enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO

ianuarie 2019 – aprilie 2020

Malware

Raportul ENISA privind situația amenințărilor

Prezentare generală

Malware-ul este un tip comun de atac cibernetic sub formă de software rău intenționat. Familiile de malware includ criptomineri, viruși, ransomware, viermi și spyware. Obiectivele sale comune sunt furtul de informații sau de identitate, spionajul și blocarea serviciului.[1]

În cursul anului 2019, criptominerii au fost una dintre cele mai răspândite familii de malware din peisajul amenințărilor[2], având ca rezultat costuri IT ridicate, consum crescut de energie electrică și productivitate redusă a angajaților.[3] Ransomware-ul a prezentat o ușoară creștere în 2019 comparativ cu 2018, dar rămâne în continuare pe ultimele locuri din lista de tipuri de malware.[2]

Protocoalele web și e-mail au fost cei mai frecvenți vectori de atac inițiali utilizați pentru răspândirea malware-ului. Cu toate acestea, prin utilizarea tehnicilor de forță brută sau exploatarea vulnerabilităților sistemului, anumite familii de malware au putut să se răspândească și mai mult în interiorul unei rețele. Deși detecțiile globale de atacuri au rămas la nivelurile anului precedent, s-a înregistrat o reorientare notabilă de la obiectivele de consum la cele de afaceri.[4]

Constatări

400 000_de detectări de spyware și adware preinstalate pe dispozitive mobile[4]

13 %_creștere a numărului de detectări malware Windows la stațiile de lucru pentru afaceri la nivel global[4]

71 %_din organizații s-au confruntat cu activități malware care s-au răspândit de la un angajat la altul[47]

46,5 %_din toate programele malware din mesajele de e-mail găsite în tipul de fișier „.docx”[24]

50 %_creștere a numărului de programe malware concepute pentru a fura date personale sau programe de spionaj (stalkerware)[15]

67%_din programele de malware au fost livrate prin conexiuni HTTPS criptate[48]

Kill chain

Etapă din fluxul de activitate de atac

Amploarea scopului

Malware

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

Cele mai răspândite tipuri de programe malware

Emotet a fost cea mai răspândită varietate de malware în 2019 și evoluează în 2020. Emotet a fost descoperit inițial în 2014 ca troian bancar. De atunci, a fost actualizat cu funcționalitate de comandă și control (C2), mecanisme suplimentare de eludare, cum ar fi capacitatea de a recunoaște dacă rulează într-un mediu cu încercare și capacitatea de a furniza sarcini utile periculoase, cum ar fi Trickbot și Ryuk.[7] Figura de mai sus prezintă clasificarea programelor malware-ului care vizează operațiuni bancare detectate în 2019.

În perioada de raportare, Emotet a evoluat într-un botnet[2], și-a intensificat activitatea[8] și a inițiat noi campanii localizate de spam cu funcționalitate de spear-phishing pentru a instala ransomware sau a fura informații.[5] În cursul anului 2019, detecțiile Emotet au crescut cu 73 % față de anul precedent, vizând în principal stațiile de lucru pentru afaceri din Statele Unite și Regatul Unit, astfel cum se arată în figura de mai jos.[4]

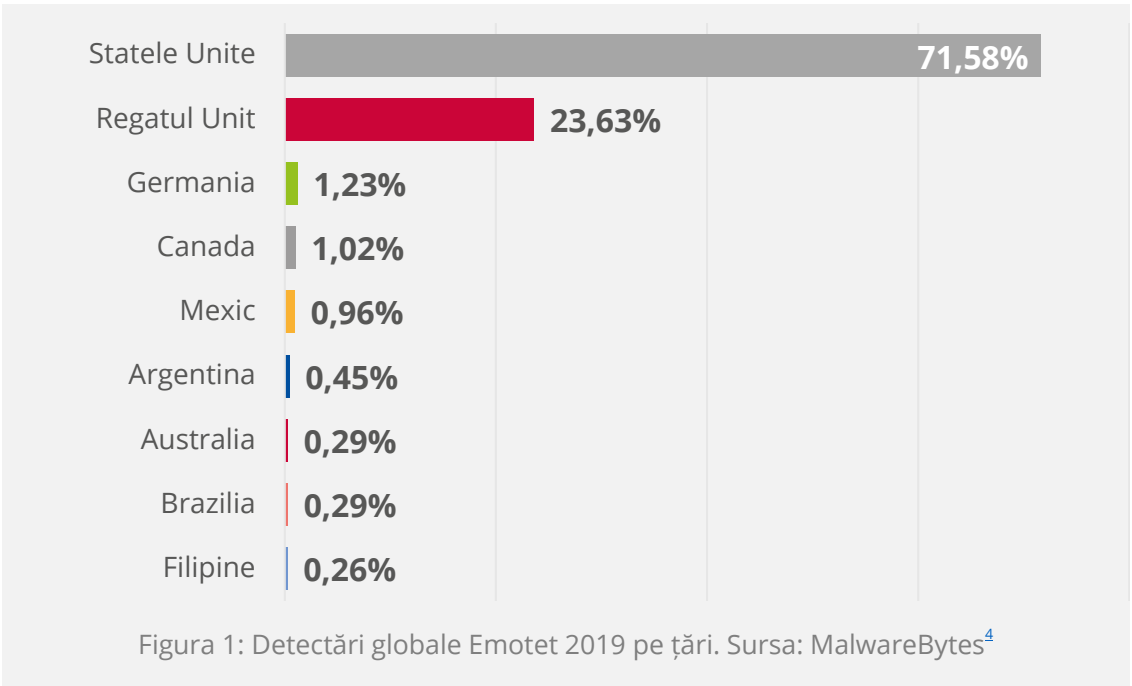


Figura 1: Detectări globale Emotet 2019 pe țări. Sursa: MalwareBytes[4]

Reorientare către ținte comerciale

Deși detectările de malware la nivel global au rămas la aceleași niveluri ca în 2018[4,9], s-a observat o creștere de 13 % a programelor malware care vizează întreprinderile în ceea ce privește serviciile, educația și comerțul cu amănuntul fiind printre sectoarele cele mai grav afectate.[4] Se estimează că peste o treime din atacurile cu malware care vizează operațiuni bancare din 2019 au privit utilizatorii corporativi, cu intenția de a compromite resursele financiare ale întreprinderii.[10] Primele cinci tipuri de programe malware[4] care vizează companiile au fost Trojan.Emotet, Adware.InstallCore, HackTool.WinActivator, Riskware.BitCoinMiner și Virus.Renamer. Atacurile ransomware care vizează sectorul public au crescut în 2019 datorită capacității sale de a plăti răscumpărări mai mari.[11] Întrucât infractorii cibernetici vizează ținte cu valoare ridicată, au fost concepute noi tipuri de malware pentru a se răspândi lateral în interiorul unei rețele corporative mai degrabă decât prin intermediul internetului.[12]

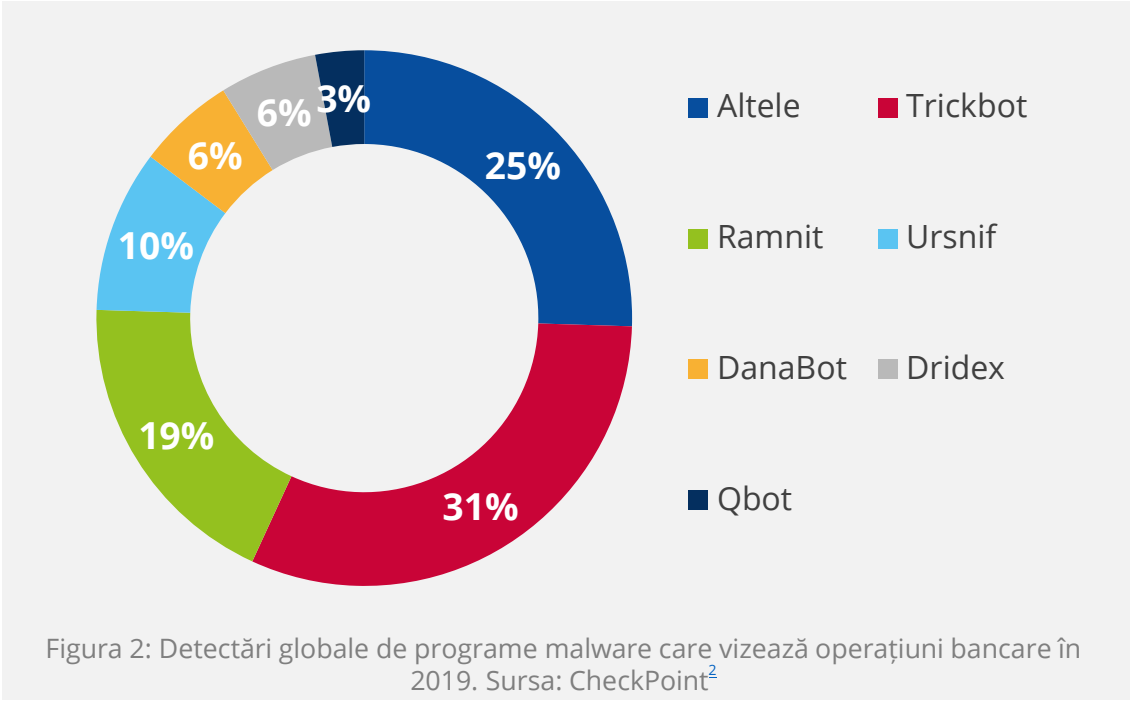


Figura 2: Detectări globale de programe malware care vizează operațiuni bancare în 2019. Sursa: CheckPoint[2]

_ Malware ca serviciu (Malware-as-a-service, MaaS)

Malware-ul ca serviciu (MaaS) se referă la un malware specific vândut în forumurile subterane, care oferă clienților (infractorilor cibernetici) instrumentele și infrastructura necesare pentru atacuri țintite. Un proprietar MaaS oferă acest serviciu prin livrarea unui kit care include un program de încărcare inițială, un server de comandă și control (C2) și un backdoor pentru preluarea controlului complet al computerului infectat.

Un cercetător în domeniul securității[13] a identificat recent patru tipuri de atacuri care utilizau diverse instrumente din portofoliul malware-ului ca serviciu (MaaS) al Golden Chickens (GC), confirmând lansarea de variante îmbunătățite cu actualizări ale codului la trei dintre aceste instrumente.

- **TerraLoader**. Un program de încărcare multifuncțional scris în PureBasic. TerraLoader este un produs emblematic din portofoliul de servicii GC MaaS.
- **more_eggs**. Un malware backdoor capabil să transmită către un server C2 fix și să execute sarcini utile suplimentare descărcate dintr-o resursă web externă. Backdoor-ul este scris în JavaScript.
- **VenomLNK**. Un fișier de comenzi rapide Windows generat probabil de o versiune mai nouă a kitului de construcție VenomKit.

_Creștere bruscă a numărului de programe malware care vizează operațiuni bancare prin telefonul mobil

Aplicațiile mobile concepute pentru a fura date de plată, date de identificare și fonduri din conturile bancare ale victimelor au crescut cu 50 % în prima jumătate a anului 2019.[14] În mod tradițional, factorii de amenințare au folosit tehnici de phishing pentru a obține date de identificare bancare, fie afișând o pagină falsă care imită pagina de autentificare a băncii, fie introducând aplicații mobile false care seamănă cu aplicațiile bancare originale. Cu toate acestea, în 2019, infractorii cibernetici au devenit mai creativi, precum Trojan-Banker.AndroidOS.Gustuff.a, care a reușit să controleze o aplicație bancară legitimă utilizând abuziv funcțiile de accesibilitate ale sistemului de operare, automatizând astfel tranzacțiile rău intenționate.[15] Noi versiuni de malware financiar mobil se găsesc des la vânzare pe forumuri subterane[15] și se dezvoltă constant tehnici noi de eludare. Un nou element adăugat notabil descoperit în 2019 a fost capacitatea malware-ului de a utiliza senzori de mișcare și de a fi declanșat numai atunci când un telefon inteligent se află în deplasare, astfel cum procedează troianul Anubis care vizează operațiuni bancare prin telefonul mobil într-un efort de a detecta un mediu de încercare.[16] Cele mai populare programe malware care au vizat operațiuni bancare în cursul anului 2019[11] au fost Asacub (44,4 %), Svpeng (22,4 %), Agent (19,1 %), Faketoken (12 %) și Hqwar (3,8 %).

_Malware fără fișiere

Programele malware fără fișiere nu conțin un fișier executabil și pot eluda filtrele de securitate obișnuite și tehnicile de elaborare a unei liste albe. Din acest motiv, această familie de malware poate avea până la zece ori mai multe șanse de reușită decât celelalte.[18] În loc de un fișier executabil, acest tip de malware necesită ca atacatorul să injecteze cod rău intenționat în software-ul deja instalat și de încredere, fie de la distanță (de exemplu, în cazul instrumentelor de gestionare Windows sau WMI și PowerShell), fie prin descărcarea activă a fișierelor de documente (și anume, documente de birou) care conțin macro-uri rău intenționate.[19] După un atac reușit, malware-ul poate dobândi persistență prin registru, planificatorul de sarcini încorporat sau WMI. Atacurile malware fără fișiere au crescut cu 265 % în prima jumătate a anului 2019.[20] Majoritatea acestor atacuri au fost bazate pe scripturi (38 %), în timp ce altele au executat un atac în memorie (in-memory) (24 %) sau au abuzat de instrumentele de sistem încorporate (20 %).[21]

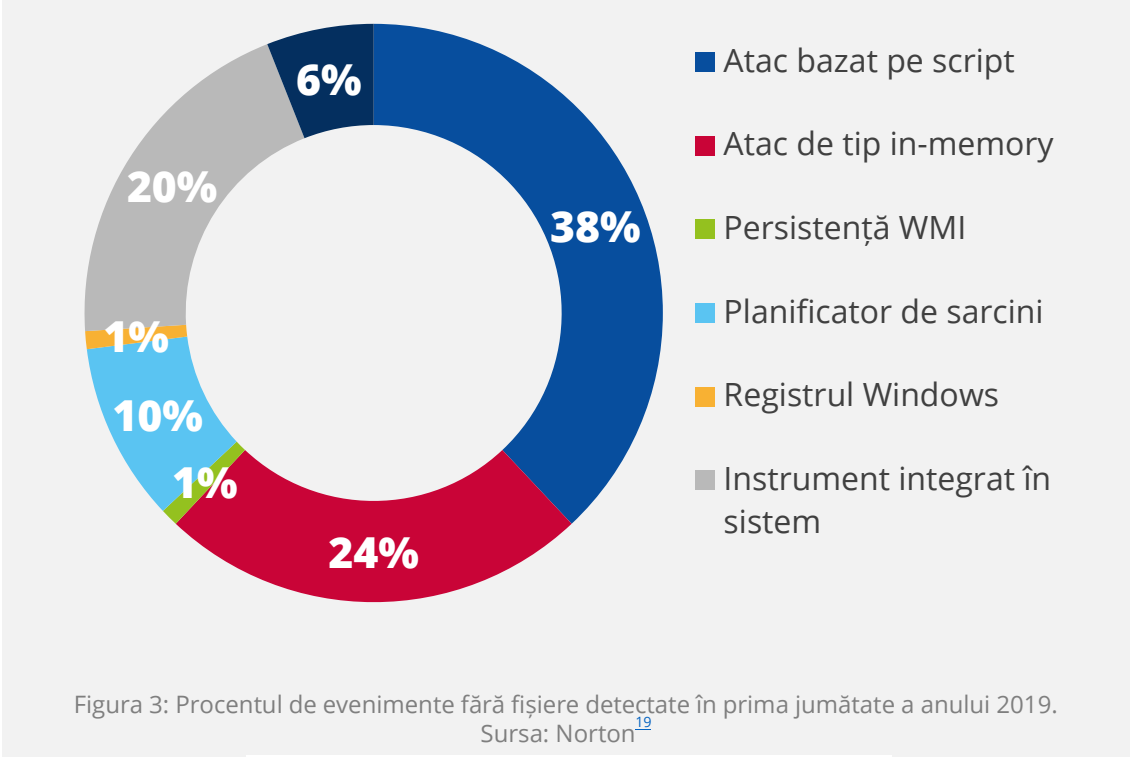


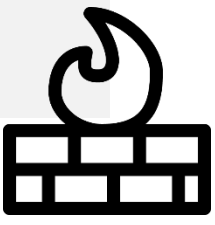
Figura 3: Procentul de evenimente fără fișiere detectate în prima jumătate a anului 2019. Sursa: Norton[19]

Cum să preveniți și să vă apărați de un atac fără fișiere?

Cel mai eficace mod în care organizațiile se pot apăra împotriva atacurilor fără fișiere este prin menținerea software-ului la zi. Deoarece majoritatea infectărilor fără fișiere apar în aplicațiile Microsoft și în special în fișierele „.docx”, este deosebit de important să se actualizeze în continuare acest software la cea mai recentă versiune. De asemenea, Microsoft și-a actualizat pachetul Windows Defender pentru a detecta activitatea neregulată folosind aplicația PowerShell.

Potrivit unui cercetător în domeniul securității[18], cheia contracarării cu succes a unei campanii de atac fără fișiere este tratarea fiecăreia dintre fazele ciclului de viață al amenințării cu o abordare de apărare integrată și la niveluri multiple. În această abordare, este important să se investigheze diferitele etape ale atacului și să se întreprindă următoarele activități:

- analizarea și măsurarea acțiunilor efectuate de atacator;
- identificarea tehnicilor utilizate;
- monitorizarea activităților din PowerShell sau alte motoare de scriptare;
- accesarea datelor agregate privind amenințările;
- controlarea stării sistemului vizat;
- oprirea proceselor arbitrare;
- remedierea proceselor care fac parte din atac;
- izolarea dispozitivelor infectate.



Situația botnet și comandă și control (C&C)

În general, traficul global de botnet a crescut cu 71,5 % din 2018[2]. Botnet-urile observate cel mai des au fost Emotet (41 %), Trickbot (25 %) și DanaBot (5 %)[2]. În Rusia s-a observat o creștere notabilă a traficului de botnet-uri (143 %), atribuită în principal procedurilor de înregistrare relaxate și interesului mai scăzut al agențiilor de aplicare a legii.[14] În cursul anului 2019, Rusia a găzduit majoritatea botnet-urilor C2, urmată de Statele Unite, Țările de Jos, China și Franța. Infractorii cibernetici au utilizat algoritmii de generare a numelui de domeniu (DGA) pentru a sprijini multe comunicări C2. 50 % din aceste înregistrări au avut loc în domenii de nivel superior (TLD) „.com” și „.net”. În perioada de raportare, astfel de înregistrări de nume de domeniu au scăzut cu 71 %, în favoarea altor protocoale de comunicare, cum ar fi peer-to-peer (P2P).[13]

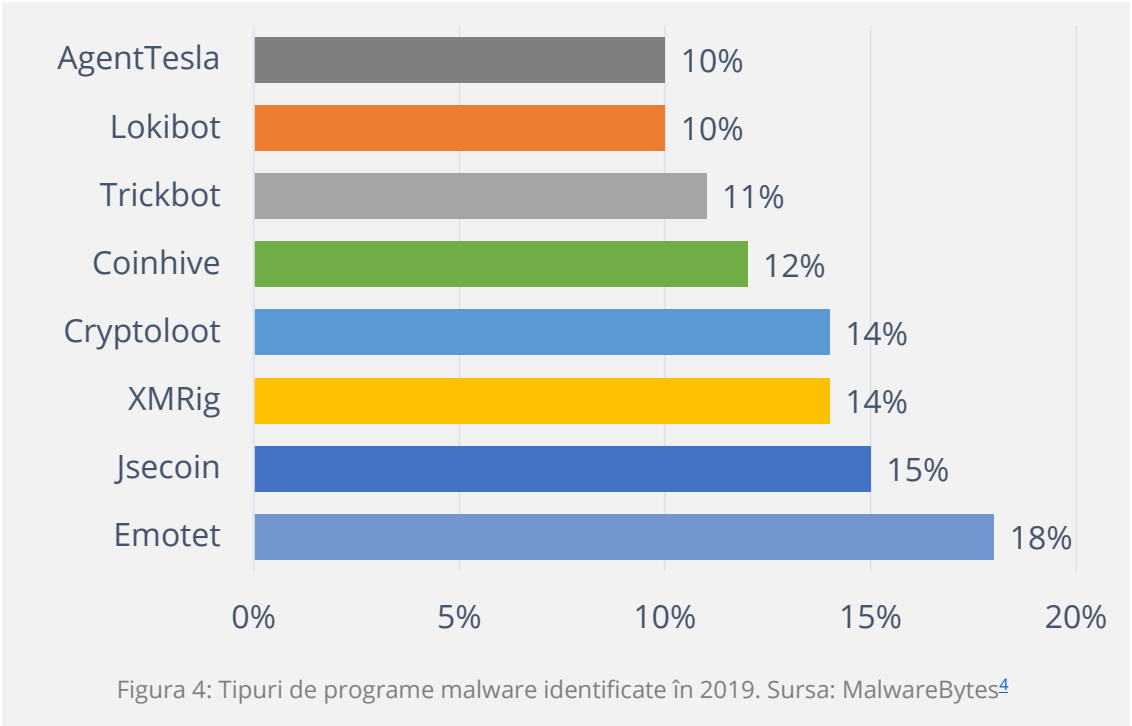


Figura 4: Tipuri de programe malware identificate în 2019. Sursa: MalwareBytes[4]

Cum

Potrivit unui studiu din 2019, 94 % din toate tipurile de malware au fost livrate prin e-mail.[24] Deși acesta este considerat un vector de punct de intrare, este interesant de observat că, după un atac reușit, malware-ul ar putea descărca o sarcină utilă suplimentară care prezintă un comportament asemănător cu viermii pentru a permite răspândirea laterală în rețea (Emotet și Trickbot). Mai mult, după livrarea inițială a programelor malware, în majoritatea cazurilor (71 %) acestea s-au răspândit prin activitatea angajaților. De asemenea, au atras atenția noi vulnerabilități din protocolul desktop la distanță (RDP), întrucât acestea permit executarea de cod la distanță (RCE) și, prin urmare, pot fi atacate de viermi (wormable).[30] Deși aceste vulnerabilități nou descoperite nu au fost exploatate la scară largă, este de așteptat ca un vierme nou să poată viza sisteme necorectate în viitorul apropiat.[31]

Incidente

- **Airbus** a suferit o încălcare a securității datelor care afectează angajații din Europa.[34, 35]
- Programele malware de furt de date de pe cardurile bancare (card skimming) instalate pe site-ul **Agenției americane de colectare a datoriilor medicale (American Medical Collection Agency – AMCA)** au dus la furtul a 12 milioane de date cu caracter personal ale pacienților.[36]
- Furnizorul principal de diagnostice de laborator **LifeLabs** a fost victima unui atac de ransomware, care a condus la furtul a 15 milioane de conturi conținând rezultatele testelor și numerele cardurilor de sănătate.[37,38]
- Un atac ransomware asupra **orașului Pensacola, Florida** a dus la punerea la dispoziție online a 2 GB de date, care conținea eventual informații personale identificabile (PII).[39]
- Datele cu caracter personal ale celor 2 400 de **angajați ai forțelor armate din Singapore** este posibil să fi fost divulgate prin phishing de e-mail prin programe malware rău intenționate.[40]

Măsuri de atenuare

Acțiuni propuse

- Aplicarea detectării programelor malware pentru toate canalele de intrare/ieșire, inclusiv e-mail, rețea, web și sisteme de aplicații pe toate platformele aplicabile (și anume, servere, infrastructură de rețea, computere personale și dispozitive mobile).
- Inspectarea traficului SSL/TLS, permițând firewall-ului să decripteze ceea ce este transmis către și de pe site-uri internet, comunicări prin e-mail și aplicații mobile.
- Stabilirea de interfețe între funcțiile de detectare a programelor malware (vânarea de amenințări bazate pe informații) și gestionarea incidentelor de securitate pentru a stabili capacități de răspuns eficiente.
- Utilizarea instrumentelor disponibile pentru analiza programelor malware pentru partajarea informațiilor malware și reducerea programelor malware (și anume MISP).[32]
- Elaborarea politicilor de securitate care specifică procesele care trebuie urmate în caz de infectare.
- Înțelegerea capacităților diferitelor instrumente de securitate și dezvoltarea de noi soluții de securitate. Identificarea lacunelor și aplicarea principiului apărării în profunzime (Defense-in-Depth).
- Utilizarea filtrării e-mailurilor (sau a filtrării spamului) pentru e-mailurile rău intenționate și eliminarea atașamentelor executabile.
- Monitorizarea periodică a rezultatelor testelor antivirus.[30,42]
- Monitorizarea jurnalelor utilizând soluția de gestionare a incidentelor și evenimentelor de securitate (SIEM). Sursele jurnalului de indicativi sunt alertele antivirus, detecție și răspuns pentru stațiile de lucru (EDR), jurnalele serverului proxy, jurnalele Windows Event și Sysmon[43], jurnalele sistemului de detectare a intruziunilor (IDS)[44], etc.
- Dezactivarea sau reducerea accesului la funcțiile PowerShell.[45]

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

în ETL 2020

Referințe

1. „What is Malware" (Ce este malware-ul). Veracode. https://www.veracode.com/security/malware

2. „Cyber Security Report" (Raport privind securitatea cibernetică). 2019. Checkpoint. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

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. „2020 State of Malware Report" (Raportul 2020 privind situația malware-ului). Februarie 2020. Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

5. „Evasive Threats,Pervasive Effects" (Amenințări evazive, efecte extinse), 2019. Trend Micro, Research. https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

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

7. „Emotet is back: botnet springs back to life with new spam campaign" (Emotet s-a întors: botnetul revine cu o nouă campanie de spam). 16 septembrie 2019. Malwarebytes Labs. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

8. „Increased Emotet Malware Activity" (Creșterea activității malware a Emotet), 22 ianuarie 2020. US CERT. https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity

9. „SonicWall Security Metrics" (Indici de cuantificare de securitate SonicWall), SonicWall. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

10. „Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection" (Peste o treime din atacurile cu malware care vizează operațiuni bancare din 2019 au vizat utilizatori corporativi, demonstrând necesitatea protecției). 16 aprilie 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

11. „Internet organised crime threat assessment" (Evaluarea amenințării pe care o reprezintă criminalitatea organizată online), 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

12. „Narrowed Sights, Bigger Payoffs: Ransomware in 2019" (Obiective mai mici, beneficii mai mari: ransomware în 2019), 6 iunie 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

13. „GOLDEN CHICKENS: Evolution of the MaaS" (GOLDEN CHICKENS: Evoluția MaaS). 20 iulie 2020. QuoIntelligence. https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/

14. „From Supply Chain to Email, Mobile and the Cloud" (De la lanțul de aprovizionare la e-mail, mobil și cloud), 25 iulie 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

15. „Mobile malware evolution 2019" (Evoluția malware-ului mobil în 2019). 25 februarie 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

16. „Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics" (Aplicații Google Play livrează programul malware care vizează operațiuni bancare, Anubis, care utilizează tactici de eludare bazate pe mișcare). 17 ianuarie 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

17. „Spamhaus Botnet Threat Report 2019" (Raportul Spamhaus privind amenințările Botnet în 2019). 28 ianuarie 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

18. „What Is Fileless Malware?" (Ce este malware-ul fără fișiere?). McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

19. „What is fileless malware and how does it work?" (Ce este malware-ul fără fișiere și cum funcționează?) . Norton. https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html

20. „Trend Micro Report Reveals 265% Growth In Fileless Events" (Raportul Trend Micro evidențiază o creștere de 265 % în evenimente fără fișiere). 28 august 2019. Trend Micro. https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2019/2019-08-28.html

21. „Understanding Fileless Threats" (Înțelegerea amenințărilor fără fișiere), 29 iulie 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats

22. „SonicWall Sees Dramatic Jump In IoT Malware, Encrypted Threats, Web App Attacks Through Third Quarter" (SonicWall constată un salt dramatic în malware-ul IoT, amenințări criptate, atacuri asupra aplicațiilor web până în al treilea trimestru). 22 octombrie 2019. SonicWall. https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/

23. „2020 Vulnerability and Threat Trends" (Tendințele din 2020 în ceea ce privește vulnerabilitățile și amenințările). 2020. SKYBOX. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020_VT_Trends-Report-reduced.pdf

24. „Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection" (Peste o treime din atacurile cu malware care vizează operațiuni bancare din 2019 au vizat utilizatori corporativi – demonstrând necesitatea protecției). 16 aprilie 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

25. „Internet organised crime threat assessment" (Evaluarea amenințării pe care o reprezintă criminalitatea organizată online), 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

26. „Narrowed Sights, Bigger Payoffs: Ransomware in 2019" (Obiective mai mici, beneficii mai mari: ransomware în 2019), 6 iunie 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

27. „From Supply Chain to Email, Mobile and the Cloud" (De la lanțul de aprovizionare la e-mail, mobil și cloud), 25 iulie 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

28. „Mobile malware evolution 2019" (Evoluția malware-ului mobil în 2019). 25 februarie 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

29. „Mobile banking malware surges in 2019" (Creștere bruscă a numărului de programe malware care vizează operațiuni bancare prin telefonul mobil în 2019). 25 iulie 2019. Computer Weekly. https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

30. „Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics" (Aplicații Google Play livrează programul malware care vizează operațiuni bancare, Anubis, care utilizează tactici de eludare bazate pe mișcare). 17 ianuarie 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

31. „BlueKeep attacks are happening, but it's not a worm" (Au loc atacuri BlueKeep, dar nu este un vierme). 3 noiembrie 2019. ZDNet. https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/

32. Proiecte MISP. http://www.misp-project.org/

33. „PowerShell, fileless malware's great attack vector" (PowerShell, marele vector de atac al programelor malware fără fișiere). 25 februarie 2019. Panda. https://www.pandasecurity.com/mediacenter/malware/powershell-fileless-malware-attack-vector/

34. „Airbus Statement on Cyber Incident" (Declarația Airbus privind incidentul cibernetic). 30 ianuarie 2019. Airbus. https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html

35. „Airbus data breach impacts employees in Europe" (Încălcarea securității datelor de la Airbus afectează angajații din Europa), 30 ianuarie 2019. ZDNet. https://www.zdnet.com/article/airbus-data-breach-impacts-employees-in-europe/

36. „Massive Quest Diagnostics data breach impacts 12 million patients" (Încălcarea masivă a securității datelor de la Quest Diagnostics afectează 12 milioane de pacienți). 4 iunie 2019. ZDNet. https://www.zdnet.com/article/massive-quest-diagnostics-data-breach-impacts-12-million-patients/

37. „Hackers crack 15M LifeLabs accounts, obtain lab results and health card numbers" (Hackerii sparg 15 milioane de conturi LifeLabs, obțin rezultate de laborator și numere de carduri de sănătate). 17 decembrie 2019. Daily Hive. https://dailyhive.com/calgary/lifelabs-hacked-cyber-attack

38. „Why the LifeLabs Hack Likely Is Worse than Most" (De ce este probabil ca atacul cibernetic de la LifeLabs să fie mai rău decât majoritatea). 18 decembrie 2019. The Tyee. https://thetyee.ca/Analysis/2019/12/18/LifeLabs-Data-Hack/

39. „Personal Information in City of Pensacola Cyberattack" (Informații cu caracter personal în atacul cibernetic asupra orașului Pensacola). 17 ianuarie 2020. City of Pensacola. https://www.cityofpensacola.com/CivicSend/ViewMessage/Message/100944

40. „Personal data of 2,400 Mindef, SAF staff may have been leaked" (Este posibil ca datele personale ale 2 400 de angajați ai Mindef, SAF să fi fost divulgate), 22 decembrie 2019. The Straits Times - Singapore. https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

Referințe

41. AVTEST – The Independent IT-Security Institute (AVTEST – Institutul independent de securitate IT). https://www.av-test.org/en/

42. „Real world protection tests" (Teste de protecție în lumea reală). AV Comparatives. https://www.av-comparatives.org/dynamic-tests/

43. „The ThreatHunting Project" (Proiectul ThreatHunting). https://www.threathunting.net/data-index

44. Mark Russinovich, Thomas Garnier. "Sysmon v11.10." 24 iunie 2020. Microsoft. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

45. „Guide to Intrusion Detection and Prevention Systems (IDPS)" [Ghid pentru sistemele de detecție și prevenire a intruziunilor (Intrusion Detection and Prevention Systems – IDPS)]. Februarie 2007. CSRC. https://csrc.nist.gov/publications/detail/sp/800-94/final

47. „Most malware in Q1 2020 was delivered via encrypted HTTPS connections" (Cele mai multe programe malware din T1 2020 au fost livrate prin conexiuni HTTPS criptate). 25 iunie 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

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

„Situația amenințărilor devine extrem de dificil de cartografiat. Atacatorii nu numai că dezvoltă noi tehnici pentru a eluda sistemele de securitate, dar amenințările cresc în complexitate și precizie în atacurile țintite.”

în ETL 2020

Documente conexe

CITIȚI RAPORTUL

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

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 trebui 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