enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO

Ianuarie 2019 – aprilie 2020

Spionajul cibernetic

Raportul ENISA privind situația amenințărilor

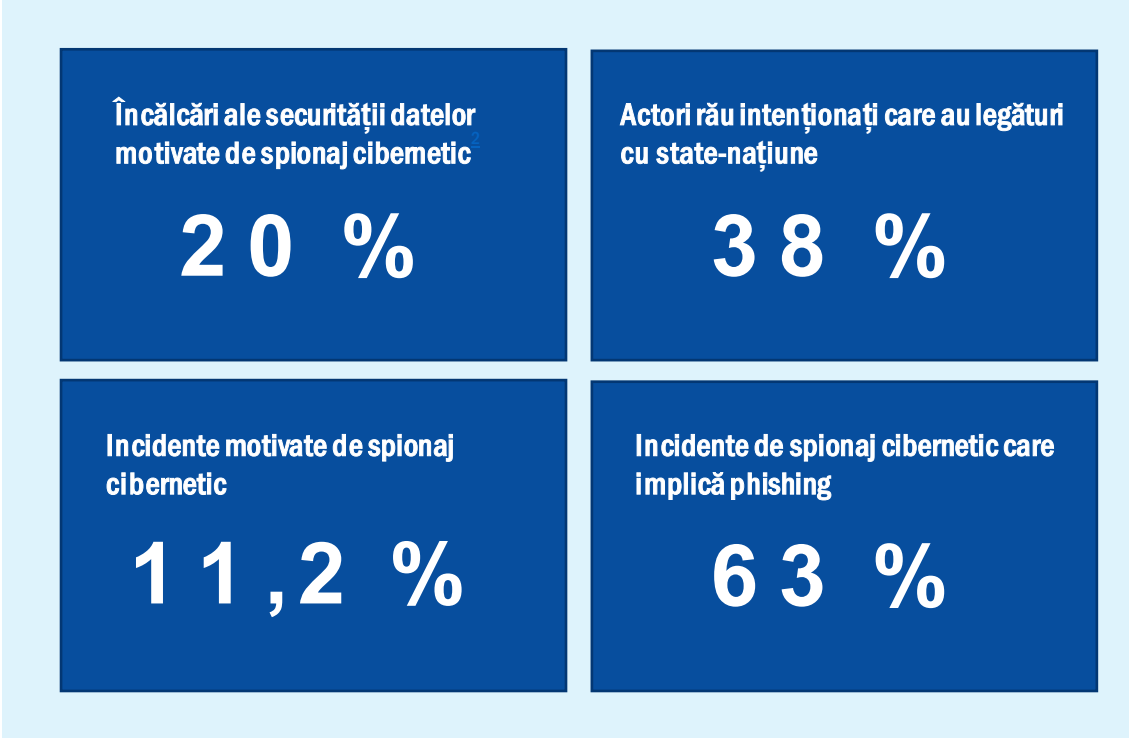
Prezentare generală

Spionajul cibernetic este considerat atât o amenințare, cât și un motiv în protocolul de combatere a amenințărilor la adresa securității cibernetice. Acesta este definit ca „utilizarea rețelelor de calculatoare pentru a obține acces ilicit la informații confidențiale, de obicei cele deținute de un guvern sau o altă organizație”.[1]

În 2019, multe rapoarte au dezvăluit că organizațiile mondiale consideră spionajul cibernetic (sau spionajul susținut de state-națiune) o amenințare în creștere care afectează sectoarele industriale, precum și infrastructurile critice și strategice din întreaga lume, inclusiv ministere guvernamentale, căi ferate, prestatorii de servicii de telecomunicații, companii din domeniul energetic, spitale și bănci. Spionajul cibernetic se concentrează pe dirijarea geopoliticii și pe furtul de secrete de stat și comerciale, drepturi de proprietate intelectuală și informații protejate în domenii strategice. De asemenea, acesta mobilizează actori din economie, industrie și servicii de informații străine, precum și actori care lucrează în numele lor. Într-un raport recent, analiștii de informații despre amenințări nu au fost surprinși să afle că 71 % din organizații tratează spionajul cibernetic și alte amenințări ca pe o „cutie neagră” și încă învață despre acestea.

În 2019, **a crescut numărul de atacuri cibernetice susținute de state-națiune care vizează economia și este probabil ca această tendință să continue**. În detaliu, atacurile susținute de state-națiune și alte atacuri promovate de adversari asupra Internetului industrial al obiectelor (IIoT) sunt în creștere în sectorul utilităților, al petrolului și gazelor naturale și în sectoarele de producție. De asemenea, atacurile cibernetice efectuate de grupuri de amenințări persistente avansate (APT) indică faptul că atacurile financiare sunt adesea motivate de spionaj. Folosind tactici, tehnici și proceduri (TTP) asemănătoare celor ale omologilor lor de spionaj, grupuri precum Cobalt Group, Carbanak și FIN7 ar fi vizat cu succes instituții financiare mari și lanțuri de restaurante.

- Comisia pentru afaceri externe a Parlamentului European a solicitat statelor membre să înființeze o unitate de apărare cibernetică și să colaboreze în ceea ce privește apărarea lor comună. Aceasta a afirmat că „mediul strategic al Uniunii s-a deteriorat ... pentru a face față multiplelor provocări care afectează, în mod direct sau indirect, securitatea statelor sale membre și a cetățenilor săi; întrucât printre aspectele care afectează securitatea cetățenilor UE se numără: conflictele armate imediat la estul și la sudul continentului european, și statele fragile; terorismul și în special jihadismul, atacurile cibernetice și campaniile de dezinformare; amestecul extern în procesele politice și electorale europene”.[42]
- Factorii de amenințare motivați de câștiguri financiare, politice sau ideologice își vor concentra din ce în ce mai mult atacurile asupra rețelelor de furnizori cu programe de securitate cibernetică slabe. Adversarii care practică spionajul cibernetic și-au deplasat încet tiparele de atac spre exploatarea partenerilor de gradul trei și patru din lanțul de aprovizionare.[1]



Incidente

- Ministerul Apărării Naționale din Coreea de Sud a anunțat că hackeri necunoscuți au compromis sistemele informatice din cadrul biroului de achiziții publice al ministerului.[3]
- Departamentul de Justiție al Statelor Unite a anunțat o operațiune finanțată de un stat străin cu un botnet menit să perturbe prin vizarea companiilor din sectoarele media, aerospațial, financiar și al infrastructurii critice.[16]
- Compania norvegiană de software Visma a dezvăluit că a fost vizată de hackeri care încercau să fure secretele comerciale de la clienții firmei.[4]
- Anumite persoane au fost surprinse în primele etape ale accesului la sistemele informatice ale mai multor partide politice și ale Parlamentului federal australian.[17]
- Compania europeană aerospațială Airbus a dezvăluit că a fost vizată de presupuși hackeri susținuți de state-națiune care au furat informații personale și de identificare IT ale mai multor angajați.[19]
- În urma unui atac asupra forțelor militare indiene din Kashmir, hackeri pakistanezi au vizat aproape 100 de site-uri și sisteme critice ale guvernului indian.[5]
- Comisia Electorală Națională din Indonezia a raportat că indivizi chinezi și ruși au încercat să acceseze baza de date a alegătorilor înainte de alegerile prezidențiale și legislative din Indonezia.[20]
- Hackeri străini au vizat mai multe agenții guvernamentale europene înainte de alegerile UE din mai.[21]
- Direcția australiană a semnalelor a dezvăluit că a efectuat atacuri cibernetice împotriva ISIS în Orientul Mijlociu.[22]
- Poliția finlandeză a cercetat un atac DoS împotriva serviciului web folosit pentru a publica rezultatele alegerilor din Finlanda.[6]
- Biroul Amnesty International din Hong Kong a anunțat că a fost victima unui atac cibernetic.[23]
- Forțele israeliene de apărare au lansat un atac aerian asupra grupării Hamas după tentativele fără succes ale acesteia de intruziune asupra unor ținte israeliene.[7]

- O rețea iraniană de site-uri și conturi ar fi fost folosită pentru a răspândi informații false despre Statele Unite, Israel și Arabia Saudită.[24]
- Agențiile guvernamentale croate au fost vizate de o serie de atacuri de către hackeri neidentificați susținuți de stat. Încărcăturile utile ale malware-ului au fost Empire backdoor și SilentTrinity, niciunul dintre acestea nemaifiind văzut înainte.[26]
- Libia a arestat doi bărbați acuzați că lucrează cu o „fermă de troli" rusă pentru a influența alegerile din mai multe țări africane.[27]
- Câteva mari companii industriale germane, inclusiv BASF, Siemens și Henkel, au anunțat că au fost victimele unei campanii de hacking susținute de stat.[28]
- Un grup susținut de stat ar fi efectuat o serie de atacuri cibernetice împotriva unor jurnaliști, membri ai comunității academice, avocați, activiști pentru drepturile omului și politicieni egipteni.[8]
- Un grup de hacking susținut de stat i-a vizat pe diplomați și pe utilizatori rusofoni din Europa de Est folosind malware-ul numit Attor.[29]
- S-a constatat că o firmă israeliană de securitate cibernetică a vândut programe de spyware utilizate pentru a viza înalți oficiali ai guvernului și militari din cel puțin 20 de țări, exploatând o vulnerabilitate din WhatsApp.[32]
- O campanie de 7 ani a unui grup de spionaj neidentificat de limbă spaniolă s-a dovedit a fi avut ca rezultat furtul de fișiere de cartografiere sensibile de la înalți oficiali din armata venezueleană.[10]
- Un grup de spionaj cibernetic susținut de stat ar fi desfășurat o campanie de phishing vizând agenții guvernamentale chineze și întreprinderi de stat pentru informații legate de domeniul economic, comerț, probleme de apărare și relații externe.[33]
- Ministerul ceh de externe a fost victima unui atac cibernetic de către un stat străin nespecificat.[34]
- Un actor nestatal a vizat partidul laburist britanic cu un atac DDoS major care a scos temporar offline computerele partidului înainte de alegerile naționale".[36]

Incidente

Cazul General Electric

Xiaoqing Zheng, un cetățean american de origine chineză, a fost acuzat că spionează în detrimentul General Electric (GE). Domnul Zheng ar fi sustras secretele tehnologiei turbinei GE și le-ar fi livrat unui om de afaceri chinez care se presupune că le-a livrat unui oficial chinez. Domnul Zheng a lucrat pentru GE între 2008 și 2018.[15]

Departamentul de justiție al Statelor Unite i-a acuzat pe cei doi bărbați că au furat informații pentru a-și promova propriile interese comerciale în două companii de cercetare și dezvoltare a turbinelor – Liaoning Tianyi Aviation Technology Co Ltd și Nanjing Tianyi Avi Tech Co Ltd.[47]

Modul de operare al acestui factor de amenințare din interior a inclus:

- copierea secretelor pe o unitate USB până când GE a blocat utilizarea acestor dispozitive;
- criptarea secretelor și utilizarea steganografiei pentru a ascunde fișiere de date în codul binar al fișierelor foto digitale;
- conectarea unui iPhone la computerul de birou pentru a copia imaginea;
- trimiterea fișierelor la propria adresă personală de e-mail.

Măsuri de atenuare

Datorită naturii cuprinzătoare a acestei amenințări, mai multe dintre măsurile de atenuare recomandate pentru alte amenințări în acest raport ar putea fi utilizate ca parte a următoarelor controale de atenuare de referință:[2]

- identificarea rolurilor critice ale misiunii în cadrul organizației și estimarea expunerii lor la riscurile de spionaj. evaluarea unor astfel de riscuri pe baza informațiilor comerciale (și anume, informații privind întreprinderile).
- crearea de politici de securitate care să adapteze controalele de securitate privind resursele umane, întreprinderile și operațiunile pentru a acoperi diminuarea riscurilor. Acestea trebuie să conțină reguli și practici pentru sensibilizare, guvernanța corporativă și operațiunile de securitate.
- stabilirea de practici corporative pentru a comunica și a instrui personalul în ceea ce privește regulile elaborate.
- elaborarea unui criteriu de evaluare (KPIs) pentru a evalua operațiunea și a o adapta la modificările viitoare.
- crearea unei liste albe pentru serviciile de aplicații critice, în funcție de nivelul de risc evaluat.
- evaluarea vulnerabilităților și corectarea regulată a software-ului cu ajutorul patch-urilor, în special pentru sistemele aflate în perimetru.
- aplicarea principiului nevoii de a cunoaște pentru definirea drepturilor de acces și stabilirea de controale pentru a monitoriza utilizarea abuzivă a profilurilor privilegiate.
- stabilirea de parametri de filtrare a conținutului pentru toate canalele de intrare și de ieșire (de exemplu, e-mail, site web, trafic de rețea).

Referințe

1. „Cyber Threatscape Report. 2019 (Raportul privind peisajul amenințărilor cibernetice 2019).” IDefense - Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

2. „Data Breach Investigations Report 2020” (Raportul investigațiilor privind încălcarea securității datelor 2020), DBR & Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

3. Catalin Cimpanu. „Hackers breach and steal data from South Korea's Defense Ministry” (Hackerii au spart și au furat date de la Ministerul Apărării din Coreea de Sud), 16 ianuarie 2019. ZDNet. https://www.zdnet.com/article/hackers-breach-and-steal-data-from-south-koreas-defense-ministry/

4. Jack Stubbs. „China hacked Norway's Visma to steal client secrets: investigators” (China a spart rețeaua companiei de software Visma din Norvegia pentru a fura secretele clienților: anchetatori) 6 februarie 2019. Reuters. https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141

5. Kate Fazzini. „In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides” (În conflictul dintre India și Pakistan, există un război online latent de mulți ani și niște hackeri foarte buni de ambele părți). 28 februarie 2019. CNBC. https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html

6. Kati Pohjanpalo. „Finland Detects Cyber Attack on Online Election-Results Service” (Finlanda detectează un atac cibernetic asupra serviciului online pentru rezultatele alegerilor) 10 aprilie 2019. Bloomberg.

https://www.bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service

7. Lily Hay Newman „What Israel's Strike on Hamas Hackers Means For Cyberwar” (Ce înseamnă atacul Israelului asupra hackerilor din Hamas pentru războiul cibernetic), 5 iunie 2019. Wired. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

8. „Egypt Is Using Apps to Track and Target Its Citizens, Report Says” (Potrivit raportului, Egiptul folosește aplicații pentru a-și urmări și ataca cetățenii), 3 octombrie 2019. The New York Times. https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html

9. Colin Lencher. „Huawei accuses the US of 'launching cyber attacks' against the company” (Huawei acuză SUA că „lansează atacuri cibernetice” împotriva companiei), 4 septembrie 2019. The Verge. https://www.theverge.com/2019/9/4/20849092/huawei-cyberattacks-us-government-netowrks-employee-harassment

10. Catalin Cimpanu „A cyber-espionage group has been stealing files from the Venezuelan military” (Un grup de spionaj cibernetic a furat dosare de la armata venezueleană), 5 august 2019. ZDNet. https://www.zdnet.com/article/a-cyber-espionage-group-has-been-stealing-files-from-the-venezuelan-military/

11. Catalin Cimpanu. „Croatian government targeted by mysterious hackers” (Guvernul croat a fost vizat de hackeri misterioși), 5 iulie 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

12. Michael McGowan. „China behind massive Australian National University hack, intelligence officials say” (China, în spatele atacului masiv de hacking care a vizat Universitatea Națională Australiană, declară oficialii din domeniul informațiilor), 6 iunie 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

13. „General election 2019: Labour Party hit by second cyber-attack” (Alegeri generale 2019: Partidul Laburist lovit de al doilea atac cibernetic), 12 noiembrie 2019. BBC. https://www.bbc.com/news/election-2019-50388879

14. Nicole Perlroth, Matthew Rosenberg. „Russians Hacked Ukrainian Gas Company at Center of Impeachment” (Hackeri ruși au atacat compania ucraineană de gaz din centrul cazului pentru demiterea președintelui american), 13 ianuarie 2020. The New York Times. https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html

15. Danny Bradbury . „GE Engineer Charged for Novel Data Theft” (Inginer GE pus sub acuzare pentru un furt de date inedit), 24 aprilie 2019. Info Security. https://www.infosecurity-magazine.com/infosec/ge-engineer-charged-data-theft-1/

16. „U.S. announces disruption of 'Joanap' botnet linked with North Korea” (SUA anunță combaterea botnetului „Joanap” cu legături cu Coreea de Nord). 30 ianuarie 2019. CyberScoop. https://www.cyberscoop.com/joanap-botnet-north-korea-department-of-justice/

17. „The cyber attack on Parliament was done by a 'state actor' – here's how experts figure that out” (Atacul cibernetic asupra Parlamentului a fost realizat de un „actor de stat” – iată cum își dau seama experții). 20 februarie 2019. ABC News. https://www.abc.net.au/news/2019-02-20/cyber-activists-or-state-actor-attack-how-experts-tell/10825466

18. „While Trump was meeting with Kim Jong Un in Vietnam, North Korean hackers reportedly attacked targets in the US” (În timp ce Trump se întâlnea cu Kim Jong Un în Vietnam, hackeri nord-coreeni ar fi atacat ținte din SUA). 5 martie 2019. Business Insider. https://www.businessinsider.com/north-korean-hackers-trump-kim-meeting-mcafee-2019-3

19. „Airbus hit by series of cyber attacks on suppliers” (Airbus a fost vizat de o serie de atacuri cibernetice asupra furnizorilor). 26 septembrie 2019. France 24. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

20. „Indonesia Says Election Under Attack From Chinese, Russian Hackers" (Indonezia spune că alegerile sunt atacate de hackeri chinezi și ruși). 12 martie 2019. Bloomberg. https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers

21. „Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections" (Avertisment privind spionajul cibernetic: grupuri de hackeri ruși intensifică atacurile înainte de alegerile europene). 21 martie 2019. ZDNet. https://www.zdnet.com/article/cyber-espionage-warning-russian-hacking-groups-step-up-attacks-ahead-of-european-elections/

22. „Australian cyber soldiers hacked Islamic State and crippled its propaganda unit – here's what we know" (Soldați cibernetici australieni au atacat Statul Islamic și au paralizat unitatea de propagandă a acestuia – iată ce știm). 18 decembrie 2019. ABC News. https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426

23. „State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack" (Hackeri susținuți de stat vizează Amnesty International Hong Kong cu un atac cibernetic sofisticat). 25 aprilie 2019. Amnesty International. https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

24. „New Report Shows How a Pro-Iran Group Spread Fake News Online" (Noul raport arată modul în care un grup pro-Iran a răspândit știri false online). 14 mai 2019. The New York Times. https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html

25. „China behind massive Australian National University hack, intelligence officials say" (China, în spatele atacului masiv de hacking care a vizat Universitatea Națională Australiană, declară oficialii din domeniul informațiilor). 6 iunie 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

26. „Croatian government targeted by mysterious hackers" (Guvernul croat a fost vizat de hackeri misterioși). 5 iulie 2019. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

27. „Two Russians accused of election interference arrested in Libya" (Doi ruși acuzați de ingerință electorală arestați în Libia). 8 iulie 2019. Cyber Scout. https://cyberscout.com/en/blog/two-russians-accused-of-election-interference-arrested-in-libya

28. „BASF, Siemens, Henkel, Roche target of cyber attacks" (BASF, Siemens, Henkel, Roche ținte ale atacurilor cibernetice). 24 iulie 2019. Reuters. https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

29. „New espionage malware found targeting Russian-speaking users in Eastern Europe" (S-a găsit un nou malware de spionaj care vizează utilizatori rusofoni din Europa de Est), 10 octombrie 2019. ZDNet. https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

30. „Advanced Israeli spyware is targeting Moroccan human rights activists" (Program avansat de spyware israelian vizează activiști marocani pentru drepturile omului). noiembrie 2019. TheNextWeb. https://thenextweb.com/security/2019/10/14/advanced-israeli-spyware-is-targeting-moroccan-human-rights-activists/

31. „Hacking the hackers: Russian group hijacked Iranian spying operation, officials say" (Hackeri vizați de hacking: un grup rus a deturnat operațiunea de spionaj iraniană, declară oficialii). 21 octombrie 2019. Reuters. https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

32. „Israeli spyware allegedly used to target Pakistani officials' phones" (Un program de spyware israelian ar fi fost utilizat pentru a viza telefoanele oficialilor pakistanezi). 18 decembrie 2019. The Guardian. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones

33. „A phishing campaign with nation-state hallmarks is targeting Chinese government agencies" (O campanie de phishing cu semne distinctive ale statului-națiune vizează agențiile guvernamentale chineze). 8 august 2019. Cyber Scoop. https://www.cyberscoop.com/china-phishing-anomali-nation-state-apt/

34. „Foreign power was behind cyber attack on Czech ministry: Senate" (O putere externă s-a aflat în spatele atacului cibernetic asupra ministerului ceh: senatul). 13 august 2019. Reuters. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

35. „Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications" (Tehnicieni Huawei au ajutat oficiali guvernamentali din două țări africane să urmărească rivali politici și să acceseze comunicații criptate). 15 august 2019. The Wall Street Journal. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

36. „Labour suffers second cyber-attack in two days" (Partidul Laburist suferă al doilea atac cibernetic în două zile), 12 noiembrie 2019. The Guardian. https://www.theguardian.com/politics/2019/nov/12/labour-reveals-large-scale-cyber-attack-on-digital-platforms

37. „Extensive hacking operation discovered in Kazakhstan" (Operațiune extinsă de hacking descoperită în Kazahstan). 23 noiembrie 2019. ZDNet. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

Referințe

38. „A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems" (O echipă notorie de hackeri iranieni vizează sisteme de control industrial). 20 noiembrie 2019. Wired. https://www.wired.com/story/iran-apt33-industrial-control-systems/

39. „Russian 'Gamaredon' Hackers Back at Targeting Ukraine Officials" (Hackerii ruși „Gamaredon" vizează din nou oficiali din Ucraina). 6 decembrie 2019. Security Week. https://www.securityweek.com/russian-gamaredon-hackers-back-targeting-ukraine-officials

40. „Iran announced it foiled 'really massive' foreign cyber attack" (Iranul a anunțat că a împiedicat un atac cibernetic străin „cu adevărat masiv"). 11 decembrie 2019. Security Affairs. https://securityaffairs.co/wordpress/94981/cyber-warfare-2/iran-foreign-cyber-attack.html

41. „Croatian government targeted by mysterious hackers" (Guvernul croat a fost vizat de hackeri misterioși). 5 iulie 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

42. „Raport referitor la punerea în aplicare a politicii externe și de securitate comune – raport anual" 18 decembrie 2019. Parlamentul UE. https://www.europarl.europa.eu/doceo/document/A-9-2019-0054_RO.html

43. „Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent" (Hackeri chinezi sunt învinuiți de intruziune la gigantul din industria energetică Telvent). 26 septembrie 2012. Krebs on Security. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information

44. „Energy Manufacturer Also Victimized by IE Zero Day in Watering Hole Attack" (Producător de energie victimizat, de asemenea, de IE Zero Day în atacul Watering Hole). 2 ianuarie 2013. The Threat Post. https://threatpost.com/energy-manufacturer-also-victimized-ie-zero-day-watering-hole-attack-010213/77359/

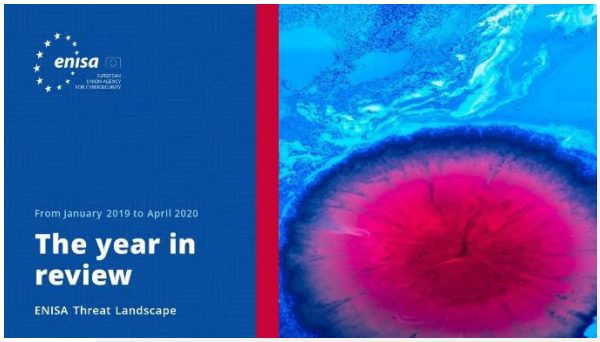
45. „The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity" (Conexiunea franceză: atacul CVE-2014-0322, axat pe industria aerospațială franceză, prezintă asemănări cu activitatea turbinei Capstone din 2012). 25 februarie 2014. CrowdStrike Blog. https://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/

46. „Advanced Persistent Threat Groups" (Grupuri de amenințări persistente avansate). Fireeye. https://www.fireeye.com/current-threats/apt-groups.html

47. „U.S. accuses pair of stealing secrets, spying on GE to aid China" (SUA acuză 2 persoane de furt de secrete, spionând GE pentru a ajuta China). 23 aprilie 2019. Reuters. https://www.reuters.com/article/us-usa-justice-ge/us-accuses-pair-of-stealing-secrets-spying-on-ge-to-aid-china-idUSKCN1RZ240


„În cursul anului 2019 a crescut
numărul de atacuri cibernetice
susținute de state-națiune care
vizează economia.”
în ETL 2020

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

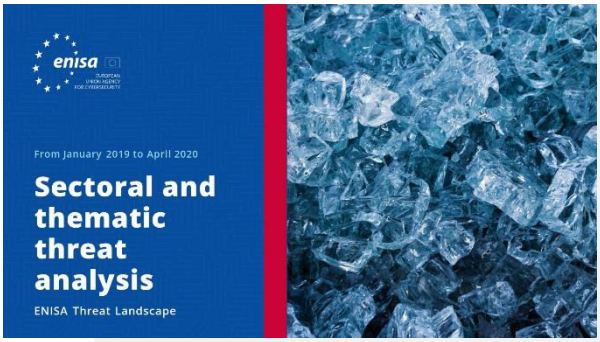
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Teme de cercetare

Recomandări privind teme de cercetare în 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 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