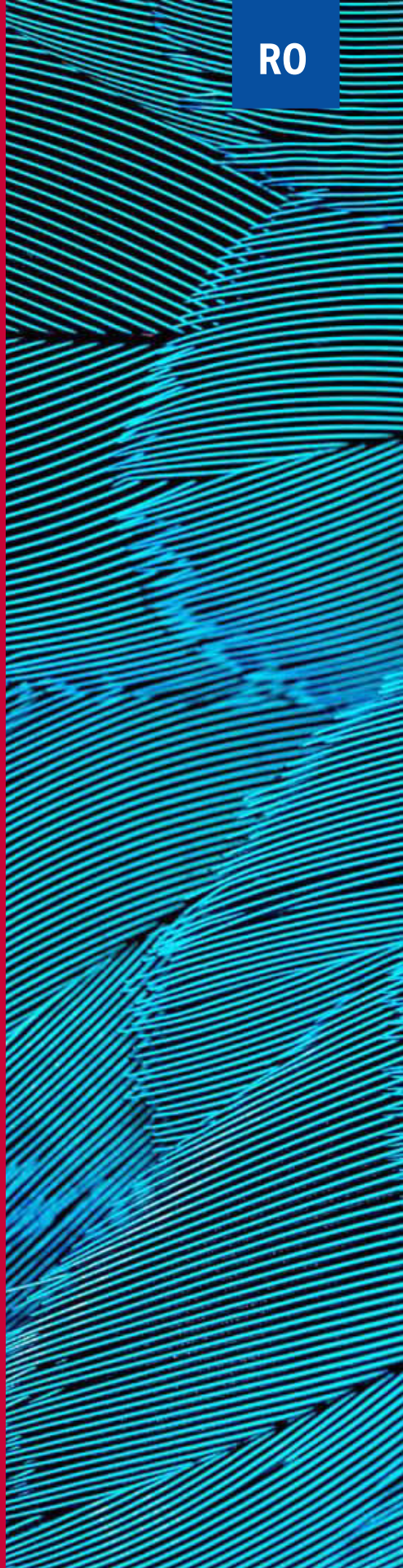
RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



ianuarie 2019 – aprilie 2020

# Blocarea distribuită a serviciului (DDoS)

## Raportul ENISA privind situația amenințărilor

# Prezentare generală

Se știe că atacurile de blocare distribuită a serviciului (DDoS) apar atunci când utilizatorii unui sistem sau serviciu nu pot accesa informațiile, serviciile sau alte resurse relevante. Această etapă poate fi realizată prin epuizarea serviciului sau supraîncărcarea componentei infrastructurii rețelei.[1] Actorii rău intenționați au mărit numărul de atacuri vizând mai multe sectoare, cu motive diferite. În timp ce mecanismele și strategiile de apărare devin din ce în ce mai robuste, actorii rău intenționați își dezvoltă, de asemenea, abilitățile tehnice. Rapoartele[3,4,5] sugerează că a crescut utilizarea tehnicilor de atac reflectate și amplificate care facilitează noi vectori, în afară de cei cunoscuți în mod obișnuit (amplificarea UDP etc.).[6] Actorii rău intenționați își îmbunătățesc și tacticile comerciale, începând să-și promoveze serviciile pe internet. Din punct de vedere istoric, serviciile DDoS au fost promovate în forumurile „dark web", dar în prezent folosesc canale comune de socializare precum YouTube și Redit pentru a-și promova serviciile.[2]

În 2019, se observă noi intrări în lista primelor 10 țări sursă care generează trafic DDoS (Hong Kong, Africa de Sud etc.).[7] De asemenea, a fost anul în care s-a observat o creștere a activității DDoS prin rețelele botnet. Dispozitivele IoT constituie un „focar" pentru botnet-uri DDoS, iar China (24 %), Brazilia (9 %) și Iranul (6 %) au fost considerate țările cele mai infectate cu agenți botnet.[3] Un cercetător în domeniul securității a prezis că, implementarea și distribuția rețelelor 5G va determina o creștere exponențială a numărului de dispozitive conectate, de unde extinderea rețelelor botnet.[3]

Deși atacurile DoS nu sunt noi pentru securitatea cibernetică și apărătorii rețelei, nivelul lor de complexitate este în creștere și se observă că actorii rău intenționați desfășoară activ mai multe activități de recunoaștere decât înainte.[3,8]

# Constatări

**241 %_** creștere a numărului total de atacuri în T3 2019 comparativ cu aceeași perioadă a anului 2018[3]

**79,7 %_** din toate atacurile DDoS au fost SYN-Floods[7]

**86 %_** din atacurile atenuate din T3 2019 foloseau mai mult de doi vectori[9]

**84 %_** din atacurile DDoS au durat mai puțin de 10 minute[10,11]

**509_** ore a fost durata celui mai lung atac DDoS din T2 2019[3]

# Kill chain

**Blocarea serviciului**

| Recunoaștere | Înarmare | Livrare | Exploatare |
|---|---|---|---|

*Etapa fluxului de activitate de atac*

*Amploarea scopului*

Instalare

Comandă și control

Acțiuni privind obiectivele

Cadrul Cyber Kill Chain® a fost dezvoltat de Lockheed Martin, fiind adaptat după un concept militar legat de structura unui atac. Pentru a studia un anumit vector de atac, utilizați această diagramă kill-chain pentru a trasa fiecare etapă a procesului și a face referire la instrumentele, tehnicile și procedurile utilizate de atacator.

MAI MULTE INFORMAȚII

## Cele mai importante cinci atacuri DDoS

**INUNDAȚII SYN DE 500-580 MILIOANE DE PACHETE PE SECUNDĂ.** Dintre toate tehnicile utilizate de actorii rău intenționați, inundația SYN este considerată în continuare un tip de atac dificil de combătut pe baza caracteristicilor sale, a infrastructurii vizate și a faptului că necesită mai mult hardware pentru a gestiona un volum mare de pachete. În ianuarie 2019, un cercetător în domeniul securității a observat un record de activitate de inundații SYN care distribuia 500 de milioane de pachete pe secundă (mpps) vizând unul dintre clienții săi, iar ulterior, în aprilie 2019, volumul a crescut la 580 mpps.[12]

**WS-DISCOVERY.** Web services dynamic discovery[13] (WS-Discovery) este un protocol de descoperire multicast. S-a observat că acesta este utilizat mai ales de dispozitivele IoT pentru a descoperi automat fiecare nod din rețelele locale (LAN), dar, la fel ca alte protocoale, nu poate fi utilizat doar pentru scopul propus, în special în domeniul IoT.[5] Actorii rău intenționați l-au considerat un teren propice pentru amplificarea atacurilor. Un cercetător în domeniul securității a raportat[3] un factor de amplificare de 95x, în timp ce un alt cercetător a raportat o creștere de 15 000 % în comparație cu dimensiunea originală a octeților.[14]

**ATACURI REFLECTATE ȘI AMPLIFICATE.** Aceste tipuri de atacuri sunt cunoscute demult și pe scară largă ca prezentând o solicitare mică pentru a furniza o sarcină utilă mai mare. Pe scurt, actorul rău intenționat va falsifica adresa IP a expeditorului (victima) și, ulterior, gazda destinatarului va trimite toate răspunsurile aferente victimei.[9] Această metodologie este eficace în principal pe protocolul bazat pe UDP datorită naturii lor fără conexiune și a factorului de amplificare (și anume, CLDAP are un factor de amplificare de x50-x70). Cu toate acestea, protocolul TCP nu este predispus la acest tip de atac.[15]

Un bun exemplu de astfel de tentative sunt atacurile de inundații SYN-ACK reflectate și amplificate – acest tip de inundație nu trebuie să aibă neapărat o lățime de bandă mare pentru a avea impact. În schimb, având un raport ridicat de pachete pe secundă, se poate menține atacul sub radar și îi crește eficacitatea.[3]

**ATACURI DDoS TIP BIT-AND-PIECE/CARPET BOMBING.** Se știe că acest tip de atac negativ de serviciu (DRDoS) distribuit și reflectant vizează în principal industriile furnizorilor de servicii de telecomunicații.[17] Într-un exemplu[18] de astfel de atac, a fost vizată o selecție aleatorie de adrese IP ale unui furnizor de servicii de internet, pentru a reflecta traficul către routerele tip edge ale furnizorului. Astfel, victima nu a reușit să identifice DDoS până când serviciul său a fost copleșit de propria gamă IP selectată.[19]

**ATACURI DDOS CU VECTORI MULTIPLI.** Actorii rău intenționați efectuează adesea vectori multipli de atacuri DoS pentru a adăuga complexitate și varietate încercării lor. Aceasta înseamnă că, prin simpla automatizare a diferitelor tipuri de atac asupra stratului de aplicație (inundație HTTP, inundație DNS etc.) și asupra stratului rețea (reflectare/amplificare UDP/TCP etc.), se va urmări maximizarea impactului prin saturarea lățimii de bandă, precum și a resurselor sau serviciilor în mediul vizat.[16]

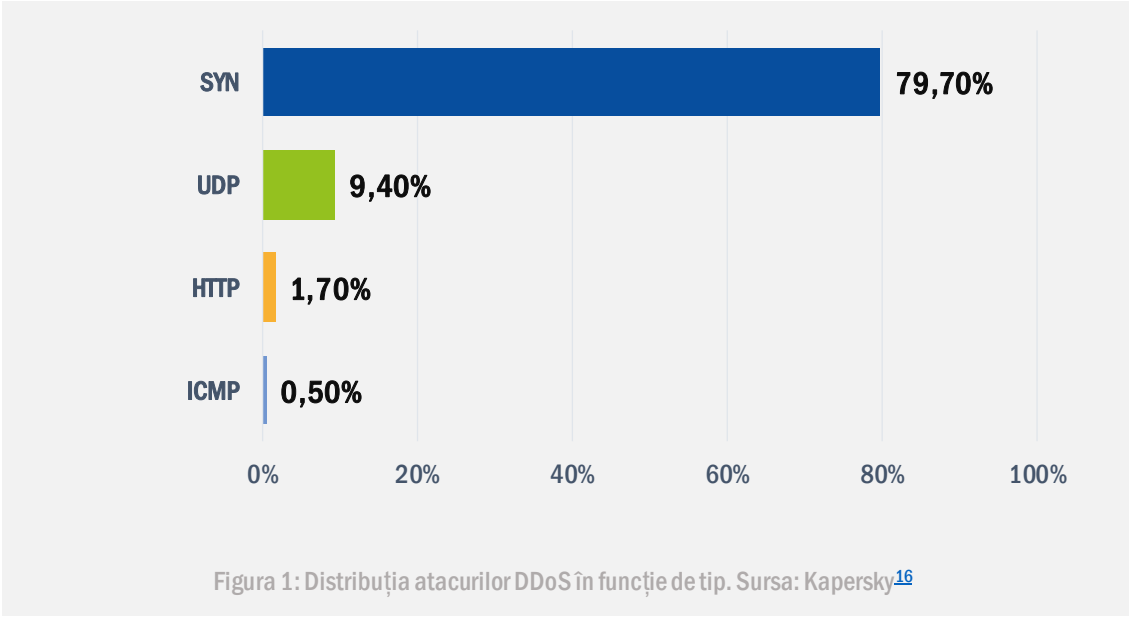



Figura 1: Distribuția atacurilor DDoS în funcție de tip. Sursa: Kapersky[16]

# Vectori de atac

## _ Modalitate

La fel ca anii precedenți, 2019 nu a făcut excepție în ceea ce privește inundațiile UDP. Potrivit unui cercetător în domeniul securității, inundația UDP a fost cel mai popular vector de atac, iar echipa consideră că acest lucru ar putea fi legat de adoptarea dominantă a acestui protocol în industriile cu risc ridicat, cum ar fi jocurile. Inundația SYN, răspunsul DNS și atacurile bazate pe TCP au urmat inundațiile UDP în lista celor mai importanți vectori de atac.

De asemenea, în această perioadă au fost observate atacuri cu vectori multipli. Cu toate acestea, un cercetător în domeniul securității consideră că unele dintre atacurile cu vectori multipli constituie un produs secundar neintenționat al unei tentative DoS.[11]

Un raport de securitate cibernetică[17] a sugerat că atacurile de amplificare DNS au fost observate de către echipa sa ca vector de atac DDoS de top, urmat de inundații HTTP și atacuri TCP SYN. Observările vectorilor de atac în T3 2019 au fost similare cu inundațiile SYN, vectorul de top urmat de atacurile UDP, TCP și HTTP.

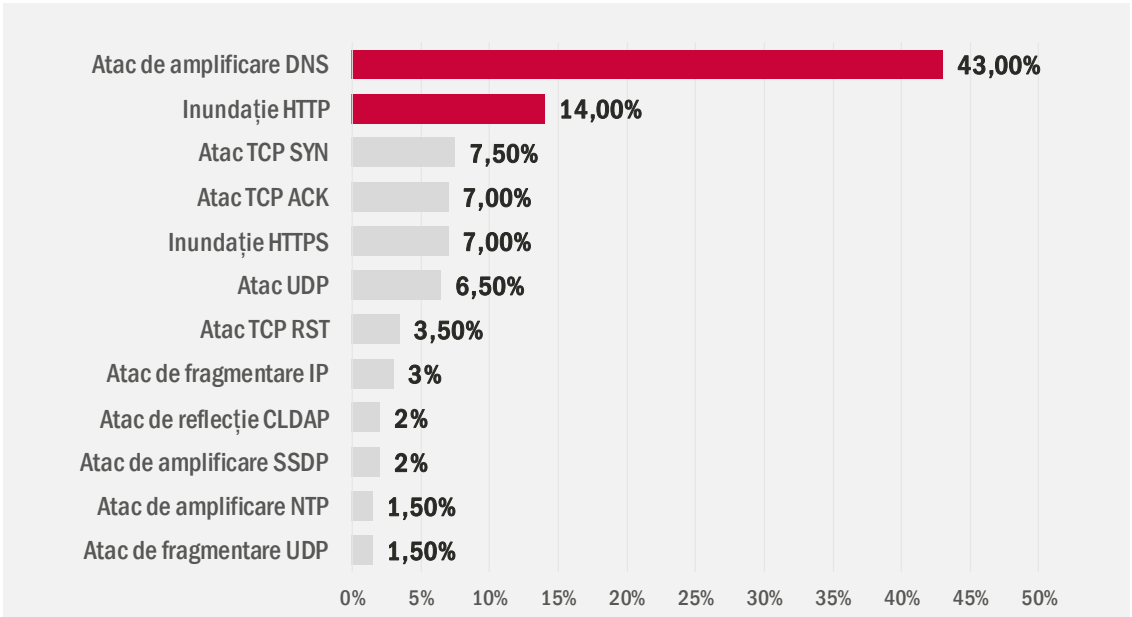



Figura 2: Distribuția vectorilor de atac DDoS. Sursa: NexusGuard[17]

## Durata atacului

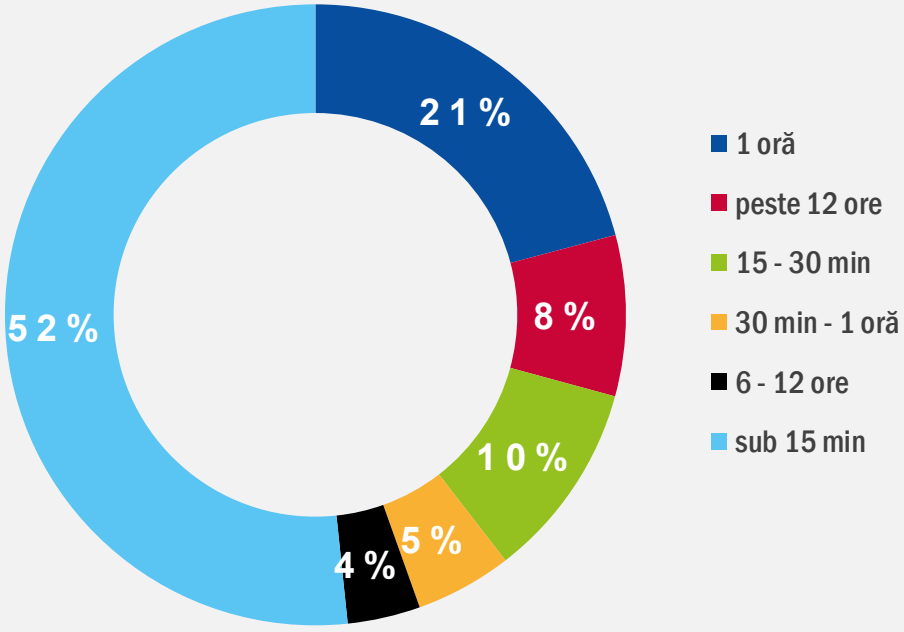



Figura 3 - Sursa: Imperva[11]

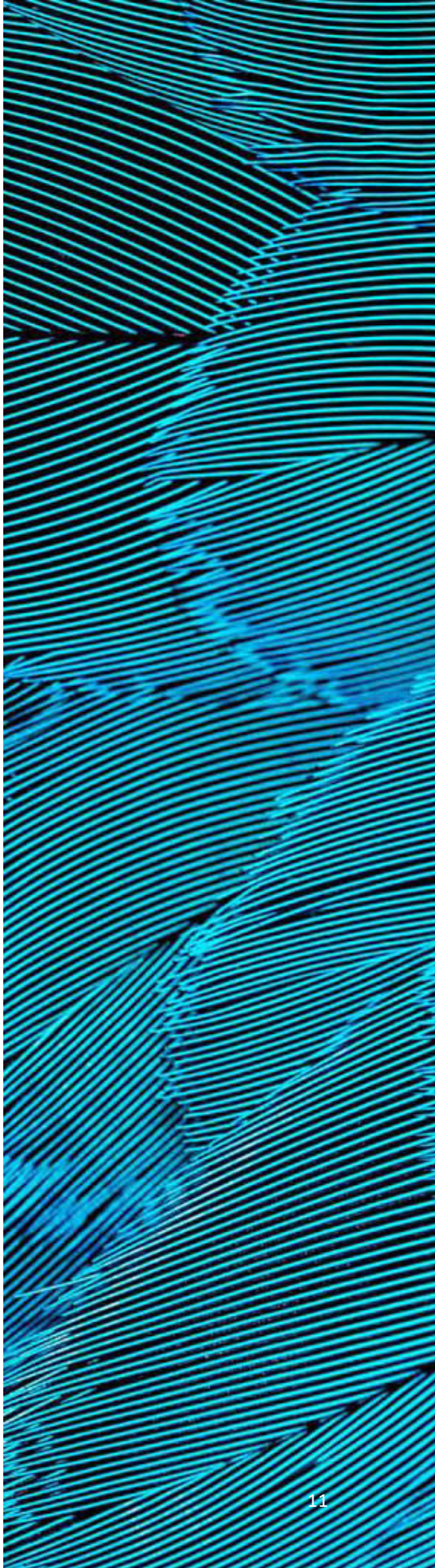
# Măsuri de atenuare

## Măsuri propuse

- Înțelegerea serviciilor și a resurselor critice și prioritizarea apărării acolo unde acestea pot fi suprasolicitate. Asigurarea existenței unui plan de răspuns pentru astfel de scenarii.[20]
- În funcție de cerințe, luarea în considerare a serviciului de protecție DDoS sau a unui furnizor de servicii gestionat DDoS. Utilizarea unor metode precum monitorizarea, pentru identificarea rapidă a infecțiilor.[1]
- Similar punctului de mai sus, publicarea serviciilor prin rețele de livrare a conținutului poate fi o modalitate eficientă de a absorbi tentativele volumetrice (necesită existența altor tehnici pentru atacuri mai sofisticate).[21]
- Furnizorii de servicii Internet și Cloud joacă un rol critic în apărarea împotriva atacurilor DDoS. Un plan și un canal de comunicare clar cu aceștia este cheia pentru un răspuns de succes la un atac de blocare a serviciului.
- Dezvoltarea unei posturi defensive proactive și puternice înainte de apariția unui eșec critic, implicând echipa și furnizorii aferenți pentru a configura și a regla controalele pe baza cerințelor comerciale specifice.[22] Facilitarea serverelor cache sau introducerea de interogări/cereri neadecvate în stratul aplicației la sursă și punerea în aplicare a BCP[23] pentru furnizorii de servicii sunt exemple bune de măsuri proactive.
- Asigurați-vă că testați și reevaluați tehnicile, tehnologiile și furnizorii de produse de apărare.
- Produceți un registru de risc analizând mediul în detaliu. Începeți de la activele critice din interior și mergeți spre amprenta și prezența dvs. pe Internet.[24]

**„Deși atacurile DDoS nu sunt noi pentru securitatea cibernetică și apărătorii rețelei, nivelul lor de complexitate este în creștere și se observă că actorii rău intenționați desfășoară în mod activ mai multe activități de recunoaștere decât înainte”**

**în ETL 2020**



# Referințe


1. „Understanding Denial-of-Service Attacks" (Înțelegerea atacurilor de blocare a serviciului), 20 noiembrie 2019. CISA. https://www.us-cert.gov/ncas/tips/ST04-015

2. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. „DDoS attacks in Q1 2019" (Atacuri DDoS în T1 2019), 21 mai 2019. Kaspersky. https://securelist.com/ddos-report-q1-2019/90792/

3. „Q4 2019 - The State of DDoS Weapons Report" (T4 2019 – Raport privind situația armelor DDoS) 2019. A10 Networks. https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

4. Chad Seaman. „Anatomy of a SYN-ACK Attack" (Anatomia unui atac SYN-ACK). 2 iulie 2019. 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%" (Un nou tip de atac DDoS poate amplifica puterea atacului cu peste 15.300 %). 18 septembrie 2019. 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" (Atacuri DDoS în T4 2018), 7 februarie 2019. Kaspersky. https://securelist.com/ddos-attacks-in-q4-2018/89565/

7. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. „DDoS attacks in Q3 2019" (Atacuri DDoS în T3 2019), 11 noiembrie 2019. Kaspersky. https://securelist.com/ddos-report-q3-2019/94958/

8. „2019 Website Threat Research Report" (Raport de cercetare a amenințărilor asupra site-urilor web 2019). 2019. Sucuri

9. „DDoS attacks up 241% in Q3 2019 compared to same period last year" (Numărul de atacuri DDoS a crescut cu 241 % în T3 2019 comparativ cu aceeași perioadă a anului anterior). 19 noiembrie 2019. 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" (Raport semestrial privind tendințele DDoS 2019). 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" (Raportul privind situația amenințărilor DDoS la nivel global 2019). 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" (Actualizare: Acest atac DDoS a dezlănțuit cele mai multe pachete pe secundă. Iată de ce este important). 30 aprilie 2019. 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" (Protocolul Web Services Dynamic Discovery (WS-Discovery) Versiunea 1.1), 1 iulie 2009. 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" (Nou vector DDoS observat în sălbăticie: atacurile WSD lovesc 35/Gbps). 18 septembrie 2019. 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" (Alertă de amenințare: atacuri de amplificare TCP). 9 noiembrie 2019. 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" (Conform raportului Kaspersky, peste jumătate din atacurile DDoS din T3 au avut loc în septembrie). 11 noiembrie 2019. 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" (Raport privind amenințările DDoS T1 2019). 2019. NexusGuard. https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q1

18. „International traffic – DDoS" (Trafic internațional – DDoS). 22 septembrie 2019. 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" [Atacul DDoS prin bombardare cu saturație (carpet-bombing) doboară ISP-ul din Africa de Sud pentru o zi întreagă]. 24 septembrie 2019. 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" (Îndrumări în urma atacurilor DoS recente, înaintea alegerilor generale din 2019). 13 noiembrie 2019. NCSC. https://www.ncsc.gov.uk/guidance/guidance-following-recent-dos-attacks-2019-general-election

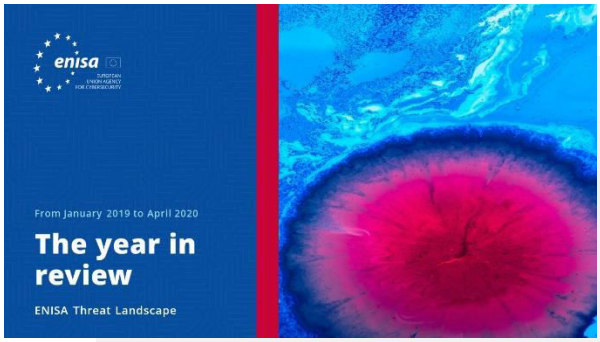
**21**. V. Revuelto, S. Meintanis, K. Socha. „DDoS Overview and Response Guide" (Prezentare generală și ghid de răspuns DDoS). 10 martie 2017. CERT-EU. https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf

**22.** „State of the Internet/Security DDoS and Application Attacks, Volume 5, Issue 1" (Starea securității internetului: DDoS și atacuri asupra aplicațiilor, volumul 5, numărul 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" (Filtrarea intrării în rețea: înfrângerea atacurilor de blocare a serviciului care utilizează falsificarea adreselor IP sursă). Mai 2000. IETF Tools. https://tools.ietf.org/html/bcp38

**24.** Pierluigi Paganini. „Cyber Defense Magazine Sept Edition 2019" (Revista Cyber Defense, ediția septembrie 2019). 4 septembrie 2019. SecurityAffairs. https://securityaffairs.co/wordpress/90795/breaking-news/cyber-defense-magazine-september-2019.html

# Documente conexe




Raportul ENISA privind situația amenințărilor **Trecerea în revistă a anului**

Rezumat al tendințelor de securitate cibernetică pentru perioada ianuarie 2019 – aprilie 2020.

**CITIȚI RAPORTUL**


Raportul ENISA privind situația amenințărilor
**Lista celor mai importante 15 amenințări**

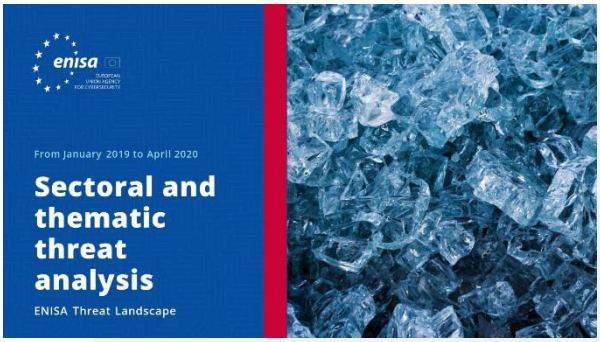
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

**CITIȚI RAPORTUL**


Raportul ENISA privind situația amenințărilor
**Teme de cercetare**

Recomandări privind teme de cercetare din diferite sectoare din securitatea cibernetică și informațiile privind amenințările cibernetice.

**CITIȚI RAPORTUL**




CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Analiza sectorială și tematică a amenințărilor**

Analiza contextualizată a amenințărilor în perioada ianuarie 2019 - aprilie 2020.


CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Tendințe emergente**

Principalele tendințe în securitatea cibernetică observate în perioada ianuarie 2019 - aprilie 2020.


CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
**Prezentare generală a informațiilor privind amenințările cibernetice**

Situația actuală a informațiilor privind amenințările cibernetice în UE.

# Despre

## _Agenție

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică
contribuie la politica cibernetică a UE, sporește credibilitatea produselor, serviciilor și proceselor TIC cu ajutorul sistemelor de certificare a securității cibernetice, cooperează cu statele membre și organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu părțile interesate cheie pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, în cele din urmă, pentru a menține securitatea digitală a societății europene și a cetățenilor. Mai multe informații cu privire la ENISA și activitatea sa sunt disponibile la adresa www.enisa.europa.eu.


**Contribuitori**

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) și *toți membrii Grupului părților interesate al ENISA CTI:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) și Thomas Hemker.

**Editori**

Marco Barros Lourenço (ENISA) și Louis Marinos (ENISA).

**Date de contact**

Pentru întrebări despre această lucrare, vă rugăm să utilizați adresa enisa.threat.information@enisa.europa.eu.

Pentru întrebări din partea mass-media despre această lucrare, vă rugăm să utilizați adresa press@enisa.europa.eu.


**Dorim să aflăm părerea dumneavoastră despre acest raport!**
Vă rugăm să acordați câteva momente completării chestionarului. Pentru a accesa formularul, faceți clic aici.

**Aviz juridic**

Trebuie luat în considerare faptul că această publicație reprezintă punctele de vedere și interpretările ENISA, cu excepția cazului în care se prevede altfel. Această publicație nu trebuie interpretată ca o acțiune juridică a ENISA sau a organismelor ENISA, cu excepția cazului în care aceasta a fost adoptată în conformitate cu Regulamentul (UE) nr. 526/2013. Această publicație nu reprezintă neapărat stadiul actual al tehnologiei și ENISA o poate actualiza periodic.

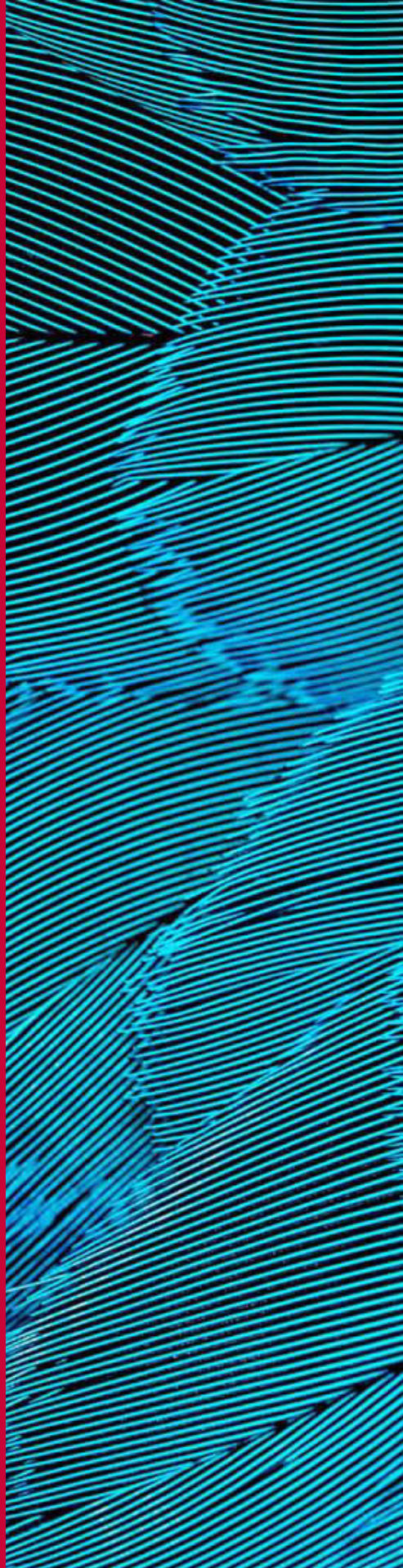
Sursele terțe sunt citate corespunzător. ENISA nu este responsabilă pentru conținutul surselor externe, inclusiv al site-urilor externe menționate în această publicație.

Această publicație are doar scop informativ și rebuie să fie accesibilă în mod gratuit. Nici ENISA și nici persoanele care acționează în numele său nu sunt responsabile pentru modul în care ar putea fi utilizate informațiile conținute în această publicație.



**ISBN:** 978-92-9204-354-4
**DOI:** 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Telefon: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



https://www.enisa.europa.eu