PL

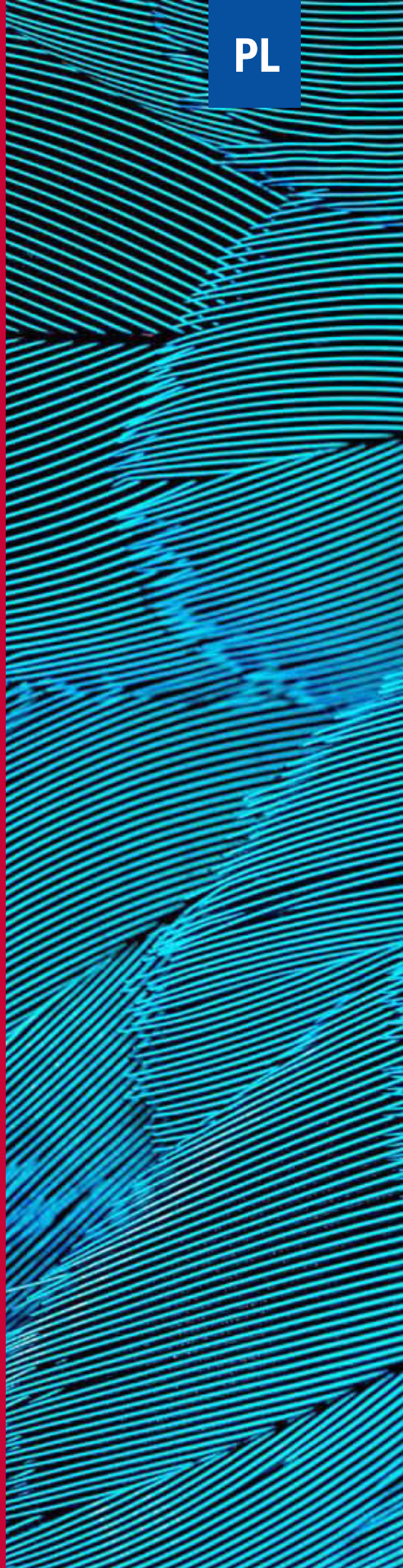
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Od stycznia 2019 r. do kwietnia 2020 r.

# Rozproszona odmowa usługi

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



# Informacje ogólne

Ataki typu DDoS (Distributed Denial of Service, rozproszona odmowa usługi) powodują, że użytkownicy systemu lub usługi nie mogą uzyskać dostępu do odpowiednich informacji, usług lub innych zasobów. Efekt ten można osiągnąć przez wyczerpanie potencjału usługi lub przeciążenie elementu infrastruktury sieciowej[1]. Rośnie liczba ataków, dokonywanych przez sprawców o różnych motywach, podobnie jak liczba atakowanych sektorów. Choć mechanizmy i strategie obronne stają się coraz bardziej niezawodne, również sprawcy szkodliwych działań rozwijają swoje umiejętności techniczne. Według raportów[3,4,5], wzrosło wykorzystanie technik ataku odbitego i wzmocnionego, umożliwiających tworzenie nowych wektorów innych niż powszechnie znane (wzmocnienie UDP itp.)[6]. Sprawcy szkodliwych działań ulepszają również swoje taktyki handlowe, otwarcie reklamując swoje usługi w sieci. Wcześniej usługi DDoS były reklamowane na forach „ciemnej sieci", teraz już promowane są na wspólnych kanałach mediów społecznościowych, takich jak YouTube czy Reddit[2].

W 2019 roku w pierwszej dziesiątce krajów źródłowych generujących ruch DDoS pojawiły się nowe (Hongkong, RPA itp.)[7]. Był to również rok, w którym odnotowano wzrost działań DDoS prowadzonych przez botnety. Urządzenia IoT są „wylęgarnią" botnetów DDoS, a za kraje najbardziej zainfekowane agentami botnetów uznano Chiny (24%), Brazylię (9%) i Iran (6%)[3]. Analitycy bezpieczeństwa przewidzieli, że wdrożenie i upowszechnienie sieci 5G spowoduje wykładniczy wzrost liczby podłączonych urządzeń, a więc i ekspansję sieci botnetów[3].

Ataki typu DoS nie są nowością dla bezpieczeństwa cybernetycznego i obrońców sieci, jednak poziom ich zaawansowania rośnie, a sprawcy szkodliwych działań prowadzą aktywne działania rozpoznawcze bardziej intensywnie niż wcześniej[3,8].

# Wnioski

**241%** wzrost łącznej liczby ataków w III kwartale 2019 r. w porównaniu z tym samym okresem 2018 r.[3]

**79,7%** wszystkich ataków typu DDoS było atakami typu SYN-Flood[7]

**86%** ataków powstrzymanych w III kwartale 2019 r. wykorzystywało więcej niż dwa wektory[9]

**84%** ataków typu DDoS trwało mniej niż 10 minut[10,11]

**509** godzin trwał najdłuższy atak typu DDoS w drugim kwartale 2019 r.[3]

# Kill chain

**Odmowa usługi (DoS)**

| Rozpoznanie | Uzbrojenie | Dostarczenie | Wykorzystanie |
|---|---|---|---|

*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

## Pięć najważniejszych ataków typu DDoS

**500–580 MILIONÓW PAKIETÓW SYN FLOOD NA SEKUNDĘ.** Wśród wszystkich technik używanych przez sprawców szkodliwych działań ataki typu SYN Flood są wciąż uważane za jedne z trudniejszych do obrony ze względu na ich charakterystykę, docelową infrastrukturę oraz fakt, że wymagają one więcej sprzętu do obsługi dużej ilości pakietów. W styczniu 2019 r. analityk bezpieczeństwa zaobserwował rekordową aktywność SYN Flood, gdy do jednego z jego klientów wysyłane było 500 milionów pakietów na sekundę (mpps), a w kwietniu 2019 r. wielkość ta wzrosła do 580 mpps[12].

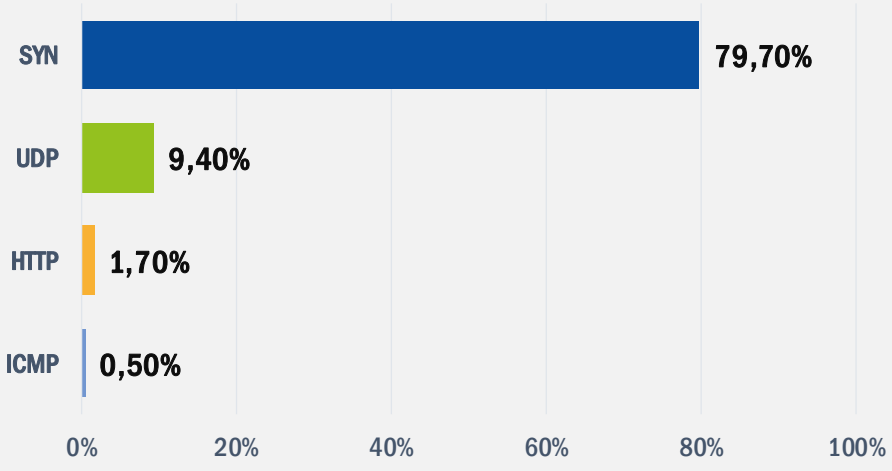
**WS-DISCOVERY.** Web services dynamic discovery[13] (WS-Discovery) to protokół wykrywania z multiemisją. Używany jest głównie przez urządzenia IoT do automatycznego wykrywania węzłów w sieciach lokalnych (LAN), ale, podobnie jak inne protokoły, może być użyty niezgodnie z przeznaczeniem, szczególnie w obszarze IoT[5]. Sprawcy szkodliwych działań odkryli, że jest to dobre podłoże do wzmacniania ataków. Jeden z analityków bezpieczeństwa ujawnił[3] współczynnik wzmocnienia 95, podczas gdy inny odnotował wzrost o 15 000% w porównaniu z pierwotną wielkością w bajtach[14].

**ATAKI ODBITE I WZMOCNIONE.** Tego typu ataki są od dawna powszechnie znane z tego, że do dostarczenia dużego ładunku wystarcza w nich małe żądanie. Mówiąc w skrócie, sprawca szkodliwych działań wysyła do hosta sfałszowane żądania z adresem IP nadawcy (ofiary), a host wysyła wszystkie odpowiedzi do ofiary[9]. Ta metoda jest skuteczna głównie w protokole opartym na UDP ze względu na jego bezpołączeniowy charakter i współczynnik wzmocnienia (CLDAP daje współczynnik wzmocnienia 50–70). Jednak protokół TCP nie jest podatny na tego typu ataki[15].

Dobrym przykładem takich prób są odbite i wzmocnione zalewowe ataki SYN-ACK – uzyskanie efektu nie musi wymagać dużej przepustowości. Przeciwnie, duża przepustowość może spowodować, że atak pozostanie niezauważony i zwiększyć jego skuteczność[3].

**ATAKI DDOS TYPU BIT-AND-PIECE / BOMBARDOWANIE DYWANOWE**. Ten rodzaj ataku typu DRDoS (Distributed Reflective Denial of Service) jest znany głównie z atakowania branży telekomunikacyjnej i dostawców usług[17]. W jednym z przypadków[18] takiego ataku celem stały się losowo wybrane adresy IP dostawcy usług internetowych, które odbijały ruch do routerów brzegowych dostawcy. W ten sposób ofiara nie była w stanie rozpoznać DDoS, dopóki jej usługi nie zostały przeciążone przez część jej własnego zakresu adresów IP[19].

**WIELOWEKTOROWE ATAKI DDOS**. Sprawcy szkodliwych działań często używają wielu wektorów ataków DoS, aby zwiększyć ich złożoność i zróżnicowanie. Oznacza to, że automatyzując różne rodzaje ataków w warstwie aplikacji (HTTP Flood, DNS Flood itp.) i warstwie sieciowej (odbicie/wzmocnienie UDP/TCP itp.), będą się starali uzyskać maksymalny efekt przez nasycenie przepustowości, zasobów lub usług w docelowym środowisku[16].




Rysunek 1: Rozkład ataków DDoS według typu. Źródło: Kaspersky[16]

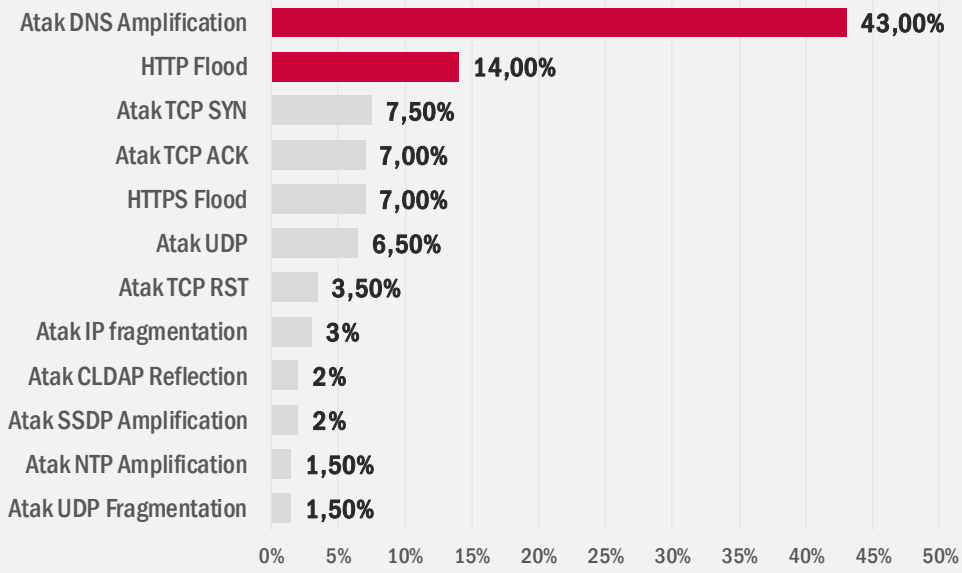
# Wektory ataku

## Jak

Podobnie jak w poprzednich latach, pod względem ataków typu UDP Flood rok 2019 nie był wyjątkiem. Według analityka bezpieczeństwa UDP Flood był najpopularniejszym wektorem ataku, a zespół uważa, że może to być związane z dominującym wykorzystaniem protokołu UDP w obszarach wysokiego ryzyka, takich jak gry. Na liście głównych wektorów ataków UDP Flood wyprzedzał SYN Flood, oraz ataki oparte na odpowiedzi DNS i protokole TCP.

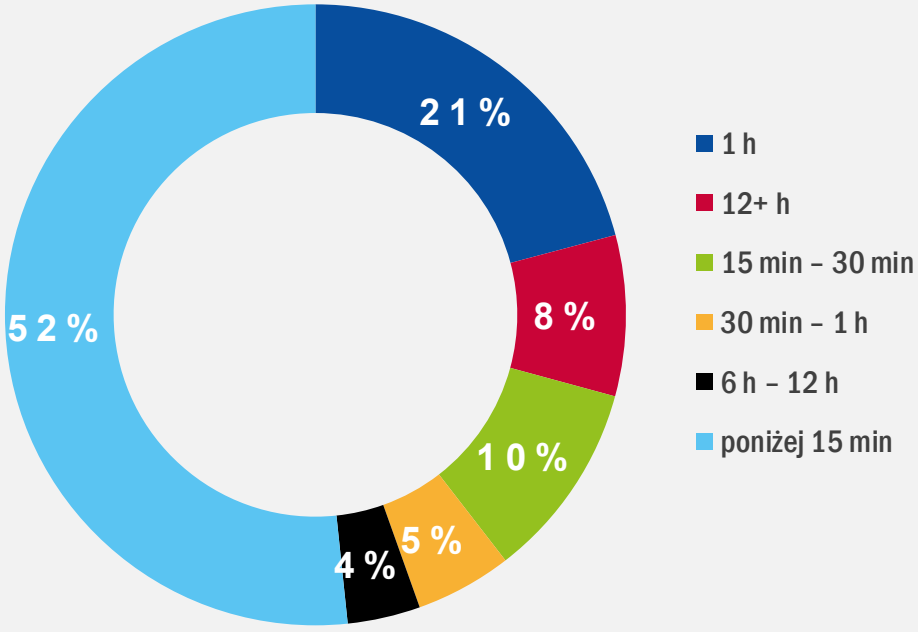
W tym okresie obserwowano również ataki wielowektorowe. Jednak analityk bezpieczeństwa uważa, że niektóre ataki wielowektorowe są niezamierzonym efektem ubocznym próby DoS[11].

Według autorów raportu na temat bezpieczeństwa cybernetycznego[17] ataki typu DNS Amplification były głównym wektorem ataków DDoS, a kolejnymi – ataki typu HTTP Flood i TCP SYN. Podobne spostrzeżenia dotyczyły ataków SYN Flood, które na liście głównych wektorów ataku w III kwartale 2019 r. znalazły się na pierwszym miejscu przed atakami UDP, TCP i HTTP.




Rysunek 2: Rozkład wektorów ataków DDoS. Źródło: NexusGuard[17]

## Czas trwania ataku




Rysunek 3 – źródło: Imperva[11]

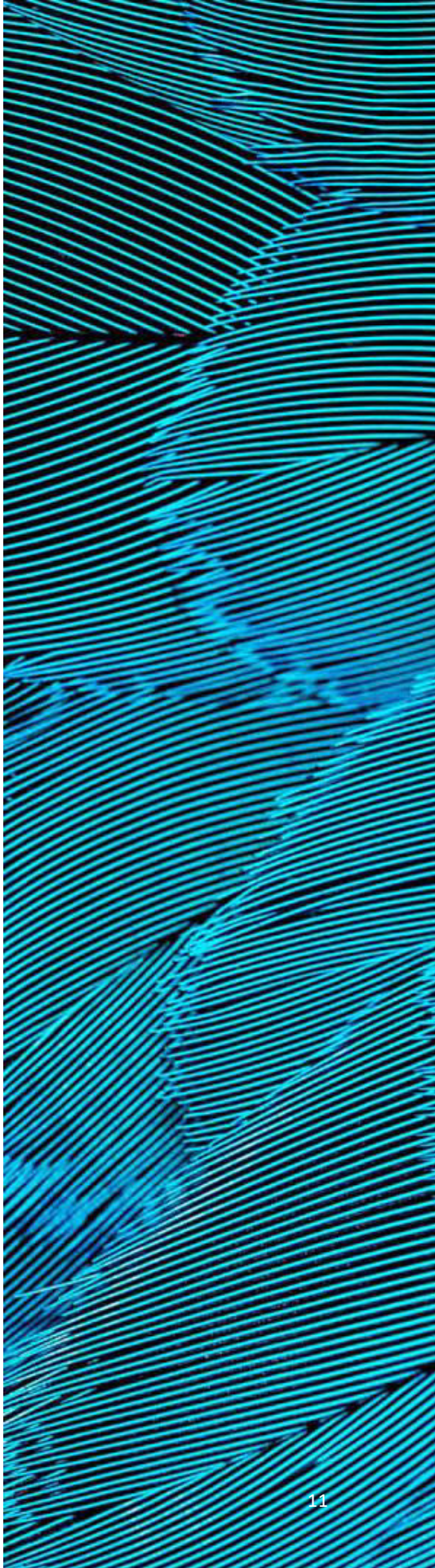
# Ograniczenie ryzyka

## Proponowane działania

- Przeanalizowanie usług i krytycznych zasobów oraz ustalenie priorytetów obrony w razie ich przeciążenia. Przygotowanie planu reagowania na takie sytuacje[20].
- W zależności od wymagań, rozważenie skorzystania z usługi ochrony przed DDoS lub dostawcy usług posiadającego ochronę przed DDoS. Stosowanie metod takich jak monitorowanie w celu szybkiego wykrycia infekcji[1].
- Podobnie jak powyżej, skutecznym sposobem uniemożliwiania prób wolumetrycznych może być wykorzystanie sieci dostarczania treści (wymaga innych technik dla realizowania bardziej wyrafinowanych ataków)[21].
- Newralgiczną rolę w ochronie przed atakami DDoS odgrywają dostawcy usług internetowych i dostawcy usług w chmurze. Kluczem do skutecznej odpowiedzi na atak typu DoS jest posiadanie jasnego planu i kanału komunikacji.
- Wypracowanie silnej, proaktywnej postawy obronnej przed wystąpieniem krytycznej awarii, zaangażowanie odpowiedniego zespołu i dostawców do skonfigurowania i dostrojenia mechanizmów kontroli w oparciu o określone wymagania biznesowe[22]. Dobrymi przykładami proaktywnych środków są usprawnienie serwerów pamięci podręcznej lub porzucanie niewłaściwych zapytań/żądań w warstwie aplikacji u źródła i wdrażanie BCP[23] dla usługodawców.
- Należy pamiętać, by testować i ponownie oceniać swoje techniki obrony, wykorzystywane technologie i dostawców usług.
- Opracowanie rejestru zagrożeń przez dokładne przeanalizowanie swojego środowiska. Począwszy od krytycznych zasobów wewnętrznych, a kończąc na swoim śladzie i obecności w internecie.[24]

„Ataki typu DDoS nie są nowością dla bezpieczeństwa cybernetycznego i obrońców sieci, jednak poziom ich zaawansowania rośnie, a sprawcy szkodliwych działań prowadzą aktywne działania rozpoznawcze bardziej intensywnie niż wcześniej.”

w: ETL 2020



# Bibliografia


1. „Understanding Denial-of-Service Attacks", 20 listopada 2019 r. CISA. https://www.us-cert.gov/ncas/tips/ST04-015

2. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. „DDoS attacks in Q1 2019", 21 maja 2019 r. Kaspersky. https://securelist.com/ddos-report-q1-2019/90792/

3. „Q4 2019 - The State of DDoS Weapons Report". 2019. A10 Networks. https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

4. Chad Seaman. „Anatomy of a SYN-ACK Attack". 2 lipca 2019 r. Akamai. https://blogs.akamai.com/sitr/2019/07/anatomy-of-a-syn-ack-attack.html

5. Brandon Vigliarolo. „A new type of DDoS attack can amplify attack strength by more than 15,300%". 18 września 2019 r. TechRepublic. https://www.techrepublic.com/article/a-new-type-of-ddos-attack-can-amplify-attack-strength-by-more-than-15300/

6. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. „DDoS attacks in Q4 2018", 7 lutego 2019 r. Kaspersky. https://securelist.com/ddos-attacks-in-q4-2018/89565/

7. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. „DDoS attacks in Q3 2019", 11 listopada 2019 r. Kaspersky. https://securelist.com/ddos-report-q3-2019/94958/

8. „2019 Website Threat Research Report". 2019 r., sucuri

9. „DDoS attacks up 241% in Q3 2019 compared to same period last year". 19 listopada 2019 r. Neustar. https://www.home.neustar/about-us/news-room/press-releases/2019/ddos-attacks-up-241--in-q3-2019-compared-to-same-period-last-year#

10. „2019 Half-Year DDoS Trends Report". 2019. Corero Security. https://www.corero.com/blog/infographic-2019-mid-year-ddos-trends-report/

11. Nadav Avital, Avishay Zawoznik, Johnathan Azaria, Kim Lambert. „2019 Global DDoS Threat Landscape Report". 2019. Imperva. https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/

12. Tomer Shani. „Updated: „This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important". 30 kwietnia 2019 r. Imperva. https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

13. „Web Services Dynamic Discovery (WS-Discovery) Version 1.1", 1 lipca 2009 r. OASIS. http://docs.oasis-open.org/ws-dd/discovery/1.1/wsdd-discovery-1.1-spec.html

14. Jonathan Respeto. „New DDoS Vector Observed in the Wild: WSD attacks hitting 35 Gbps". 18 września 2019 r. Akamai. https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html

15. „Threat Alert: „TCP Amplification Attacks" 9 listopada 2019 r. Radware. https://blog.radware.com/security/2019/11/threat-alert-tcp-reflection-attacks/

16. „Kaspersky report finds over half of Q3 DDoS attacks occurred in September". 11 listopada 2019 r. Kaspersky. https://usa.kaspersky.com/about/press-releases/2019_kaspersky-report-finds-over-half-of-q3-ddos-attacks-occurred-in-september

17. „DDoS Threat Report 2019 Q1". 2019. NexusGuard. https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q1

18. „International traffic – DDoS". 22 września 2019 r. Cool Ideas. https://coolzone.cisp.co.za/announcements.php?announcement=2038-international-traffic-ddos-cool-ideas

19. Catalin Cimpanu. „Carpet-bombing' DDoS attack takes down South African ISP for an entire day". 24 września 2019 r. ZDNet. https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

**20.** „Guidance following recent DoS attacks in the run up to the 2019 General Election". 13 listopada 2019 r. NCSC. https://www.ncsc.gov.uk/guidance/guidance-following-recent-dos-attacks-2019-general-election

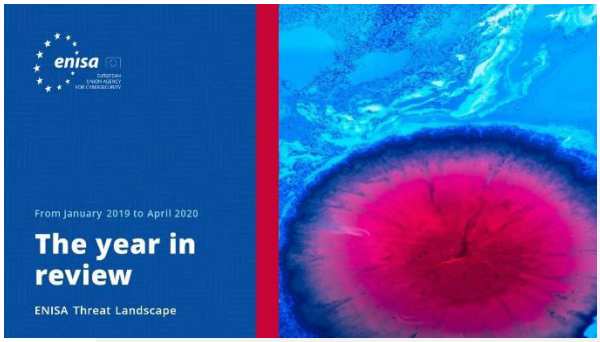
**21.** V. Revuelto, S. Meintanis, K. Socha. „DDoS Overview and Response Guide". 10 marca 2017 r. CERT-EU. https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf

**22.** „State of the Internet/Security DDoS and Application Attacks, Volume 5, Issue 1". 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf

**23.** P. Fergusson, D. Senie. „Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing". Maj 2000 r. IETF Tools. https://tools.ietf.org/html/bcp38

**24.** Pierluigi Paganini. „Cyber Defense Magazine Sept Edition 2019". 4 września 2019 r. SecurityAffairs. https://securityaffairs.co/wordpress/90795/breaking-news/cyber-defense-magazine-september-2019.html

# 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**

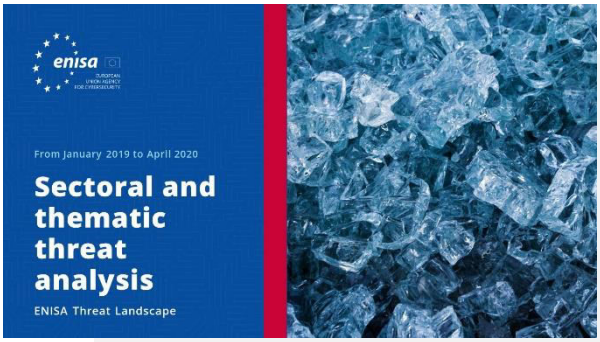
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

**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 odpornością 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.

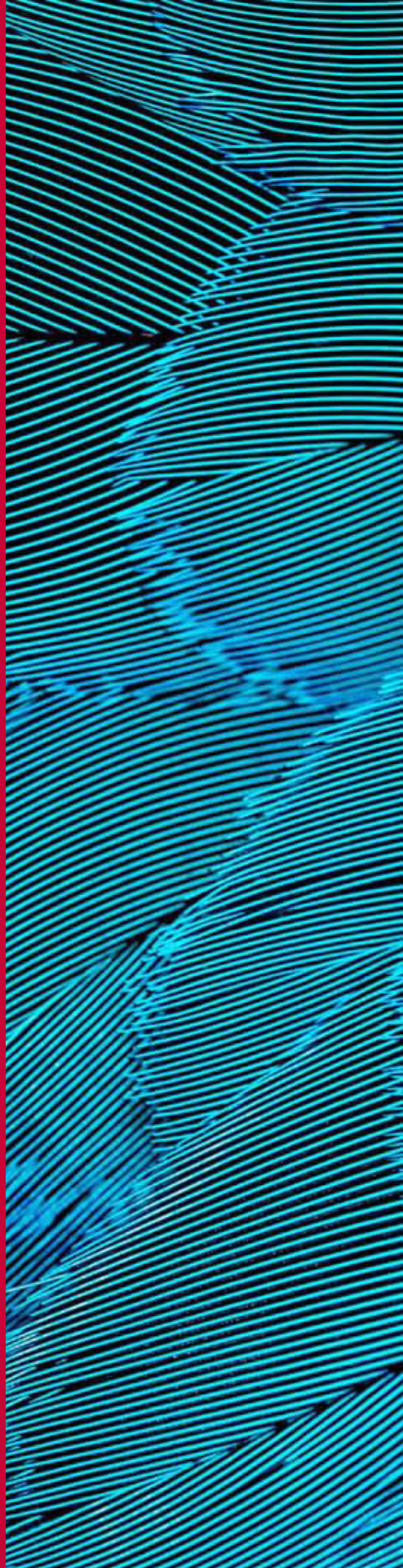
Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

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