enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Wykaz piętnastu największych zagrożeń

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

Największe zagrożenia

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

1. Złośliwe oprogramowanie

Analiza i trendy zagrożenia złośliwym oprogramowaniem w okresie od stycznia 2019 r. do kwietnia 2020 r. Złośliwe oprogramowanie zajęło 1. pozycję w krajobrazie zagrożeń, utrzymując ją tym samym od 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

2. Ataki przez strony internetowe

Analiza trendów ataków przez strony internetowe w okresie od stycznia 2019 r. do kwietnia 2020 r. Ataki przez strony internetowe zajęły 2. pozycję w krajobrazie zagrożeń, utrzymując ją tym samym od 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

3. Phishing

Analiza trendów zagrożenia phishingiem w okresie od stycznia 2019 r. do kwietnia 2020 r. Ataki phishingowe zajęły 3. pozycję w krajobrazie zagrożeń, awansując z 4. pozycji w 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

4. Ataki oparte na aplikacjach sieciowych

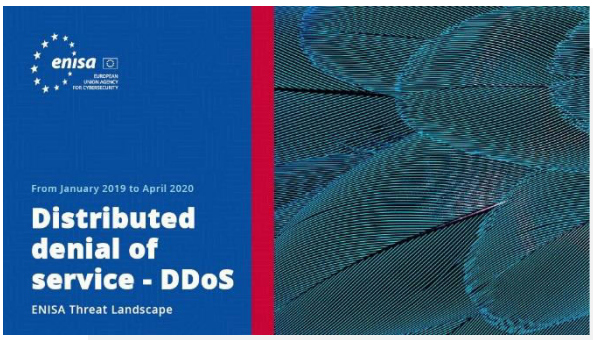
Analiza i trendy ataków opartych na aplikacjach sieciowych w okresie od stycznia 2019 r. do kwietnia 2020 r. Ataki oparte na aplikacjach sieciowych zajęły 4. pozycję w krajobrazie zagrożeń, spadając z 3. pozycji w 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

5. Spam

Analiza trendów ataków spamowych w okresie od stycznia 2019 r. do kwietnia 2020 r. Spam zajął 5. pozycję w krajobrazie zagrożeń, awansując z 6. pozycji w 2018 r.



PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

6. DDoS

Analiza trendów ataków DDoS w okresie od stycznia 2019 r. do kwietnia 2020 r. Ataki DDoS zajęły 6. pozycję w krajobrazie zagrożeń, spadając z 5. pozycji w 2018 r.

Największe zagrożenia

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

7. Kradzież tożsamości

Analiza i trendy zagrożenia kradzieżą tożsamości w okresie od stycznia 2019 r. do kwietnia 2020 r. Kradzież tożsamości zajęła 7. pozycję w krajobrazie zagrożeń, awansując z 13. pozycji w 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

8. Naruszenie bezpieczeństwa danych

Analiza trendów ataków związanych z naruszeniem bezpieczeństwa danych w okresie od stycznia 2019 r. do kwietnia 2020 r. Naruszenia bezpieczeństwa danych zajęły 8. pozycję w krajobrazie zagrożeń, utrzymując ją tym samym od 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

9. Zagrożenie wewnętrzne

Analiza trendów zagrożeń wewnętrznych w okresie od stycznia 2019 r. do kwietnia 2020 r. Zagrożenia wewnętrzne zajęły 9. pozycję w krajobrazie zagrożeń, utrzymując ją tym samym od 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

10. Botnety

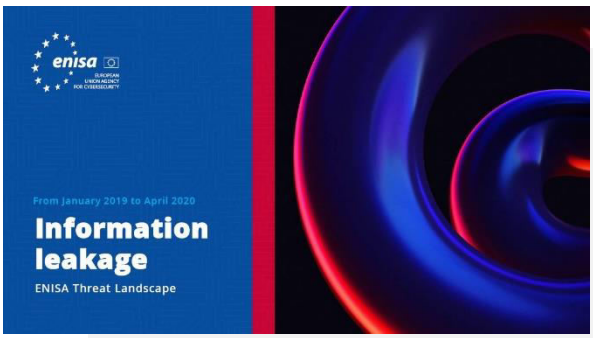
Analiza i trendy zagrożenia botnetami w okresie od stycznia 2019 r. do kwietnia 2020 r. Ataki botnetów zajęły 10. pozycję w krajobrazie zagrożeń, spadając z 7. pozycji w 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

11. Ingerencja fizyczna, uszkodzenie, kradzież i utrata

Ingerencja fizyczna, uszkodzenie, kradzież i utrata zajęły 11. pozycję w krajobrazie zagrożeń, spadając z 10. pozycji w 2018 r.



PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

12. Wyciek informacji

Analiza trendów zagrożeń wyciekiem informacji w okresie od stycznia 2019 r. do kwietnia 2020 r. Ataki związane z wyciekiem informacji zajęły 12. pozycję w krajobrazie zagrożeń, spadając z 11. pozycji w 2018 r.

Największe zagrożenia

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

13. Oprogramowanie typu ransomware

Analiza i trendy zagrożenia oprogramowaniem typu ransomware w okresie od stycznia 2019 r. do kwietnia 2020 r. Oprogramowanie typu ransomware zajęło 13. pozycję w krajobrazie zagrożeń, awansując z 14. pozycji w 2018 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń

14. Szpiegostwo w sieci

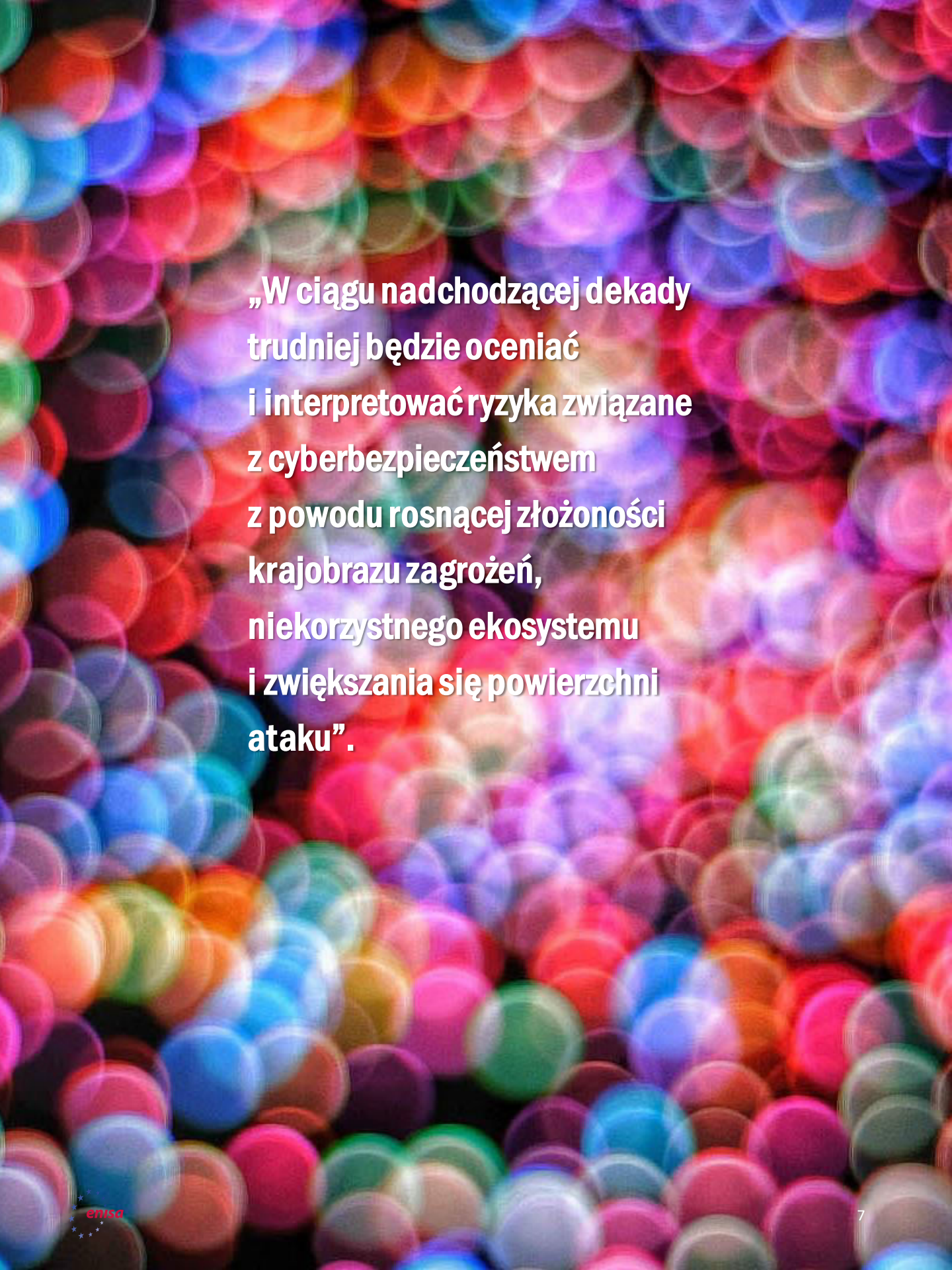
Analiza trendów szpiegostwa w sieci w okresie od stycznia 2019 r. do kwietnia 2020 r. Szpiegostwo w sieci znalazło się na 14. pozycji w krajobrazie zagrożeń, awansując z 15. pozycji w 2018 r.

PRZECZYTAJ RAPORT

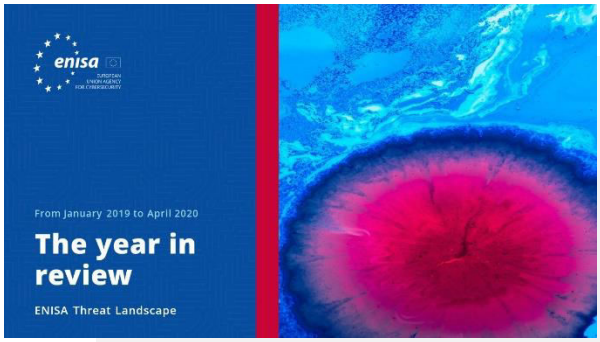
Raport ENISA o krajobrazie zagrożeń

15. Złośliwe wydobywanie kryptowalut (cryptojacking)

Analiza trendów cryptojackingu w okresie od stycznia 2019 r. do kwietnia 2020 r. Ataki związane z cryptojackingiem zajęły 15. pozycję w krajobrazie zagrożeń, spadając z 13. pozycji w 2018 r.


„W ciągu nadchodzącej dekady
trudniej będzie oceniać
i interpretować ryzyka związane
z cyberbezpieczeństwem
z powodu rosnącej złożoności
krajobrazu zagrożeń,
niekorzystnego ekosystemu
i zwiększania się powierzchni
ataku”.

Powiązany



PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Przegląd roku

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

PRZECZYTAJ RAPORT

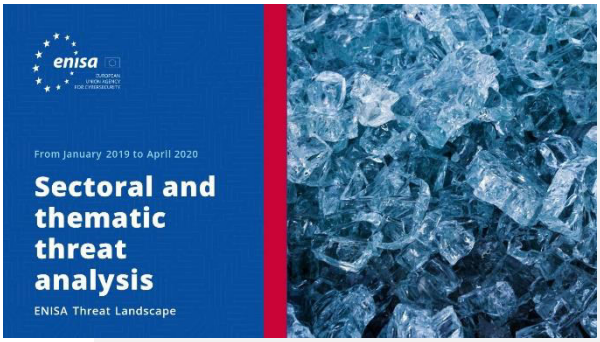
Raport ENISA o krajobrazie zagrożeń
Najważniejsze incydenty w UE i na świecie

Najważniejsze incydenty związane z cyberbezpieczeństwem 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.

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