enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Najważniejsze incydenty w UE i na świecie

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

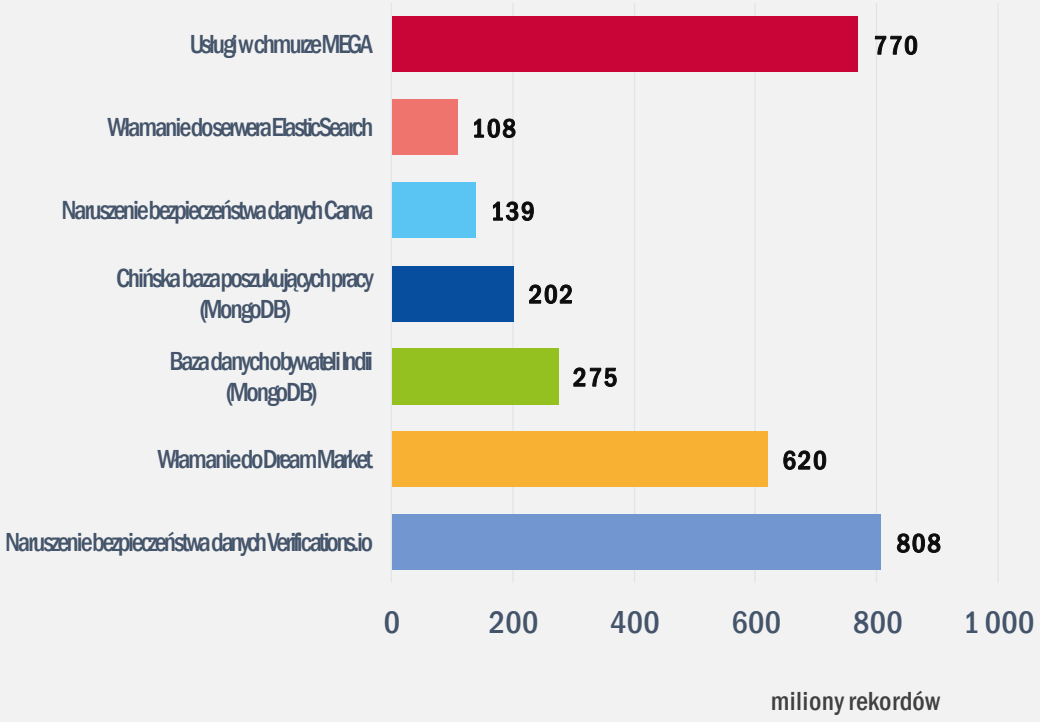
Informacje ogólne

Rok 2019 przyniósł wzrost wyrafinowania potencjalnych zagrożeń w związku z używaniem przez wielu cyberprzestępców exploitów, kradzieży poświadczeń i ataków wieloetapowych. Liczba incydentów naruszenia bezpieczeństwa danych jest wciąż bardzo wysoka, a ilość skradzionych informacji finansowych i poświadczeń użytkowników rośnie. W niektórych przypadkach niezałatanie – w rozsądnych ramach czasowych – znanej luki w zabezpieczeniach, mogącej mieć wpływ na używane oprogramowanie lub biblioteki, może mieć poważne konsekwencje.

W ciągu ostatniej dekady **szkodliwe oprogramowanie znalazło się na liście 15 największych zagrożeń ENISA, ale wciąż wiele systemów bezpieczeństwa nie jest w stanie wykryć tego zagrożenia**. Przez wiele lat złośliwe oprogramowanie było rozprzestrzeniane głównie za pośrednictwem poczty elektronicznej w postaci złośliwego spamu, zaś ostatnio przy użyciu precyzyjnie spreparowanych wiadomości phishingowych. Firmy technologiczne i dostawcy usług poczty e-mail zainwestowali w filtry antyspamowe, poprawiając wykrywanie złośliwych załączników. Jednak **cyberprzestępcy wprowadzają innowacje, by zwiększyć swoje szanse na dotarcie do potencjalnych ofiar**. Wiele z tych innowacji opłaciło się w tym okresie sprawcom szkodliwych działań.

Pandemia COVID-19 wywarła presję na podmioty opieki zdrowotnej i ich pracowników na całym świecie, a ochrona zdrowia stała się jednym z najważniejszych sektorów wymagających ochrony przed cyberatakami. Liczba incydentów związanych z oprogramowaniem typu ransomware atakującym sektor ochrony zdrowia była wysoka już wcześniej, ale podczas pandemii wzrosła.

Najczęstsze incydenty naruszenia bezpieczeństwa danych



Chronologia

2019

_ Styczeń

Naruszenie bezpieczeństwa danych chmury MEGA w Nowej Zelandii spowodowało ujawnienie 770 milionów wiadomości e-mail i 21 milionów haseł[1].

_ Luty

Z serwerów amerykańskiej firmy Verification.io wyciekło ok. 800 milionów rekordów[2].

_ Marzec

Norweska firma Norsk Hydro stała się ofiarą oprogramowania typu ransomware[3].

_ Październik

Witryny internetowe i narodowa telewizja Gruzji padły ofiarą skoordynowanego cyberataku[30].

_ Wrzesień

Firma Mastercard w Belgii doznała naruszenia bezpieczeństwa danych, które dotknęło ok. 90 tys. klientów w Europie[9].

_Sierpień

W bułgarskim urzędzie podatkowym doszło do naruszenia bezpieczeństwa danych, w wyniku czego ujawnione zostały dane osobowe wszystkich dorosłych obywateli kraju[8].

_ Listopad

Włoski UniCredit stał się ofiarą wycieku danych – ujawnieniu uległy 3 miliony rekordów[10].

_ Grudzień

Działanie hiszpańskiej firmy Prosegur zakłócił atak oprogramowania typu ransomware[11].

2020

_ Styczeń

Celem cyberataku stało się Ministerstwo Spraw Zagranicznych Austrii[12].

_ Kwiecień

Facebook (USA) zgłosił naruszenie bezpieczeństwa danych, w wyniku którego z serwerów wyciekło 540 mln rekordów użytkowników[4].

_ Maj

Niemieckie firmy Thyssen-Krupp i Bayer zostały zaatakowane przez oprogramowanie szpiegowskie[5].

_ Lipiec

Firma City Power z RPA padła ofiarą ataku typu ransomware, co zakłóciło dostawy energii w Johannesburgu[7].

_ Czerwiec

Pięć szpitali w Rumunii zostało zaatakowanych przez ransomware Badrabbit[6].

_ Luty

Chorwacka INA Group padła ofiarą ataku typu ransomware[13].

_ Marzec

Cyberprzestępcy włamali się do sieci ENTSO-E w Belgii[14].

_ Kwiecień

Dane ponad 500 tys. kont Zoom (USA) wystawiono na sprzedaż w „ciemnej sieci" (dark web)[31].

Najczęściej atakowane sektory

Na linii ognia

Sektorami najczęściej atakowanymi w tym okresie były usługi cyfrowe, administracja rządowa i branża technologiczna. Atakowani dostawcy usług cyfrowych są często wykorzystywani jako etap pośredni w osiągnięciu innych, bardziej atrakcyjnych celów. Z kolei ataki na branżę technologiczną umożliwiały sprawcom szkodliwych działań łamanie zabezpieczeń łańcucha dostaw lub poszukiwanie luk w zabezpieczeniach do późniejszego wykorzystania.

Platforma poczty e-mail **verifications.io**[18] doznała poważnego naruszenia bezpieczeństwa danych z powodu niezabezpieczonej bazy danych MongoDB. Ujawnione zostały dane z ponad 800 milionów wiadomości e-mail, zawierające poufne informacje, w tym dane osobowe (umożliwiające ustalenie tożsamości).

Popularne forum hakerskie, hostowane przez usługę chmurową **MEGA**[1], opublikowało ponad 770 milionów adresów e-mail i 21 milionów unikalnych haseł. Ujawnione przez analityka bezpieczeństwa jako „Collection #1", stały się najistotniejszym zbiorem danych uwierzytelniających w historii.

Dostawca rozwiązań chmurowych i wirtualizacyjnych **Citrix** padł ofiarą ukierunkowanego cyberataku. Aby uzyskać dostęp do systemów Citrix, napastnicy wykorzystali kilka krytycznych luk w zabezpieczeniach oprogramowania, takich jak CVE-2019-19781, i zastosowali technikę zwaną rozpylaniem haseł.

Dostawca hostingu w chmurze **iNSYNQ**[19] został zaatakowany przez oprogramowanie typu ransomware, przez co klienci nie mieli dostępu do swoich danych przez ponad tydzień i byli zmuszeni do polegania na lokalnych kopiach zapasowych.

Najczęściej atakowane sektory

Usługi cyfrowe_ W roku 2019 atakowane były usługi takie jak poczta e-mail, platformy społecznościowe i platformy pracy zespołowej oraz dostawcy chmury. Były one również używane jako platformy pośrednie do dalszych ataków.

Administracja rządowa_ Korzyści finansowe z okupów sprawiają, że sektor publiczny jest jednym z najbardziej atrakcyjnych celów ataków oprogramowania typu ransomware.

Branża technologiczna_ Branża technologiczna była atakowana w 2019 r. głównie poprzez ataki na łańcuch dostaw, które próbowały zagrozić rozwojowi oprogramowania poprzez exploity zero-day i ataki typu backdoor.

Branża finansowa_ W omawianym okresie znacznie wzrosła liczba ataków na organizacje finansowe – nie tylko banki.

Ochrona zdrowia_ Liczba ataków na sektor opieki zdrowotnej stale rośnie.

Trendy

_Powszechność

- W 2019 roku na całym świecie zaobserwowano intensywną **aktywność trojanów**. Najczęściej występującymi i niebezpiecznymi typami złośliwego oprogramowania były Emotet i Agent Tesla.
- **Phishing** Jedną z najbardziej skutecznych technik dostarczania złośliwych narzędzi pozostawał phishing, czyli wyłudzanie informacji. Do skutecznych przynęt phishingowych należą oszustwa telefoniczne, fałszywe faktury, płatności, oferty oraz ogłoszenia kupna i sprzedaży.
- **Ransomware** wciąż przynosi sprawcom szkodliwych działań znaczne korzyści finansowe. W niedawnym badaniu wskazano kampanie ransomware sterowane przez ludzi[17], w których cyberprzestępcy stosują metody kradzieży danych uwierzytelniających i przemieszczania poziomego tradycyjnie kojarzone z ukierunkowanymi atakami, takimi jak ataki ze strony służb obcych państw.
- **Skimming kart płatniczych** stał się w latach 2019 i 2020 znaczącym zagrożeniem ze względu na rosnącą liczbę kupujących online.
- **Włamanie do poczty służbowej** jest rosnącym zagrożeniem ze względu na ogromną ilość skradzionych w ciągu ostatniej dekady danych uwierzytelniających i danych osobowych.
- Firmy doświadczają miesięcznie średnio dwunastu ataków z użyciem kradzionych danych uwierzytelniających (**credential stuffing**), podczas których atakujący jest w stanie znaleźć prawidłowe dane uwierzytelniające.

Wnioski

84% ataków wykorzystuje inżynierię społeczną

67% złośliwego oprogramowania przesłano z użyciem szyfrowanych połączeń HTTPS[34]

230 000 nowych odmian złośliwego oprogramowania dziennie

6 miesięcy (średnio) potrzeba, by wykryć naruszenie bezpieczeństwa danych

71% organizacji doświadczyło działania złośliwego oprogramowania, które rozprzestrzeniało się od jednego pracownika do drugiego[35]

Sprawcy

_Kto

Ustalenie albo przypisanie odpowiedzialności za incydent związany z cyberbezpieczeństwem osobie lub grupie jest wciąż bardzo trudnym i często bezwartościowym zadaniem. Jednak z perspektywy analizy zagrożeń konieczne jest klasyfikowanie zachowań, zrozumienie dynamiki i *sposobu działania* niektórych przeciwników. Analiza ta często pomaga obrońcom szukać konkretnych ścieżek i przewidzieć następne działania przeciwników.

Na przykład **grupa Lazarus**, rzekomo sponsorowana przez państwo grupa zaawansowanego ciągłego zagrożenia (APT), wydawała się w opisywanym okresie wykazywać większą aktywność ataków o podłożu zarówno finansowym, jak i szpiegowskim. Grupa była powiązana z kilkoma incydentami, w tym z kampanią **AppleJeus**, ukierunkowaną na użytkowników platform handlu kryptowalutami i ich systemy[22]. Do głównych incydentów przypisywanych tej grupie należą:

- włamanie do indyjskiej elektrowni jądrowej i agencji badań kosmicznych w listopadzie 2019 r.;
- zakłócenie działania aplikacji do handlu kryptowalutami dla administratorów giełd w październiku 2019 r.;
- atak na bankomaty i banki w Indiach, wykryty we wrześniu 2019 r.;
- ataki na użytkowników Androida w Korei Południowej za pomocą trojańskich aplikacji wykrytych w sklepie Google Play w sierpniu 2019 r.

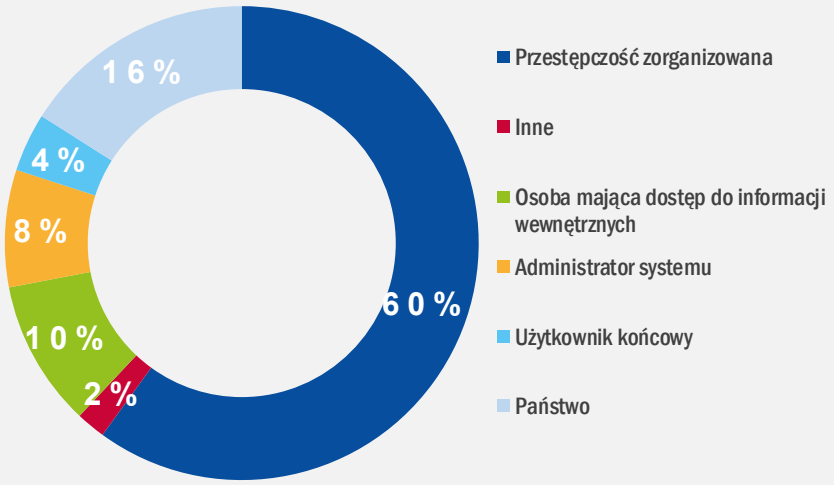
Najbardziej aktywni sprawcy

TURLA_ Według doniesień w 2019 r. grupa atakowała serwery e-mail Microsoft Exchange w sektorach edukacyjnym, rządowym, wojskowym, badawczym i farmaceutycznym w ponad 40 krajach[23]

APT27_ Jak informowano, grupa włamała się na serwery SharePoint organizacji rządowych w dwóch krajach Bliskiego Wschodu.

VICIOUS PANDA_ W kwietniu 2020 r. celem tej grupy miała być mongolska administracja publiczna.[24]

GAMAREDON_ Od grudnia 2019 roku prawdopodobnie ta grupa atakowała Ministerstwo Obrony Ukrainy w ramach kampanii typu spear phishing.[25]



Motywy

_Dlaczego

Choć określenie głównego motywu cyberataku jest trudne, możemy je jednak sklasyfikować na podstawie skutków incydentu.

Finansowe: W omawianym okresie największa liczba incydentów skutkowała kradzieżą informacji, danych i poświadczeń użytkowników. W większości przypadków celem jest kradzież danych/informacji i sprzedaż ich w „ciemnej sieci". Można również wskazać inne sposoby wykorzystania tych informacji/danych w celu umożliwienia innych rodzajów ataków o zupełnie innych skutkach, takich jak szpiegostwo lub oszustwa finansowe. Ponad 620 milionów danych kont skradzionych z 16 zaatakowanych witryn internetowych wystawiono na sprzedaż na popularnej w „ciemnej sieci" platformie handlowej Dream Market.

Szpiegostwo: Szpiegostwo jest motywem rosnącej liczby zgłaszanych ataków, głównie z powodu trwających napięć geopolitycznych i handlowych. Liczba incydentów nie jest wielka, jednak ich rozmiar i znaczenie stawiają je na drugim miejscu na liście pięciu najważniejszych motywacji ENISA. Do godnych uwagi incydentów należy odnotowany w kwietniu 2019 r., w efekcie którego pracownik General Electric i chiński biznesmen zostali oskarżeni przez Departament Sprawiedliwości Stanów Zjednoczonych o szpiegostwo gospodarcze i kradzież tajemnic handlowych General Electric[20]. Agencja France Presse (AFP) poinformowała, że Airbus padł ofiarą wyrafinowanej kampanii szpiegowskiej. Według doniesień atakujący włamali się do systemów informatycznych kilku dostawców Airbusa, a stamtąd przeniknęli do systemów informatycznych firmy[21].

Pięć najważniejszych motywów: finanse, szpiegostwo, dezorganizacja, polityka, odwet.

Najważniejsze motywy

Poniższy rysunek pokazuje, że **finanse** są wciąż głównym motywem większości cyberataków. W niektórych przypadkach w jednym ataku można wskazać wiele motywów. Na przykład często połączone są szpiegostwo, polityka, finanse i dezorganizacja. Źródłem wielu incydentów są zautomatyzowane systemy, które realizują je „jako usługę" opłacaną w kryptowalucie. Usługi te obejmują dystrybucję oprogramowania ransomware, dowodzenia i kontroli (C2), DDoS (rozproszonej odmowy usługi), spamu i innych nielegalnych działań.

Wektory ataku

_Jak

Cyberataki wymagają średnio trzech kroków, by dotrzeć do cennych zasobów ofiary. Analizując najczęściej używane wektory ataku, musimy ustalić priorytety dla punktu wejścia, sposobu działania i działań na zasobach. Są to najbardziej krytyczne etapy, które wymagają odrębnego podejścia w strategii obronnej.

Punkt wejścia: W 2019 roku do najczęściej stosowanych technik rozpoczęcia cyberataku należały ataki siłowe typu brute force z użyciem skradzionych danych uwierzytelniających, socjotechnika, błędy konfiguracji i wykorzystanie aplikacji internetowych. Na przykład wykorzystanie aplikacji internetowych było często używane jako punkt wejścia ze względu na rosnącą popularność tego typu aplikacji do przesyłania danych do chmury. W przypadku wielu incydentów istotnym punktem wejścia były błędy konfiguracji chmury i niewłaściwe wykorzystanie systemów. Przy wykorzystaniu inżynierii społecznej do planowania ataku stosuje się takie narzędzia, jak phishing i włamanie do służbowej poczty e-mail[16]. Rzadziej używane, ale równie ważne techniki to wykorzystanie luk w zabezpieczeniach (niezałatane terminowo luki systemów i typu zero-day) oraz backdoory oprogramowania, często wykorzystywane w bardziej złożonych i wyrafinowanych atakach.

Działanie: Instalowanie złośliwego oprogramowania to technika najczęściej stosowana na etapie działania. Po zainstalowaniu złośliwego oprogramowania pomaga ono przeciwnikowi przeprowadzić rozpoznanie, poruszać się po systemach i sieciach ofiary, instalować dodatkowe narzędzia, takie jak oprogramowanie typu ransomware, kraść dane i komunikować się z serwerem C2.

Pięć rodzajów zasobów najbardziej pożądanych przez cyberprzestępców

01_Własność przemysłowa i tajemnice handlowe

Własność przemysłowa i tajemnice handlowe są najbardziej pożądanymi zasobami ze względu na ich wysoką wartość dla ich właścicieli, rynku, a w niektórych przypadkach dla świata przestępczego.

02_Tajemnice państwowe/wojskowe

Są to wszelkie informacje, które państwo uważa za poufne. W roku 2019 napięcia handlowe i dyplomatyczne między krajami sprawiły, że tego typu informacje stały się jeszcze bardziej atrakcyjne.

03_Infrastruktura serwerowa

Infrastruktura serwerowa to pierwsze wrażliwe zasoby niebędące danymi. Przejęcie infrastruktury serwerowej ofiary jest głównym celem wielu ataków.

04_Dane uwierzytelniania

Dane uwierzytelniania są cennymi zasobami do generowania zysków, służą także do wspierania innych ataków.

05_Dane finansowe

Dane finansowe, takie jak dane bankowe, informacje o kartach kredytowych i płatnościach są zawsze cenne dla cyberprzestępców.

Analiza strategiczna

_Co zmieniło się w krajobrazie z nastaniem pandemii COVID-19?

W roku 2019 ENISA kontynuowała mapowanie krajobrazu zagrożeń, wspierając decydentów i twórców polityk w definiowaniu strategii ochrony obywateli, organizacji i cyberprzestrzeni. Praca ta jest częścią strategii ENISA mającej na celu dostarczanie strategicznych analiz zainteresowanym stronom. Na wniosek Komisji Europejskiej i państw członkowskich tematem przewodnim była w 2019 roku kolejna generacja telefonii komórkowej, czyli 5G. **Agencja będzie nadal sporządzać tematyczne krajobrazy zagrożeń, a w roku 2020** koncentruje się na sztucznej inteligencji.

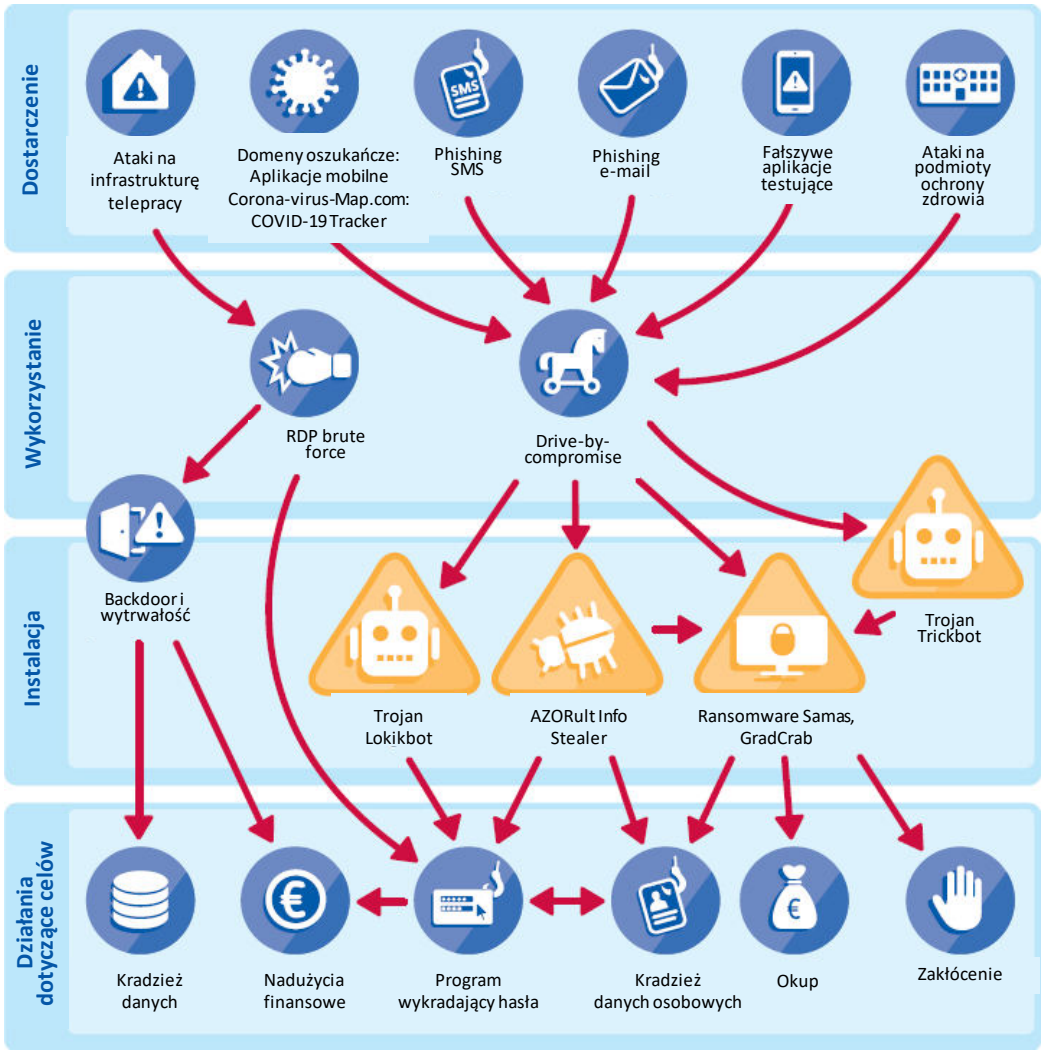
Pandemia COVID-19 to płodny okres dla sprawców szkodliwych działań, przeprowadzających ataki na wrażliwe obszary, takie jak dostawcy usług medycznych i osoby pracujące w domu. ENISA mapuje krajobraz zagrożeń występujących podczas pandemii i doradza w zakresie środków zaradczych, które powinny zmniejszyć ekspozycję na zagrożenia.

ENISA udostępnia swoje związane z pandemią COVID-19 zalecenia dotyczące bezpieczeństwa cybernetycznego w różnych aspektach, w tym pracy zdalnej, zakupów online i e-zdrowia, a także udziela poszkodowanym sektorom wartościowych i aktualnych porad na temat bezpieczeństwa[32].

Szpital Uniwersytecki w Brnie w Czechach doznał podczas pandemii COVID-19 cyberataku[33], co zmusiło go do przekierowania pacjentów i odroczenia operacji. Incydent jest uważany za krytyczny, ponieważ szpital ten jest siedzibą jednego z największych w Czechach laboratoriów przeprowadzających testy na COVID-19.

Krajobraz zagrożeń w czasie pandemii COVID-19

ENISA przygotowała wiele zasobów dla kampanii uświadamiającej i udostępniła inne przeznaczone dla ekspertów ds. bezpieczeństwa cybernetycznego wewnętrzne i zewnętrzne zasoby obejmujące kwestie bezpieczeństwa w aspekcie wyzwań pojawiających się podczas pandemii COVID-19. Jednym z takich zasobów była analiza największych zagrożeń w tym okresie.



Bibliografia

1. „MEGA Data Breach Exposed 773 Million Email Addresses and Passwords". 19 stycznia 2019 r. Latest Hacking News. https://latesthackingnews.com/2019/01/19/mega-data-breach-exposed-773-million-email-addresses-and-passwords/

2. „Largest Leak in History: Email Data Breach Exposes Over Two Billion Personal Records". 8 kwietnia 2019 r. CPO Magazine. https://www.cpomagazine.com/cyber-security/largest-leak-in-history-email-data-breach-exposes-over-two-billion-personal-records/

3. „LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company". 20 marca 2019 r. Recorded Future. https://www.recordedfuture.com/lockergoga-ransomware-insight/

4. „Researchers find 540 million Facebook user records on exposed servers". 3 kwietnia 2019 r. Tech Crunch. https://techcrunch.com/2019/04/03/facebook-records-exposed-server/

5. „Winnti: Attacking the Heart of the German Industry". 24 lipca 2019 r. Web.br. https://web.br.de/interaktiv/winnti/english/

6. „Cyber-attacks against 5 hospitals in Romania. CCR's website, also hacked". 20 czerwca 2019 r. Romanian Journal. https://www.romaniajournal.ro/society-people/cyber-attacks-five-hospitals-romania-ccr-website-hacked/

7. „Here's how ransomware attacks like the one on CityPower work – and why some victims end up paying criminals millions". 25 lipca 2019 r. Business Insider South Africa. https://www.businessinsider.co.za/ransomware-attack-on-citypower-johannesburg-why-victims-pay-criminals-2019-7

8. „Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged". 30 sierpnia 2019 r. Bank Info Security. https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000

9. „Breach Of Mastercard Loyalty Program Affected 90K Germans' Data". 23 sierpnia 2019 r. PYMNTS.com. https://www.pymnts.com/news/security-and-risk/2019/mastercard-loyalty-program-data-breach-germany/

10. „UniCredit confirms data breach". 28 października 2019 r. PrivSec Report. https://gdpr.report/news/2019/10/28/privacy-unicredit-confirms-data-breach/

11. „Prosegur Hacked: Spanish SOC Provider Hit by Ryuk Ransomware". 28 listopada 2019 r. Computer Business Review. https://www.cbronline.com/news/prosegur-hacked-ransomware

12. „Serious cyber-attack' on Austria's foreign ministry". 5 stycznia 2020 r. BBC. https://www.bbc.com/news/world-europe-50997773

13. „Croatia's largest petrol station chain impacted by cyber-attack". 20 lutego 2020 r. ZDNet. https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/

14. „European power grid organization says its IT network was hacked". 9 marca 2020 r. Cyberscoop. https://www.cyberscoop.com/european-entso-breach-fingrid/

15. „Fullz House hackers pivot from phishing to Magecart card skimming attacks". 26 listopada 2019 r. ZDNet. https://www.zdnet.com/article/fullz-house-threat-group-pivots-from-phishing-to-magecart-card-skimming-attacks/

16. „FBI warns of cloud based BEC attacks". 8 kwietnia 2020 r. Info Security. https://www.infosecurity-magazine.com/news/fbi-warns-of-cloudbased-bec-attacks/

17 „Microsoft Alerts Healthcare to Human-Operated Ransomware". 1 kwietnia 2020 r. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/microsoft-alerts-healthcare-to-human-operated-ransomware/d/d-id/1337463

18. „Verification.io suffers major data breach". 15 marca 2019 r. PrivSec Report. https://gdpr.report/news/2019/03/15/verification-io-suffers-major-data-breach/

19. „Inside the Insynq attack: 'We had to assume they were listening'". 8 sierpnia 2019 r. Accounting Today. https://www.accountingtoday.com/news/inside-the-insynq-ransomware-attack-we-had-to-assume-they-were-listening

20. „Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets". 23 kwietnia 2019 r. Departament Sprawiedliwości USA. https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

21. „Airbus supply chain hacked in a cyberespionage campaign" 27 września 2019 r. CERT-EU. https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf

22. „Lazarus group's 'AppleJeus' sequel targets cryptocurrency traders". 10 stycznia 2020 r. The Cyber-Security Source. https://www.scmagazineuk.com/lazarus-groups-applejeus-sequel-targets-cryptocurrency-traders/article/1670446

23 „Russian Nation-State Group Employs Custom Backdoor for Microsoft Exchange Server". 7 lipca 2019 r. Dark Reading. https://www.darkreading.com/application-security/russian-nation-state-group-employs-custom-backdoor-for-microsoft-exchange-server/d/d-id/1334628

24. „Vicious Panda: The COVID Campaign". 12 marca 2020 r. Check Point Research. https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

25. „Gamaredon APT Improves Toolset to Target Ukraine Government, Military". 5 lutego 2020 r. Threat Post. https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/

26. „Virus attacks Spain's defense intranet, foreign state suspected: paper". 26 marca 2019 r. Reuters. https://www.reuters.com/article/us-spain-security-cyberattack/virus-attacks-spains-defense-intranet-foreign-state-suspected-paper-idUSKCN1R7115

27 „115 Million Pakistani Mobile Users Data Go on Sale on Dark Web". 10 kwietnia 2020 r. Rewterz. https://www.rewterz.com/articles/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web

28. „Your business hit by a data breach? Expect a bill of $3.92 million". 23 lipca 2019 r. ZDNet. https://www.zdnet.com/article/your-business-hit-by-a-data-breach-expect-a-bill-of-3-92-million/

29. „Cyber Security Statistics for 2019". 21 marca 2019 r. Cyber Defense. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

30. „Georgia 'I'll Be Back' Cyber Attack Terminates TV, Takes Down 15,000 Websites". 29 października 2019 r. Forbes. https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites/#1a5746347a48

31. „Half a million Zoom accounts for sale on the dark web". 16 kwietnia 2020 r. We Live Security by ESET. https://www.welivesecurity.com/2020/04/16/half-million-zoom-accounts-sale-dark-web/

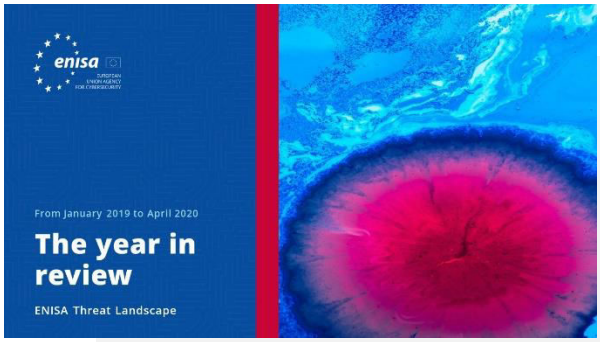
32. „ENISA COVID-19 Resources". ENISA. https://www.enisa.europa.eu/topics/wfh-covid19

33. „Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak". 17 marca 2020 r. Security Magazine. https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak

34. „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/

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

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

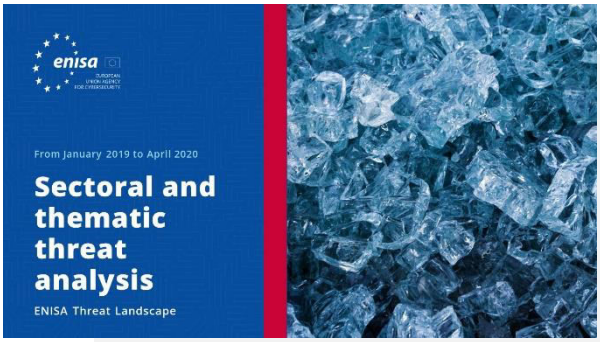
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

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

Inne publikacje

Mapa współpracy między siecią CSIRTS a organami ścigania

Plan działań dotyczący współpracy pomiędzy zespołami CSIRT, w szczególności z krajowymi i rządowymi – organami ścigania (LE) oraz sądownictwem.

PRZECZYTAJ RAPORT

Raport dotyczący stanu rozwoju reagowania na incydenty w państwach członkowskich UE

Badanie obejmujące analizę obecnego systemu reagowania operacyjnego na incydenty w sektorach NISD i wskazanie najnowszych zmian.

PRZECZYTAJ RAPORT

Model oceny dojrzałości ENISA dla sieci CSIRT

Zaktualizowana wersja opracowania „Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity", opublikowanego przez ENISA w 2017 r.

PRZECZYTAJ RAPORT

„Stopień zaawansowania zagrożeń wzrósł w roku 2019, a wielu przeciwników wykorzystuje luki w zabezpieczeniach, kradzież uwierzytelnień i ataki wieloetapowe”.

w: ETL 2020

Informacje o age

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. Cyberbezpieczeństwawnosi 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