RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ianuarie 2019 – aprilie 2020

Furtul de identitate

Raportul ENISA privind peisajul amenințărilor

Prezentare generală

Furtul de identitate sau frauda de identitate este utilizarea ilicită a informațiilor personale identificabile (PII) ale victimei de către un impostor pentru a face uz de identitatea acelei persoane și a obține un avantaj financiar și alte beneficii.

Potrivit unui raport anual de securitate, au fost depistate cel puțin 900 de cazuri internaționale de furt de identitate sau infracțiuni legate de identitate.[1] Cele mai semnificative incidente raportate au fost:

- expunerea informațiilor cu caracter personal a aproape 106 milioane de clienți ai băncilor americane și canadiene în urma incidentului de încălcare a securității datelor la Capital One din martie 2019;[2]
- expunerea a 170 de milioane de nume de utilizator și parole utilizate de dezvoltatorul de jocuri digitale Zynga în septembrie 2019;
- furtul a 20 de milioane de conturi de la serviciul britanic de streaming audio Mixcloud;[3]
- compromiterea informațiilor cu caracter personal a 600 000 de șoferi și 57 de milioane de utilizatori din incidentul de încălcare a securității datelor la Uber din noiembrie 2019;[3]
- și furtul a 9 milioane de date personale de la clienții EasyJet, inclusiv cărți de identitate și carduri de credit.

Tendința furtului de identitate se reflectă într-o mare măsură în încălcările securității datelor, care, comparativ cu 2018, au înregistrat un număr record de 3 800 de cazuri divulgate public, 4,1 miliarde de înregistrări expuse și o creștere cu 54 % a numărului de încălcări ale securității datelor raportate.[4]

Constatări

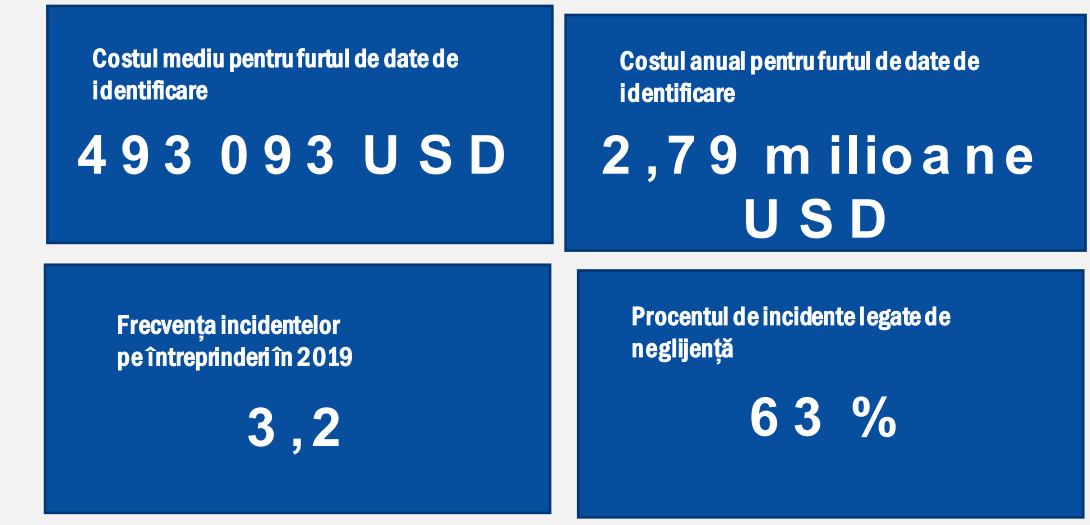
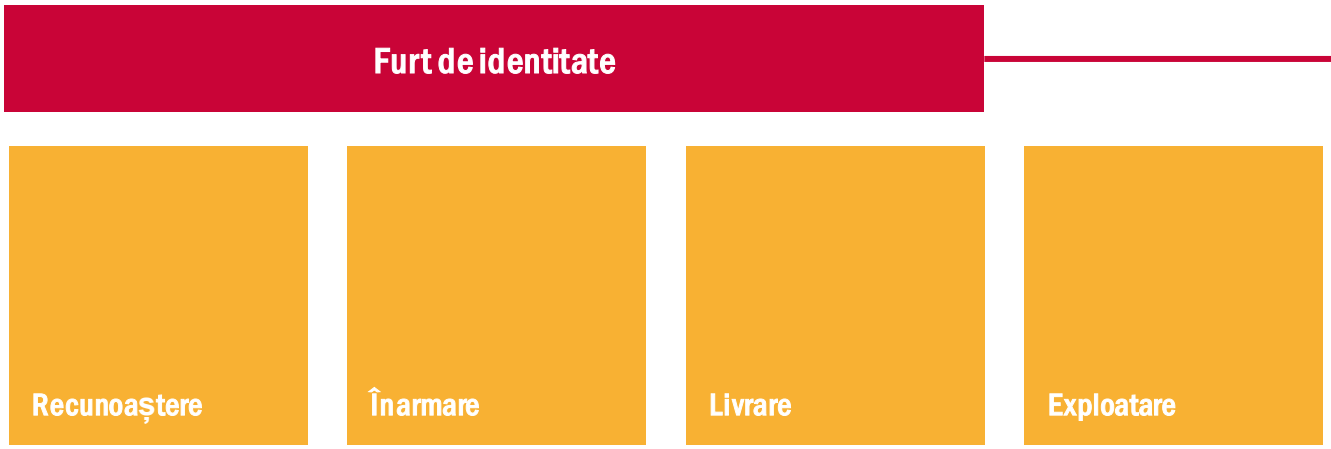


Figura 1: Sursa: Dintr-un studiu de securitate IBM – Costul amenințărilor din interior: Raport global[13]

Amenințarea reprezentată de furtul de identitate

În 2019, unii actori rău intenționați din spatele unor incidente majore din ultimii ani au fost aduși în fața justiției. În iunie, Departamentul de Poliție din New York, în colaborare cu FBI, i-a adus în fața justiției pe membrii grupului „Fraud Ring", care au operat în interiorul și în afara Statelor Unite și au reușit în 2012 să fure date de identificare de pe dispozitive iPhone în valoare de 1 milion USD (aproximativ 846 000 EUR) într-o operațiune de furt de identitate pe scară largă. Până la momentul în care grupul a fost oprit, suma totală furată a ajuns la 19 milioane USD (aproximativ 16 milioane EUR).[4] O lună mai târziu, s-a anunțat public „acordul Equifax".5 Equifax a fost obligată să accepte să despăgubească FTC (Comisia Federală pentru Comerț a Statelor Unite), CFPB (Biroul pentru protecția financiară a consumatorilor), 48 de state, Districtul Columbia și Puerto Rico pentru încălcarea securității datelor sale din 2017 într-un cuantum de cel puțin 575 de milioane USD (aproximativ 487 de milioane EUR). Din cauza acestei încălcări a securității datelor, despre care s-a considerat că „ar fi putut fi în întregime prevenită", au fost divulgate aproape 148 de milioane de adrese și numere de securitate socială din SUA. La sfârșitul anului, Brazilia a amendat Facebook cu 1,6 milioane USD (aproximativ 1,35 milioane EUR) în numele cetățenilor brazilieni pentru scurgerea de date de la Cambridge Analytica.[3]

Kill chain



Etapa fluxului 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

Atacuri de imitare a mărcii

În concordanță cu tendința din 2018, anumite mărci sunt preferate în atacurile de imitare datorită reputației lor puternice. Deși aceste mărci – cum ar fi Microsoft (44 %) și Amazon (17 %) – continuă să conducă în clasamentul atacurilor de imitare a mărcii din 2019, sunt notabile noi intrări în top precum Agenția de Administrare Fiscală a Statelor Unite (Internal Revenue Service – IRS).[7] Informațiile sensibile incluse în Declarația privind salariile și impozitele (W-2) au fost întotdeauna atrăgătoare pentru impostori, care au făcut uz de identitatea IRS în 10 % din e-mailurile bazate pe înșelăciune cu privire la identitate în acest an de raportare. Drept urmare, formularele W-2 valide și formularele standard de declarație fiscală individuală din SUA (1040) sunt disponibile pe dark web și costă între 1 și 52 USD.

Acest material, combinat cu numerele de asigurare socială (Social Security Number – SSN) și datele de naștere, care sunt, de asemenea, disponibile, permite oricărui hacker fără experiență care dorește să investească o sumă de 1 000 USD (aproximativ 846 EUR) să acceseze în mod legal un cont bancar din Statele Unite pentru a depune o declarație fiscală falsă, a solicita o rambursare și a retrage o investiție care s-a dublat sau triplat. Conform anchetei penale a IRS, peste 10 000 de declarații fiscale individuale cu cereri de rambursare de peste 83 de milioane USD (aproximativ 70 de milioane EUR) au fost potențial frauduloase.[9]

Ciclul etapelor pentru escrocheria fiscală „Dirty Dozen”

Figura 2 - Sursa: BDO[19]

Tendințe

_Identități de schimb de SIM

Această tehnică a fost utilizată din 2016, vizând deținătorii de criptomonede. Cu toate acestea, în 2019, aceeași tehnică a fost utilizată împotriva persoanelor sau conturilor cu vizibilitate mare, cu intenția de a fura identitatea victimei. Au fost înregistrate o serie de victime ale schimbului de SIM, cum ar fi Jack Dorsey (CEO Twitter), Jessica Alba (actriță), Shane Dawson (actor), Amanda Cerny (actriță, de două ori victimă), Matthew Smith (actor, de patru ori victimă) și King Bach (artist).[10] De asemenea, schimbul de SIM a fost utilizat în mod considerabil în două cazuri; la cea mai mare bancă din Mozambic, de unde s-au furat până la 50 000 USD (aproximativ 42 300 EUR) din conturi ale întreprinderilor de profil înalt, precum și în Brazilia unde conturile a 5 000 de victime, în principal politicieni, miniștri și guvernatori, au fost piratate de un grup infracțional organizat.[11]

_Carduri cadou folosite ca troian de compromitere a e-mailului de afaceri (BEC)

Atacurile BEC au provocat pierderi de miliarde de euro în 2019. În astfel de incidente, atacatorii fac uz de identitatea unei persoane de încredere, de regulă din cadrul întreprinderii, iar victima este păcălită să facă o tranzacție financiară sau să divulge informații sensibile, cu caracter personal sau corporative. În mai mult de jumătate din atacurile BEC, victima a fost ademenită să cumpere un card cadou. În timpul procesului de cumpărare, au fost interceptate informații sensibile, cum ar fi datele de identificare ale contului bancar. De asemenea, victima a fost obligată să trimită cardul cadou atacatorului, ca opțiune de retragere anonimă, ireversibilă și directă. Suma medie furată per card cadou a ajuns la 1 500 USD (aproximativ 1 269 EUR).[12]

Constatări

20 %_ **din atacurile de înșelăciune cu privire la identitate au folosit conturi compromise**[7]

30 %_ **din atacurile care vizau conturile executivilor de nivel C au fost compromise folosind înșelăciunea cu privire la numele afișat**[7]

65 %_ **din atacurile BEC au atras victimele să cumpere carduri cadou**[12]

3,32 EUR_ **milioane costul mediu al unei încălcări a securității datelor**

95 %_ **din participanții la un sondaj Eurobarometru au considerat că furtul de identitate este o infracțiune gravă**

Doppelgangeri digitali

Tehnica antifraudă „măști digitale” a fost expusă atunci când mai mult de 60 000 de identități digitale furate au apărut ca produs de tranzacționare pe piața darknet Genesis în aprilie 2019. Acești doppelgangeri erau ușor de cumpărat la un preț de 5-200 USD fiecare. Proprietarul unui doppelganger poate imita mai ușor un utilizator real într-un magazin online sau un serviciu de plată, mai ales dacă acest lucru este combinat cu autentificări și parole furate. În afară de achiziționarea de doppelgangeri digitali, au apărut noi instrumente pentru a ajuta potențialul imitator, cum ar fi browserul Tenebris, care încorporează un generator ce permite dezvoltarea de amprente și măști digitale unice.[11]

În ultimii ani, skimmerii, căutătorii în coșurile de gunoi, hackerii, imitatorii de administratori și phisherii au fost identificați drept principalele grupuri din spatele atacurilor de furt de identitate. Această listă s-a extins în 2019 odată cu adăugarea de visheri și smisheri. Visherii înșeală prin apeluri telefonice. Spre deosebire de imitatorii de la telefon, visherii pretind că reprezintă o organizație bine-cunoscută și oferă asistență victimei cu un serviciu, de exemplu gestionarea de software de calculator, finanțe sau o rambursare a impozitului. Smisherii trimit mesaje SMS false și, dacă destinatarul răspunde, dispozitivul său este deturnat direct sau redirecționat către un site web de phishing.

Figura de mai jos prezintă principalele tipuri de date pierdute în 2019, unde datele de e-mail reprezintă cel mai mare număr de date pierdute sau furate. Aceste cifre relevă gravitatea situației atunci când se consideră că e-mailurile pot conține informații sensibile cu caracter personal, corporative și guvernamentale.

Cele mai importante tipuri de date pierdute în 2019

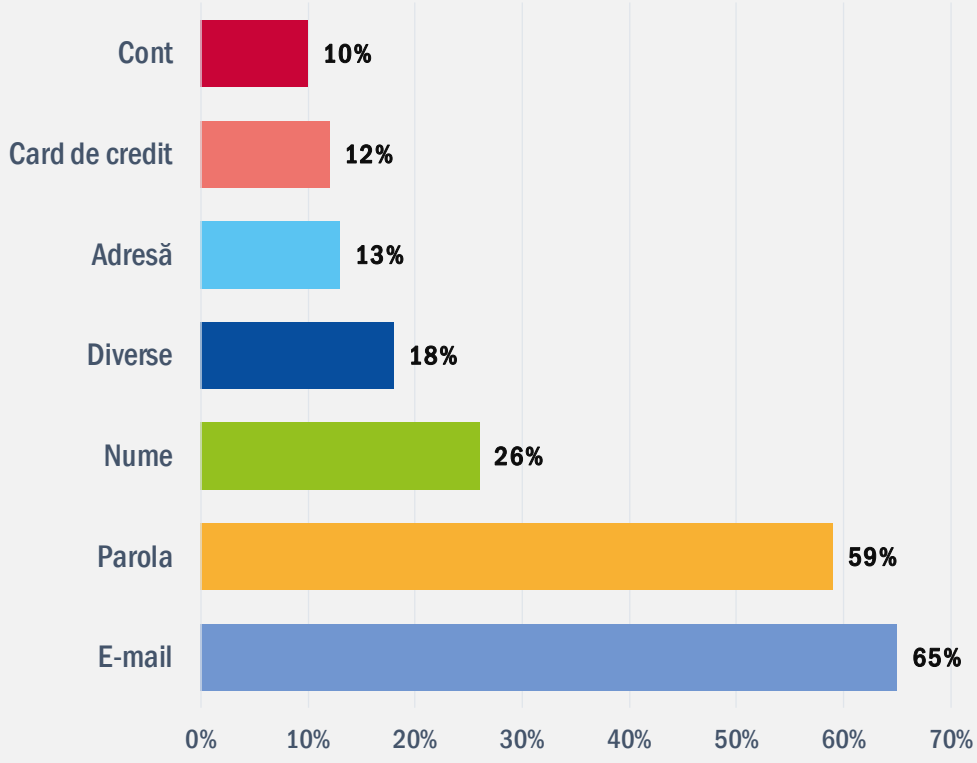


Figura 3 - Sursa: RiskBased SECURITY[8]

Vectori de atac

Modalitate

- **CLOUD CA INTERFAȚĂ DE ATAC PENTRU DATELE CLIENȚILOR**. În anul de raportare, o rețea de livrare de conținut (CDN), Amazon CloudFront a fost compromisă.[14] Site-urile web găzduite sau legate de bibliotecile de pe infrastructura Amazon au fost expuse, dezvăluind conținut încărcat la nivel extern, inclusiv date referitoare la cardul de credit.
- **URL PHISHING**. Tehnicile comune de URL-uri malware[16] de ocupare ilegală a unui domeniu (domain squatting), de stabilire a unui domeniu paralel (domain shadowing) și scurtături de URL-uri (URL shorteners) au fost utilizate din nou în 2019. În ultimul trimestru al anului 2019, s-a observat că 26 % din domeniile rău intenționate foloseau un certificat securizat și unul din trei astfel de certificate era SSL. Acest truc a profitat de încrederea vizitatorilor, care obișnuiau să se bazeze pe pictograma lacăt din browserele lor ca semn de securitate.[15]
- **Înșelătoria W2**. Un alt atac care vizează datele întreprinderilor și organizațiilor pentru a accesa informații sensibile este înșelătoria W2. Înșelătoria începe prin falsificarea adresei de retur (spoofing) a unui membru executiv al departamentului de finanțe sau de resurse umane pentru a obține datele angajaților. Aceste înregistrări sunt utilizate apoi pentru furtul de identitate. Înșelătoria este numită după formularul de impozitare american W2 utilizat pentru raportarea salariilor angajaților. Această înșelătorie de inginerie socială, deși veche (raportată pentru prima dată în 2016 de IRS), a crescut constant cu 10 % în fiecare an în ultimii ani.[9,17]
- **NIMCY**. În 2019, un instrument de spear-phishing, Nimcy, a fost introdus de grupul responsabil pentru familia de malware Zebrocy. Acesta a fost dezvoltat folosind limbajul de programare Nim (fost Nimrod), creat de același grup de hackeri. Acest nou program de descărcare și backdoor a fost folosit pentru a fura date de identificare de conectare, apăsări de taste, comunicări și fișiere de la diplomați, oficiali ai apărării și personalul ministerului din sectorul afacerilor externe. Atacatorii păreau să se concentreze asupra guvernelor din Asia Centrală, cu o preferință pentru Pakistan și India.[14]

- **AMENINȚĂRI PE MOBIL.** În 2019 a fost observată o creștere a aplicațiilor mobile rău-intenționate, iar aceasta a continuat în 2020. Chiar și platforme de încredere și utilizate pe scară largă, cum ar fi Google Play, găzduiau aplicații cu scopul de a fura date de identificare (de exemplu, Acesse SantaMobile, ID Modulo). Cu toate acestea, numărul de descărcări a fost extrem de redus, ceea ce arată că potențialele victime nu au fost păcălite.[20]
- **TROJAN-BANKER.ANDROIDOS.SVPENG.AK** Al optulea cel mai popular troian mobil și cel mai popular troian bancar mobil, responsabil de 1,75 % și, respectiv, 16,85 % din atacurile unice, vizează în principal credențialele bancare ale victimelor și codurile de autorizare cu doi factori. Majoritatea victimelor acestui troian se află în Rusia, care devine astfel țara de top în ceea ce privește ponderea utilizatorilor atacați de troieni bancari mobili.[21]
- **FORMJACKING**. Formjacking-ul a fost extrem de frecvent în 2018, dar numărul atacurilor pare să scadă considerabil în primul trimestru al anului 2019. Cu toate acestea, începând din luna mai, cu atacul unui furnizor american de asistență medicală și cu furtul datelor de identificare pentru conectare, numărul atacurilor a continuat să crească pe parcursul anului. În luna respectivă a fost înregistrat un număr record de 1,1 milioane de detectări. Cele cinci țări cu cele mai multe detectări de formjacking în 2019 au fost Statele Unite (51,8 %), Australia (8,1 %), India (5,7 %), Regatul Unit (4,1 %) și Brazilia (3,5 %). Grupul de hackeri Megacart are legături puternice cu cea mai mare parte a dezvoltării de instrumente de formjacking și cu atacurile asupra British Airways, Newegg, Feedify și Ticketmaster.[22]

Măsuri de atenuare

Acțiuni propuse

- Evitați să utilizați managerul de parole furnizat de browser. Dacă este necesar unul, utilizați un manager de parole protejat offline.[23]
- Verificați identitatea oricărui expeditor al unei cereri de transfer de bani prin telefon sau personal.[19]
- Nu comunicați informații sensibile, cum ar fi fișele pacienților, în note scrise de mână, pentru a preveni pierderea sau rătăcirea acestora. Fișierele digitale sunt mai bune pentru datele cu o durată scurtă de viață, iar ulterior acestea ar trebui să fie distruse complet.
- Utilizați „vânarea de amenințări" în cadrul întreprinderii dvs. pentru a consolida planurile de securitate. Vânarea de amenințări este desfășurată de membri calificați ai echipei centrului de operațiuni de securitate (security operation centre – SOC) pentru a identifica proactiv vulnerabilitățile și a preveni amenințările care le exploatează.
- Utilizați politici precum reguli bazate pe viteză pentru a atenua frauda de identitate, în special pentru tranzacțiile cu cardul de plată. Datele automatizate ale tranzacțiilor valide pot furniza suficiente informații pentru definirea optimă a politicii.
- Utilizați metoda de autentificare single-sign-on (SSO), atunci când este disponibilă, aceasta permițând unui utilizator să acceseze mai multe aplicații cu același set de date de identificare digitale. Utilizarea acesteia este foarte recomandată pentru a minimiza numărul de conturi de utilizator și datele de identificare stocate.
- Instalați protecția punctului final prin intermediul programelor antivirus, dar blocați, de asemenea, executarea corectă a fișierelor (de exemplu, blocați execuția în folderul temp).
- Autentificarea cu mai mulți factori este o măsură de securitate pentru a combate piratarea sau pierderea parolelor și pentru a asigura succesul procesului de autentificare cu mai multe chei. Introducerea autentificării adaptive cu mai mulți factori optimizează procesul de autentificare pe baza comportamentului utilizatorului și a contextului asociat.

- Verificați URL-urile care sunt trimise prin e-mail sau vizitate aleatoriu pe baza adresei IP, a ASN-ului asociat IP-ului, a proprietarului domeniului și a relației dintre acest domeniu și altele, înainte de a lua măsuri suplimentare.
- Organizațiile care utilizează servicii cloud ar trebui să aibă operațiuni puternice de securitate cloud și, de preferință, să utilizeze simultan o arhitectură de stocare locală, stocare privată în cloud și stocare publică în cloud pentru a proteja informațiile cu caracter personal ale clienților lor.
- Impuneți utilizarea unor metode de criptare puternice și actualizate, cum ar fi TLS 1.3 (folosind chei efemere) pentru date sensibile, pentru a preveni pirateria.
- Protejați în mod adecvat toate documentele de identitate și copiile (fizice sau digitale) împotriva accesului neautorizat.
- Nu dezvăluiți informațiile de identitate destinatarilor nesolicitați și nu trebuie să răspundeți solicitărilor prin telefon sau e-mail sau personal.
- Impuneți utilizarea dispozitivelor protejate prin parolă, asigurând o bună calitate a datelor de identificare, precum și metode sigure pentru stocarea acestora.
- Asigurați o bună calitate a datelor de identificare și metode sigure pentru stocarea acestora pe toate mediile utilizate.
- Acordați o atenție deosebită atunci când utilizați rețele Wi-Fi publice, întrucât fraudatorii le piratează sau le imită. Dacă folosiți o astfel de rețea, evitați accesul la aplicații și date sensibile. Folosiți un serviciu VPN de încredere pentru a vă conecta la rețelele Wi-Fi publice.
- Verificați în mod regulat orice nereguli în desfășurarea tranzacțiilor documentate prin extrasele bancare sau chitanțele primite.
- Instalați filtrarea conținutului pentru a filtra atașamentele nedorite, mesajele cu conținut rău intenționat, spamul și traficul de rețea nedorit.
- Impuneți utilizarea soluțiilor de prevenire a pierderii de date (Data Loss Prevention – DLP).

Referințe

1. „2019 identity theft report released" (A fost publicat raportul privind furtul de identitate din 2019), 31 iulie 2019. ITJ. https://www.itij.com/latest/news/2019-identity-theft-report-released

2. „Capital One data breach: What you can do now following bank hack" (Încălcarea securității datelor la Capital One: ce puteți face acum după un atac informatic asupra băncii), 12 august 2019. C|Net. https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/

3. „Cybercrime Diary, Vol. 4, No. 4: Who's Hacked? Latest Data Breaches And Cyberattacks" (Jurnalul criminalității cibernetice, vol. 4, nr. 4: Cine este piratat? Ultimele încălcări ale securității datelor și atacuri cibernetice). 8 ianuarie 2020. Cyber crime Magazine. https://cybersecurityventures.com/cybercrime-diary-q1-2020-whos-hacked-latest-data-breaches-and-cyberattacks/

4 „$19 million worth of iPhones stolen in massive identity theft scam" (IPhone-uri în valoare de 19 milioane USD furate într-o înșelătorie masivă de furt de identitate), 15 iunie 2019. 9To5Mac. https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/

5. „Equifax to pay at least $575 million as part of FTC settlement" (Equifax va plăti cel puțin 575 milioane USD ca parte a acordului FTC), 22 iulie 2019. C|Net. https://www.cnet.com/news/equifax-to-pay-at-least-575m-as-part-of-ftc-settlement/

6. „2019 data breaches: 4 billion records breached so far" (Încălcări ale securității datelor din 2019: până acum s-a încălcat securitatea a 4 miliarde de înregistrări), Norton. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

7. „Q1 2019: Email Fraud and Identity Deception Trends" (T1 2019: tendințe în materie de fraudă prin e-mail și înșelăciune de identitate), Agari. https://www.agari.com/insights/ebooks/2019-q1-report/

8. „Data Breach QuickView Report, 2019 Q3 trends" (Raportul QuickView privind încălcarea securității datelor, tendințe în T3 2019) Noiembrie 2019. RiskBased SECURITY. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf

9. „IRS issues 2019 annual report; highlights program areas across the agency" (IRS emite raportul anual 2019; evidențiază domeniile programului din întreaga agenție), 6 ianuarie 2020. IRS. https://www.irs.gov/newsroom/irs-issues-2019-annual-report-highlights-program-areas-across-the-agency

10. „Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too" (Hackerii au vizat directorul general al Twitter Jack Dorsey într-un atac tip „SIM Swap." Și tu ești în pericol), 5 septembrie 2019. The New York Times. https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

11. „IT threat evolution Q2 2019" (Evoluția amenințărilor informatice în T2 2019), 19 august 2019. Kaspersky. https://securelist.com/it-threat-evolution-q2-2019/91994/

12. „Phishing Activity Trends Report" (Raport privind tendințele activității de phishing), 12 septembrie 2019. Grupul de lucru anti-phishing. https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf

13. „The Cost of Insider Threats" (Costul amenințărilor din interior), IBM. https://www.ibm.com/downloads/cas/LQZ4RONE

14. „APT trends report Q2 2019" (Raportul APT privind tendințele în T2 2019), 1 august 2019. Kaspersky. https://securelist.com/apt-trends-report-q2-2019/91897/

15. „Proof Point Q3 2019 threat report: Emotets return, rats reign supreme and more" (Raportul Proof Point privind amenințările din T3 2019: Emotet se întorc, RAT dețin supremația și altele), Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

16. ENISA Threat Landscape Report 2018 (Raportul ENISA privind situația amenințărilor în 2018). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

17. „Q2 2019 Cryptocurrency Anti-Money Laundering Report" (Raportul privind combaterea spălării banilor în T2 2019), Cipher Trace. https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

18. „Latest Quarterly Threat Report - Q1 2019" (Ultimul raport trimestrial privind amenințările – T1 2019), Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

19. „BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare" (Raportul BDO din toamna anului 2019 privind amenințările cibernetice: accentul pe asistență medicală), octombrie 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

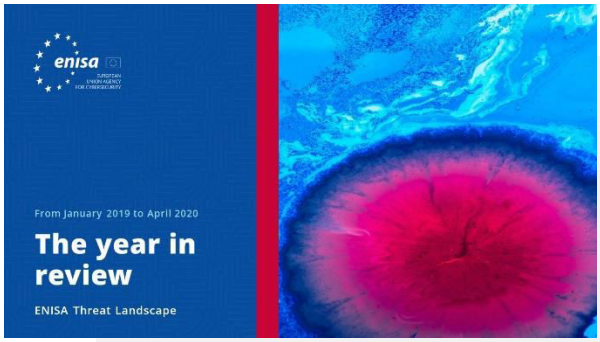
20. „IT threat evolution Q1 2019. Statistics" (Evoluția amenințărilor IT în T1 2019. Statistici), 23 mai 2019. Kaspersky. https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

21. „IT threat evolution Q3 2019. Statistics" (Evoluția amenințărilor IT în T3 2019. Statistici), 29 noiembrie 2019. Kaspersky. https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

22. „FORMJACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month" (Modul în care codul JavaScript rău intenționat fură date ale utilizatorilor de pe mii de site-uri internet în fiecare lună), august 2019. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-formjacking-deep-dive-en.pdf

23. „Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web" (Frauda fiscală și „Furtul de identitate la cerere" continuă să prindă contur pe Dark Web), VMWare. https://www.carbonblack.com/resources/threat-research/tax-fraud-identity-theft-dark-web/

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

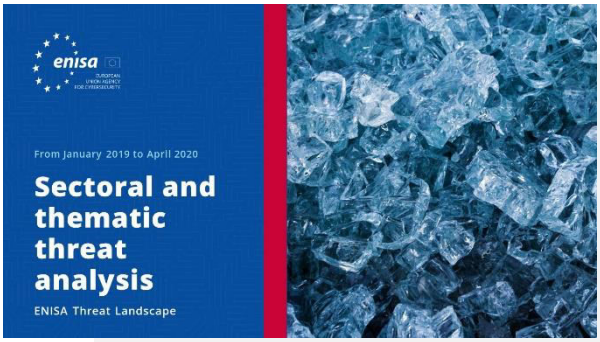
Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

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 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 sunt disponibile la adresa www.enisa.europa.eu.

Contribuitori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) și *toți membrii Grupului părților interesate al ENISA CTI:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) și Thomas Hemker.

Editori

Marco Barros Lourenço (ENISA) și Louis Marinos (ENISA).

Date de contact

Pentru întrebări despre această lucrare, vă rugăm să utilizați adresa enisa.threat.information@enisa.europa.eu.

Pentru întrebări din partea mass-media despre această lucrare, vă rugăm să utilizați adresa press@enisa.europa.eu.

Dorim să aflăm părerea dumneavoastră despre acest raport!
Vă rugăm să acordați câteva momente completării chestionarului. Pentru a accesa formularul, faceți clic aici.

Aviz juridic

Trebuie luat în considerare faptul că această publicație reprezintă punctele de vedere și interpretările ENISA, cu excepția cazului în care se prevede altfel. Această publicație nu trebuie interpretată ca o acțiune juridică a ENISA sau a organismelor ENISA, cu excepția cazului în care aceasta a fost adoptată în conformitate cu Regulamentul (UE) nr. 526/2013. Această publicație nu reprezintă neapărat stadiul actual al tehnologiei și ENISA o poate actualiza periodic.

Sursele terțe sunt citate corespunzător. ENISA nu este responsabilă pentru conținutul surselor externe, inclusiv al site-urilor externe menționate în această publicație.

Această publicație are doar scop informativ și trebuie să fie accesibilă în mod gratuit. Nici ENISA și nici persoanele care acționează în numele său nu sunt responsabile pentru modul în care ar putea fi utilizate informațiile conținute în această publicație.

ISBN: 978-92-9204-354-4

DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia

Telefon: +30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu