enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO

Ianuarie 2019 – aprilie 2020

Atacurile online

Raportul ENISA privind situația amenințărilor

Prezentare generală

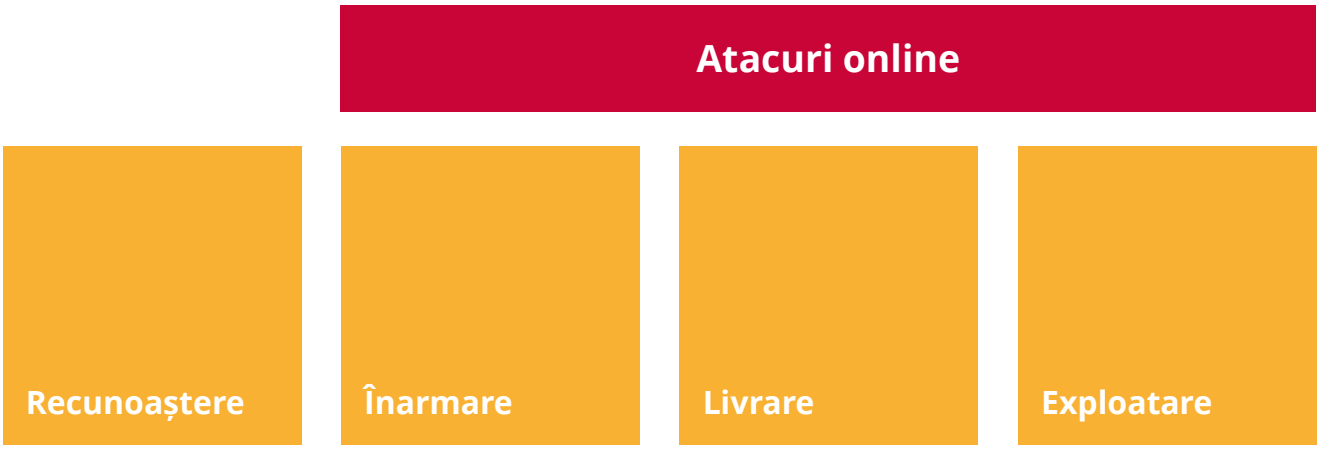
Atacurile online reprezintă o metodă atractivă prin care factorii de amenințare pot înșela victimele folosind sistemele și serviciile web ca vector de amenințare. Aria de atac este vastă, acoperind, de exemplu, facilitarea adreselor URL sau scripturilor rău intenționate pentru a direcționa utilizatorul sau victima către site-ul web dorit sau descărcarea conținutului rău intenționat (atacuri de tip watering hole[1], atacuri de tip drive-by[2]) și injectarea unui cod rău intenționat într-un site legitim, dar compromis pentru a fura informații (adică formjacking[3]) pentru câștig financiar, furt de informații sau chiar extorcare prin ransomware.[4] În plus față de aceste exemple, exploit-urile browserului de internet și compromiterea sistemului de gestionare a conținutului (CSM) sunt vectori importanți observați de diferite echipe de cercetare și folosiți de actori rău intenționați.

De exemplu, atacurile de tip forță brută vizează o operație prin suprasolicitarea unei aplicații web cu încercări de autentificare cu nume de utilizator și parolă. Atacurile online pot afecta disponibilitatea site-urilor web, a aplicațiilor și a interfețelor de programare a aplicațiilor (API), încălcând confidențialitatea și integritatea datelor.

„Creșterea complexității aplicațiilor web și a generalizării serviciilor lor creează dificultăți în a le proteja împotriva amenințărilor, având diverse motivații, de la daune financiare sau reputaționale la furtul de informații critice sau cu caracter personal.”

în ETL 2020

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

La nivel general

- **FURT DE DATE ALE UTILIZATORULUI PRIN PROGRAME MALWARE DE FORMJACKING**. Injecția de cod rău intenționat în site-uri web este o tehnică bine cunoscută utilizată de infractorii cibernetici. Formjacking-ul a fost raportat anterior mai ales în activitățile de minare a criptomonedelor. Cu toate acestea, potrivit unui cercetător în domeniul securității[4], actorii rău intenționați folosesc această tehnică pentru a ataca datele utilizatorilor și detaliile bancare. Site-urile vizate au rămas infectate, în medie, timp de 45 de zile. În mai 2019, același cercetător în domeniul securității a raportat blocarea a aproape 63 de milioane de solicitări web rău intenționate legate de formjacking.
- **„MAGECART" MERGE MAI DEPARTE, VIZÂND LANȚUL DE APROVIZIONARE.** Potrivit unui cercetător în domeniul securității, una dintre companiile franceze din mass-media digitală a fost vizată de actorul rău intenționat Group12. Acesta a infectat inventarul publicitar al site-ului, difuzând un codul rău intenționat (skimmer) și infectând mii de site-uri web care găzduiau reclama.[5] S-a observat că operațiunea acestui grup a fost eficientizată prin înființarea infrastructurii de skimming cu doar câteva luni înainte de începerea campaniei. Astfel, un utilizator final ar putea fi infectat doar vizitând un site web care găzduiește reclama respectivă.[6]
- **PLATFORME DE MESAGERIE ȘI DE COLABORARE ONLINE.** Acestea devin puntea de legătură între actorii rău intenționați și victime pe așa-numita backdoor SLUB. În cursul lunii martie 2019, un cercetător în domeniul securității a identificat o campanie care folosea atacuri de tip watering hole pentru a infecta victimele prin exploatarea vulnerabilității CVE-2018-81747. Atacul a implicat scheme de infecție în mai multe etape. Un exemplu al modului în care funcționează aceste scheme este descărcarea unui fișier DLL, utilizarea unui PowerShell pentru executarea acestuia, descărcarea malware-ului și derularea backdoor-ului principal. Interesant este că malware-ul se conectează la un serviciu de mesagerie al spațiului de lucru Slack pentru a trimite rezultatele comenzilor, care au fost livrate printr-un fragment GitHub Gist în care, potențial, atacatorul adăuga comenzi.[7,8]

- **EXTENSIA BROWSER-ULUI, FRAUDĂ ȘI PUBLICITATE RĂU INTENȚIONATĂ.** Un cercetător în domeniul securității a descoperit o campanie de publicitate rău intenționată foarte răspândită care utiliza extensii Google Chrome; aceasta a afectat aproximativ 1,7 milioane de utilizatori. Aceste extensii Chrome ascundeau caracteristica publicitară de utilizatorii finali pentru a menține browserul infectat conectat la infrastructura C2. Cercetătorul în domeniul securității a concluzionat că această campanie și-a sporit activitatea în perioada martie - iunie 2019, deși există suspiciuni că era activă cu mult timp înainte.[9] Un alt cercetător în domeniul securității a observat că activitatea publicitară NewTab, care facilitează extensiile browserului, a crescut la sfârșitul anului 2019.[11]
- **SITE-URI GOOGLE UTILIZATE PENTRU GĂZDUIREA ÎNCĂRCĂTURII UTILE DRIVE-BY.** Programul malware cunoscut sub numele de „LoadPCBanker" (Win32.LoadPCBanker.Gen) a fost găsit în șablonul dulapurilor de fișiere Google Sites (Clasic Google Sites). Potrivit unui cercetător în domeniul securității, actorul a folosit mai întâi Classic Google Sites pentru a crea o pagină web și ulterior a facilitat șablonul de dulapuri de fișiere pentru a găzdui sarcinile utile. Ulterior, acesta a folosit serviciul SQL drept canal de exfiltrare pentru a trimite și a stoca date despre victime.[12,13]
- **RANSOMWARE CARE FOLOSEȘTE CONVERTITORUL VIDEO ONLINE CA MECANISM DE DESCĂRCARE DRIVE-BY.** Potrivit unui cercetător în domeniul securității, ShadowGate sau WordJScampaign sunt active din 2015, vizând software-uri publicitare și site-uri web. În cursul anului 2016, kitul de exploatare Greenflash Sundown a fost dezvoltat pentru a îmbunătăți activitatea campaniei prin injectarea kitului în serviciile de publicitate compromise și răspândirea ransomware-ului. În 2018, s-a constatat că ShadowGate livra cripto-mineri pe servere din Asia de Est pentru o perioadă scurtă de timp. Distribuția ShadowGate pe țări este prezentată în figura 1 din acest raport. Un alt cercetător în domeniul securității a raportat, de asemenea, activitatea, a cărei urmărire la condus la onlinevideoconverter[.com] ca fiind unul dintre principalele site-uri de drive-by pentru livrarea kitului de exploit-uri.[14,15,16,17,18]

Tendințe

La nivel general

- **SISTEMELE DE GESTIONARE A CONȚINUTULUI SUNT ÎNCĂ O ȚINTĂ IDEALĂ**. Având în vedere popularitatea sistemelor de gestionare a conținutului (CMS) în rândul utilizatorilor de internet, aceste sisteme reprezintă o țintă atractivă pentru actorii rău intenționați. Un cercetător în domeniul securității a identificat o creștere a exploatării unei vulnerabilități identificate în 2018 (Drupalgeddon2) care vizează platforma Drupal. În mod similar, un alt cercetător în domeniul securității a observat o tendință în exploatările WordPress care vizează vulnerabilitățile și plugin-urile terțe depășite.[19,20]

- **EXPLOIT-URILE BROWSER-ULUI DE INTERNET UTILIZATE ÎN ATACURILE DE TIP WATERING HOLE.** Un factor de amenințare a fost surprins efectuând un atac tip watering hole folosind un portal de știri în limba coreeană. În acest atac, un script rău intenționat (JavaScript) a fost injectat automat în pagina de pornire a unui site web (folosind un al doilea script) verificând browserul victimei și exploatând ulterior o vulnerabilitate Google Chrome CVE-2019-13720. Mai mult, s-a constatat că o nouă versiune a malware-ului backdoor SLUB infectează browserul victimei (vulnerabilitatea Internet Explorer CVE-2019-0752) utilizând un site watering hole specific în luna iulie 2019. Într-o altă investigație, echipa de securitate a dezvoltatorului de software a identificat un set de site-uri compromise care au fost utilizate în atacurile de tip watering hole care exploatează vulnerabilitățile iPhone-urilor.[21,22]

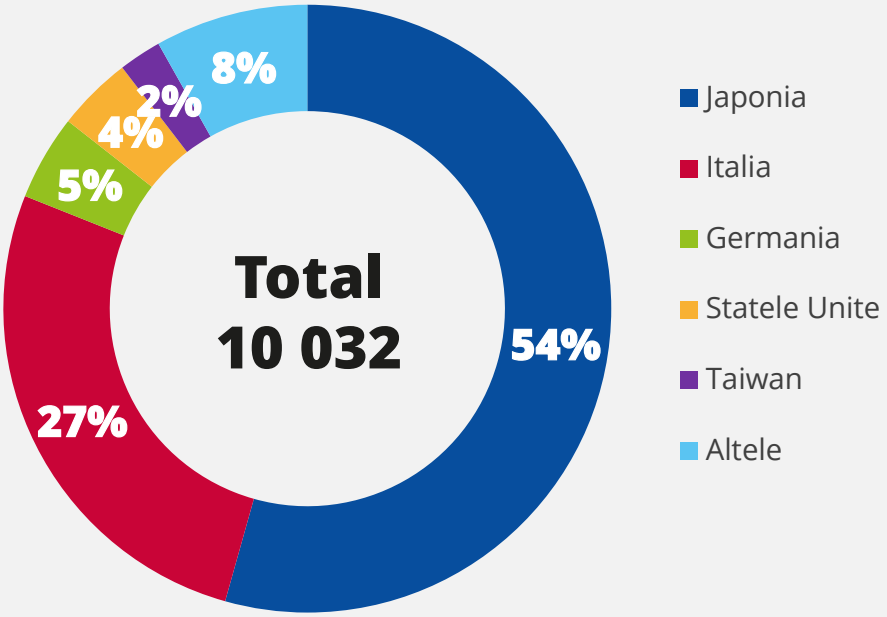


Figura 1: Distribuția procentuală a ShadowGate pe țări

Vectori de atac

Cum

- **DESCĂRCĂRI DRIVE-BY.** Acest vector de atac descarcă conținut rău intenționat pe dispozitivul victimei. În acest tip de atac, utilizatorul final trebuie să viziteze site-ul legitim care a fost compromis. Acest lucru poate fi realizat prin utilizarea de scripturi rău intenționate injectate pe site-ul legitim, derularea exploit-urilor bazate pe browser sau redirecționarea utilizatorului către un site compromis din umbră.[25,26]
- **ATACURI DE TIP WATERING HOLE.** Această tehnică este utilizată pentru atacuri țintite folosind kituri de exploit-uri cu caracteristici stealth. Cu alte cuvinte, acesta este tipul de atac utilizat când un actor rău intenționat este interesat să compromită un anumit grup de utilizatori folosind exploit-uri sau alt conținut rău intenționat (și anume, scripturi sau reclame) injectat în site-ul web.[27]
- **FORMJACKING**. În această tehnică, actorii rău intenționați injectează un cod rău intenționat în formele de plată legitime ale site-ului web. Acest atac captează în principal informații bancare și alte informații personale identificabile (PII). Într-un astfel de scenariu, utilizatorul introduce datele sale bancare sau datele cardului pe portalul de plată pentru comerț electronic. Odată ce informațiile au fost culese și trimise, scriptul rău intenționat va transmite simultan datele către portal și către actorul rău intenționat. Aceste informații sunt utilizate ulterior în scopul comiterii de diverse infracțiuni: câștig financiar, extorcare și vânzare pe piețele darknet.[3,4]
- **URL RĂU INTENȚIONAT.** Acesta este definit ca un link creat cu intenția de a distribui malware sau de a facilita o înșelătorie. Procesul implică ingineria socială a informațiilor victimei pentru a o convinge să facă clic pe URL-ul rău intenționat, care livrează malware sau conținut rău intenționat și compromite computerul victimei.[28]

Operațiunea WizardOpium

S-a găsit o vulnerabilitate de tip zero-day a Google Chrome exploatată la liber în atacuri online țintite. Defecțiunea, înregistrată ca CVE-2019-13720, afectează versiunile anterioare versiunii 78.0.3904.87 pe sistemele Microsoft Windows, Mac și Linux. Defecțiunea se află în componenta audio a browser-ului web și exploatarea sa cu succes ar putea duce la executarea arbitrară a codului.

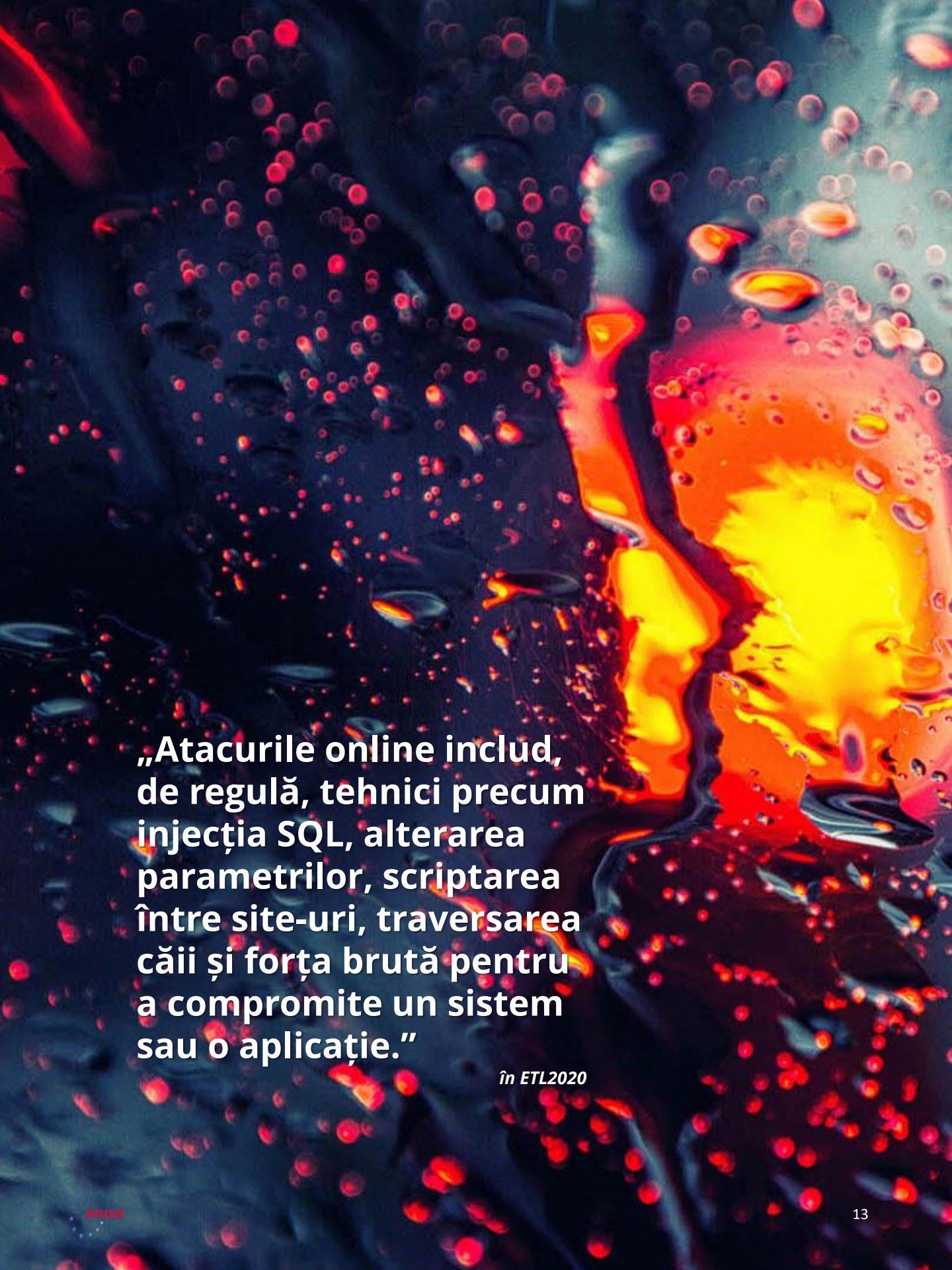
Vulnerabilitatea de tip zero-day, descoperită de un cercetător în domeniul securității și înregistrată ca CVE-2019-13720, nu a fost atribuită niciunui factor de amenințare specific, ci văzută ca parte a unei campanii identificate drept Operațiunea WizardOpium. Între timp, Google a lansat o versiune actualizată pentru versiunea Chrome 78.0.3904.87. Potrivit cercetătorului, atacul profită de o injecție în stilul watering-hole pe un portal de știri în limba coreeană. Un cod JavaScript rău intenționat inserat în pagina de destinație permite încărcarea scriptului de profilare de pe un site la distanță.[23,24]

Exploit-urile browser-ului constituie o formă de exploatare care folosește coduri rău intenționate care utilizează punctele slabe și vulnerabilitățile din software (sistem de operare și browser) sau plugin-urile aferente pentru a obține în cele din urmă acces la dispozitivul victimei.

Măsuri de atenuare

Acțiuni propuse

- Aplicarea unui bun proces și plan de gestionare a patch-urilor;
- actualizarea browser-ului de internet și a plugin-urilor aferente pentru a le menține actualizate și corectate împotriva vulnerabilităților cunoscute;
- corectarea cu patch-uri a paginilor bazate pe sistemul de gestionare a conținutului (CMS) și a portalului pentru a evita plugin-urile și add-on-urile neconfirmate;
- asigurarea că punctele finale și software-ul instalat sunt actualizate, corectate și protejate.
- izolarea aplicațiilor (lista albă a aplicațiilor) și crearea unui mediu de testare (sandbox) pentru a reduce riscul de atacuri tip compromis drive-by. De exemplu, tehnica de izolare a browserului poate proteja punctele finale de exploatarea browserului și de atacuri tip compromis drive-by;[29,30,31]
- Pentru proprietarii de site-uri web, consolidarea serverelor și a serviciilor este o abordare proactivă pentru a atenua atacurile online. Aceasta include controlul versiunii scripturilor de conținut, precum și scanarea fișierelor și scripturilor găzduite local pentru serverul sau serviciul web;[32]
- Restricționarea conținutului online este o altă tehnică de protecție împotriva atacurilor online. Instrumente de facilitare precum blocarea anunțurilor sau blocarea JavaScript vor limita, de asemenea, posibilitatea de a executa coduri rău intenționate în timp ce vizitați anumite site-uri web;[29,30]
- Monitorizarea e-mailurilor web și filtrarea conținutului pentru a detecta și a preveni livrarea de adrese URL și fișiere/încărcături utile rău intenționate.



„Atacurile online includ, de regulă, tehnici precum injecția SQL, alterarea parametrilor, scriptarea între site-uri, traversarea căii și forța brută pentru a compromite un sistem sau o aplicație.”

în ETL2020

Referințe

1. „Watering Hole", Proofpoint. https://www.proofpoint.com/uk/threat-reference/watering-hole

2. „What Is a Drive-By Download?" (Ce este o descărcare Drive-By?) Kaspersky. https://www.kaspersky.com/resource-center/definitions/drive-by-download

3. „Formjacking: Major Increase in Attacks on Online Retailers" (Formjacking: creștere semnificativă a atacurilor asupra comercianților cu amănuntul online), Broadcom. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/formjacking-attacks-retailers

4. „What is Formjacking and How Does it Work?" (Ce este Formjacking și cum funcționează?), Norton. https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html

5. „Magecart's 7 Groups: Hackers Dropping Counter-Intelligence Code in JavaScript Skimmers" (Cele 7 grupuri Magecart: hackerii introduc un cod de contrainformații în skimmeri JavaScript). 14 noiembrie 2018. CBR. https://www.cbronline.com/in-depth/magecart-analysis-riskiq

6. „How Magecart's Web-Based Supply Chain Attacks are Taking Over the Web" (Cum domină internetul atacurile din lanțul de aprovizionare online al Magecart?). 10 martie 2019. CBR. https://www.cbronline.com/analysis/riskiq-magecart-supply-chain-attacks

7. „CVE-2018-8174 Detail", 5 septembrie 2019. NIST. https://nvd.nist.gov/vuln/detail/CVE-2018-8174

8. „Join a Slack workspace" (Alăturați-vă unui spațiu de lucru Slack). Slack. https://slack.com/intl/en-gb/help/articles/212675257-Join-a-Slack-workspace

9. „New SLUB Backdoor Uses GitHub, Communicates via Slack" (Noul backdoor SLUB folosește GitHub și comunică prin Slack), 7 martie 2019. Trend Micros. https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/

10. "Security Researchers Partner With Chrome To Take Down Browser Extension Fraud Network Affecting Millions of Users" (Cercetătorii în domeniul securității se asociază cu Chrome pentru a elimina rețeaua de fraudă a extensiei browserului care afectează milioane de utilizatori), 13 februarie 2020. Cisco Duo Security. https://duo.com/labs/research/crxcavator-malvertising-2020

11. „Mac threat detections on the rise in 2019" (Numărul de detecții ale amenințărilor Mac crește în 2019), 16 decembrie 2019. Malware Bytes. https://blog.malwarebytes.com/mac/2019/12/mac-threat-detections-on-the-rise-in-2019/

12. „File Cabinet" (Dulap de fișiere), Google. https://sites.google.com/site/tiesitestutorial/create-a-page/file-cabinet

13. Google Sites. https://sites.google.com/site/

14. „Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted" (Retragerea ShadowGate Talos: campania globală de publicitate rău intenționată a fost zădărnicită), 1 septembrie 2016. https://blog.talosintelligence.com/2016/09/shadowgate-takedown.html

15. „New Bizarro Sundown Exploit Kit Spreads Locky" (Noul pachet de exploit-uri Bizarro Sundown răspândește Locky), Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/

16. „Incoming! Multiple Popular Websites Attacked for Cryptocurrency Mining via GreenFlash Sundown Exploit Kit" (Atenție, vin! Mai multe site-uri populare au fost atacate pentru minarea criptomonedelor prin kitul de exploit-uri GreenFlash Sundown), 360 Blog. https://blog.360totalsecurity.com/en/incoming-multiple-popular-websites-attacked-cryptocurrency-mining-via-greenflash-sundown-exploit-kit/

17. „ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit" (ShadowGate revine la operațiuni în întreaga lume cu un kit de exploit-uri Greenflash Sundown), 27 iunie 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/shadowgate-returns-to-worldwide-operations-with-evolved-greenflash-sundown-exploit-kit/

18. "GreenFlash Sundown exploit kit expands via large malvertising campaign" (Kitul de exploit-uri GreenFlash Sundown se extinde printr-o mare campanie de publicitate rău intenționată), 26 iunie 2019. Malware Bytes. https://blog.malwarebytes.com/threat-analysis/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/

19. „FAQ about SA-CORE-2018-002" (Întrebări frecvente despre SA-CORE-2018-002), 28 martie 2018. Drupal. https://groups.drupal.org/security/faq-2018-002

20. „Drupalgeddon2 still used in attack campaigns" (Drupalgeddon2 este folosit în continuare în campanii de atac), 7 octombrie 2019. Akamai. https://blogs.akamai.com/sitr/2019/10/drupalgeddon2-still-used-in-attack-campaigns.html

21. „Trustwave Global Security Report 2019" (Raportul Trustwave de securitate globală 2019), 2019. Trustwave.

22. „Stable Channel Update for Desktop" (Actualizare de canal stabil pentru desktop), 31 octombrie 2019.https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html

23. „Chrome 0-day exploit CVE-2019-13720 used in Operation WizardOpium" (Exploit-ul Chrome 0-day CVE-2019-13720 utilizat în Operațiunea WizardOpium). 1 noiembrie 2019. Kaspersky. https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/

24. „CVE-2019-13720 flaw in Chrome exploited in Operation WizardOpium attacks" (Defecțiunea CVE-2019-13720 în Chrome exploatată în atacurile Operațiunea WizardOpium), 1 noiembrie 2019. Security Affairs. https://securityaffairs.co/wordpress/93278/hacking/cve-2019-13720-lazarus-attacks.html

25. „Web Browser-Based Attacks" (Atacuri online bazate pe browser). Morphisec. https://www.morphisec.com/hubfs/1111/briefs/BrowserAttacksBrief-190327.pdf

26. „The 5 most common cyber attacks in 2019" (Cele mai frecvente 5 atacuri cibernetice din 2019). 9 mai 2019. IT Governance. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks

27. „Exploit Kits: Their Evolution, Trends and Impact" (Kituri de exploit-uri: evoluția, tendințele și impactul lor). 7 noiembrie 2019. Cynet. https://www.cynet.com/blog/exploit-kits-their-evolution-trends-and-impact/

28. „Web-Based Threats: First Half 2019" (Amenințări online: prima jumătate a anului 2019). 1 noiembrie 2019. Palo Alto. https://unit42.paloaltonetworks.com/web-based-threats-first-half-2019/

29. „Mitigating Drive-by Downloads" (Atenuarea descărcărilor drive-by), aprilie 2020. ACSC. https://www.cyber.gov.au/publications/mitigating-drive-by-downloads

30. „MITRE ATT&CK: Drive-by compromise" (MITRE ATT & CK: compromis drive-by), 5 decembrie 2019. MITRE.

https://resources.infosecinstitute.com/mitre-attck-drive-by-compromise/#gref

31. „Protecting users from web-based attacks with browser isolation" (Protecția utilizatorilor împotriva atacurilor online cu izolarea browserului), 26 septembrie 2019. Shi Blog – Security Solutions. https://blog.shi.com/solutions/protecting-users-from-web-based-attacks-with-browser-isolation/

32. "https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257". 11 aprilie 2019. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257

Documente conexe

CITIȚI RAPORTUL

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

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

CITIȚI RAPORTUL

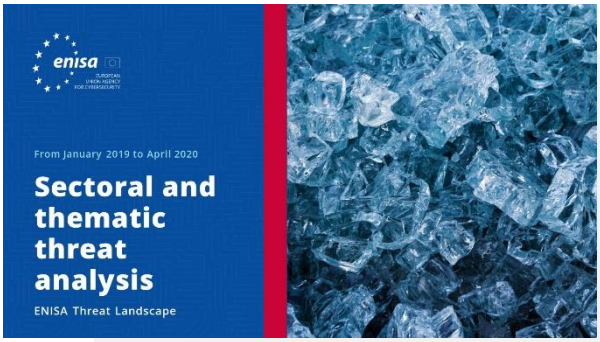
Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

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

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 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 a fost adoptată în conformitate cu Regulamentul (UE) nr. 526/2013. Această publicație nu reprezintă neapărat stadiul actual al tehnologiei, ENISA putând să o actualizeze din când în când.

Sursele terțe sunt citate corespunzător. ENISA nu este responsabilă pentru conținutul surselor externe, inclusiv a 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

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu