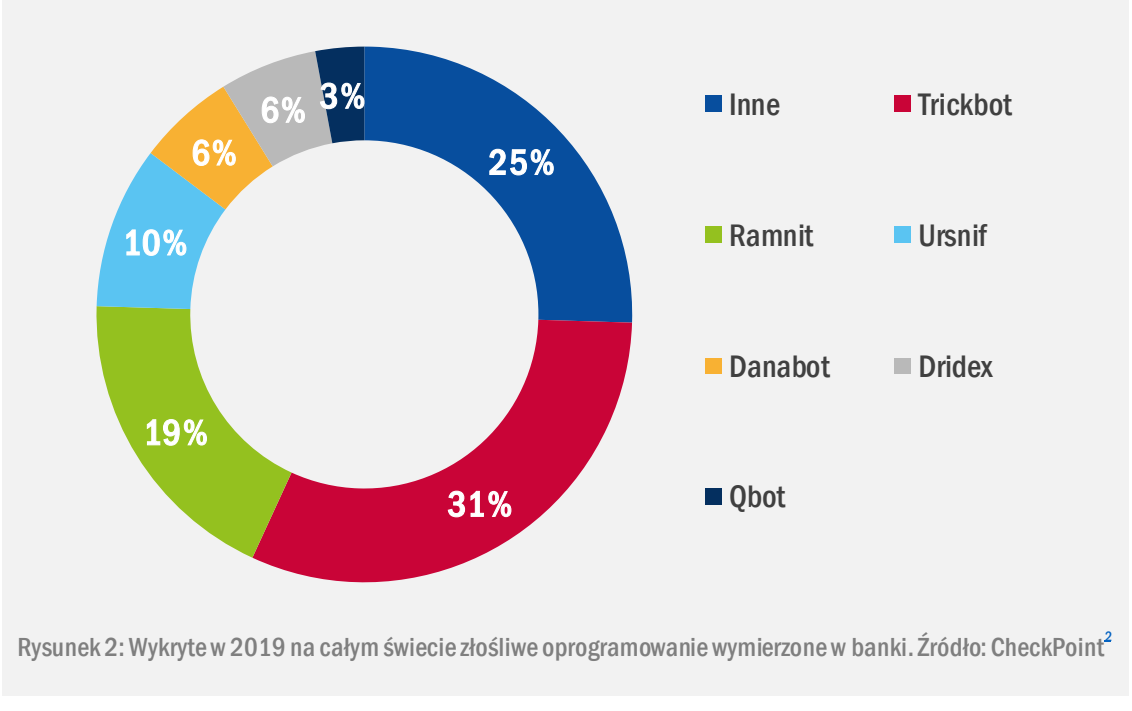
W okresie objętym raportem Emotet ewoluował, zmieniając się w botnet[2], zwiększył aktywność[8] i zainicjował nowe, lokalne kampanie rozsyłania spamu z użyciem profilowanego wyłudzania informacji, by instalować oprogramowanie ransomware lub wykradać informacje[5]. W 2019 r. liczba wykrytych przypadków Emotet wzrosła o 73% w porównaniu z poprzednim rokiem; oprogramowanie to obrało za cel głównie punkty końcowe firm w Stanach Zjednoczonych i Wielkiej Brytanii, zgodnie z poniższym wykresem[4].



Rysunek 1: Odsetek wykrytych przypadków konia trojańskiego Emotet w 2019 r. z podziałem na kraje. Źródło: MalwareBytes[4]

Zmiana na rzecz celów biznesowych

Choć liczba wykrytych przypadków złośliwego oprogramowania w 2018 r. pozostawała na tym samym poziomie[4,9], zaobserwowano wzrost o 13% w przypadku liczby przypadków złośliwego oprogramowania biorącego na cel organizacje z sektora usług, edukacji i handlu detalicznego, z uwzględnieniem najbardziej dotkniętych sektorów[4]. Przypuszcza się, że ponad jedna trzecia ataków z użyciem złośliwego oprogramowania wymierzonego w banki w 2019 r. była skierowana przeciwko użytkownikom z sektora przedsiębiorstw i miała na celu narażenie na szwank zasobów finansowych firm[10]. Pięć najczęściej spotykanych szczepów złośliwego oprogramowania[4], które miały uderzyć w firmy, to Trojan.Emotet, Adware.InstallCore, HackTool.WinActivator, Riskware.BitCoinMiner i Virus.Renamer. Liczba przypadków oprogramowania ransomware wymierzonego przeciwko sektorowi publicznemu wzrosła w 2019 r. z powodu zdolności tego sektora do wypłacania większych okupów[11]. Ponieważ cyberprzestępcy uderzają w cele o większej wartości, zaprojektowano nowe rodzaje złośliwego oprogramowania, które mają rozprzestrzeniać się poziomo w sieci firmowej, a nie przez internet[12].



Rysunek 2: Wykryte w 2019 na całym świecie złośliwe oprogramowanie wymierzone w banki. Źródło: CheckPoint[2]

Trendy

_ Malware-as-a-service (MaaS)

Termin malware-as-a-service (MaaS) odnosi się do szczególnego złośliwego oprogramowania sprzedawanego na ukrytych forach, oferujących klientom (cyberprzestępcom) narzędzia i infrastrukturę niezbędne do profilowanych ataków. Właściciel MaaS świadczy usługi, dostarczając zestaw składający się z początkowego modułu ładującego, serwera zarządzania i kontroli (C2) oraz tylnego wejścia do przejęcia kontroli nad zarażonym komputerem.

Analityk bezpieczeństwa[13] niedawno zidentyfikował cztery rodzaje ataków z wykorzystaniem różnych narzędzi z portfolio Malware-as-a-Service (MaaS) o nazwie Golden Chickens (GC), potwierdzając opublikowanie ulepszonych wariantów z aktualizacją kodu do trzech z tych narzędzi.

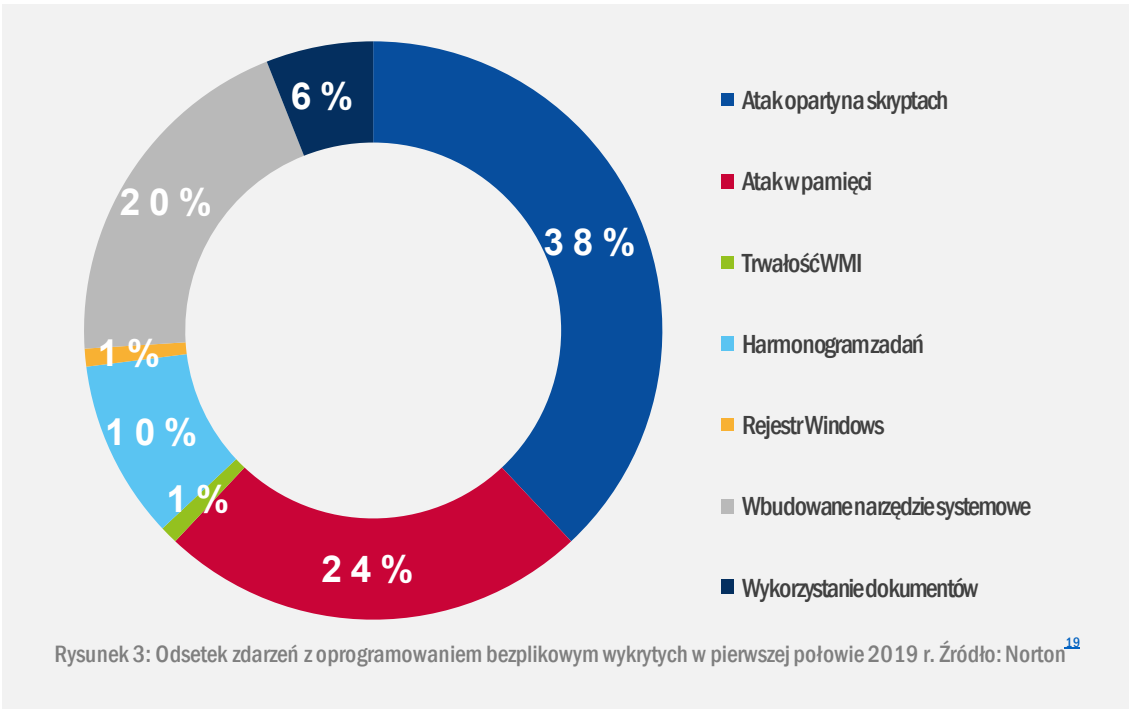
- **TerraLoader**. Wielofunkcyjny moduł ładujący napisany w języku PureBasic. TerraLoader to flagowy produkt w ofercie usług MaaS GC.
- **more_eggs**. Złośliwe oprogramowanie typu backdoor, z funkcją wysyłania sygnałów do stałego serwera C2 i wykonywania dodatkowych programów pobranych z zewnętrznego zasobu sieciowego. Moduł typu backdoor napisano w języku JavaScript.
- **VenomLNK**. Plik skrótu w Windows prawdopodobnie generowany przez nowszą wersję zestawu do samodzielnego montażu VenomKit.

Złośliwe oprogramowanie wymierzone w banki, przeznaczone dla urządzeń mobilnych: gwałtowny wzrost

W pierwszej połowie 2019 r. liczba aplikacji mobilnych służących do wykradania danych o płatnościach, poświadczeń i funduszy z rachunków bankowych ofiar wzrosła o 50%[14]. Sprawcy zagrożeń stosowali tradycyjnie techniki wyłudzania informacji do zdobycia poświadczeń bankowych poprzez wyświetlenie fałszywej strony naśladującej stronę logowania do banku albo poprzez wprowadzanie fałszywych aplikacji mobilnych przypominających oryginalne aplikacje bankowe. W 2019 r. cyberprzestępcy stali się jednak bardziej kreatywni, jak w przypadku Trojan-Banker.AndroidOS.Gustuff.a, który był w stanie kontrolować legalną aplikację bankową, nadużywając funkcji dostępności systemu operacyjnego, automatyzując w ten sposób złośliwe transakcje[15]. Nowe wersje złośliwego oprogramowania wymierzonego w instytucje finansowe, przeznaczonego dla urządzeń mobilnych, były często oferowane na sprzedaż na ukrytych forach[15]; ciągle rozwijano też nowe techniki unikania wykrycia. Istotnym nowym dodatkiem odkrytym w 2019 r. była możliwość wykorzystywania przez złośliwe oprogramowanie czujników ruchu, by uruchamiało się tylko wtedy, gdy smartfon się porusza, jak w przypadku wirusa bankowego dla urządzeń mobilnych trojanAnubis; miała ona na celu wykrywanie środowiska piaskownicy[16]. Najpopularniejsze złośliwe programy wymierzone w banki w 2019 r.[11] to Asacub (44,4%), Svpeng (22,4%), Agent (19,1%), Faketoken (12%) i Hqwar (3,8%).

_Bezplikowe złośliwe oprogramowanie

Bezplikowe złośliwe oprogramowanie nie zawiera plików i może łatwo przenikać przez filtry zabezpieczające i pokonywać techniki umieszczania na białej liście. Dlatego też złośliwe oprogramowanie z tej rodziny może być aż dziesięciokrotnie skuteczniejsze od innych[18]. Oprogramowanie to nie zawiera pliku wykonywalnego, więc wymaga od atakującego wstrzyknięcia złośliwego kodu do już zainstalowanego i zaufanego oprogramowania, zdalnie (np. w przypadku instrumentacji zarządzania Windows (WMI) lub PowerShell)[19]. Po skutecznym ataku złośliwe oprogramowanie zagnieżdża się trwale, używając do tego celu rejestru, wbudowanego harmonogramu zadań lub WMI. Liczba przypadków bezplikowego złośliwego oprogramowania wzrosła o 265% w pierwszej połowie 2019 r.[20] Większość takich ataków była oparta na skryptach (38%), zaś inne przeprowadzały atak w pamięci (24%) lub nadużywały wbudowanych narzędzi systemowych (20%)[21].



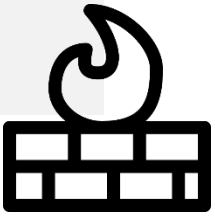
Rysunek 3: Odsetek zdarzeń z oprogramowaniem bezplikowym wykrytych w pierwszej połowie 2019 r. Źródło: Norton[19]

Jak zapobiegać atakom bezplikowym i bronić się przed nimi?

Najskuteczniejszym sposobem obrony organizacji przed atakami bezplikowymi jest aktualizowanie oprogramowania. Ponieważ do największej liczby infekcji bezplikowych dochodzi w przypadku aplikacji Microsoft, szczególnie z użyciem plików „.docx", niezwykle ważne jest częste aktualizowanie tego oprogramowania do najnowszej wersji. Firma Microsoft zaktualizowała także pakiet Windows Defender, by wykrywał nietypową aktywność z wykorzystaniem aplikacji PowerShell.

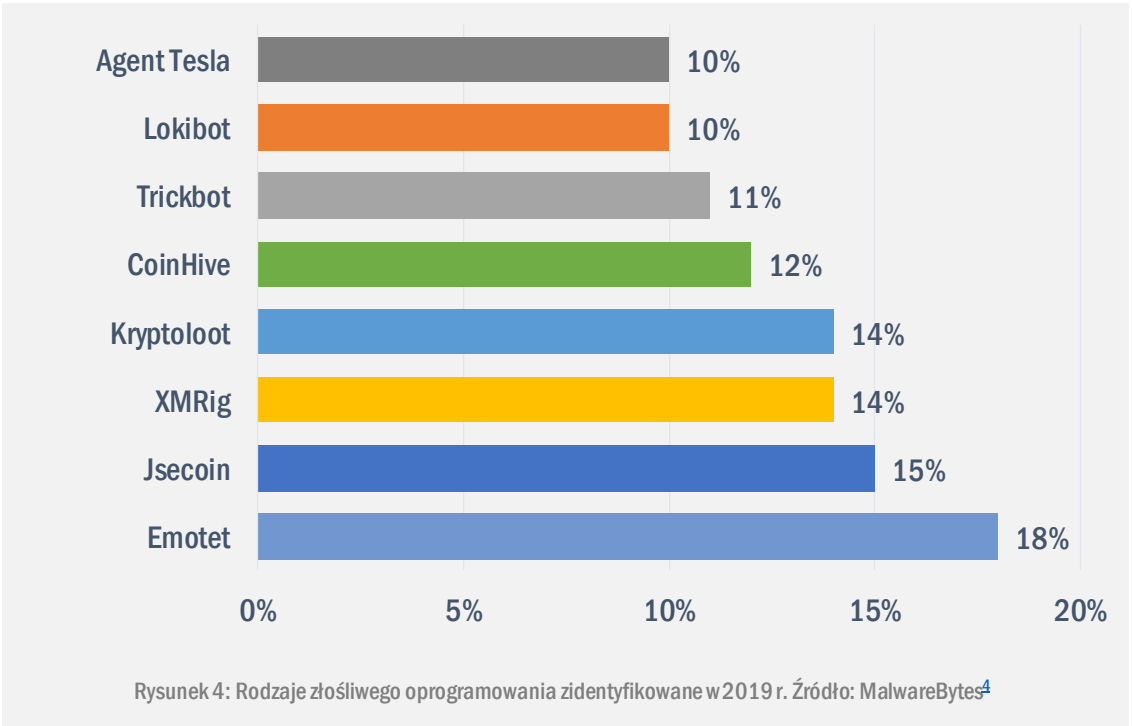
Zdaniem analityka bezpieczeństwa[18], kluczem do skutecznego przeciwdziałania atakom jest podjęcie działań przeciwko każdej fazie cyklu życia zagrożenia ze zintegrowanym i wielopoziomowym podejściem do obrony. W ramach tego podejścia istotne jest przemieszczanie się między różnymi etapami ataku i podejmowanie następujących działań:

- analiza i pomiar działań wykonywanych przez atakującego;
- identyfikacja zastosowanych technik;
- monitowanie aktywności aplikacji PowerShell lub innych silników skryptowych;
- dostęp do zagregowanych danych zagrożeń;
- kontrolowanie stanu zagrożonego systemu;
- wstrzymywanie arbitralnych procesów;
- przeciwdziałanie procesom stanowiącym element ataku;
- izolowanie zainfekowanych urządzeń.



_Krajobraz botnetów zarządzania i kontroli (Command and Control – C&C)

Ogólny ruch botnetów na całym świecie zwiększył się o 71,5% od 2018 r.[2] Najczęściej obserwowanymi botnetami były Emotet (41%), Trickbot (25%) i DanaBot (5%)[2]. W Rosji zaobserwowano znaczny wzrost ruchu generowanego przez botnety (143%), spowodowany głównie złagodzeniem procedur rejestracji i mniejszym zainteresowaniem ze strony organów ścigania[14]. W roku 2019 większość botnetów typu C2 pochodziła z Rosji, a dalej uplasowały się Stany Zjednoczone, Holandia, Chiny i Francja. Przestępcy wykorzystywali algorytmy generowania domen (DGA) do obsługi komunikacji C2. Połowa tych rejestracji miała miejsce w przypadku domen najwyższego poziomu (TLD) „.com" i „.net"[15]. W okresie objętym raportem liczba takich rejestracji domen spadła o 71% z korzyścią na rzecz innych protokołów, jak peer-to-peer (P2P)[13].



Rysunek 4: Rodzaje złośliwego oprogramowania zidentyfikowane w 2019 r. Źródło: MalwareBytes[4]

_Jak

Według badania z 2019 r. 94% wszystkich rodzajów złośliwego oprogramowania zostało dostarczonych za pośrednictwem poczty e-mail[24]. Chociaż pocztę e-mail zalicza się do wektorów punktu dostępowego, warto zauważyć, że po udanym ataku złośliwe oprogramowanie może pobrać kolejną porcję oprogramowania, która przejawia zachowania podobne do robaka, by rozpowszechniać się w sieci w sposób poziomy (Emotet i Trickbot). Ponadto po początkowym wprowadzeniu złośliwego oprogramowania w większości przypadków (71%) rozprzestrzeniało się ono wskutek działań pracowników. Po raz kolejny nowe luki w protokole zdalnego pulpitu (RDP) znalazły się w centrum uwagi, gdyż umożliwiają one zdalne wykonywanie kodu (RCE), a zatem zmianę w robaka[30]. Choć te nowo odkryte luki nie zostały wykorzystane na dużą skalę, przypuszcza się, że nowy robak może w niedalekiej przyszłości atakować systemy, w których nie zainstalowano poprawek[31].

_Incydenty

- Koncern **Airbus** padł ofiarą naruszenia danych, które dotknęło pracowników w Europie[34, 35].
- Złośliwe oprogramowanie kopiujące dane kart płatniczych zainstalowane w witrynie **American Medical Collection Agency** umożliwiło kradzież danych osobowych 12 milionów pacjentów[36].
- Liczący się dostawca wyposażenia do diagnostyki laboratoryjnej, **LifeLabs**, padł ofiarą ataku z użyciem oprogramowania ransomware, skutkującego przejęciem 15 milionów kont zawierających wyniki badań i numery kartotek pacjentów[37,38].
- Atak z użyciem złośliwego oprogramowania przeprowadzony w **City of Pensacola, w stanie Floryda**, spowodował udostępnienie w sieci 2 GB danych, które mogły zawierać dane osobowe[39].
- Wyłudzanie informacji z użyciem złośliwego oprogramowania przesyłanego pocztą e-mail mogło doprowadzić do wycieku danych 2400 **członków singapurskich sił zbrojnych**[40].

Ograniczenie ryzyka

Proponowane działania

- Wdrożenie wykrywania złośliwego oprogramowania dla wszystkich kanałów przychodzących i wychodzących, w tym poczty elektronicznej, sieci, systemów sieciowych i aplikacji na wszystkich odpowiednich platformach (tj. serwerach, infrastrukturze sieciowej, komputerach osobistych i urządzeniach mobilnych).
- Kontrola ruchu SSL/TLS umożliwiająca zaporze deszyfrowanie danych przesyłanych do witryn i z nich, komunikacji z użyciem poczty e-mail oraz aplikacji mobilnych.
- Stworzenie interfejsów między funkcjami wykrywania złośliwego oprogramowania (polowanie na zagrożenia ukierunkowane przez wywiad) oraz zarządzanie incydentami bezpieczeństwa w celu stworzenia skutecznych możliwości reagowania.
- Użycie dostępnych narzędzi do analizy złośliwego oprogramowania w celu udostępniania informacji o nim i przeciwdziałania mu (np. MISP)[32].
- Stworzenie zasad bezpieczeństwa określających procesy, zgodnie z którymi należy postępować w przypadku infekcji.
- Zapoznanie się z możliwościami, jakie oferują różne narzędzia zabezpieczające i tworzenie nowych rozwiązań z dziedziny bezpieczeństwa. Identyfikacja luk i stosowanie zasady ochrony głębokiej.
- Stosowanie filtrowania poczty (lub filtrowania spamu) pod kątem złośliwych wiadomości e-mail i usuwania wykonywalnych załączników.
- Regularne monitorowanie wyników testów antywirusowych[30,42].
- Monitorowanie dzienników z użyciem rozwiązania z dziedziny zarządzania incydentami i zdarzeniami (SIEM). Sugerowanymi źródłami danych dziennika są ostrzeżenia antywirusowe, punkty końcowe wykrywania i reagowania (EDR), dzienniki serwera proxy, dzienniki zdarzeń Windows i monitora systemu[43], dzienniki systemu wykrywania nieautoryzowanego dostępu (IDS)[44] itp.
- Wyłączanie funkcji PowerShell lub ograniczenie dostępu do nich[45].

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

w: ETL 2020

Bibliografia

1. „What is Malware". Veracode. https://www.veracode.com/security/malware
2. „Cyber Security Report". 2019. Checkpoint. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf
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. „2020 State of Malware Report". Luty 2020 r. Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
5. „Evasive Threats, Pervasive Effects" 2019. Trend Micro, Research. https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf
6. „SonicWall Cyber Threat Report". 2020. SonicWall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/
7. „Emotet is back: botnet springs back to life with new spam campaign". 16 września 2019 r. Malwarebytes Labs. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/
8. „Increased Emotet Malware Activity" 22 stycznia 2020 r. US CERT. https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity
9. „SonicWall Security Metrics" SonicWall. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics
10. „Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". 16 kwietnia 2019 r. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection
11. „Internet organised crime threat assessment", 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf
12. „Narrowed Sights, Bigger Payoffs: Ransomware in 2019", 6 czerwca 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019
13. „GOLDEN CHICKENS: Evolution of the MaaS". 20 lipca 2020 r. QuoIntelligence. https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
14. „From Supply Chain to Email, Mobile and the Cloud", 25 lipca 2019 r. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/
15. „Mobile malware evolution 2019". 25 lutego 2020 r. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/
16. „Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics". 17 stycznia 2019 r. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/
17. „Spamhaus Botnet Threat Report 2019". 28 stycznia 2020 r. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019
18. „What Is Fileless Malware?". McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html
19. „What is fileless malware and how does it work?". Norton. https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html
20. „Trend Micro Report Reveals 265% Growth In Fileless Events". 28 sierpnia 2019 r. Trend Micro. https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2019/2019-08-28.html
21. „Understanding Fileless Threats", 29 lipca 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats

22. „SonicWall Sees Dramatic Jump In IoT Malware, Encrypted Threats, Web App Attacks Through Third Quarter". 22 października 2019 r. SonicWall. https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/

23. „2020 Vulnerability and Threat Trends". 2020. SKYBOX. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020_VT_Trends-Report-reduced.pdf

24. „Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". 16 kwietnia 2019 r. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

25. „Internet organised crime threat assessment", 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

26. „Narrowed Sights, Bigger Payoffs: Ransomware in 2019", 6 czerwca 2019 r. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

27. „From Supply Chain to Email, Mobile and the Cloud", 25 lipca 2019 r. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

28. „Mobile malware evolution 2019". 25 lutego 2020 r. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

29. „Mobile banking malware surges in 2019". 25 lipca 2019 r. ComputerWeekly. https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

30. „Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics". 17 stycznia 2019 r. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

31. „BlueKeep attacks are happening, but it's not a worm". 3 listopada 2019 r. ZDNet. https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/

32. MISP Projects. http://www.misp-project.org/

33. „PowerShell, fileless malware's great attack vector". 25 lutego 2919 r. Panda. https://www.pandasecurity.com/mediacenter/malware/powershell-fileless-malware-attack-vector/

34. „Airbus Statement on Cyber Incident". 30 stycznia 2019 r. Airbus. https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html

35. „Airbus data breach impacts employees in Europe", 30 stycznia 2019 r. ZDNet. https://www.zdnet.com/article/airbus-data-breach-impacts-employees-in-europe/

36. „Massive Quest Diagnostics data breach impacts 12 million patients". 4 czerwca 2019 r. ZDNet. https://www.zdnet.com/article/massive-quest-diagnostics-data-breach-impacts-12-million-patients/

37. „Hackers crack 15M LifeLabs accounts, obtain lab results and health card numbers". 17 grudnia 2019 r. Daily Hive. https://dailyhive.com/calgary/lifelabs-hacked-cyber-attack

38. „Why the LifeLabs Hack Likely Is Worse than Most". 18 grudnia 2019 r. The Tyee. https://thetyee.ca/Analysis/2019/12/18/LifeLabs-Data-Hack/

39. „Personal Information in City of Pensacola Cyberattack". 17 stycznia 2020 r. City of Pensacola. https://www.cityofpensacola.com/CivicSend/ViewMessage/Message/100944

40. „Personal data of 2,400 Mindef, SAF staff may have been leaked", 22 grudnia 2019 r. The Straits Times – Singapur. https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

Bibliografia

41. AVTEST – The Independent IT-Security Institute. https://www.av-test.org/en/

42. „Real world protection tests". AV Comparatives. https://www.av-comparatives.org/dynamic-tests/

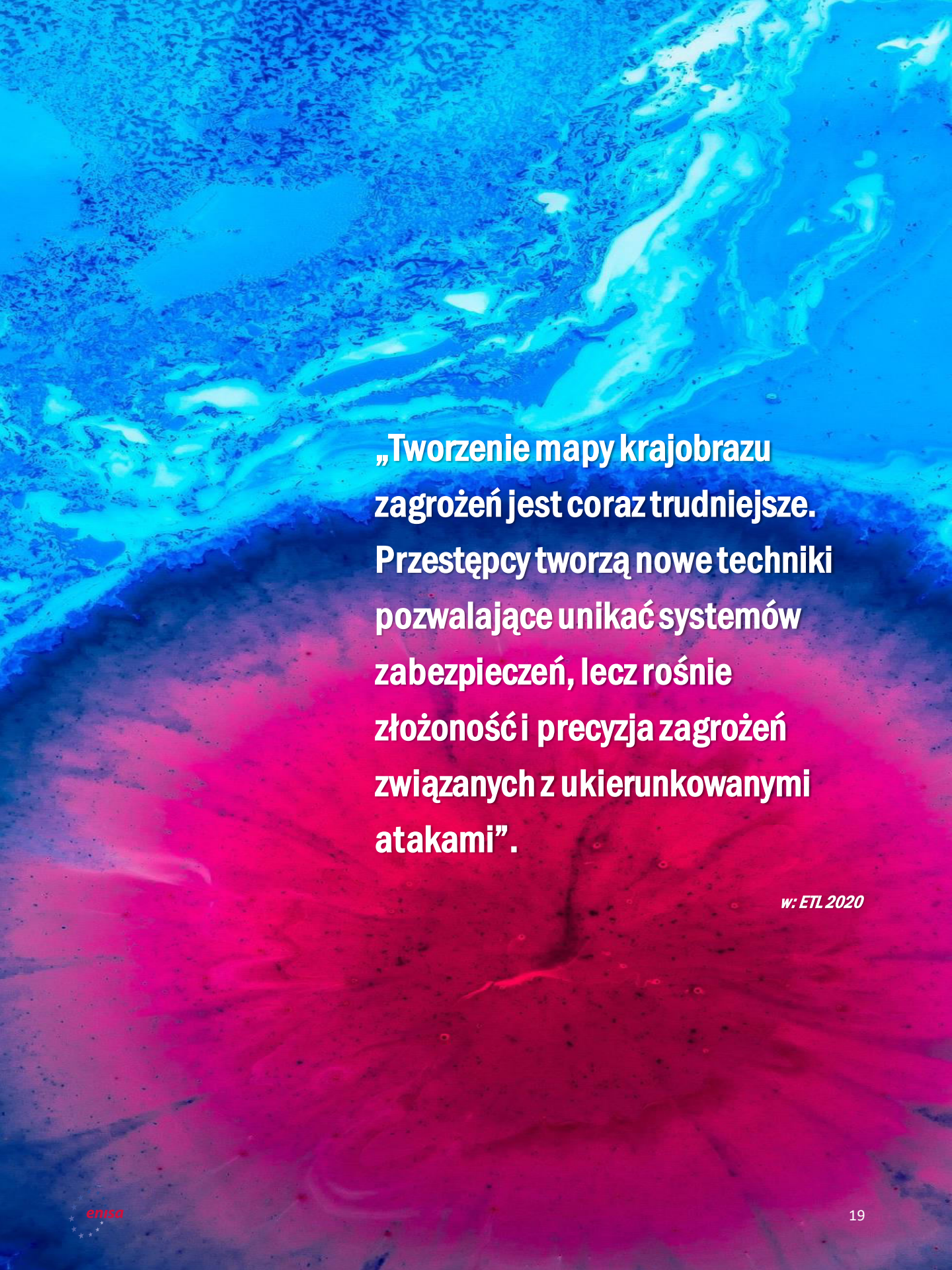
43. „The ThreatHunting Project". https://www.threathunting.net/data-index

44. Mark Russinovich, Thomas Garnier. „Sysmon v11.10". 24 czerwca 2020 r. Microsoft. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

45. „Guide to Intrusion Detection and Prevention Systems (IDPS)". Luty 2007 r. CSRC. https://csrc.nist.gov/publications/detail/sp/800-94/final

47. „Most malware in Q1 2020 was delivered via encrypted HTTPS connections". 25 czerwca. 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

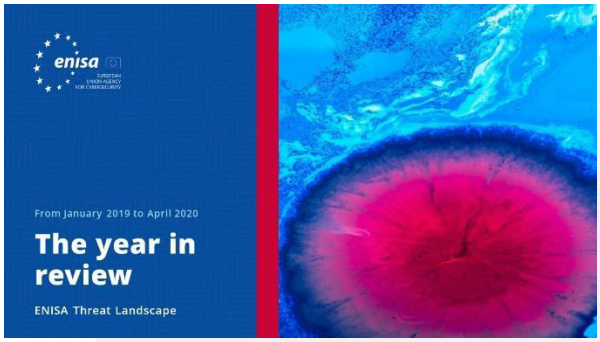
48. „Malware statistics and facts for 2020", 29 lipca 2020 r. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/



„Tworzenie mapy krajobrazu zagrożeń jest coraz trudniejsze. Przestępcy tworzą nowe techniki pozwalające unikać systemów zabezpieczeń, lecz rośnie złożoność i precyzja zagrożeń związanych z ukierunkowanymi atakami”.

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

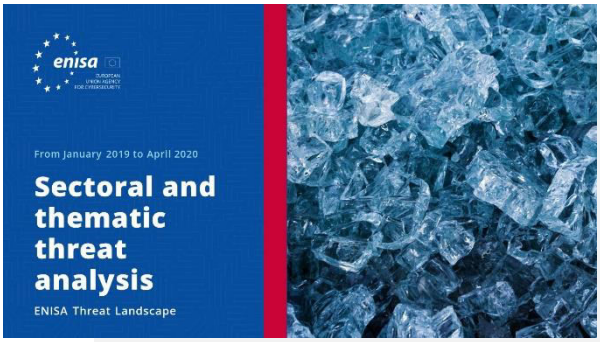
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu