RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ianuarie 2019 – aprilie 2020

Criptojacking (minarea ilicită de criptomonede)

Raportul ENISA

Prezentare generală

Criptojacking (cunoscut și sub numele de minare de criptomonede) este utilizarea neautorizată a resurselor unui dispozitiv pentru minarea criptomonedelor. Țintele includ orice dispozitiv conectat, cum ar fi calculatoarele și telefoanele mobile; cu toate acestea, infractorii cibernetici vizează din ce în ce mai mult infrastructurile de cloud.[1] Acest tip de atac nu a atras prea mult atenția agențiilor de aplicare a legii, abuzul de acest tip de atac fiind rar raportat[2], în principal din cauza consecințelor sale negative relativ puține. Cu toate acestea, organizațiile pot constata costuri IT mai mari, componente de calculator degradate, consum crescut de energie electrică și productivitate scăzută a angajaților din cauza stațiilor de lucru mai lente.[3]

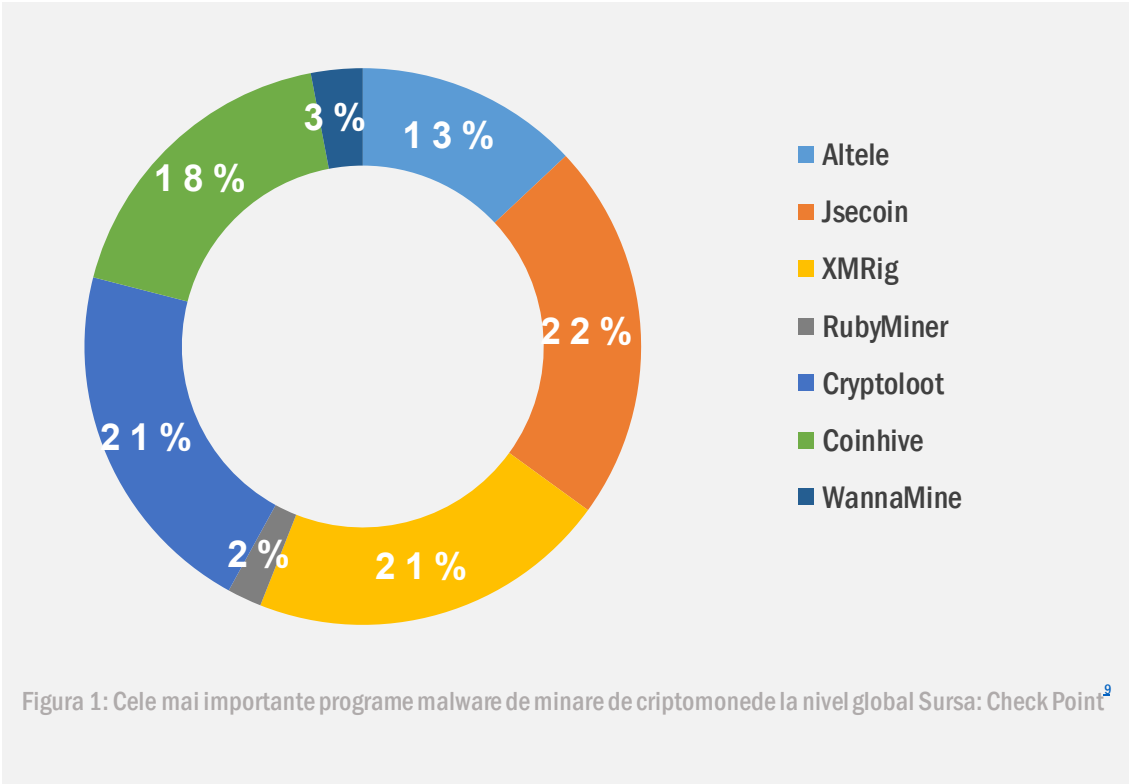


Figura 1: Cele mai importante programe malware de minare de criptomonede la nivel global Sursa: Check Point[9]

Constatări

64,1_milioane de accesări ale programelor de criptojacking până la sfârșitul anului 2019

78 %_scădere a activităților de minare ilicită de criptomonede în a doua jumătate a anului 2019, comparativ cu prima jumătate

Activitățile au crescut cu 9 % în prima jumătate a anului 2019, comparativ cu ultimele 6 luni din 2018.[4,5]

65 %_din cele mai populare 120 de burse din trimestrul III 2019 au avut procese slabe sau poroase de cunoaștere a clienților (know your customer – KYC)

32 % din burse au tranzacționat monede de confidențialitate.[6]

39,3%_din infecțiile de minare de criptomonede din 2019 au vizat Japonia.

20,8 % din infecțiile de minare de criptomonede au vizat India și 14,2 % Taiwan. Figura 1 prezintă cele cinci țări cu cele mai numeroase tentative detectate de infectare cu malware-ul minerului de criptomonede pentru 2018 și 2019.[7]

13 %_din incidentele de minare ilicită de criptomonede sunt atribuite trojan.Win32.Miner.bbb

În perioada noiembrie 2018 – octombrie 2019, următorii cei mai activi mineri au fost Trojan.Win32.Miner.ays (11,35 %), Trojan.JS.Miner.m (11,12 %).[6]

Kill chain

Criptojacking

Recunoaștere	Înarmare	Livrare	Exploatare

Etapa fluxului de activitate de atac

Amploarea scopului

Criptojacking

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

Tendințe

_Serviciul popular de minare de criptomonede Coinhive a fost închis

Coinhive a apărut în septembrie 2017 și s-a promovat ca fiind o sursă alternativă de venituri pentru dezvoltatorii web în loc de banner publicitar.[24] Folosea biblioteci JavaScript, care puteau fi instalate pe site-uri web, și puterea de procesare a vizitatorilor pentru a mina în mod legitim criptomoneda. Până la închiderea sa, în martie 2019, serviciul a fost utilizat extrem de abuziv de factorii de amenințare care au injectat un cod în site-uri piratate pentru a mina criptomoneda Monero și pentru a redirecționa fonduri în propriile buzunare. După închiderea sa, volumul de accesări ale programelor de criptojacking bazate pe web a scăzut cu 78 % în a doua jumătate a anului 2019.[4] Ca urmare a acestei scăderi, infractorii cibernetici au început să se concentreze pe ținte cu valoare mai ridicată, cum ar fi servere puternice[9] și infrastructuri cloud.[1] Locul Coinhive în top a fost ocupat de atunci[9] de Jsecoin (22 %), XMRig (21 %) și Cryptoloot (21 %). Distribuția malware-ului de minare a criptomonedelor de top la nivel global este prezentată în figura 1.

_Mai multe atacuri asupra infrastructurilor cloud

În prima jumătate a anului 2019 s-a constatat o tendință de creștere în ceea ce privește incidentele de atacuri de minare a criptomonedelor pe cloud.[15,25] Mediile cloud utilizează de regulă mecanisme care adaptează resursele la cerere și, prin urmare, sunt ținte profitabile pentru rularea software-ului de minare. Aceasta este însă în detrimentul proprietarilor de site-uri web, care la rândul lor, trebuie să plătească facturi mai mari pentru depășirea cotelor.[15] În prima jumătate a anului 2019, vulnerabilitățile în programul de stocare în cloud au crescut cu 46 % comparativ cu aceeași perioadă din 2018.[26] Atacatorii au reușit să exploateze interfețele de programare a aplicațiilor (API-uri) și platformele de gestionare a containerelor pentru a instala imagini rău intenționate (de exemplu, Docker și Kubernetes) și pentru a mina criptomonede.[25]

Incidente

Aprilie 2019_ **Campania de criptojacking numită Beapy a exploatat vulnerabilitatea EternalBlue și a afectat întreprinderi din China**[3]

Mai 2019_ **PCASTLE, malware-ul de minare a criptomonedelor Monero, a vizat în cea mai mare parte sistemele bazate în China utilizând tehnici de sosire fără fișiere**[19]

Peste 50 000 de servere aparținând companiilor din sectoarele sănătății, telecomunicațiilor, mass-media și IT s-au dovedit a fi infectate de malware care extrage criptomoneda TurtleCoin (TRTL).[20]
O nouă familie de malware numită BlackSquid a folosit opt exploit-uri cunoscute, inclusiv EternalBlue și DoublePulsar, și ulterior s-a răspândit pe serverele web din Thailanda și Statele Unite astfel încât să livreze scripturi de minare a criptomonedei Monero.[17,21]

August 2019_ **În 11 registre de limbaj RubyGem au fost găsite programe malware de criptojacking, expunând mii de utilizatori la codul de minare a criptomonedelor**[22]

Tendințe

_Trecerea la programe de minare a criptomonedelor bazate pe fișiere

În 2019, a fost observată o scădere a criptojacking-ului bazat pe browser în favoarea minării criptomonedelor bazate pe fișiere. Atacurile de minare a criptomonedelor bazate pe fișiere[27] s-au răspândit prin malware și au folosit exploit-uri preexistente pe sisteme de operare neperfectate, cum ar fi EternalBlue și alte vulnerabilități cu risc ridicat. Factorii care au contribuit la această schimbare au fost închiderea popularului furnizor de servicii de minerit online Coinhive[1] și scăderea valorilor criptomonedelor.[10] Un alt factor este că minarea criptomonedelor bazată pe fișiere a fost întotdeauna mai eficientă decât minarea online, fiind de 25 de ori mai profitabilă.[3] Factorii de amenințare și-au adaptat programele malware cu instrumente suplimentare, pentru a extrage informații sensibile din computerul victimei.

_Atacurile de criptojacking la nivel mondial sunt în scădere

În 2019, s-a observat o tendință descendentă[5] în atacurile de criptojacking, în principal datorită închiderii Coinhive[6], eforturilor coordonate ale agențiilor de aplicare a legii și deprecierii criptomonedei Monero. Cu toate acestea, deoarece se știe că atacurile de criptojacking urmăresc valorile criptomonedelor, un serviciu similar cu Coinhive poate apărea și poate determina o nouă creștere. Statisticile timpurii pentru 2020 arată o creștere de 30 % pe bază anuală în martie.

_Monero a rămas criptomoneda preferată

Similar cu tendințele anterioare, Monero (XMR) a fost criptomoneda preferată pentru activitățile de criptojacking din 2019. Motivul este dublu; în primul rând, Monero este axat pe confidențialitate și anonimat și, prin urmare, tranzacțiile nu pot fi urmărite. În al doilea rând, algoritmul Proof-of-Work este conceput pentru a face minarea viabilă cu un CPU standard, spre deosebire de hardware-ul specializat. În trimestrul III al anului 2019, 32 % din burse au tranzacționat monede de confidențialitate, cum ar fi Monero. Cu toate acestea, în așteptarea noilor reglementări împotriva spălării banilor, multe burse au optat pentru retragerea monedelor de confidențialitate.

_Cele mai vizate țări

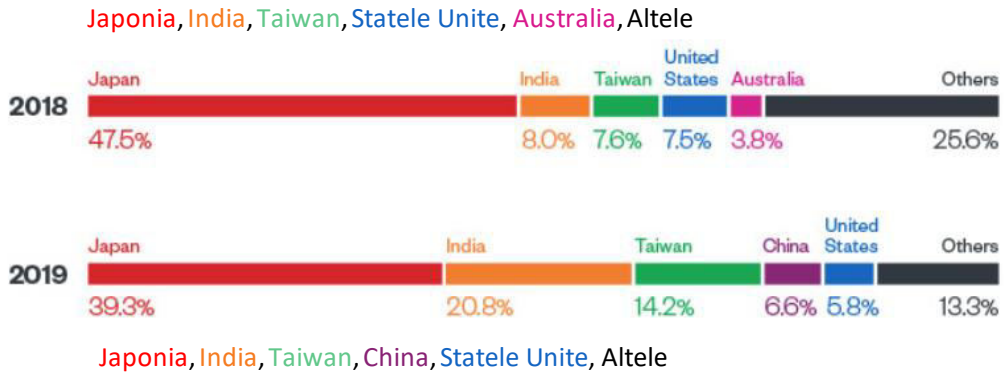


Figura 2: Cele mai vizate țări de criptojacking. Sursa: Trend Micro[7]

Vectori de atac

_Tehnici

Infractorii cibernetici au folosit următoarele tehnici pentru a executa sau livra mineri de criptomonede:

- prin încorporarea capabilităților de criptojacking în programele malware existente;[10]
- prin compromiterea site-urilor;[11]
- prin atacuri drive-by persistente;[12]
- prin utilizarea rețelelor sociale;[13]
- prin utilizarea aplicațiilor mobile și a magazinelor de aplicații;[14]
- prin utilizarea kiturilor de exploit-uri;[15]
- prin utilizarea rețelelor de publicitate și a publicității necorespunzătoare;[16]
- prin utilizarea suportului amovibil[17]
- și prin utilizarea minerilor de criptomonede „wormable”.[18]

Figura 3: Cât poate câștiga un botnet pentru minare de monede în 30 de zile? Sursa: Broadcom[3]

Acțiuni propuse

- Monitorizarea utilizării bateriei de pe dispozitivele utilizatorilor și, în cazul unor creșteri suspecte în utilizarea CPU, scanarea pentru prezența minerilor de criptomonede pe bază de fișiere.
- Aplicarea filtrării conținutului pentru a filtra atașamentele nedorite, e-mailurile cu conținut rău intenționat și mesajele nesolicitate (spam).
- Aplicarea filtrării protocolului de minare Stratum, precum și alcătuirea unei liste negre cu adresele IP și domeniile pool-urilor populare de minare.
- Instalarea de protecție a punctului final prin intermediul unor programe antivirus sau extensii ale browserului care blochează mineri de criptomonede.
- Efectuarea de audituri regulate de securitate pentru a detecta anomaliile rețelei.
- Aplicarea unei gestionări robuste a vulnerabilităților și patch-urilor.
- Utilizarea unei liste albe pentru a preveni rularea unor fișiere executabile necunoscute la punctele de ieșire.
- Investirea în creșterea gradului de conștientizare a utilizatorilor cu privire la criptojacking, în special în ceea ce privește comportamentul de navigare securizat.
- Aplicarea de patch-uri și remedieri împotriva exploit-urilor bine-cunoscute, cum ar fi Eternal Blue, pe ținte mai puțin evidente, cum ar fi sistemele de gestionare a cozii, terminalele POS și chiar automatele.
- Monitorizarea și alcătuirea unei liste negre a fișierelor executabile comune de minare a criptomonedelor.

Referințe

1. Sergiu Gatlan. „Cryptominers Still Top Threat In March Despite Coinhive Demise" (În martie, minerii de criptomonede reprezintă în continuare o amenințare importantă, în ciuda dispariției Coinhive) 9 aprilie 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top-threat-in-march-despite-coinhive-demise/

2. „Internet Organised Crime Threat Assessment (IOCTA)" (Evaluarea amenințării pe care o reprezintă criminalitatea organizată online) 2019. EUROPOL. https://www.europol.europa.eu/iocta-report

3. „Beapy: Cryptojacking Worm Hits Enterprises in China" (Beapy: vierme de criptojacking atacă întreprinderi din China) 24 aprilie 2019. BROADCOM. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

4 Bill Conner. „SONICWALL Cyber Threat Report" (Raportul SONICWALL privind amenințările cibernetice) 2020. SONICWALL https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. Yessi Bello Perez. „Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019" (Victime nevinovate au fost supuse unor atacuri de tip criptojacking de 52,7 milioane de ori în prima jumătate a anului 2019) 24 iulie 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-first-half-2019/

6. Ben Noble. „A Third of Cryptocurrency Exchanges Still Host Privacy Coins Despite Fears of Impending FATF Travel Rule" (O treime din bursele de criptomonede găzduiesc în continuare monede de confidențialitate, în ciuda temerilor privind o regulă iminentă de călătorie FATF) 27 noiembrie 2019. CIPHERTRACE https://ciphertrace.com/ciphertrace-q3-2019-caml-press-release/

7. „Defending Systems Against Cryptocurrency Miner Malware" (Apărarea sistemelor împotriva malware-ului miner de criptomonede) 28 octombrie 2019. Trend Micro. https://www.trendmicro.com/vinfo/be/security/news/cybercrime-and-digital-threats/defending-systems-against-cryptocurrency-miner-malware

8. „Kaspersky Security Bulletin '19 Statistics" (Buletinul de securitate Kaspersky, Statistici 2019) 2009. Kaspersky. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf

9. „CYBER SECURITY REPORT" (RAPORT DE SECURITATE CIBERNICĂ) 2020. Check Point Research cp<r>. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

10. Ionut Ilascu. „EternalBlue Exploit Serves Cryptojacking Campaign" (Exploit-ul EternalBlue servește campania de criptojacking Beapy) 25 aprilie 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/eternalblue-exploit-serves-beapy-cryptojacking-campaign/

11. „New mining worm PsMiner uses multiple high-risk vulnerabilities to spread" (Noul vierme de minare PsMiner folosește multiple vulnerabilități cu risc ridicat pentru a se răspândi) 12 martie 2019. 360 Total Security. https://blog.360totalsecurity.com/en/new-mining-worm-psminer-uses-multiple-high-risk-vulnerabilities-to-spread/

12. Dan Thorp-Lancaster. „New drive-by cryptocurrency mining scheme persists after you exit your browser window" (Noua schemă drive-by de minare a criptomonedelor persistă după ce ieșiți din fereastra browserului) 9 noiembrie 2017. Windows Central. https://www.windowscentral.com/new-drive-cryptocurrency-mining-scheme-persists-even-after-you-exit-your-browser-window

13. Dr. Michaeal McGuire. „Social Media Platforms and the Cybercrime Economy" (Platformele de comunicare socială și economia cibernetică) 2019. Bromium. https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

14. Axelle Apvrille. „Abusing cryptocurrencies on Android smartphones" (Abuzarea criptomonedelor pe smartphone-urile Android) 2019. Fortinet. https://fortinetweb.s3.amazonaws.com/fortiguard/research/currency-insomnihack19.pdf

15. „2019 Midyear Security Roundup Evasive Threats Pervasive Effects" (Breviar de securitate la jumătatea anului 2019: amenințări evazive, efecte extinse) 2019. TrendMicro https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

16. Margi Murphy. "YouTube shuts down hidden cryptojacking adverts" (YouTube închide reclame ascunse de criptojacking) 29 ianua rie 2018. The Telegraph https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/

17. Matthew Beedham. „New cryptocurrency mining malware is spreading across Thailand and the US" (Noi programe malware pentru minarea criptomonedelor se răspândesc în Thailanda și SUA) 4 iunie 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/06/04/security-crypto-jacking-mining-malware/

18. Sean Lyngaas. „BlueKeep is back. For now, attackers are just using it for cryptomining" (BlueKeep s-a întors. Deocamdată, atacatorii îl folosesc doar pentru minarea criptomonedelor) 4 noiembrie 2019. CyberScoop. https://www.cyberscoop.com/bluekeep-exploited-cryptomining/

19. Janus Agcaoili. „Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques" (PCASTLE, malware-ul de minare a monedei Monero, atacă din nou China și acum utilizează tehnici de sosire fără fișiere cu niveluri multiple) 5 iunie 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/

20. Marie Huillet. „Researchers Say 50,000 Servers Worldwide Infected With Privacy Coin Cryptojacking Malware" (Cercetătorii afirmă că, la nivel mondial, 50 000 de servere sunt infectate cu programe malware de criptojacking de monede de confidențialitate) 29 mai 2019. Cointelegraph. https://cointelegraph.com/news/researchers-say-50-000-servers-worldwide-infected-with-privacy-coin-cryptojacking-malware

21. Johnlery Triunfante, Mark Vicente. „BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner" (BlackSquid se strecoară în servere și unități cu 8 exploit-uri notorii pentru a livra minerul XMRig) 27 august 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/

22. „Malicious cryptojacking code found in 11 Ruby libraries" (Cod de criptojacking rău intenționat găsit în 11 biblioteci Ruby) 2 august 2019, Decrypt. https://decrypt.co/8602/malicious-cryptjacking-code-found-in-11-ruby-libraries

23. Brook Chelmo. „Cryptojacking in 2019: Cryptocurrency Value Keeping Attack Vector in Play" (Criptojacking în 2019: valoarea criptomonedei menține vectorul de atac în joc) 6 august 2019. SonicWall. https://blog.sonicwall.com/en-us/2019/08/cryptojacking-in-2019-cryptocurrency-value-keeping-attack-vector-in-play/

24. Catalin Cimpanu. „Coinhive cryptojacking service to shut down in March 2019" (Serviciul de criptojacking Coinhive se închide în martie 2019) 17 februarie 2019. ZD Net. https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/

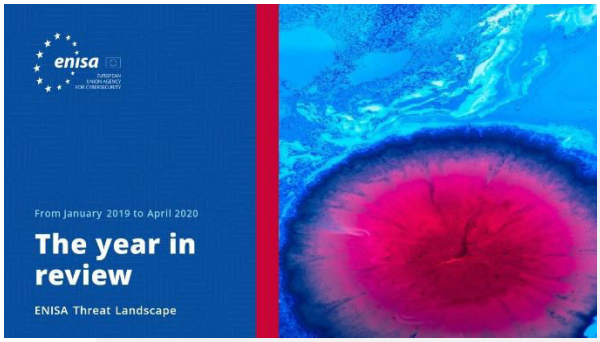
25. Tom Hegel. „Making it Rain - Cryptocurrency Mining Attacks in the Cloud" (Plouă cu bani – Atacuri de minare de criptomonede în cloud) 14 martie 2019. AT&T Business. https://cybersecurity.att.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/

26. „How a Prominent Cryptomining Botnet is Paving the Way for a Lucrative and Illicit Revenue Model" (Modul în care un botnet important de minare de criptomonede deschide calea către un model de venituri lucrativ și ilicit) August 2019. Carbon Black. https://www.carbonblack.com/resources/access-mining/

27. „Cryptojacking Attacks: Who's Mining on Your Coin?" (Atacuri de criptojacking: cine îți exploatează moneda?) 5 aprilie 2019. Security Intelligence. https://securityintelligence.com/cryptojacking-attacks-whos-mining-on-your-coin/

28. „Malware Creates Cryptominer Botnet Using EternalBlue and Mimikatz" (Programul malware creează botnet miner de criptomonede utilizând EternalBlue și Mimikatz) 12 aprilie 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/malware-creates-cryptominer-botnet-using-eternalblue-and-mimikatz/

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**

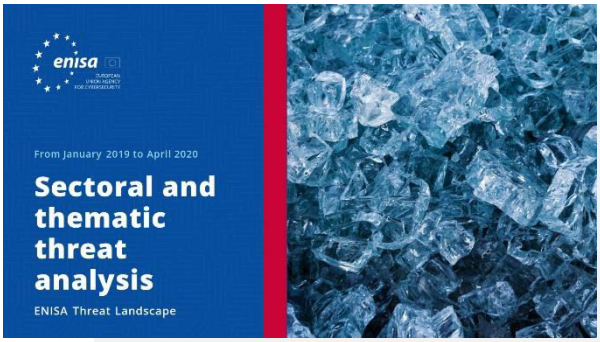
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

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 ar 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 trebuie 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