enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Szpiegostwo w sieci

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

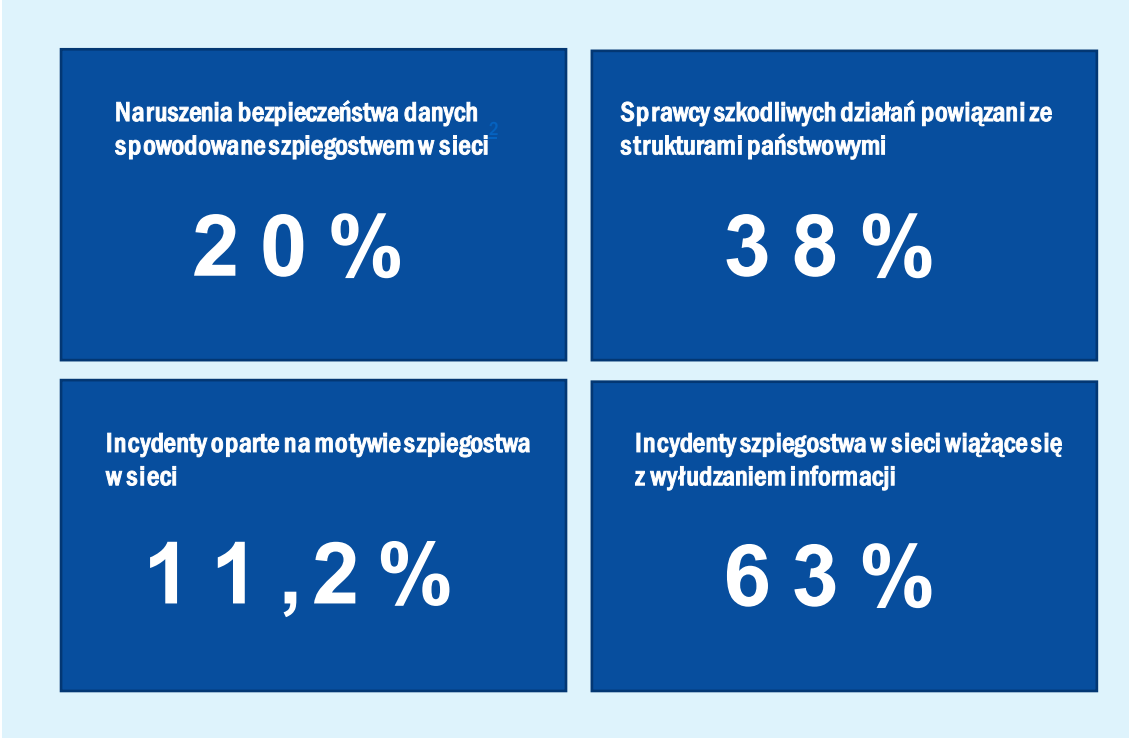
Informacje ogólne

Szpiegostwo w sieci jest uważane zarówno za zagrożenie, jak i za motyw przestępstw. Definiuje się je jako „użycie sieci komputerowych w celu uzyskania nielegalnego dostępu do informacji poufnych, zazwyczaj będących w posiadaniu organizacji rządowej lub innej”[1].

W roku 2019 w wielu raportach ujawniono, że organizacje globalne uważają szpiegostwo w sieci (lub szpiegostwo sponsorowane przez struktury państwowe) za rosnące zagrożenie dla sektorów przemysłowych, jak również dla infrastruktury o znaczeniu krytycznym i strategicznym na całym świecie, w tym dla ministerstw, kolei, dostawców usług telekomunikacyjnych, dostawców energii, szpitali i banków. Szpiegostwo w sieci skupia się na manipulowaniu geopolityką oraz na wykradaniu tajemnic państwowych i handlowych, materiałów chronionych prawem własności intelektualnej i informacji zastrzeżonych w sektorach strategicznych. Powoduje ono mobilizację sprawców ze służb gospodarczych, przemysłowych i wywiadu, jak również sprawców działających w ich imieniu. Zgodnie z opublikowanym niedawno raportem analitycy zajmujący się wywiadem dotyczącym zagrożeń odkryli, że 71% organizacji traktuje szpiegostwo w sieci i inne zagrożenia jako „czarną magię”, której dopiero trzeba się nauczyć.

W 2019 r. **liczba skierowanych przeciwko gospodarce cyberataków sponsorowanych przez struktury państwowe wzrosła i prawdopodobnie ten trend się utrzyma**. W ujęciu szczegółowym: rośnie liczba sponsorowanych przez struktury państwowe cyberataków i innych ataków ukierunkowanych na przeciwnika w przemysłowym Internecie Rzeczy (IoT) w sektorze gospodarki komunalnej, ropy i gazu ziemnego oraz produkcyjnym. Ponadto cyberataki przeprowadzane przez grupy zaawansowanych trwałych zagrożeń (APT) sugerują, że motywem ataków finansowych jest często szpiegostwo. Korzystając z taktyki, technik i procedur (TTP) podobnych do stosowanych przez ich szpiegowskie odpowiedniki takie grupy, jak Cobalt Group, Carbanak i FIN7 prawdopodobnie przeprowadziły skuteczne ataki na duże instytucje finansowe i sieci restauracji.

- Komisja Spraw Zagranicznych Parlamentu Europejskiego wezwała państwa członkowskie do stworzenia jednostki ds. cyberobrony i współpracy nad wspólnymi metodami obrony. W dokumencie tym stwierdzono, że „środowisko strategiczne Unii pogarsza się (...) aby stawić czoła różnorodnym wyzwaniom, które bezpośrednio lub pośrednio wpływają na bezpieczeństwo jej państw członkowskich i jej obywateli; do kwestii mających wpływ na bezpieczeństwo obywateli UE należą: konflikty zbrojne w krajach graniczących bezpośrednio ze wschodnią i południową granicą kontynentu europejskiego oraz państwa niestabilne; terroryzm – a w szczególności dżihadyzm, cyberataki i kampanie dezinformacyjne; zagraniczna ingerencja w europejskie procesy polityczne i wyborcze”[42].
- Sprawcy zagrożeń motywowani korzyściami finansowymi, politycznymi lub ideologicznymi coraz częściej będą kierować ataki na sieci dostawców dysponujących nieskutecznymi programami cyberbezpieczeństwa. Przeciwnicy zajmujący się szpiegostwem w sieci powoli zmieniają wzorce ataków, by wykorzystywać partnerów w łańcuchu dostaw będących trzecią albo czwartą stroną[1].



Incydenty

- Ministerstwo Obrony Narodowej Korei Południowej ogłosiło, że nieznani hakerzy naruszyli systemy komputerowe w biurze zamówień publicznych tego ministerstwa[3].
- Departament Sprawiedliwości Stanów Zjednoczonych poinformował o sponsorowanej przez zagraniczne struktury państwowe operacji z użyciem botneta, której celem było zakłócenie działalności firm z sektora mediów, lotnictwa, finansów i infrastruktury krytycznej[16].
- Norweska firma z branży oprogramowania Visma ujawniła, że stała się celem hakerów, którzy próbowali wykraść tajemnice handlowe klientom firmy[4].
- Osoby fizyczne zostały schwytane na wczesnym etapie uzyskiwania dostępu do systemów komputerowych kilku partii politycznych i australijskiego parlamentu federalnego[17].
- Europejska firma lotnicza Airbus ujawniła, że była celem domniemanych hakerów sponsorowanych przez organizacje państwowe, którzy wykradli dane osobowe i identyfikacyjne wielu pracowników[19].
- Po ataku wojsk indyjskich w Kaszmirze (Pakistan) pakistańscy hakerzy wzięli na celownik prawie 100 indyjskich rządowych witryn internetowych i systemów o znaczeniu krytycznym[5].
- Indonezyjska Narodowa Komisja Wyborcza poinformowała, że Chińczycy i Rosjanie przeprowadzili sondowanie bazy danych wyborców przed wyborami prezydenckimi i ustawodawczymi w tym kraju[20].
- Przed majowymi wyborami w UE zagraniczni hakerzy podjęli działania wymierzone w kilka europejskich agencji rządowych[21].
- Służby Australian Signal Directorate ujawniły, że prowadziły cyberataki przeciwko ISIS na Bliskim Wschodzie[22].
- Fińska policja wykryła atak typu DoS przeciwko usłudze internetowej używanej do publikowania wyników wyborów w Finlandii[6].
- Hongkońskie biuro organizacji Amnesty International poinformowało, że padło ofiarą cyberataku[23].
- Izraelskie Siły Obrony dokonały nalotu na tereny kontrolowane przez organizację Hamas po jej bezskutecznych próbach włamania do systemów izraelskich[7].

- Irańska sieć witryn i kont internetowych została rzekomo wykorzystana do rozpowszechniania fałszywych informacji o Stanach Zjednoczonych, Izraelu i Arabii Saudyjskiej[24].
- Chorwackie agencje rządowe stały się celem serii ataków przeprowadzonych przez niezidentyfikowanych hakerów sponsorowanych przez organizacje rządowe. Przesyłane złośliwe oprogramowanie, które miało na celu uzyskanie nieautoryzowanego dostępu, to Empire i SilentTrinity; w obu przypadkach było to pierwsze wystąpienie tych programów[26].
- Libia aresztowała dwóch mężczyzn oskarżonych o współpracę z rosyjską „farmą trolli" w celu wpłynięcia na wybory w kilku krajach afrykańskich[27].
- Kilka dużych niemieckich firm przemysłowych, w tym BASF, Siemens i Henkel, poinformowało, że padły ofiarą sponsorowanej przez struktury państwowe kampanii hakerskiej[28].
- Grupa sponsorowana przez struktury państwowe rzekomo przeprowadziła serię cyberataków skierowanych przeciwko egipskim dziennikarzom, naukowcom, prawnikom, aktywistom walczącym o prawa człowieka i politykom[8].
- Sponsorowana przez struktury państwowe grupa hakerów wzięła na cel dyplomatów i wysoko postawionych użytkowników języka rosyjskiego w Europie Wschodniej, używając złośliwego oprogramowania o nazwie Attor[29].
- Odkryto, że izraelska firma zajmująca się cyberbezpieczeństwem sprzedawała oprogramowanie szpiegowskie używane do ataków na wysokich rangą urzędników państwowych i wojskowych w co najmniej 20 krajach, wykorzystując lukę w zabezpieczeniach aplikacji WhatsApp[32].
- Odkryto, że siedmioletnia kampania niezidentyfikowanej grupy szpiegowskiej posługującej się językiem hiszpańskim doprowadziła do kradzieży poufnych plików z informacjami o przyporządkowaniu wysokich rangą oficerów armii wenezuelskiej[10].
- Sponsorowana przez struktury państwowe grupa cyberszpiegów rzekomo przeprowadziła kampanię skierowaną przeciwko chińskim agencjom rządowym i przedsiębiorstwom państwowym, mającą na celu wyłudzenie informacji gospodarczych, dotyczących obronności i stosunków zagranicznych[33].
- Czeskie Ministerstwo Spraw Zagranicznych padło ofiarą cyberataku przeprowadzonego przez nieustalone inne państwo[34].
- Nienależący do struktur państwowych sprawca przeprowadził na brytyjską Partię Pracy atak typu DDoS, który spowodował chwilową niedostępność systemów komputerowych partii tuż przed wyborami krajowymi[36].

Incydenty

Przypadek General Electric

Xiaoqing Zheng, obywatel amerykański chińskiego pochodzenia, został oskarżony o działalność szpiegowską wymierzoną w koncern General Electric (GE). Zheng miał wykraść tajemnice dotyczące technologii turbin GE, a następnie przekazać je chińskiemu biznesmenowi, który miał dostarczyć je chińskim dygnitarzom. Zheng pracował dla koncernu GE w latach 2008–2018[15].

Departament Sprawiedliwości Stanów Zjednoczonych oskarżył dwóch mężczyzn o kradzież informacji w celu ich wykorzystania z myślą o własnych interesach w dwóch firmach zajmujących się badaniami i rozwojem technologii turbin: Liaoning Tianyi Aviation Technology Co Ltd i Nanjing Tianyi Avi Tech Co Ltd.[47]

Wśród sposobów działania tego sprawcy stanowiącego zagrożenie wewnętrzne można wymienić:

- kopiowanie informacji poufnych na pamięć USB do chwili, gdy koncern GE zablokował możliwość korzystania z takich urządzeń;
- szyfrowanie informacji poufnych i stosowanie technik steganograficznych do ukrywania plików danych w kodzie binarnym cyfrowych plików ze zdjęciami;
- podłączanie iPhone'a do komputera stacjonarnego w celu skopiowania obrazów;
- przesyłanie plików na swój osobisty adres e-mail.

Ograniczenie ryzyka

Ze względu na wieloraki charakter tego zagrożenia kilka środków łagodzących zalecanych w niniejszym raporcie w odniesieniu do innych zagrożeń można zastosować w ramach następujących podstawowych środków łagodzących[2]:

- Identyfikacja ról krytycznych o znaczeniu dla organizacji i oszacowanie narażenia na ryzyka związane ze szpiegostwem. Ocena takich ryzyk w oparciu o informacje biznesowe (np. wywiad gospodarczy).
- Tworzenie polityk bezpieczeństwa uwzględniających metody kontroli na poziomie zasobów ludzkich, przedsiębiorstwa i operacyjnym, pozwalających uwzględnić łagodzenie ryzyka. Powinny one obejmować zasady i praktyki dotyczące zwiększania świadomości, ładu korporacyjnego i działań związanych z bezpieczeństwem.
- Tworzenie praktyk korporacyjnych mających na celu informowanie pracowników o stworzonych zasadach i szkolenie ich.
- Stworzenie kryteriów oceny (KPI), by tworzyć analizy porównawcze operacji i dostosowywać je do nadchodzących zmian.
- Tworzenie listy dozwolonych zasobów dla usług aplikacji o znaczeniu krytycznym w zależności od ocenianego poziomu ryzyka.
- Ocena luk w zabezpieczeniach i regularna aktualizacja oprogramowania, szczególnie w przypadku systemów na obwodzie.
- Wdrożenie zasady uzasadnionego dostępu do informacji przy określaniu praw dostępu i tworzeniu metod kontroli w celu monitorowania nadużyć profili uprawnionych.
- Konfiguracja filtrowania treści dla wszystkich kanałów przychodzących i wychodzących (np. poczta e-mail, WWW, ruch w sieci).

Bibliografia

1. „Cyber Threatscape Report. 2019." IDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf
2. „Data Breach Investigations Report 2020" DBR i Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf
3. Catalin Cimpanu.„Hackers breach and steal data from South Korea's Defense Ministry", 16 stycznia 2019 r. ZDNet. https://www.zdnet.com/article/hackers-breach-and-steal-data-from-south-koreas-defense-ministry/
4. Jack Stubbs. „China hacked Norway's Visma to steal client secrets: investigators", 6 lutego 2019 r. Reuters. https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141
5. Kate Fazzini. „In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides". 28 lutego 2019 r. CNBC. https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html
6. Kati Pohjanpalo. „Finland Detects Cyber Attack on Online Election-Results Service". 10 kwietnia 2019 r. Bloomberg. https://www.bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service
7. Lily Hay Newman „What Israel's Strike on Hamas Hackers Means For Cyberwar" 5 czerwca 2019 r. Wired. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/
8. „Egypt Is Using Apps to Track and Target Its Citizens, Report Says", 3 października 2019 r. The New York Times. https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html
9. Colin Lencher. „Huawei accuses the US of 'launching cyber attacks' against the company" 4 września 2019 r. The Verge. https://www.theverge.com/2019/9/4/20849092/huawei-cyberattacks-us-government-netowrks-employee-harassment
10. Catalin Cimpanu „A cyber-espionage group has been stealing files from the Venezuelan military", 5 sierpnia 2019 r. ZDNet. https://www.zdnet.com/article/a-cyber-espionage-group-has-been-stealing-files-from-the-venezuelan-military/
11. Catalin Cimpanu. „Croatian government targeted by mysterious hackers", 5 lipca 2019 r. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/
12. Michael McGowan. „China behind massive Australian National University hack, intelligence officials say", 6 czerwca 2019 r. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say
13. „General election 2019: Labour Party hit by second cyber-attack", 12 listopada 2019 r. BBC. https://www.bbc.com/news/election-2019-50388879
14. Nicole Perlroth, Matthew Rosenberg. „Russians Hacked Ukrainian Gas Company at Center of Impeachment", 13 stycznia 2020 r. The New York Times. https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html
15. Danny Bradbury. „GE Engineer Charged for Novel Data Theft", 24 kwietnia 2019 r. Info Security. https://www.infosecurity-magazine.com/infosec/ge-engineer-charged-data-theft-1/
16. „U.S. announces disruption of 'Joanap' botnet linked with North Korea". 30 stycznia 2019 r. CyberScoop. https://www.cyberscoop.com/joanap-botnet-north-korea-department-of-justice/
17. „The cyber attack on Parliament was done by a 'state actor' — here's how experts figure that out". 20 lutego 2019 r. ABC News. https://www.abc.net.au/news/2019-02-20/cyber-activists-or-state-actor-attack-how-experts-tell/10825466
18. „While Trump was meeting with Kim Jong Un in Vietnam, North Korean hackers reportedly attacked targets in the US". 5 marca 2019 r. Business Insider. https://www.businessinsider.com/north-korean-hackers-trump-kim-meeting-mcafee-2019-3
19. „Airbus hit by series of cyber attacks on suppliers". 26 września 2019 r. France 24. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

20. „Indonesia Says Election Under Attack From Chinese, Russian Hackers". 12 marca 2019 r. Bloomberg. https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers

21. „Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections". 21 marca 2019 r. ZDNet. https://www.zdnet.com/article/cyber-espionage-warning-russian-hacking-groups-step-up-attacks-ahead-of-european-elections/

22. „Australian cyber soldiers hacked Islamic State and crippled its propaganda unit – here's what we know". 18 grudnia 2019 r. ABC News. https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426

23. „State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack". 25 kwietnia 2019 r. Amnesty International. https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

24. „New Report Shows How a Pro-Iran Group Spread Fake News Online". 14 maja 2019 r. The New York Times. https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html

25. „China behind massive Australian National University hack, intelligence officials say". 6 czerwca 2019 r. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

26. „Croatian government targeted by mysterious hackers". 5 lipca 2019 r. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

27. „Two Russians accused of election interference arrested in Libya". 8 lipca 2019 r. Cyber Scout. https://cyberscout.com/en/blog/two-russians-accused-of-election-interference-arrested-in-libya

28. „BASF, Siemens, Henkel, Roche target of cyber attacks". 24 lipca 2019 r. Reuters. https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

29. „New espionage malware found targeting Russian-speaking users in Eastern Europe", 10 października 2019 r. ZDNet. https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

30. „Advanced Israeli spyware is targeting Moroccan human rights activists". Listopad 2019 r. TheNextWeb. https://thenextweb.com/security/2019/10/14/advanced-israeli-spyware-is-targeting-moroccan-human-rights-activists/

31. „Hacking the hackers: Russian group hijacked Iranian spying operation, officials say". 21 października 2019 r. Reuters. https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

32. „Israeli spyware allegedly used to target Pakistani officials' phones". 19 grudnia 2019 r. The Guardian. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones

33. „A phishing campaign with nation-state hallmarks is targeting Chinese government agencies". 8 listopada 2019 r. Cyber Scoop. https://www.cyberscoop.com/china-phishing-anomali-nation-state-apt/

34. „Foreign power was behind cyber attack on Czech ministry: Senate". 13 sierpnia 2019 r. Reuters. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

35. „Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications". 15 sierpnia 2019 r. The Wall Street Journal. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

36. „Labour suffers second cyber-attack in two days", 12 listopada 2019 r. The Guardian. https://www.theguardian.com/politics/2019/nov/12/labour-reveals-large-scale-cyber-attack-on-digital-platforms

37. „Extensive hacking operation discovered in Kazakhstan". 23 listopada 2019 r. ZDNet. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

Bibliografia

38. „A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems". 20 listopada 2019 r. Wired. https://www.wired.com/story/iran-apt33-industrial-control-systems/

39. „Russian 'Gamaredon' Hackers Back at Targeting Ukraine Officials". 6 grudnia 2019 r. Security Week. https://www.securityweek.com/russian-gamaredon-hackers-back-targeting-ukraine-officials

40. „Iran announced it foiled 'really massive' foreign cyber attack". 11 grudnia 2019 r. Security Affairs. https://securityaffairs.co/wordpress/94981/cyber-warfare-2/iran-foreign-cyber-attack.html

41. „Croatian government targeted by mysterious hackers". 5 lipca 2019 r. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

42. „Sprawozdanie w sprawie realizacji wspólnej polityki zagranicznej i bezpieczeństwa – sprawozdanie roczne", 18 grudnia 2019 r. Parlament Europejski. https://www.europarl.europa.eu/doceo/document/A-9-2019-0054_EN.html

43. „Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent". 26 sierpnia 2012 r. Krebs on Security. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information

44. „Energy Manufacturer Also Victimized by IE Zero Day in Watering Hole Attack". 2 stycznia 2013 r. The Threat Post. https://threatpost.com/energy-manufacturer-also-victimized-ie-zero-day-watering-hole-attack-010213/77359/

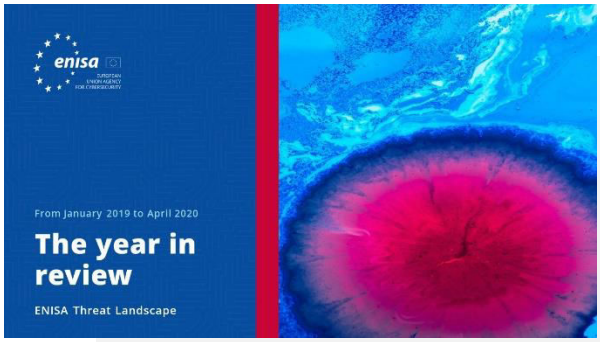
45. „The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity". 25 lutego 2014 r. Blog CrowdStrike. https://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/

46. „Advanced Persistent Threat Groups". Fireeye. https://www.fireeye.com/current-threats/apt-groups.html

47. „U.S. accuses pair of stealing secrets, spying on GE to aid China". 23 kwietnia 2019 r. Reuters. https://www.reuters.com/article/us-usa-justice-ge/us-accuses-pair-of-stealing-secrets-spying-on-ge-to-aid-china-idUSKCN1RZ24O


„Liczba skierowanych przeciwko gospodarce cyberataków sponsorowanych przez struktury państwowe wzrosła w 2019 r.”
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

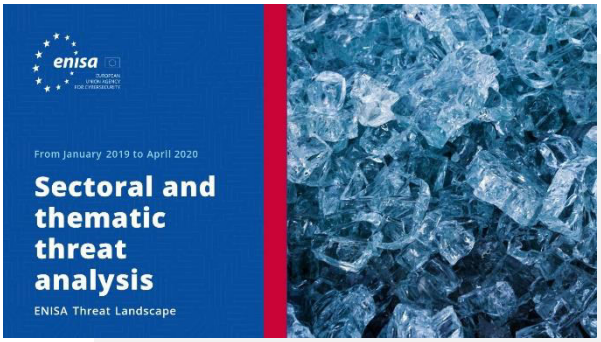
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Tematyka badan

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

PRZECZYTAJ RAPORT



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.

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