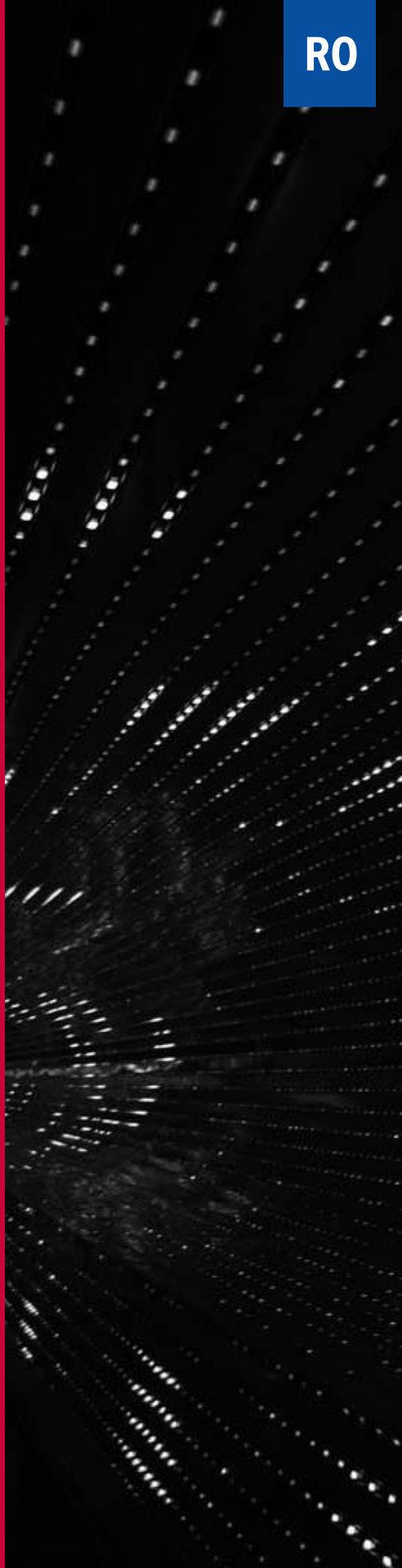
RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



Ianuarie 2019 – aprilie 2020

Botnet

Raportul ENISA privind situația amenințărilor

Prezentare

Botnet este o rețea de dispozitive conectate infectate cu malware bot. Aceste dispozitive sunt utilizate în mod obișnuit de către actori rău intenționați pentru a desfășura atacuri de blocare distribuită a serviciului (DDoS). Operând într-un mod peer-to-peer (P2P)[1] sau dintr-un centru de comandă și control (C2)[2], rețelele botnet sunt controlate de la distanță de un actor rău intenționat pentru a opera într-un mod sincronizat în vederea obținerii unui anumit rezultat.[3]

Progresele tehnologice în domeniul calculului distribuit și al automatizării au creat o oportunitate pentru actorii rău intenționați de a explora noi tehnici și a-și îmbunătăți instrumentele și metodele de atac. Datorită acestui fapt, rețelele botnet funcționează în moduri mult mai distribuite și automatizate și sunt disponibile de la furnizorii de servicii cu autoservire și gata de utilizare.

Boții rău intenționați, denumiți „boți răi”, nu numai că evoluează constant, dar abilitățile oamenilor și nivelul de dezvoltare al boților devin extrem de specializate în anumite aplicații, cum ar fi furnizorii de servicii de apărare sau chiar tehnicile de evaziune.[4] Dintr-o perspectivă diferită, botnet-urile oferă un vector pentru ca infractorii cibernetici să lanseze diverse operațiuni de la fraudă în e-banking la ransomware, minarea criptomonedelor și atacuri DDoS.[5]

Constatări

7,7_milioane de dispozitive IoT sunt conectate la internet în fiecare zi

Dintre acestea, se estimează că 1 din 20 de dispozitive se află în spatele unui firewall sau al unor instrumente similare de securitate a rețelei.[6]

57 %_creștere a numărului de variante Mirai detectate în 2019

Deși se știe că variantele Mirai folosesc predominant tentative prin forță brută (brute force) pentru compromiterea dispozitivelor IoT, în cursul anului 2019 s-a înregistrat o creștere atât a tentativelor de tip forță brută (51 %), cât și a tentativelor de exploatare a internetului (87 %).[7]

300 000_de notificări ale traficului de botnet Emotet observate în cursul anului 2019

Aceasta reprezintă cu peste 100 000 de alerte de victime mai mult decât în aceeași perioadă din 2018. Cercetătorii au considerat că s-a înregistrat o creștere cu 913 % a numărului de eșantioane Emotet comparativ cu a doua jumătate a anilor 2018 și 2019.[7]

60 %_din activitatea botnet-urilor rivale noi este asociată cu furtul de date de identificare[9]

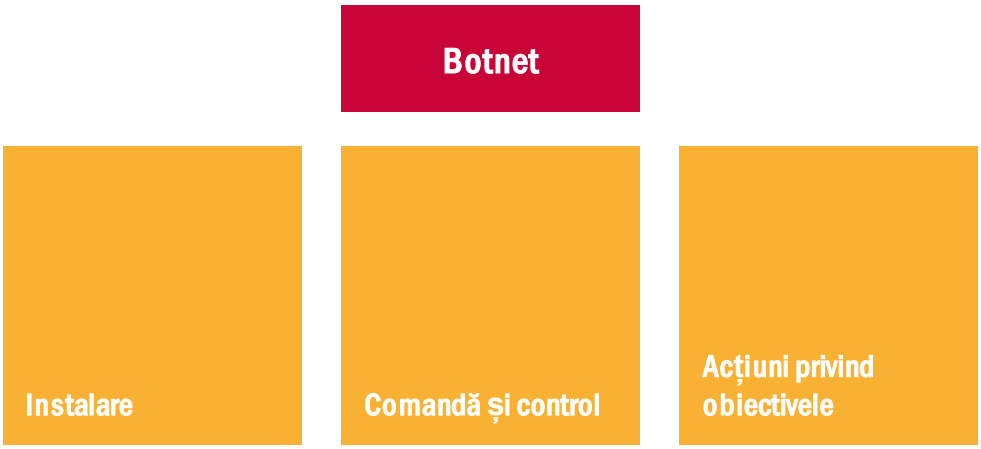
17 602_ servere C2 pentru botnet-uri complet funcționale găsite în 2019

o creștere cu 71,5 % față de anul 2018.[5]

Kill chain

Etapă din fluxul de activitate de atac

Amploarea scopului



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

Tendințe

_Boții înseamnă sume mari de bani

Boții facilitează capabilitățile forței brute ademenind victimele să cumpere articole în ediție limitată sau articole din oferte promoționale și, ulterior, să le revândă la un preț mai mare. Acest fapt a fost identificat prin analiza unei oferte de muncă în care persoana care a publicat anunțul căuta un dezvoltator de software cu experiență în eludarea mijloacelor de apărare de securitate, creând boți cu tehnici de eludare (de exemplu, informații extrase de pe site-uri de internet, evitarea reCAPTCHA, generarea de cookie-uri etc.) și fiind dispus să plătească 15 000 USD (aproximativ 12 750 EUR) pentru candidatul potrivit.[4]

_Silexbot de blocare

În iunie 2019, un cercetător din domeniul securității[17] a analizat un nou eșantion de bot dezvoltat pentru a perturba funcționalitățile dispozitivelor IoT nesigure. Cu alte cuvinte, acest bot a fost conceput pentru a utiliza datele de identificare cunoscute/implicite ale dispozitivelor IoT pentru a se conecta și, ulterior, a distruge dispozitivul prin ștergerea configurațiilor de rețea și adăugarea unei reguli a tabelelor IP de a suspenda toate conexiunile. Pe lângă capacitățile tehnice, un element interesant a fost nota lăsată pe eșantionul de malware[7]. Factorul de amenințare își cere scuze pentru activitatea sa și explică acțiunile sale ca o modalitate de a preveni exploatarea în masă a dispozitivelor IoT nesigure pentru a construi rețele bot în scopuri rău intenționate.

_Echobot și vectorul său de amenințare în creștere

În iunie 2019, un cercetător în domeniul securității a identificat o versiune actualizată a Echobot. În analiza respectivă, cercetătorul a observat un eșantion compilat x86 care duce la vectori de atac utilizați de această variantă Mirai în 26 de incidente diferite.[10] În luna august, un alt cercetător în domeniul securității a constatat o creștere a Echobot exploatând 50 de vulnerabilități diferite, inclusiv „injectarea comenzilor prin HTTP" (CPAI-2016-0658).[25,26] În decembrie 2019, o altă echipă a detectat o versiune îmbunătățită a Echobot incluzând 71 de exploit-uri. Exploit-urile nou adăugate vizau vulnerabilități vechi și noi și aveau o capacitate adăugată semnificativă de a viza dispozitivele sistemului de control industrial (ICS). Acestea au inclus companii și dispozitive precum Mitsubishi, controale de livrare a aplicațiilor Citrix NetScaler, firewall pentru aplicații web Barracuda și instrumente de gestionare a punctelor de ieșire.[27]

_Necurs este în scădere, în timp ce Emotet este din nou în creștere

În ianuarie 2019, s-a observat că Necurs a trecut la o campanie de spam de tip amator, ceea ce i-a determinat pe cercetători să considere că actorii rău intenționați din spatele acesteia au înregistrat o scădere semnificativă a abilităților.[20] În schimb, activitatea Emotet a crescut substanțial din septembrie 2019 și a continuat să crească spre sfârșitul anului 2019, livrând binare compilate unice care reprezintă vectorul de livrare persistent și mecanisme de comunicare.[7] O analiză a relevat o creștere accentuată a distribuției Emotet prin e-mail.[22]

Tendințe

_Retadup, botnetul din spatele Monero-Mining a căzut

Retadup a fost activ în cea mai mare parte ca viermele Monero-mining care a dezvoltat capacități polimorfe.[23] Acesta a infectat dispozitive Windows în America Latină. Acest bot avea capacități variind de la minare la aplicarea unui cod personalizat și a descărcat fișiere pe dispozitivele victimelor (s-a observat, de asemenea, că distribuie programul de ransomware STOP[24]). Un cercetător în domeniul securității a început să monitorizeze activitatea Retadup în martie 2019 și a observat că protocolul C2 a fost conceput într-un mod simplu. Echipa a identificat o eroare în protocol care le-a permis să elimine infecțiile de la victimă prin preluarea serverului C2. Infrastructura pentru această activitate rău intenționată a fost identificată ca aflându-se în cea mai mare parte în Franța. Botnetul a fost eliminat cu colaborarea Jandarmeriei Naționale (Franța) și au fost dezinfectate aproximativ 850 000 de calculatoare.

_Mirai a murit, trăiască Mirai

Este posibil ca, tocmai din cauza lipsei de abilități și caracteristici din codul original, Mirai și variante sale să domine în continuare în cadrul familiilor de botnet, peste 20 000 de eșantioane unice fiind observate lunar în prima jumătate a anului 2019. Aceste variante utilizează diferite tehnici pentru compromiterea IoT-urilor, de la parole implicite puternic codificate sparte prin forță brută la exploit-uri.[6] De asemenea, există o mare diversitate de arhitecturi de sistem vizate de aceste variante, potrivit a doi cercetători în domeniul securității. Mai multe statistici despre activitatea Emotet sunt prezentate în Figura 1.[7,18]

_Botnetul P2P Robotop

Activitatea lui Robotop a fost observată pentru prima dată în august 2019 de către o echipă de cercetare a securității ca program botnet P2P. Primul eșantion capturat a fost un fișier ELF suspect. În cursul lunii octombrie, echipa de cercetare a identificat un alt eșantion (fișier ELF) care se dovedește a fi programul de descărcare a eșantionului anterior. La o analiză ulterioară, echipa de cercetare a descoperit că botnetul Robotop poate suporta șapte funcții, și anume tunel invers (reverse shell), auto-dezactivare, colectarea informațiilor despre proces și rețea, colectarea informațiilor despre bot, executarea fișierelor cu URL specificat, atacuri DDoS și desfășurarea de atacuri de sistem. În mod interesant, se pare că un atac DDoS nu este principalul său caz de utilizare, potrivit cercetătorului. Spre deosebire de alte rețele botnet, acest bot se răspândea prin exploatarea vulnerabilității Webmin RCE (CVE-2019-1507[28]).[11]

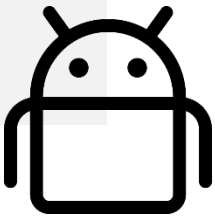
_Mozi, un alt botnet bazat pe DHT

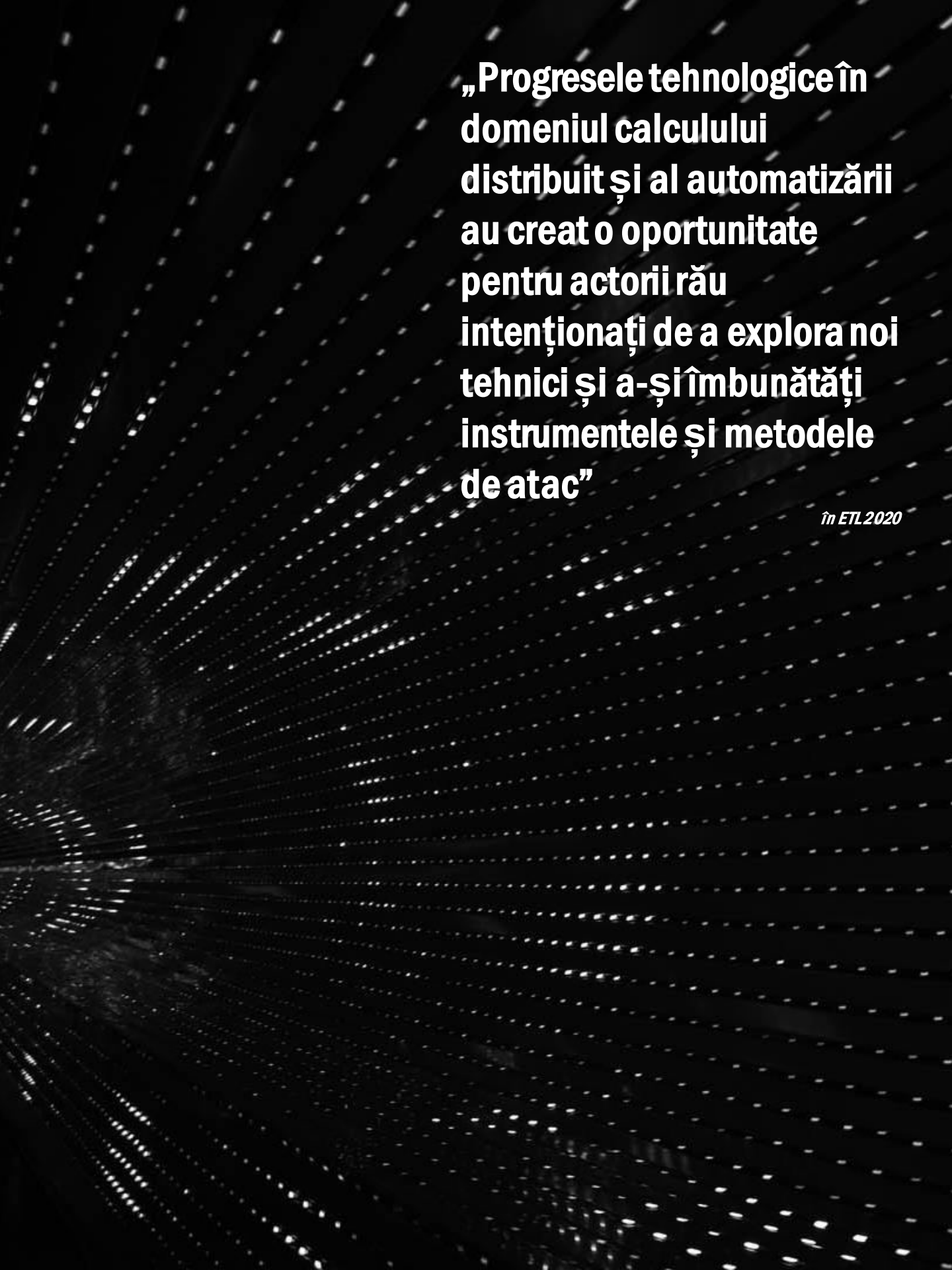
Desemnat după numele său de fișier de propagare, Mozi a fost identificat ca un botnet nou bazat pe DHT, observat de un cercetător în domeniul securității în septembrie 2019. O analiză inițială a eșantionului efectuată de un alt cercetător în domeniul securității[38] l-a identificat ca fiind Gafgyt. Aceasta se datorează însă faptului că eșantionul a reutilizat parțial codul de la Gafgyt. Acest botnet se răspândește utilizând câteva exploit-uri și exploatând parole slabe pentru telnet. Analiza funcționalităților sale a arătat că ar putea fi capabil să ruleze atacuri DDoS, să culeagă informații, să execute și să actualizeze eșantionul/sarcina (payload) utilizând un URL specificat și să execute comenzi.[29, 30]

Statistici despre activitatea Emotet

Constatare	Statistică
Numărul total de ASn detectate:	5 430
Numărul total de adrese IP unice detectate:	120 764
Număr total de țări participante:	193
Număr total de e-mailuri trimise:	10 935 346
Număr total de adrese URL de distribuție:	4 726
RCPT distincte vizate:	8 052 961

Figura 1: Sursa: Spamhaus[5]





„Progresele tehnologice în domeniul calculului distribuit și al automatizării au creat o oportunitate pentru actorii rău intenționați de a explora noi tehnici și a-și îmbunătăți instrumentele și metodele de atac”

în ETL 2020

Statistici și alte cifre relevante

Potrivit unui cercetător în domeniul securității, **7,7 milioane de dispozitive IoT sunt conectate la Internet în fiecare zi** și se estimează că doar 1 din 20 se află în spatele unui dispozitiv de tip firewall sau al unui instrument similar de securitate a rețelei.[6] Această estimare relevă faptul că **dispozitivele IoT sunt încă vulnerabile și susceptibile la exploatare** prin amenințări de securitate cibernetică, cum ar fi Mirai.

- În prima jumătate a anului 2019, activitatea botnet-urilor și găzduirea serverelor C2 au crescut substanțial.[32] Această creștere a reprezentat 7 % din toate detecțiile de botnet și 1,8 % din C2-urile din întreaga lume. Serviciile financiare și clienții lor au fost sectorul vizat cel mai des.
- Thailanda a fost prima țară din top în ceea ce privește găzduirea serverelor C2, în timp ce Malaezia a ocupat locul al doilea, urmată de Filipine, Singapore și Indonezia.
- Pe baza cercetărilor Interpol, botnetul Andromeda a fost cel mai dominant în ceea ce privește detectarea, deși a fost eliminat în 2017.[33] Conficker[34] a ocupat locul al doilea, urmat de Necurs[35], Sality[36] și Gozi[37].

În cursul anului 2019, numărul de variante Mirai detectate a crescut cu peste 57 %, comparativ cu 2018, astfel cum se arată în figura 2.

Deși se știe că variantele Mirai utilizează tentative prin forță brută (brute force) predominant pentru compromiterea dispozitivelor IoT, în cursul anului 2019 a existat o creștere atât a tentativelor prin forță brută (51 %), cât și a tentativelor de exploatare a internetului (87 %).

Numărul de eșantioane Mirai

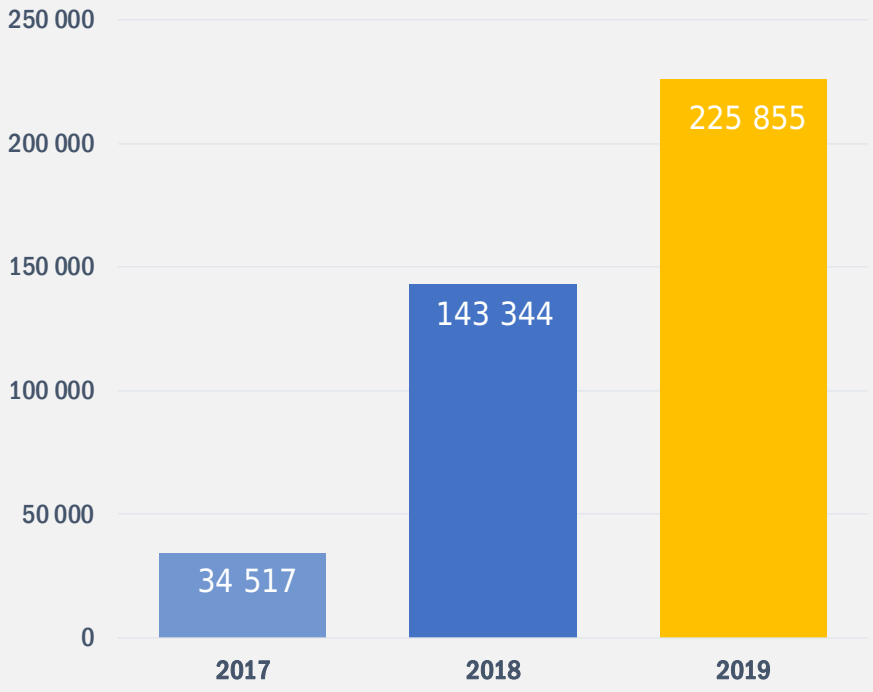


Figura 2 - Sursa: NETSCOUT[7]

Constatări

_Statistici și alte cifre relevante

- În cursul anului 2019, un cercetător în domeniul securității a observat aproape 300 000 de notificări în plus cu privire la traficul de botnet Emotet și cu peste 100 000 de alerte de victime mai mult decât în aceeași perioadă din 2018. Cercetătorul consideră că a existat o creștere cu 913 % a numărului de eșantioane Emotet comparativ cu a doua jumătate a anilor 2018 și 2019.[7,22]
- S-a înregistrat o creștere a activității botnetului P2P de când Roboto și Mozi au devenit activi.[8]
- Botnet-urile bazate pe Linux au fost responsabile pentru aproape 97,4 % din atacuri.[8]
- Cea mai mare pondere de botnet-uri s-a înregistrat în Statele Unite (58,33 %) în trimestrul IV 2019. Deși aceasta reprezintă o creștere în comparație cu trimestrul III al anului 2019 (47,55 %), numărul total de servere C2 aproape s-a înjumătățit. Regatul Unit a ocupat locul patru și a ajuns pe locul al doilea cu 14,29 %, în timp ce China s-a menținut pe aceeași poziție, cu 9,52 %. Cea mai semnificativă scădere a serverelor înregistrate C2 s-a înregistrat în Țările de Jos (de la 45 % la ~ 1 %). Pentru mai multe informații despre distribuția serverelor C2 pentru botnet-uri pe țări, vezi figura 3.[8]
- În 2019, LokiBot a rămas în fruntea listei de boți care fură date de identificare, cu o creștere a numărului de activități C2 cu 74 % în comparație cu 2018. AZORult a fost pe locul doi imediat după LokiBot.[39]
- 17 602 servere C2 pentru botnet-uri erau operaționale în 2019, reprezentând o creștere cu 71,5 % în comparație cu 2018.[39]

Distribuția serverelor de C&C pentru botnet în funcție de țară

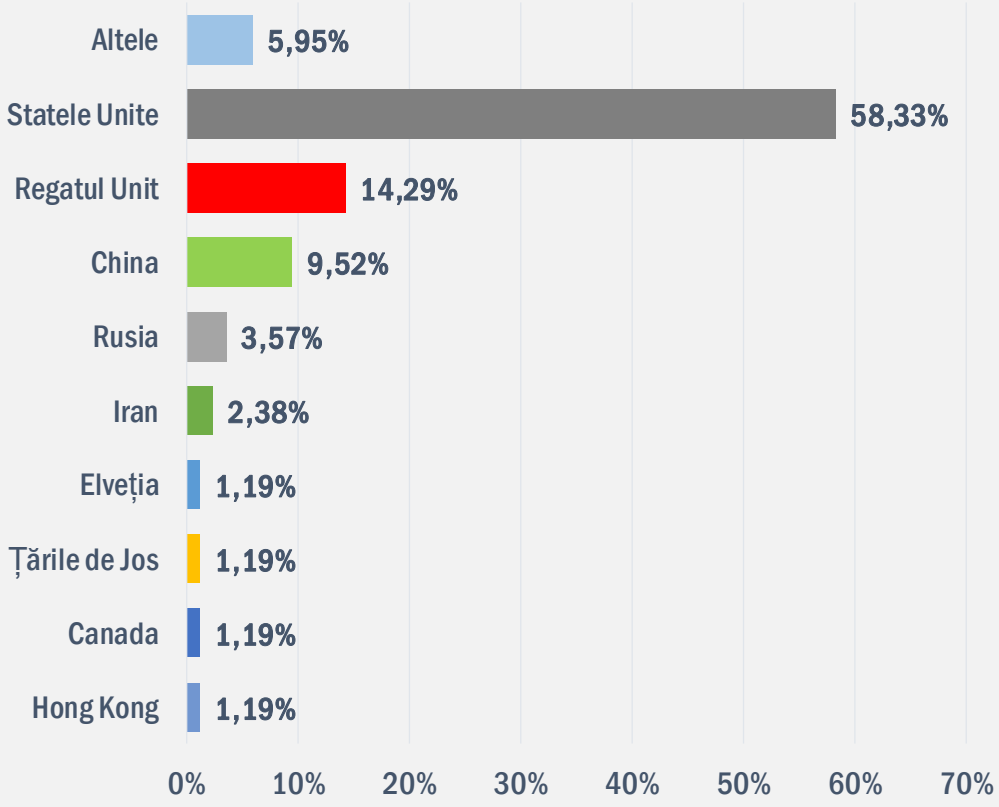


Figura 3 - Sursa: Kaspersky[8]

Vectori de atac

_ Atacuri prin botnet

Potrivit unui cercetător din domeniul securității, în 2019 aproape 60 % din activitatea botnet-urilor rivale noi a fost asociată cu **furtul de date de identificare**. După cum s-a menționat anterior, LokiBot este cel mai activ în acest domeniu. Pe lângă activitatea de furt de date de identificare, **serviciile bancare electronice și frauda financiară** sunt alte domenii în care prezența botnetului este vastă. Emotet și TrickBot sunt exemple primare ale acestei activități, cu un model actualizat care acoperă nu numai frauda în e-banking, ci și plata per instalare (pay-per-install – PPI).[9]

Mai mult, **troienii de acces la distanță (RAT)** au fost printre cele mai utilizate instrumente în activitățile rețelelor botnet C2. În cursul anului 2018, majoritatea acestor activități au fost asociate cu Adwind, dar în 2019 activitatea sa a fost redusă și înlocuită cu NanoCore.[5]

În 2019, **au fost adoptați vectori de atac specifici**. Botnet-urile folosesc diverși vectori de atac pentru a-și atinge obiectivele. Computerele infectate sau rețelele zombie sunt create prin exploatarea vulnerabilităților comune cu forță brută și alte tehnici comune de infecție.[10,11,12] Ulterior, botmasterul poate să ofere o platformă pentru diferite atacuri, inclusiv campania larg răspândită de spam și malware, furtul și reutilizarea datelor de identificare, minarea criptomonedelor și DDoS.

Un alt exemplu de vector de atac utilizatîntr-un atac de botnet este **„Triple Threat" (Amenințarea triplă)**. În această tehnică, organizația vizată este inițial infectată cu malware Emotet[7]. Apoi malware-ul Emotet furnizează troianul TrickBot, vizând și explorând informații sensibile. Dacă sunt găsite informațiile și mediul/rețeaua vizat(ă) se află în lista atacatorului, programul de ransomware Ryuk este livrat.[13]

Numărul de servere C2 pentru botnet-uri observate între 2014 și 2019

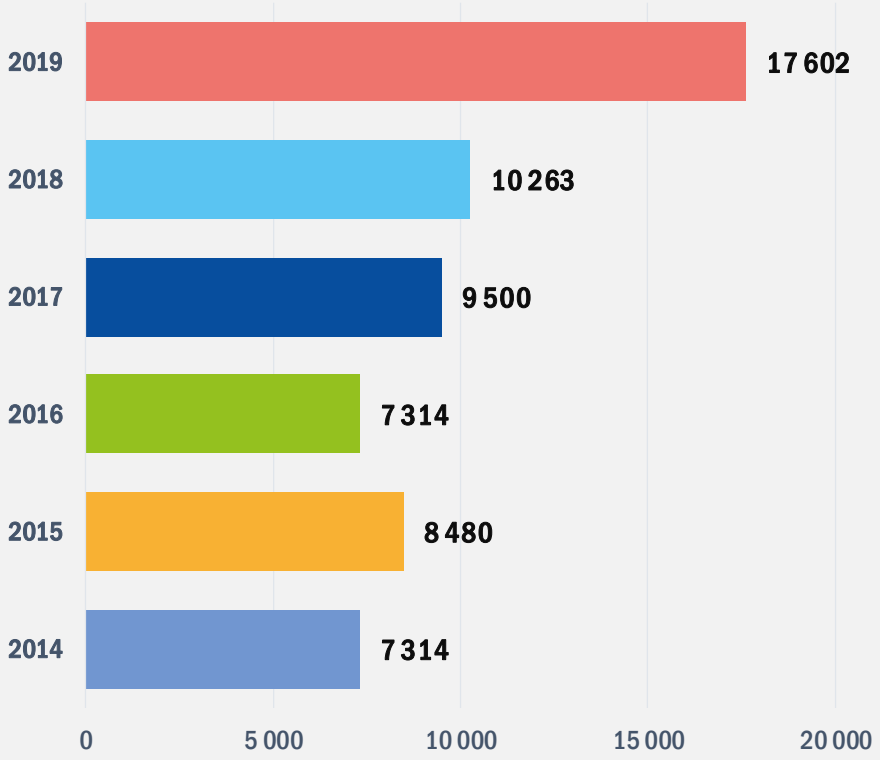


Figura 4 - Sursa: Spamhaus[5]

Măsuri de atenuare

_ Acțiuni propuse

Un aspect cheie al unei apărări solide este conceptul de cunoaștere a mediului. Acesta va contribui la identificarea activității rău intenționate în cadrul traficului pe baza posibilei linii de bază (și anume detecții comportamentale)[14] măsurată de un instrument de monitorizare a traficului.[4] Având în vedere că traficul substanțial de botnet este asociat cu activitatea DDoS, se aplică, de asemenea, tehnici de atenuare a amenințării DDoS.

- Implementarea unor fluxuri de protocol gateway de frontieră cu capacitatea de a căuta dTLD-uri (domenii descentralizate de nivel superior) pentru a bloca conexiunile la adrese IP legate de activitatea C2 a botnet-ului.[8]
- Înțelegerea și clasificarea vulnerabilităților și aplicarea unei practici puternice de corecție și actualizare.[15,16]
- Restricționarea sau blocarea pool-urilor de minare a criptomonedelor și monitorizarea mediului pentru utilizatorii necesari.[5]
- Implementarea capacităților bazate pe provocări pentru site-urile necesare pentru a verifica originea traficului (și anume reCAPTCHA).[16]
- Implementarea unor politici de parolă puternică și autentificare cu doi factori (2FA) pe servere sau infrastructură orientate către public pentru a evita să fie victima exploatării unei parole slabe/autentificări.[5]
- Implementarea și configurarea firewall-urilor de rețea și aplicație.

„Complexitatea capacităților de amenințare a crescut în 2019, mulți adversari folosind exploit-uri, furtul de date de identificare și atacurile în mai multe etape.”

în ETL 2020

Referințe

1. „Peer-to-peer (P2P).” Malwarebytes Labs https://blog.malwarebytes.com/glossary/peer-to-peer/

2. Monnappa K A. “Learning Malware Analysis” (Învățarea analizei malware) Iunie 2018. O'reilly. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d-9583-4d86-9d1e-8b2735af5168.xhtml

3. “ASEAN Cyberthreat Assessment 2020” (Evaluarea amenințării cibernetice în ASEAN în 2020) 17 februarie 2020. Interpol https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-key-cyberthreats-in-Southeast-Asia

4 “State of The Internet Security - DDoS and Application Attacks Report: Volume 5, Issue 1.” (Situația securității internetului – Raport privind atacurile DDoS și 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

5. „Spamhaus Botnet Threat Report 2019” (Raportul Spamhaus privind amenințarea botnet pe 2019) 28 ianuarie 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

6. „NETSCOUT Threat Intelligence Report: Powered by ATLAS - Findings from H1 2019” (Raportul NETSCOUT privind informații despre amenințări: elaborat de ATLAS – constatări din primul semestru al anului 2019) 2019.

7. „NETSCOUT Threat Intelligence Report - With key findings from the 15th Annual Worldwide Infrastructure Security Report (WISR) - Findings from H2 2019.” [Raportul NETSCOUT privind informații despre amenințări – cu principalele constatări din cel de al 15-lea Raport anual privind securitatea infrastructurii de la nivel mondial (WISR) - constatări din cel de-al doilea semestru al anului 2019] 2019. NETSCOUT. https://www.netscout.com/threatreport

8. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. „DDoS attacks in Q4 2019.” (Atacuri DDoS în trimestrul IV 2019) 13 februarie 2020. Kaspersky. https://securelist.com/ddos-report-q4-2019/96154/

9. Alina Dettmer. „What is Pay Per Install.?” [Ce este plata per instalare (pay-per-install – PPI)?] 26 octombrie 2017. Aye Studios. https://www.ayetstudios.com/blog/mobile-advertising/mobile-campaign-types/pay-per-install

10. Larry Cashdollar. „Latest Echobot: 26 Infection Vectors” (Ultimul Echobot: 26 de vectori de infecție) 13 iunie 2019. Akamai. https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html

11. „The awaiting Roboto Botnet” (Botnet-ul Roboto în așteptare) 20 noiembrie 2019. Netlab. https://blog.netlab.360.com/the-awaiting-roboto-botnet-en/

12. Asher Davila. „Home & Small Office Wireless Routers Exploited to Attack Gaming Servers” (Routere wireless pentru birouri de a casă și birouri mici exploatate pentru a ataca serverele de jocuri) 31 octombrie 2019. Paloalto. https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/

13. „Triple Threat: Emotet deploys Trickbot to steal data & spread Ryuk” (Amenințare triplă:

Emotet utilizează Trickbot pentru a fura date și a răspândi Ryuk) 2 aprilie 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

14. “Bots.” Imperva. https://www.imperva.com/learn/application-security/what-are-bots/

15. Rebecca Carter. „Bot Mitigation Best Practices” (Cele mai bune practici de atenuare a boților) 19 octombrie 2018. DYN. https://dyn.com/blog/bot-mitigation-best-practices/

16. „What is a Botnet?” (Ce este un botnet?) Veracode. https://www.veracode.com/security/botnet

17. „SIRT Advisory: Silexbot bricking systems with known default login credentials” (Recomandare SIRT: sisteme de blocare Silexbot cu credențiale de autentificare implicite cunoscute). 26 iunie 2019. Akamai.

18. „Mirai Botnet Continues to Plague IoT Space” (Botnetul Mirai continuă să afecteze spațiul IoT) 10 septembrie 2019. Reversing Labs. https://blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space

19. Fundația Shadowserver. https://www.shadowserver.org/

20. „As Necurs Botnet Falls from Grace, Emotet Rises” (Pe măsură ce botnetul Necurs cade în dizgrație, Emotet crește), 27 ianuarie 2020. Threat Post. https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/

21. „Mirai malware, attacks Home Routers" (Programul malware Mirai atacă routerele de acasă".) 14 decembrie 2016. ENISA. https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

22. „Estimating Emotet's size and reach" (Estimarea dimensiunii și a influenței Emotet) 12 decembrie 2019. SPAMHAUS. https://www.spamhaus.org/news/article/791/estimating-emotets-size-%20-and-reach

23. „Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant" (Viermele Monero-Mining RETADUP devine polimorf, obține o variantă AutoHotKey) 23 aprilie 2018. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/

24. „Meet Stop Ransomware: The Most Active Ransomware Nobody Talks About" (Faceți cunoștință cu Stop Ransomware: cel mai activ ransomware despre care nu vorbește nimeni) 20 septembrie 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/meet-stop-ransomware-the-most-active-ransomware-nobody-talks-about/

25. „Command Injection Over HTTP" (Injecție de comenzi prin HTTP) 26 iulie 2016. Check Point. https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0658.html/

26. „August 2019's Most Wanted Malware: Echobot Launches Widespread Attack Against IoT Devices" (Cele mai căutate programe malware din august 2019: Echobot lansează un atac la scară largă împotriva dispozitivelor IoT) august 2019. Check Point. https://blog.checkpoint.com/2019/09/12/august-2019s-most-wanted-malware-echobot-launches-widespread-attack-against-iot-devices/

27. „Echobot Malware Now up to 71 Exploits, Targeting SCADA" (Malware-ul Echobot are acum până la 71 de exploit-uri, vizând SCADA) 18 decembrie 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada

28. „CVE-2019-15107 Detail". NIST. https://nvd.nist.gov/vuln/detail/CVE-2019-15107

29. „What is a distributed hash table?" (Ce este un tabel hash distribuit?) EDPresso. https://www.educative.io/edpresso/what-is-a-distributed-hash-table

30. „A Look into the Gafgyt Botnet Trends from the Communication Traffic Log" (Examinarea tendințelor Gafgyt Botnet din jurnalul de trafic al comunicațiilor) 23 iulie 2019. https://nsfocusglobal.com/look-gafgyt-botnet-trends-communication-traffic-log/

32. „ASEAN Cyberthreat Assessment 2020, Key Insights From The ASEAN Cybercrime Operations Desk" (Evaluarea amenințării cibernetice în ASEAN în 2020, informații cheie de la biroul ASEAN de operațiuni privind criminalitatea informatică) Interpol, 2020

33. „International team takes down virus-spewing Andromeda botnet" (Echipa internațională elimină botnetul Andromeda care proliferează viruși) 5 decembrie 2017. The Register. https://www.theregister.com/2017/12/05/international_team_takes_down_virusspewing_andromeda_botnet/

34. „The odd, 8-year legacy of the Conficker worm" (Ciudata moștenire de 8 ani a viermelui Conficker) 21 noiembrie 2016. WeLiveSecurity. https://www.welivesecurity.com/2016/11/21/odd-8-year-legacy-conficker-worm/

35. „The Necurs Botnet: A Pandora's Box of Malicious Spam" (Botnetul Necurs: o cutie a Pandorei cu spam rău intenționat) 24 aprilie 2017. https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

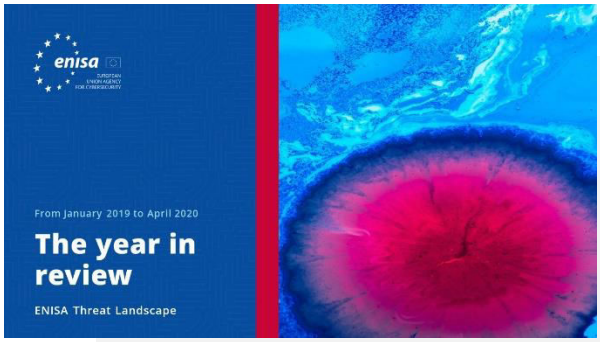
36. „White Paper: Sality: Story of a Peer to-Peer Viral Network" (Carte albă: Sality – povestea unei rețele virale peer-to-peer) 10 iunie 2011. Broadcom.

37. „Botnet C&C: Gozi". FortiGuard Labs. https://fortiguard.com/encyclopedia/botnet/7630489

38. Virustototal. https://www.virustotal.com

39. „Spamhaus Botnet Threat Report 2019" (Raportul Spamhaus privind amenințarea Botnet pe 2019). 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

Documente conexe



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

Un 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

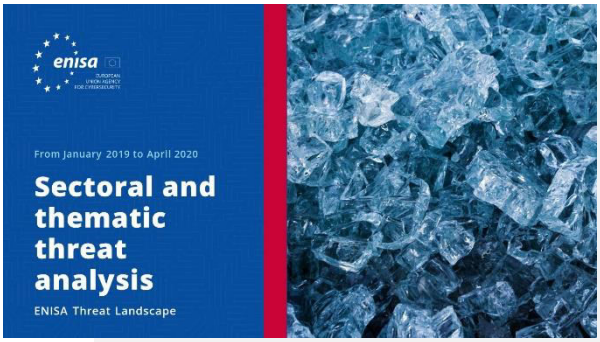
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

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 pot fi găsite 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

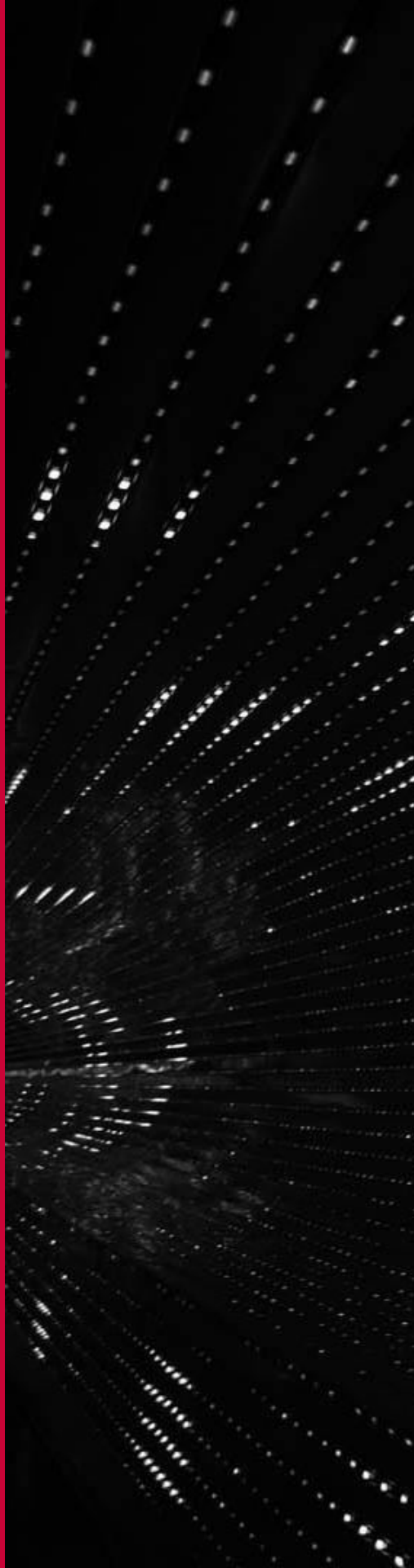
Pentru întrebări despre această lucrare, vă rugăm să utilizați adresa enisa.threat.information@enisa.europa.eu.

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.

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