RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ianuarie 2019 – aprilie 2020

Principalele incidente din UE și din întreaga lume

Raportul ENISA privind situația amenințărilor

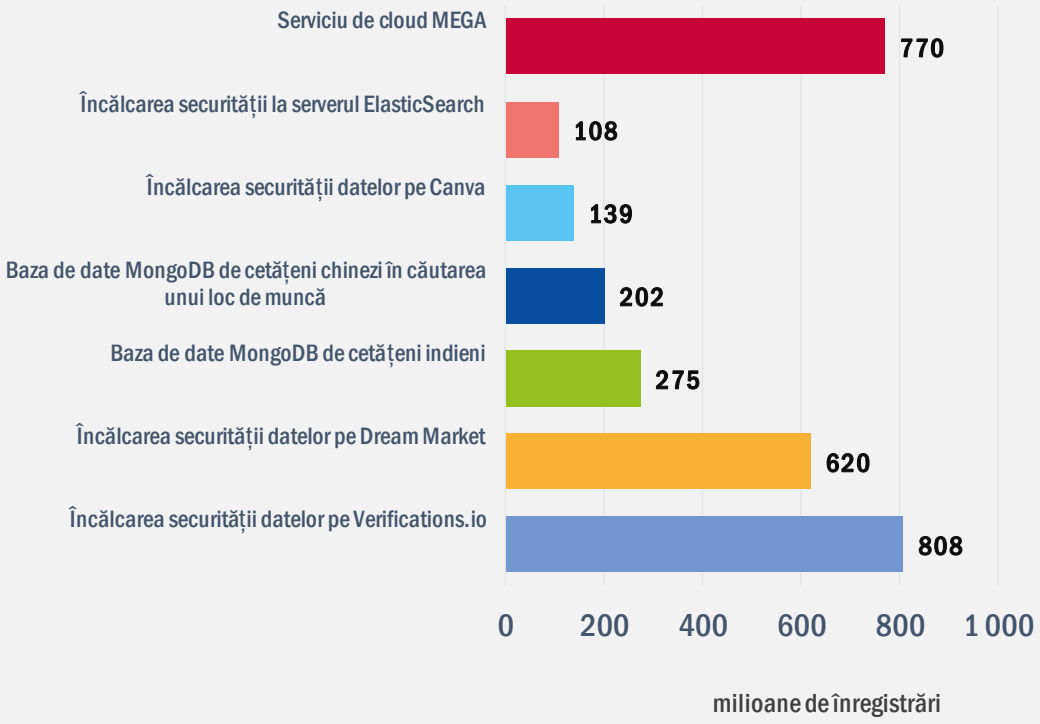
Prezentare generală

Complexitatea capacităților de amenințare a crescut în 2019, mulți adversari folosind exploit-uri, furtul de date de identificare și atacurile în mai multe etape. Numărul de incidente de încălcare a securității datelor este încă foarte ridicat, iar cantitatea de informații financiare și de date de identificare furate ale utilizatorului este în creștere. În unele cazuri, necorectarea unei vulnerabilități cunoscute care are potențialul de a afecta software-ul sau bibliotecile utilizate – într-un interval de timp rezonabil – poate avea repercusiuni grave.

În ultimul deceniu, **malware-ul a ajuns pe lista ENISA cu cele mai importante 15 amenințări, însă există în continuare multe sisteme de securitate care nu pot detecta această amenințare**. Timp de mulți ani, malware-ul a fost răspândit în principal prin spam rău intenționat pe e-mail și, mai recent, folosind mesaje de phishing elaborate în detaliu. Întreprinderile din sectorul tehnologiilor și furnizorii de servicii de e-mail au investit în filtre de spam, îmbunătățind astfel detectarea atașamentelor rău intenționate. Cu toate acestea, **adversarii inovează acum pentru a-și spori șansele de a ajunge la potențiale victime**. În această perioadă, multe dintre aceste inovații au dat rezultate pentru actorii rău intenționați.

Pandemia COVID-19 a pus sub presiune organizațiile și profesioniștii din domeniul sănătății din întreaga lume, iar sănătatea a devenit unul dintre cele mai importante sectoare care trebuie protejat împotriva atacurilor cibernetice. Numărul incidentelor care implică ransomware-uri vizând sectorul sănătății era deja ridicat, dar a crescut în timpul pandemiei.

Topul incidentelor de încălcare a securității datelor



Cronologie

2019

_ Ianuarie

MEGA cloud (NZ) a suferit o încălcare a securității datelor, expunând 770 de milioane de e-mailuri și 21 de milioane de parole.[1]

_ Februarie

Verification.io (US) a expus aproximativ 800 de milioane de înregistrări.[2]

_ Martie

Norsk Hydro (NO) a fost victima unui atac ransomware.[3]

_ August

Biroul pentru impozite pe venituri personale din Bulgaria (BG) a suferit o încălcare a securității datelor, expunând PII de la toți cetățenii adulți.[8]

_ Septembrie

Mastercard (BE) a suferit o încălcare a securității datelor care a afectat aproximativ 90 000 de clienți în Europa.[9]

_ Octombrie

Site-urile web și postul național de televiziune din Georgia (GE) au suferit un atac cibernetic coordonat.[30]

_ Noiembrie

UniCredit (IT) a fost victima unei încălcări a securității datelor, divulgându-se 3 milioane înregistrări.[10]

_ Decembrie

Prosegur (SP) a suferit un atac ransomware care i-a perturbat funcționarea.[11]

2020

_ Ianuarie

Ministerul de Externe din Austria (AT) a fost vizat de un atac cibernetic.[12]

_ Aprilie

Facebook (SUA) a raportat o încălcare a securității datelor, expunând 540 de milioane de înregistrări ale utilizatorilor pe serverele expuse.[4]

_ Mai

Thyssen-Krupp and Bayer (DE) au fost vizate de programe malware de spionaj.[5]

_ Iulie

City Power (ZA) a fost victima unui atac de tip ransomware care a întrerupt alimentarea cu energie în Johannesburg.[7]

_ Iunie

Cinci spitale din România (RO) au fost vizate de ransomware-ul Badrabbit.[6]

_ Februarie

INA Group (HR) a fost victima unui atac de tip ransomware.[13]

_ Martie

Rețeaua ENTSO-E (BE) a fost compromisă, victimă a unei intruziuni.[14]

_ Aprilie

Peste 500 000 de conturi Zoom (SUA) au fost găsite la vânzare pe Dark Web.[31]

Cele mai vizate sectoare

În vizor

Sectoarele cele mai vizate în această perioadă au fost serviciile digitale, administrația guvernamentală și industria tehnologică. Atacurile asupra furnizorilor de servicii digitale servesc adesea ca proxy pentru a ajunge la alte ținte mai atractive. În schimb, atacurile asupra industriei tehnologice au permis actorilor rău intenționați să compromită lanțul de aprovizionare sau să caute vulnerabilități de exploatat.

Platforma de e-mail **verifications.io**[18] a suferit o încălcare majoră a securității datelor[↗] din cauza unei baze de date MongoDB neprotejate. Au fost expuse date din peste 800 de milioane de e-mailuri conținând informații sensibile care includeau informații personale identificabile (PII).

Peste 770 de milioane de adrese de e-mail și 21 de milioane de parole unice au fost expuse într-un forum popular de hacking găzduit de serviciul cloud **MEGA**[1]. Aceasta a devenit cea mai semnificativă colecție de date de identificare personale vizate de atacuri de încălcare a securității datelor din istorie, numită „Colecția nr. 1”.

Furnizorul de software cloud și de virtualizare **Citrix** a fost victima unui atac cibernetic țintit. Pentru a obține acces la sistemele Citrix, atacatorii au exploatat mai multe vulnerabilități software critice, cum ar fi CVE-2019-19781 și au folosit o tehnică numită „password spraying”.

Furnizorul de servicii de găzduire cloud **iNSYNQ**[19] s-a confruntat cu un atac ransomware[↗] care a lăsat clienții în imposibilitatea de a-și accesa datele mai mult de o săptămână, obligându-i pe clienți să se bazeze pe copiile de rezervă locale.

Sectoarele cele mai vizate

Servicii digitale_ În cursul anului 2019, au fost atacate servicii precum e-mail, platforme sociale și de colaborare și furnizori de cloud. Acestea au fost folosite și ca proxy pentru atacuri ulterioare.

Administrația guvernamentală_ Rezultatele financiare provenind din răscumpărările plătite fac din sectorul public una dintre cele mai atractive ținte pentru atacurile ransomware.

Industria tehnologică_ Industria tehnologică a fost atacată în 2019, în principal prin atacuri în lanțul de aprovizionare, care au încercat să compromită dezvoltarea software-ului prin exploit-uri zero-day și atacuri backdoor (uși secrete).

Sectorul financiar_ Numărul incidentelor vizând organizațiile financiare, și nu neapărat bănci, a crescut substanțial în perioada de raportare.

Asistența medicală_ Numărul atacurilor împotriva sectorului asistenței medicale continuă să crească.

Tendințe

În general

- În 2019, s-a observat o **activitate intensă a virușilor troian** pe tot globul. Emotet și Agent Tesla au fost cele mai frecvente și periculoase tipuri de malware.
- **Phishing** a rămas una dintre cele mai reușite tehnici de livrare a instrumentelor rău intenționate. Printre momelile puternice de phishing se numără escrocheriile pe telefon, facturile false, plățile, cotațiile și bonurile de comandă și vânzare.
- **Ransomware** continuă să genereze recompense financiare substanțiale pentru actorii rău intenționați. Un studiu recent a identificat campanii de ransomware operate de oameni[17], în care adversarii folosesc furtul de date de identificare și metode de mișcare laterală asociate în mod tradițional cu atacuri țintite, cum ar fi cele ale actorilor statelor-națiune.
- Schemele de **furt de date de pe cardurile bancare (card skimming)** au devenit o amenințare semnificativă în perioada 2019 - 2020, din cauza numărului tot mai mare de cumpărători online.
- **Compromiterea e-mailului de afaceri (Business e-mail compromise – BEC)** este o amenințare în creștere ca urmare a cantității mari de date de identificare și informații personale furate în ultimul deceniu.
- Întreprinderile s-au confruntat în medie cu 12 atacuri de **umplutură de date de identificare (credential stuffing)** în fiecare lună, în care atacatorul poate să identifice datele de identificare valide.

Constatări

84 %_ din atacurile cibernetice se bazează pe inginerie socială

67 %_ din malware a fost livrat prin conexiuni HTTPS criptate[34]

230 000_ de noi tulpini de malware în fiecare zi

6_ luni, în medie, este perioada necesară pentru a detecta o încălcare a securității datelor

71 %_ din organizații s-au confruntat cu activități malware care s-au răspândit de la un angajat la altul[35]

Actori

_Cine

Cunoașterea responsabilului sau atribuirea responsabilității unei persoane ori unui grup pentru un incident de securitate cibernetică este încă o sarcină descurajantă și adesea un exercițiu inutil. Cu toate acestea, din perspectiva informațiilor privind amenințările, este esențial să se clasifice comportamentele, să se înțeleagă dinamica și modul de operare utilizat de anumiți adversari. Această analiză îi ajută adesea pe apărători să caute urme specifice și să încerce să anticipeze următoarea acțiune adversară.

Grupul Lazarus, de exemplu, un grup de amenințări persistente avansate (APT), presupus a fi susținut de stat, a fost raportat mai activ în perioada de raportare atât în atacurile motivate financiar, cât și în cele motivate de spionaj. Grupul a fost asociat cu mai multe incidente, inclusiv **campania AppleJeus** care vizează utilizatorii platformei de tranzacționare a criptomonedelor și sistemele asociate.[22] Incidentele majore atribuite acestui grup cuprind:

- piratarea unei centrale nucleare indiene și a unei organizații de cercetare spațială în noiembrie 2019;
- compromiterea unei aplicații de tranzacționare a criptomonedelor care vizează administratorii bursei în octombrie 2019;
- atacarea bancomatelor (ATM-uri) și a băncilor din India, identificată în septembrie 2019;
- vizarea utilizatorilor Android din Coreea de Sud prin intermediul aplicațiilor infectate cu viruși tip troian din Google Play Store identificate în august 2019.

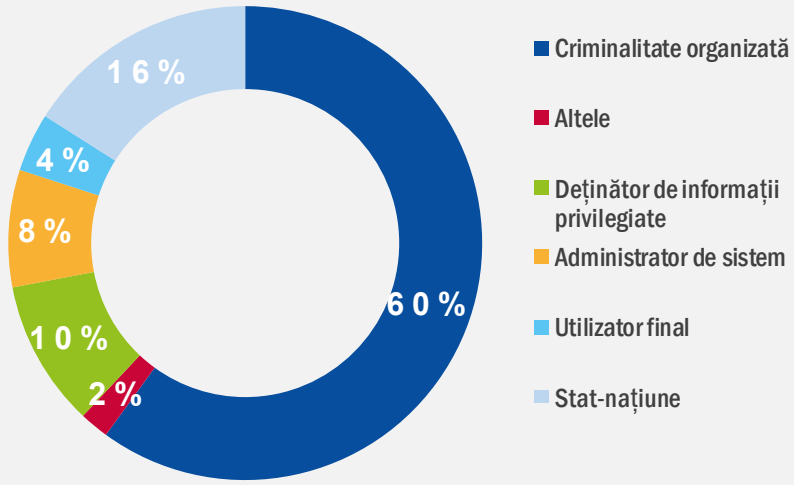
Cei mai activi actori

TURLA_ S-a raportat că grupul a vizat servere de e-mail Microsoft Exchange din sectorul educației, guvern, militar, al cercetării și cel farmaceutic din peste 40 de țări în 2019.[23]

APT27_ S-a raportat că grupul a compromis serverele SharePoint ale organizațiilor guvernamentale din două țări din Orientul Mijlociu.

VICIOUS PANDA_ În aprilie 2020, administrația publică mongolă ar fi fost vizată de acest grup.[24]

GAMAREDON_ Grupul ar fi vizat Ministerul Apărării din Ucraina într-o campanie de spear phishing în decembrie 2019.[25]



Motivații

_De ce

Deși este dificil să se determine motivația principală din spatele unui atac cibernetic, acestea pot fi totuși clasificate în funcție de rezultatul incidentului.

Financiară: Numărul de incidente care determină furtul de informații, date și date de identificare ale utilizatorului este cel mai ridicat observat în perioada de raportare. În majoritatea cazurilor, intenția este de a fura date/informații și a le vinde pe Dark Web. Pot fi identificate și alte utilizări ale acestor informații/date pentru a facilita alte tipuri de atacuri cu un rezultat complet diferit, cum ar fi spionajul sau frauda financiară. Peste 620 de milioane de detalii privind conturile au fost furate de pe 16 site-uri internet piratate și oferite spre vânzare pe piața Dark-Web Dream Market care se bucură de popularitate.

Spionaj: Acesta este un motiv din spatele unui număr tot mai mare de atacuri raportate, în principal din cauza tensiunilor geopolitice și comerciale în curs. Numărul incidentelor nu este substanțial, dar dimensiunea și amploarea lor îl plasează pe locul al doilea în lista ENISA a primelor 5 motivații. Printre incidentele demne de menționat se numără cel raportat în aprilie 2019, în care un angajat al General Electric și un om de afaceri chinez au fost puși sub acuzare de Departamentul de Justiție al Statelor Unite pentru spionaj economic și furt de secrete comerciale de la General Electric.[20] AgenceFrance Presse (AFP) a raportat că Airbus a fost victima unei campanii sofisticate de spionaj cibernetic. Atacatorii ar fi încălcat securitatea sistemelor IT ale mai multor furnizori Airbus și, de acolo, au pătruns în sistemele IT ale companiei.[21]

Cele mai importante cinci motivații: financiară, spionaj, perturbare, politică și represalii.

Motivații de top

Figura de mai jos arată că aspectul **financiar** este în continuare principalul motiv pentru majoritatea atacurilor cibernetice. În unele cazuri, într-un singur atac pot fi identificate mai multe motivații. De exemplu, spionajul, aspectele politice, financiare și perturbarea sunt adesea motive combinate. Multe incidente provin din sisteme automate și sunt livrate „sub forma unui serviciu" plătit în criptomonede. Aceste servicii includ distribuirea de ransomware, comandă și control (C2), blocare distribuită a serviciului (DDoS), spam și alte activități ilicite.

Vectori de atac

_Cum

Atacurile cibernetice parcurg în medie trei etape pentru a ajunge la activele valoroase ale victimei. Când se examinează vectorii de atac utilizați cel mai frecvent, trebuie prioritizate punctul de intrare, cursul acțiunii și acțiunea asupra activelor. Acestea sunt etapele cele mai critice care trebuie să constituie abordări distincte într-o strategie de apărare.

Punct de intrare: În cursul anului 2019, tehnicile utilizate cel mai frecvent pentru a începe un atac cibernetic includ forța brută cu datele de identificare furate, inginerie socială, erori de configurare și exploatarea aplicațiilor web. Exploatarea aplicațiilor web, de exemplu, a fost utilizată adesea ca punct de intrare din cauza creșterii utilizării acestui tip de aplicație pentru a transfera date în cloud. Erorile în configurația cloud și utilizarea incorectă a sistemelor au fost un punct de intrare esențial într-un număr mare de incidente. Utilizarea ingineriei sociale pentru a planifica un atac se bazează pe instrumente precum phishingul și compromiterea e-mailului de afaceri (BEC).[16] Alte tehnici mai puțin frecvente, dar la fel de importante, sunt exploatarea vulnerabilităților (de la sisteme neperfectate și „zero-days") și a backdoor-urilor din software, utilizate adesea în atacuri mai complexe și sofisticate.

Cursul acțiunii: Instalarea programelor malware este cea mai utilizată tehnică în etapa „cursul acțiunii". Odată instalat, un astfel de program îl ajută pe adversar să facă recunoaștere, să se deplaseze în jurul sistemelor și rețelelor victimei, să instaleze instrumente suplimentare precum ransomware, să fure date și să comunice cu un server C2.

Cinci dintre activele cele mai dorite de către infractorii cibernetici

01_Proprietatea industrială și secretele comerciale

Proprietatea industrială și secretele comerciale sunt cele mai tentante active datorită valorii ridicate pentru proprietarii lor, pentru piață și, în unele cazuri, pentru infractori.

02_Informații clasificate de stat/militare

Aceste active conțin orice informații pe care un stat le consideră sensibile. În 2019, tensiunile comerciale și diplomatice dintre țări au făcut acest tip de informații și mai atractiv.

03_Infrastructura serverului

Infrastructura serverului constituie primul tip de active sensibile care nu sunt date. În multe atacuri, preluarea infrastructurii serverului victimei este obiectivul principal.

04_Date de autentificare

Datele de autentificare sunt active valoroase pentru generarea de profituri, dar și ca obiectiv în sprijinul unui atac.

05_Date financiare

Datele financiare, cum ar fi cardul de credit, informațiile bancare și de plată, sunt întotdeauna valoroase pentru infractorii cibernetici.

_Cum s-a schimbat situația în contextul pandemiei de COVID-19?

În 2019, ENISA a continuat cartografierea situației amenințărilor, sprijinind factorii decizionali și factorii de decizie politică să definească strategii pentru apărarea cetățenilor, a organizațiilor și a spațiului cibernetic. Această activitate face parte din strategia ENISA de a oferi informații strategice părților interesate. Tema centrală în 2019 a fost următoarea generație de telecomunicații mobile, sau 5G, în urma unei cereri din partea Comisiei Europene și a statelor membre. **Agenția va continua să producă aceste rapoarte tematice privind situațiile amenințărilor, iar în 2020** accentul este plasat pe inteligența artificială.

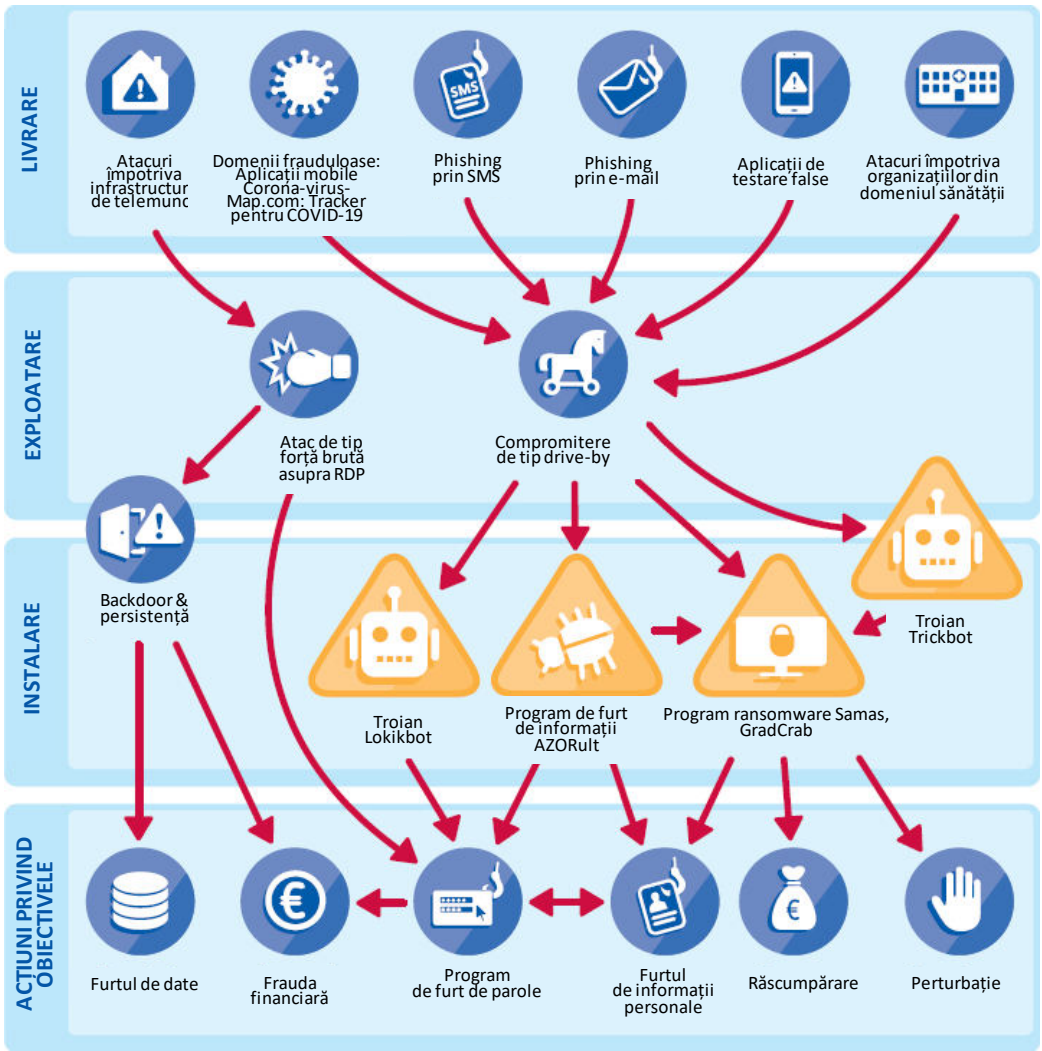
Pandemia de COVID-19 a fost o perioadă prolifică pentru actorii rău intenționați care desfășoară atacuri vizând domenii sensibile, cum ar fi furnizorii de servicii medicale și persoanele care lucrează de acasă. ENISA cartografiază situația amenințărilor întâlnite în timpul pandemiei și oferă consiliere cu privire la măsurile de atenuare care vor încerca să reducă expunerea la amenințări.

ENISA împărtășește recomandările sale în materie de securitate cibernetică cu privire la pandemia de COVID-19 pe o gamă largă de subiecte, inclusiv munca la distanță, cumpărăturile online și e-sănătatea, și oferă sectoarelor afectate recomandări valoroase și actualizate privind securitatea.[32]

Spitalul Universitar Brno din Republica Cehă a fost vizat de un atac cibernetic[33] în mijlocul pandemiei de COVID-19, ceea ce l-a forțat să redirecționeze pacienți și să amâne intervenții chirurgicale. Incidentul este considerat critic deoarece acest spital este unul dintre cele mai mari laboratoare care efectuează teste COVID-19 din Republica Cehă.

_Situația amenințărilor în contextul pandemiei de COVID-19

ENISA a pregătit numeroase resurse pentru o campanie de sensibilizare și a împărtășit alte resurse interne și externe dedicate experților în materie de securitate cibernetică, acoperind problemele de securitate asociate provocărilor întâmpinate în timpul pandemiei de COVID-19. Una dintre aceste resurse a fost analiza celor mai critice amenințări din această perioadă.



Referințe

1. „MEGA Data Breach Exposed 773 Million Email Addresses and Passwords” (Încălcarea securității datelor MEGA a expus 773 milioane de adrese de e-mail și parole). 19 ianuarie 2019. Latest Hacking News. https://latesthackingnews.com/2019/01/19/mega-data-breach-exposed-773-million-email-addresses-and-passwords/

2. „Largest Leak in History: Email Data Breach Exposes Over Two Billion Personal Records” (Cea mai mare scurgere de informații din istorie: încălcarea securității datelor prin e-mail expune peste două miliarde de înregistrări personale). 8 aprilie 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/largest-leak-in-history-email-data-breach-exposes-over-two-billion-personal-records/

3. „LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company” (Ransomware-ul LockerGoga întrerupe operațiunile la o companie norvegiană producătoare de aluminiu) 20 martie 2019. Recorded Future. https://www.recordedfuture.com/lockergoga-ransomware-insight/

4. „Researchers find 540 million Facebook user records on exposed servers” (Cercetătorii găsesc 540 de milioane de înregistrări a le utilizatorilor Facebook pe servere expuse). 3 aprilie 2019. Tech Crunch. https://techcrunch.com/2019/04/03/facebook-records-exposed-server/

5. „Winnti: Attacking the Heart of the German Industry” (Winnti: atacarea punctului central al industriei germane), 24 iulie 2019. Web.br. https://web.br.de/interaktiv/winnti/english/

6. „Cyber-attacks against 5 hospitals in Romania. CCR's website, also hacked” (Atacuri cibernetice împotriva a 5 spitale din România. Site-ul CCR a fost, de asemenea, piratat), 20 iunie 2019. Romanian Journal. https://www.romaniajournal.ro/society-people/cyber-attacks-five-hospitals-romania-ccr-website-hacked/

7. „Here's how ransomware attacks like the one on CityPower work – and why some victims end up paying criminals millions” (Iată cum funcționează atacurile de tip ransomware precum cel de la CityPower – și de ce unele victime ajung să plătească milioane infractorilor), 25 iulie 2019. Business Insider South Africa. https://www.businessinsider.co.za/ransomware-attack-on-citypower-johannesburg-why-victims-pay-criminals-2019-7

8. „Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged” (Saga încălcărilor de securitate: Agenția fiscală bulgară amendată; persoane care au efectuat testele de penetrare au fost puse sub acuzare). 30 august 2019. Bank Info Security. https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000

9. „Breach Of Mastercard Loyalty Program Affected 90K Germans' Data” (Încălcarea securității programului de loialitate Mastercard a afectat datele a 90 000 de germani), 23 august 2019. PYMNTS.com. https://www.pymnts.com/news/security-and-risk/2019/mastercard-loyalty-program-data-breach-germany/

10. „UniCredit confirms data breach” (UniCredit confirmă încălcarea securității datelor), 28 octombrie 2019. PrivSec Report. https://gdpr.report/news/2019/10/28/privacy-unicredit-confirms-data-breach/

11. „Prosegur Hacked: Spanish SOC Provider Hit by Ryuk Ransomware” (Prosegur a fost piratat: furnizor spaniol de SOC vizat de ransomware-ul Ryuk), 28 noiembrie 2019. Computer Business Review. https://www.cbronline.com/news/prosegur-hacked-ransomware

12. „Serious cyber-attack' on Austria's foreign ministry” (Atac cibernetic grav asupra Ministerului de Externe al Austriei), 5 ianuarie 2020. BBC. https://www.bbc.com/news/world-europe-50997773

13. „Croatia's largest petrol station chain impacted by cyber-attack” (Cel mai mare lanț de stații de benzină din Croația a fost afectat de un atac cibernetic), 20 februarie 2020. ZDNet. https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/

14. „European power grid organization says its IT network was hacked” (Organizație europeană de rețea electrică declară că rețeaua sa informatică a fost piratată), 9 martie 2020. Cyberscoop. https://www.cyberscoop.com/european-entso-breach-fingrid/

15. „Fullz House hackers pivot from phishing to Magecart card skimming attacks” (Hackerii Fullz House pivotează de la phishing la atacuri de furt de date de pe carduri Magecart), 26 noiembrie 2019. ZDNet. https://www.zdnet.com/article/fullz-house-threat-group-pivots-from-phishing-to-magecart-card-skimming-attacks/

16. „FBI warns of cloud based BEC attacks” (FBI avertizează asupra atacurilor BEC bazate pe cloud). 8 aprilie 2020. Info Security. https://www.infosecurity-magazine.com/news/fbi-warns-of-cloudbased-bec-attacks/

17. „Microsoft Alerts Healthcare to Human-Operated Ransomware" (Microsoft avertizează sectorul de asistență medicală cu privire la ransomware operate de oameni), 1 aprilie 2020. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/microsoft-alerts-healthcare-to-human-operated-ransomware/d/d-id/1337463

18. „Verification.io suffers major data breach" (Verification.io suferă o încălcare majoră a securității datelor). 15 martie 2019. PrivSec Report. https://gdpr.report/news/2019/03/15/verification-io-suffers-major-data-breach/

19. „Inside the Insynq attack: „We had to assume they were listening"" (În interiorul atacului Insynq: „Trebuia să presupunem căascultau") 8 august 2019. Accounting Today. https://www.accountingtoday.com/news/inside-the-insynq-ransomware-attack-we-had-to-assume-they-were-listening

20. „Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets" (Un fost inginerGE și un om de afaceri chinez au fost puși sub acuzare pentru spionaj economic și furt de secrete comerciale de la General Electric). 23 aprilie 2019. Departamentul de justiție al SUA https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

21. „Airbus supply chain hacked in a cyberespionage campaign" (Lanțul de aprovizionare Airbus a fost piratat într-o campanie de spionaj cibernetic), 27 septembrie 2019. CERT-EU. https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf

22. „Lazarus group's 'AppleJeus' sequel targets cryptocurrency traders" (O nouă varietate a programului „AppleJeus" al grupuluiLazarus vizează comercianții de criptomonede), 10 ianuarie 2020. The Cyber-Security Source. https://www.scmagazineuk.com/lazarus-groups-applejeus-sequel-targets-cryptocurrency-traders/article/1670446

23. „Russian Nation-State Group Employs Custom Backdoor for Microsoft Exchange Server" (Grupul rus al statului-națiune folosește un Backdoor personalizat pentru serverul Microsoft Exchange), 7 iulie 2019. Dark Reading. https://www.darkreading.com/application-security/russian-nation-state-group-employs-custom-backdoor-for-microsoft-exchange-server/d/d-id/1334628

24. „Vicious Panda: The COVID Campaign" (Vicious Panda: Campania COVID), 12 martie 2020. Check Point Research. https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

25. „Gamaredon APT Improves Toolset to Target Ukraine Government, Military" (Gamaredon APT îmbunătățește setul de instrumente pentru a viza guvernul ucrainean și instituțiile militare), 5 februarie 2020. Threat Post. https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/

26. „Virus attacks Spain's defense intranet, foreign state suspected: paper" [Atac cu virus și asupra rețelei de intranet a Ministerului Apărării din Spania; este suspectat un stat străin (presă)], 26 martie 2019. Reuters. https://www.reuters.com/article/us-spain-security-cyberattack/virus-attacks-spains-defense-intranet-foreign-state-suspected-paper-idUSKCN1R7115

27. „115 Million Pakistani Mobile Users Data Go on Sale on Dark Web" (Datele a 15 milioane de utilizatori pakistanezi de serviciide telefonie mobilă sunt puse la vânzare pe Dark Web), 10 aprilie 2020. Rewterz. https://www.rewterz.com/articles/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web

28. „Your business hit by a data breach? Expect a bill of $3.92 million" (Compania dvs. a fost afectată de o încălcare a securității datelor? Așteptați-vă la o factură de 3,92 milioane USD), 23 iulie 2019. ZDNet. https://www.zdnet.com/article/your-business-hit-by-a-data-breach-expect-a-bill-of-3-92-million/

29. „Cyber Security Statistics for 2019" (Statistici de securitate cibernetică pentru 2019), 21 martie 2019. Cyber Defense. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

30. „Georgia 'I'll Be Back' Cyber Attack Terminates TV, Takes Down 15,000 Websites" [Atacul cibernetic din Georgia „I'll Be Back"(Mă voi întoarce) întrerupe transmisia TV și închide 15 000 de site-uri internet]. 29 octombrie 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites/#1a5746347a48

31. „Half a million Zoom accounts for sale on the dark web" (O jumătate de milion de conturi Zoom de vânzare pe Dark Web). 16 aprilie 2020. WeLiveSecurity by ESET. https://www.welivesecurity.com/2020/04/16/half-million-zoom-accounts-sale-dark-web/

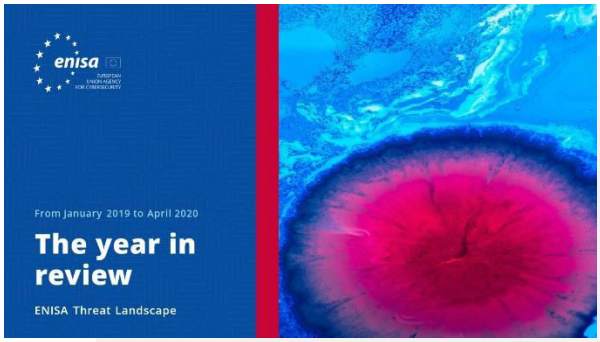
32. „ENISA COVID-19 Resources" (Resurse ENISA în contextul COVID-19). ENISA. https://www.enisa.europa.eu/topics/wfh-covid19

33. „Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak" (Spitalul universitar Brno din Republica Cehă suferă un atac cibernetic în timpul pandemiei de COVID-19), 17 martie 2020. Security Magazine. https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak

34. „Most malware in Q1 2020 was delivered via encrypted HTTPS connections" (Majoritatea programelor malware din T1 2020 au fostlivrate prin conexiuni HTTPS criptate). 25 iunie 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

35. „Malware statistics and facts for 2020" (Statisticișidate despre malware pentru 2020), 29 iulie 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/

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

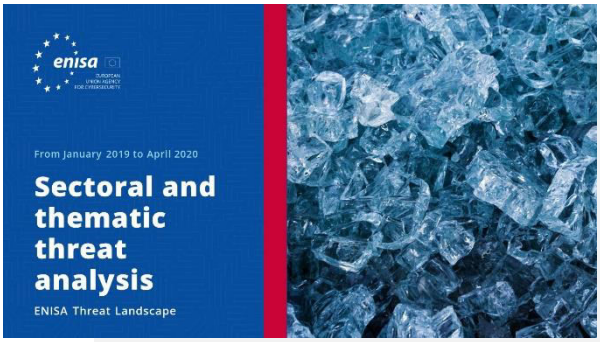
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

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.

Alte publicații

Foaie de parcurs privind cooperarea dintre echipele CSIRT și autoritățile de aplicare a legii

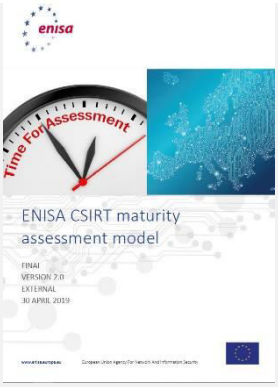
O foaie de parcurs privind cooperarea între echipele CSIRT, în special cu autoritățile de aplicare a legii naționale și guvernamentale și cu sistemul judiciar.

CITIȚI RAPORTUL

Raportul privind starea dezvoltării răspunsului la incidente al statelor membre UE

Un studiu care vizează analizele actualului set operațional de răspuns la incidente în sectoarele NISD și identifică modificările recente.

CITIȚI RAPORTUL



Modelul ENISA de evaluare a maturității CSIRT

O versiune actualizată a studiului „Provocări pentru echipele CSIRT naționale în Europa în 2016: studiu privind maturitatea CSIRT” publicat de ENISA în 2017

CITIȚI RAPORTUL

„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

Despr
e

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 cunoaștem 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

https://www.enisa.europa.eu