RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ianuarie 2019 – aprilie 2020

Phishing

Raportul ENISA privind situația amenințărilor

Prezentare generală

Phishing-ul este încercarea frauduloasă de a fura date ale utilizatorilor, cum ar fi date de conectare, informații despre cardul de credit sau chiar bani, folosind tehnici de inginerie socială. **Acest tip de atac este lansat de regulă prin mesaje de e-mail, care par a fi trimise dintr-o sursă de încredere, cu intenția de a convinge utilizatorul să deschidă un atașament rău intenționat sau să urmeze un URL fraudulos**. O formă țintită de phishing numită „spear phishing" se bazează pe cercetarea anticipată a victimelor, a șadar escrocheria pare mai autentică, făcându-l astfel unul dintre cele mai reușite tipuri de atac asupra rețelelor întreprinderilor.[1]

Un răspuns emoțional justifică acțiunile multor oameni atunci când sunt vizați de phishing și este exact ceea ce caută hackerii. Într-un context de instruire, acesta este scenariul pe care trebui să îl testeze o simulare de phishing. Instruirea utilizatorilor de e-mail este una dintre măsurile utilizate adesea pentru prevenirea phishing-ului, dar rezultatele nu sunt convingătoare deoarece factorii de amenințare își schimbă în mod constant modul de operare. Standardul de autentificare, raportare și conformare a mesajelor bazate pe domenii (domain-based message authentication, reporting, and conformance – DMARC) asigură blocarea e-mailurilor de pe domenii frauduloase, diminuând rata de succes a atacurilor de phishing, spoofing și spam[↗].

În viitor, e-mailul continuă să fie mecanismul numărul unu pentru phishing, dar nu pentru mult timp. Constatăm deja o creștere a utilizării mesajelor pe rețelele sociale, WhatsApp și altele pentru a desfășura atacuri. Cea mai relevantă schimbare va avea loc în ceea ce privește metodele utilizate pentru a trimite mesajele, care vor deveni mai sofisticate odată cu adoptarea inteligenței artificiale (IA) adversare pentru pregătirea și trimiterea mesajelor. Phishing-ul și spear phishing-ul sunt vectori de atac majori ai altor amenințări, cum ar fi amenințările neintenționate din interior[↗].

Constatări

26,2_ **miliarde pierderi în 2019 din atacuri de compromitere a e-mailului de afaceri (BEC)[20]**

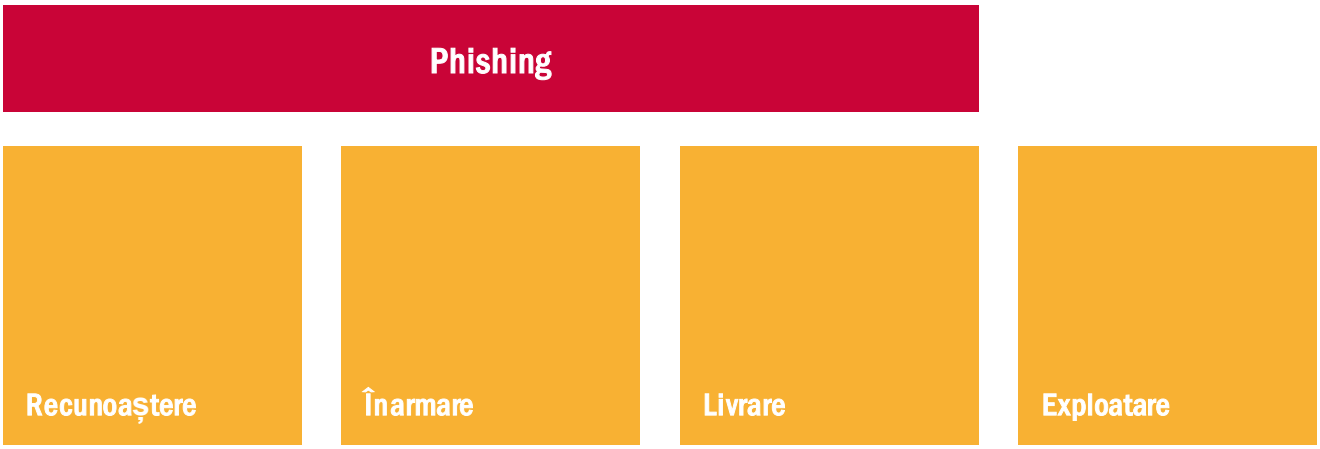
42,8 %_ **din toate atașamentele rău intenționate erau documente Microsoft Office[25]**

667 %_ **creștere a escrocheriilor de phishing în numai o lună în timpul pandemiei de COVID-19[6]**

30 %_ **din mesajele de phishing au fost livrate în zilele de luni[29]**

32,5 %_ **din toate e-mailurile au folosit cuvântul cheie „plată” în subiectul e-mailului[28]**

Kill chain



Etapă din fluxul de activitate de atac

Amploarea scopului

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

Tendințe

_Cele mai vizate tipuri de servicii sunt webmail și software-ul ca serviciu (software-as-a-service)

Conform unor proiecții, atacurile de phishing care vizează software-ul ca serviciu (SaaS) și serviciile de webmail le-au depășit pe cele contra serviciilor de plată pentru prima dată în primul trimestru al anului 2019, acesta devenind cel mai vizat sector, cu 36 % din toate atacurile de phishing.[2] Acest nou record urmează tendința din 2018, când serviciile SaaS și webmail tocmai depășiseră sectorul financiar.[3] Deși cifra a scăzut la 30,8 % până la sfârșitul anului 2019, serviciile menționate mai sus au rămas în continuare pe primele locuri de pe listă[2,3], **serviciile Microsoft 365 fiind ținta principală a phisherilor**.[4]

_Atacurile de compromitere a e-mailului de afaceri (BEC) au continuat să fie o problemă

Un studiu recent a arătat că 88 % din organizațiile din întreaga lume au suferit atacuri de tip phishing și 86 % din acestea s-au confruntat cu atacuri BEC.[16] În 2019, unul dintre serviciile cele mai vizate a fost Microsoft 365, iar accentul principal a fost pe recoltarea de date de identificare.[17] Odată ce au fost dobândite aceste date de identificare, atacatorul a putut să colecteze mai multe date organizaționale, un proces care ar putea dura săptămâni sau luni și care ar putea duce ulterior la atacuri de tip spear phishing. Atacatorul ar face uz de identitatea unui angajat, director executiv (CEO) sau chiar furnizor de încredere pentru a redirecționa fonduri sau pentru a redirecționa plăți către conturile terților.[14] În primul trimestru al anului 2019, companiile au fost vizate de atacuri BEC cu 120 % mai frecvent decât în anul anterior,[19] rezultând pierderi de până la 26,2 miliarde USD (aproximativ 22,2 miliarde EUR).[20]

_Peste două treimi din site-urile de phishing au adoptat HTTPS

În ultimii ani s-a înregistrat o creștere accentuată[13] a numărului de site-uri de phishing care au adoptat HTTPS. În ultimul trimestru al anului 2019, 74 % din site-urile de phishing foloseau HTTPS,[32] o creștere semnificativă în comparație cu doar 32 % cu numai 2 ani mai devreme. Deși tehnologii precum HTTPS și SSL sunt concepute pentru a securiza comunicațiile între un client și un server, prezența unui lacăt într-o pictogramă din bara de adrese a browserului poate crea iluzia că un site web poate fi de încredere.

De asemenea, factorii de amenințare pot folosi site-uri legitime pe care le-au piratat pentru a găzdui conținut de phishing, ceea ce face dificil pentru utilizatorul final să identifice un site ca fiind nesigur.[14] Alți factori care contribuie la creșterea abruptă a utilizării HTTPS sunt multitudinea de servicii de certificare gratuite, cum ar fi Let's Encrypt[15] și faptul că browserele moderne marchează fiecare site HTTPS ca fiind sigur, fără alte verificări.

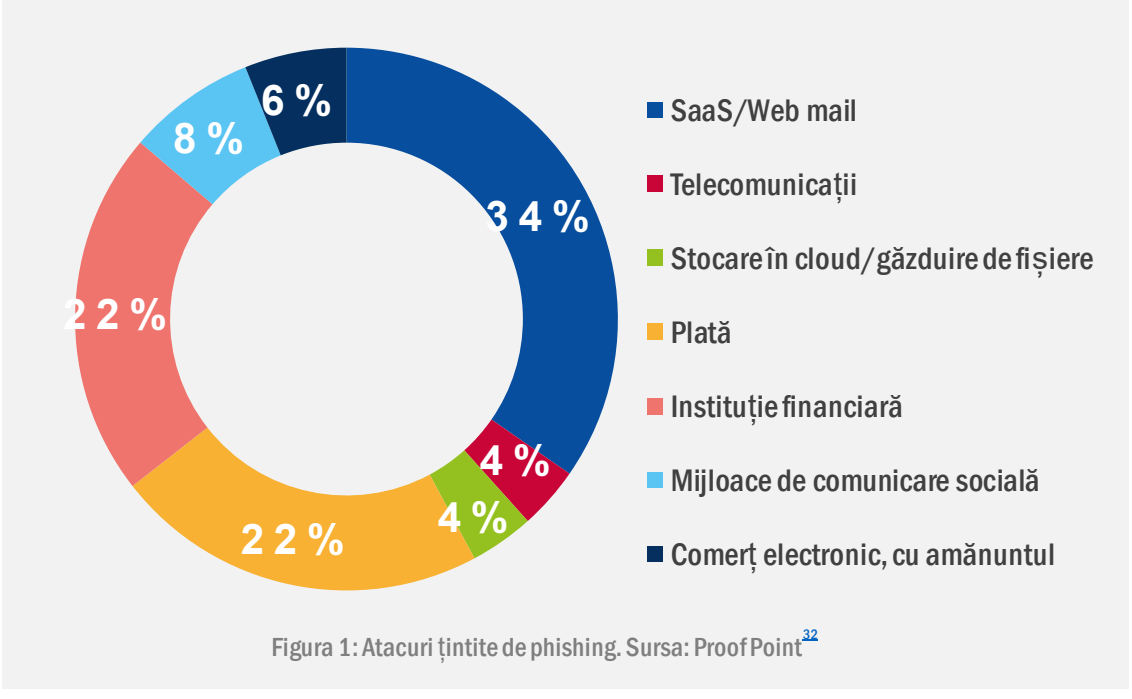


Figura 1: Atacuri țintite de phishing. Sursa: Proof Point[32]

Tendințe

_Phishing-ul ca serviciu (phishing-as-a-service) (PhaaS) în creștere

Aceste tipuri de servicii sunt de regulă pe bază de abonament sau sub forma unui kit, disponibile pentru descărcare contra cost și elimină barierele tehnologice la intrare deoarece permit unei persoane mai puțin calificate din punct de vedere tehnic să efectueze un atac țintit. Un raport al unui cercetător în materie de securitate[21] a identificat 5 334 de kituri unice de phishing disponibile până în iunie 2019. Și mai îngrijorător era costul relativ scăzut al acestor soluții, în jur de 50 - 80 USD pentru un abonament lunar. În același raport s-a afirmat că 87 % din kituri includ mecanisme de evaziune, cum ar fi codarea de caractere în HTML și criptarea conținutului. Interesant este că unele dintre aceste servicii au fost găzduite pe servicii cloud legitime, cu nume și certificate corespunzătoare sistemului de nume de domeniu (DNS). Statisticile de la doar una dintre aceste piețe darknet arată cât de reușite sunt aceste atacuri, care permit atacatorului sau grupului să fure în jur de 65 000 de conturi pe lună.[22]

_Tendințe în ceea ce privește incidentele

- S-a înregistrat o schimbare în eficacitatea atacurilor de phishing folosind stocarea în cloud, DocuSign și serviciile cloud Microsoft.
- Atacurile impostorilor includ scheme precum compromiterea e-mailului de afaceri (BEC) și tehnici de înșelăciune a identității bazate pe inginerie socială pentru a face campaniile de phishing mai eficiente.
- Phishing-ul pentru serviciile Microsoft 365 a fost schema de top, dar accentul rămâne pe recoltarea datelor de identificare.
- Peste 99 % din e-mailurile care distribuie programe malware au necesitat intervenție umană – urmărirea linkurilor, deschiderea documentelor, acceptarea avertismentelor de securitate și alte comportamente – pentru a fi eficiente.[44]

Cele mai importante teme de phishing în 2019

- Recoltare generică de date de identificare de e-mail
- Phishing de conturi Office 365
- Phishing-ul instituției financiare
- Phishing Microsoft OWA
- Phishing OneDrive
- Phishing American Express
- Phishing generic Chalbhai
- Phishing de conturi Adobe
- Phishing Docusign
- Phishing Netflix
- Phishing de conturi Dropbox
- Phishing de conturi LinkedIn
- Phishing de conturi Apple
- Phishing-ul companiei poștale/de transport maritim
- Phishing-ul documentelor Microsoft Online (Excel și Word)
- Phishing-ul setărilor Windows
- Phishing Google Drive
- Phishing PayPal

Sursa: Proof Point[32]

_COVID-19 utilizat ca momeală de phishing

Infractorii cibernetici profită de teama publicului de pandemia de COVID-19, care a apărut pentru prima dată la sfârșitul anului 2019. S-a raportat că atacurile de phishing care implică virusul au crescut cu 667 % într-o perioadă de o lună (între sfârșitul lunii februarie 2020 și sfârșitul lunii martie 2020) și doar aceste tipuri de scheme au reprezentat un procent notabil de 2 % din toate escrocheriile de phishing.[5]

Noile escrocherii au implicat e-mail-uri de phishing concepute pentru a arăta ca și cum ar proveni de la Centrul pentru controlul și prevenirea bolilor din Statele Unite (CDC)[6], Organizația Mondială a Sănătății[7] sau chiar de la echipe de profesioniști din domeniul sănătății de la universități.[8] Acestea fie au pretins în mod fals că prezintă date despre infecții în zona victimei, fie au împărtășit opinii ale experților medicali pentru a atrage victima să urmeze un link rău intenționat. Din acest motiv, FBI și OMS au emis avertismente.[8,9] Întrucât multe persoane aflate în carantină lucrau de acasă, folosind deseori sisteme de securitate învechite[11], infractorii cibernetici au încercat să exploateze oportunitățile și vulnerabilitățile emergente.[12]

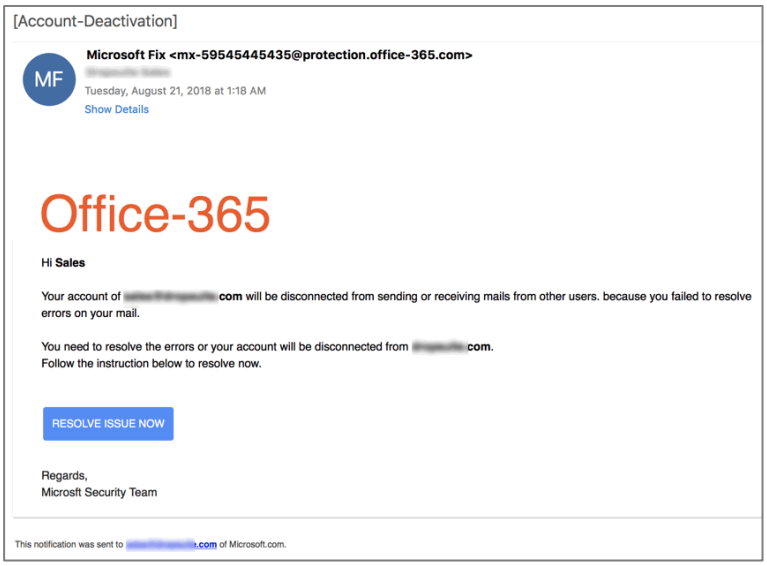


Figura 2: E-mail de phishing Office 365, credit Dropsuite[45]

_Răspunsul ENISA la pandemia de COVID-19

Pandemia de COVID-19 a adus o schimbare imensă în ceea ce privește modul în care ne trăim viața. În această lume din ce în ce mai conectată, din fericire ne putem continua viața profesională și privată în mediul virtual. În această perioadă fără precedent, Agenția UE pentru Securitate Cibernetică (ENISA) a împărtășit recomandările sale privind securitatea cibernetică[46] pe o varietate de subiecte, inclusiv munca la distanță, cumpărăturile online și e-sănătatea și a furnizat actualizări privind recomandările cheie în materie de securitate adaptate sectoarelor afectate. ENISA analizează situația amenințărilor din timpul pandemiei și oferă sfaturi cu privire la modul de diminuare a riscurilor care decurg din cele mai critice amenințări. O atenție specială este acordată phishing-ului din cauza escaladării numărului de atacuri.

Figura 3: Videoclipul ENISA despre COVID-19, pe YouTube Sursa: ENISA

Incidente

_Sectoare vizate

În 2019, sectorul medical a fost puternic vizat de atacuri de phishing (sau spear-phishing). Un cercetător în domeniul securității[42] a considerat phishing-ul ca principalul vector de atac al anului, prin utilizarea unor tactici de inginerie socială pentru a livra e-mailuri infectate cu programe malware sau cu linkuri către site-uri infectate. Alte sectoare au fost vizate, de asemenea, de atacuri de phishing, cum ar fi guvernele și alte entități din administrația publică. De exemplu, în noiembrie și decembrie 2019 mai mulți diplomați și oficiali din guvernul ucrainean au primit e-mail-uri de tip spear-phishing cu trimiteri către site-uri compromise.[43]

_Vectori de atac

Spear phishing-ul rămâne o tehnică de acces inițială extrem de răspândită utilizată de actorii rău intenționați. Acestea utilizează o varietate de tactici de inginerie socială pentru a determina destinatarii să deschidă atașamente sau să navigheze către un site infectat. Mesajele de spear phishing conțin în mod obișnuit documente Microsoft Office cu macrocomenzi sau un link către astfel de documente. După ce un utilizator selectează „Activați conținutul”, macrocomanda inclusă va începe, de regulă, executarea unui lanț de scripturi ascunse care, în cele din urmă, are ca rezultat descărcarea malware-ului din prima etapă sau malware de livrare. JavaScript și PowerShell par să rămână cele mai populare limbaje de scriptare în acest scop.

Exemple

_Un atac de phishing împotriva studenților Universității Lancaster a dus la pierderea datelor cu caracter personal[37]

_Prin atacuri de tip phishing, hackerii au furat datele de conectare a 2 500 de utilizatori Discord[38]

_Un furnizor de servicii de fitness online a fost victima unui atac de phishing[39]

_Pacienți afectați de atacul de phishing de la UConn Health[41]

_O filială a unui producător de autoturisme a pierdut 37 de milioane USD (aproximativ 31 de milioane EUR) din cauza unei escrocherii BEC[33]

Măsuri de atenuare

Acțiuni propuse

- Educarea personalului să identifice e-mailurile false și rău intenționate și să rămână vigilenți. Lansarea de campanii de phishing simulate pentru a testa infrastructura organizației, precum și capacitatea de reacție a personalului.
- Luarea în considerare a utilizării unui gateway de e-mail de securitate cu întreținere regulată (posibil automatizată) a filtrelor (anti-spam, anti-malware, filtrare bazată pe politici).
- Luarea în considerare a aplicării de soluții de securitate care utilizează tehnici de învățare automată pentru a identifica site-urile de phishing în timp real.
- Dezactivarea executării automate a codului, macro-urilor, redarea graficelor și preîncărcarea link-urilor trimise clienților de e-mail și actualizarea frecventă a acestora.
- Aplicarea unuia dintre standardele pentru reducerea mesajelor spam: cadrul de politică pentru expeditori (Sender Policy Framework – SPF)[34], autentificarea, raportarea și conformarea mesajelor bazate pe domenii (Domain-based Message Authentication, Reporting & Conformance – DMARC)[35] și e-mail identificat prin chei de domeniu (Domain Keys Identified Mail – DKIM).[36]
- În mod ideal, utilizarea unei comunicări e-mail securizată utilizând semnături digitale sau criptare, pentru tranzacții financiare critice sau atunci când faceți schimb de informații sensibile.
- Aplicarea detectării fraudelor și a anomaliilor la nivel de rețea atât pentru e-mailurile primite, cât și pentru cele trimise.
- Evitați să faceți clic pe linkuri aleatorii, în special pe linkuri scurte găsite în social media.
- Nu faceți clic pe linkuri, nici nu descărcați atașamente dacă nu aveți încredere absolută în sursa unui e-mail.

- Evitarea partajării excesive de informații personale pe rețelele sociale, de exemplu, durata absenței de la birou sau de acasă, informații de zbor etc., întrucât acestea sunt utilizate în mod activ de factorii de amenințare pentru a culege informații despre țintele lor.
- Verificarea numelui de domeniu al site-urilor pe care le vizitați pentru greșeli de tipar, în special pentru site-uri sensibile, de exemplu site-uri bancare. Factorii de amenințare înregistrează de regulă domenii false care arată asemenea celor legitime și le folosesc pentru a-și ataca țintele prin „phishing”. Căutarea doar a unei conexiuni HTTPS nu este suficientă.
- Activarea autentificării cu doi factori ori de câte ori este cazul pentru a preveni preluarea contului.
- Folosirea unei parole puternice și unice pentru fiecare serviciu online. Reutilizarea aceleiași parole pentru diverse servicii este o problemă gravă de securitate și ar trebui întotdeauna evitată. Utilizarea unor date de identificare solide și unice pentru fiecare serviciu online limitează riscul unei preluări potențiale a contului numai pentru serviciul afectat. Utilizarea unui software de gestionare a parolelor va face mai ușoară gestionarea întregului set de parole.
- Când transferați bani într-un cont, verificați de două ori informațiile bancare ale destinatarului printr-un alt mediu. E-mailurile necriptate și nesemnate nu trebuie să fie de încredere, în special pentru cazuri de utilizare sensibile precum acesta.
- Verificați cum funcționează formularele de contact, înregistrare, abonament și feedback pe site-ul dvs. web și adăugați reguli de verificare, dacă este necesar, pentru a nu putea fi exploatate de atacatori.

Referințe

1. „What Is Phishing?" (Ce este phishing-ul?). Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

2. „Phishing Activity Trends Report Q1" (Raportul privind tendințele activității de phishing T1). 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

3. „2018 Phishing Trends & Intelligence Report" (Raportul privind informațiile și tendințele de phishing din 2018), 2018. Phishlabs.

https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

4. „Microsoft remains phishers' #1 target for the fifth straight quarter" (Microsoft rămâne ținta nr. 1 a phisherilor pentru al cincilea trimestru consecutiv), 22 august 2019. Vade Secure. https://www.vadesecure.com/en/phishers-favorites-q2-2019/

5. „Threat Spotlight: Coronavirus-Related Phishing" (Punerea în evidență a amenințărilor: phishing legat de coronavirus). 26 martie 2020. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

6. „Coronavirus phishing emails: How to protect against COVID-19 scams" (E-mailuri de phishing legate de coronavirus: cum să vă protejați împotriva escrocheriilor legate de COVID-19), 2020. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

7. „Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer" (Recomandări OMS privind medicamente pentru Covid-19 deghizate pentru a distribui agentul de furt de informații Tesla Info-Stealer). 2020. IBM. https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

8. „Abnormal Attack Stories #6: Coronavirus Credential Theft" (Povești de atac anormale nr. 6: furt de date de identificare în contextul pandemiei de coronavirus), 13 martie 2020. https://abnormalsecurity.com/blog/abnormal-attack-stories-6-coronavirus-credential-theft/

9. „FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic" [FBI constată o creștere a schemelor de fraudă legate de pandemia de coronavirus (COVID-19)]. 20 martie 2020. FBI. https://www.ic3.gov/media/2020/200320.aspx

10. „Beware of criminals pretending to be WHO" (Feriți-vă de infractorii care pretind că sunt OMS). 2020. OMS. https://www.who.int/about/communications/cyber-security

11. „Global police agencies issue alerts on Covid-related cyber-crime" (Agențiile globale de poliție emit alerte cu privire la criminalitatea cibernetică legată de COVID). 6 aprilie 2020. SC Magazine. https://www.scmagazineuk.com/global-police-agencies-issue-alerts-covid-related-cyber-crime/article/1679473

12. „Catching the virus cybercrime, disinformation and the COVID-19 pandemic" (Prinderea virusului – infracționalitatea cibernetică, dezinformarea și pandemia de COVID-19). 3 aprilie 2020. EUROPOL. https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

13. „New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks" (Noul raport FireEye privind amenințările prin e-mail dezvăluie creșterea atacurilor de inginerie socială). 25 iunie 2019. FireEye. https://www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engin.html

14. „HTTPS Protocol Now Used in 58% of Phishing Websites" (Protocolul HTTPS este utilizat acum în 58% din site-urile de phishing). 24 iunie 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/https-protocol-now-used-in-58-of-phishing-websites

15. „Let's Encrypt" (Să criptăm). https://letsencrypt.org/

16. „2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike" (Raportul 2020 „Situația phishing-ului": instruire de sensibilizare în materie de securitate, raportare prin e-mail mai critică pe măsură ce se intensifică atacurile țintite). 23 ianuarie 2020. Proof Point. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

17. „Human factor report" (Raportul privind factorul uman). 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

18. „Phishing Activity Trends Report Q3" (Raportul privind tendințele activității de phishing în trimestrul III). 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

19. „Business Email Compromise Results in $26B in Losses Over the Last Three Years" (Compromiterea e-mailului de afaceri duce la pierderi de 26 miliarde USD în ultimii trei ani). 12 septembrie 2019. Proof Point. https://www.proofpoint.com/us/corporate-blog/post/business-email-compromise-results-26b-losses-over-last-three-years

20. „Business Email Compromise The $26 Billion Scam" (Compromiterea e-mailului de afaceri – escrocheria de 26 de miliarde USD), 10 septembrie 2019. FBI. https://www.ic3.gov/media/2019/190910.aspx

21. „Evasive Phishing Driven by Phishing-as-a-Service" (Phishing evaziv determinat de phishing-ul ca serviciu). 1 iulie 2019. Cyren.

https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service

22. „Phishing made easy: Time to rethink your prevention strategy?" (Phishing-ul simplificat: e timpul să vă regândiți strategia de prevenire?). 2016. Imperva. https://www.imperva.com/docs/Imperva-HII-phishing-made-easy.pdf

23. „Q3 2019: Email Fraud and Identity Deception Trends" (T3 2019: tendințe în materie de fraudă prin e-mail și înșelăciune de identitate). 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

24. „FBI: BEC Losses Soared to $1.8 Billion in 2019" (FBI: Pierderile BEC au crescut la 1,8 miliarde USD în 2019). 12 februarie 2020. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/fbi-bec-losses-soared-to-18/

25. „Email: Click with Caution" (E-mail: faceți clic cu precauție). Iunie 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

26. „Experts report a rampant growth in the number of malicious, lookalike domains" (Experții raportează o creștere galopantă a numărului de domenii-replică rău intenționate). 18 noiembrie 2019. https://securityaffairs.co/wordpress/94021/hacking/lookalike-domains-tls-certificate.html

27. „Proofpoint Q3 2019 Threat Report — Emotet's return, RATs reign supreme, and more" (Raportul Proof Point privind amenințările din T3 2019: Emotet se întorc, RAT dețin supremația și altele). 7 noiembrie 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

28. „Human Factor Report" (Raport privind factorul uman). 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

29. „2019 Phishing and fraud report" (Raport privind phishing-ul și frauda din 2019), 2019. F5 Labs. https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

30. „Report: Microsoft, PayPal, and Netflix Most Impersonated Brands in Phishing Attacks in Q1 2019" (Raport: Microsoft, PayPal și Netflix sunt mărcile cele mai imitate în atacuri de phishing în T1 2019), 8 mai 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-microsoft-paypal-and-netflix-most-impersonated-brands-in-phishing-attacks-in-q1-2019

31. „Spam and phishing in Q3 2019" (Spam-ul și phishing-ul în T3 2019). 26 noiembrie 2019. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

32. „Phishing Activity Trends Report" (Raport privind tendințele activității de phishing). 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

33. „Toyota Subsidiary Loses $37 Million Due to BEC Scam" (Filiala Toyota pierde 37 de milioane USD din cauza escrocheriei BEC), 20 septembrie 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/

34. Open SPF. http://www.openspf.org/

35. „Domain-based Message Authentication, Reporting & Conformance" (Autentificarea, raportarea și conformarea mesajelor bazate pe domenii). DMARC. https://dmarc.org/

Referințe

36. „DomainKeys Identified Mail (DKIM)" (E-mail identificat prin chei de domeniu) DKIM. http://www.dkim.org/

37. „Cyber incident" (Incident cibernetic). 22 iulie 2019. Lancaster University. https://www.lancaster.ac.uk/news/phishing-attack

38. „Hackers publish login credentials of 2500 Discord users" (Hackerii publică datele de conectare a 2 500 de utilizatori Discord), 22 iulie 2019. Cyware Social. https://cyware.com/news/hackers-publish-login-credentials-of-2500-discord-users-8d3ea2c7

39. „Bodybuilding.com Breach: Proof That An Organization's Biggest Cyber Risk Is Its People" (Încălcarea securității la Bodybuilding.com: dovada că cel mai mare risc cibernetic al unei organizații este reprezentat de oamenii săi), 24 aprilie 2019. Forbes. https://www.forbes.com/sites/jameshadley/2019/04/24/bodybuilding-com-breach-proof-that-an-organizations-biggest-cyber-risk-is-its-people/#1ea113751bef

40. „Phishing Attack Exposes 600k Health Records" (Atacul de phishing dezvăluie 600 de fișe medicale), 19 iunie 2019. Secure World. https://www.secureworldexpo.com/industry-news/healthcare-data-breach-example-2019

41. „326,000 Patients Impacted in UConn Health Phishing Attack" (326 000 de pacienți afectați de atacul de phishing de la UConn Health). 25 februarie 2019. Health IT Security. https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack

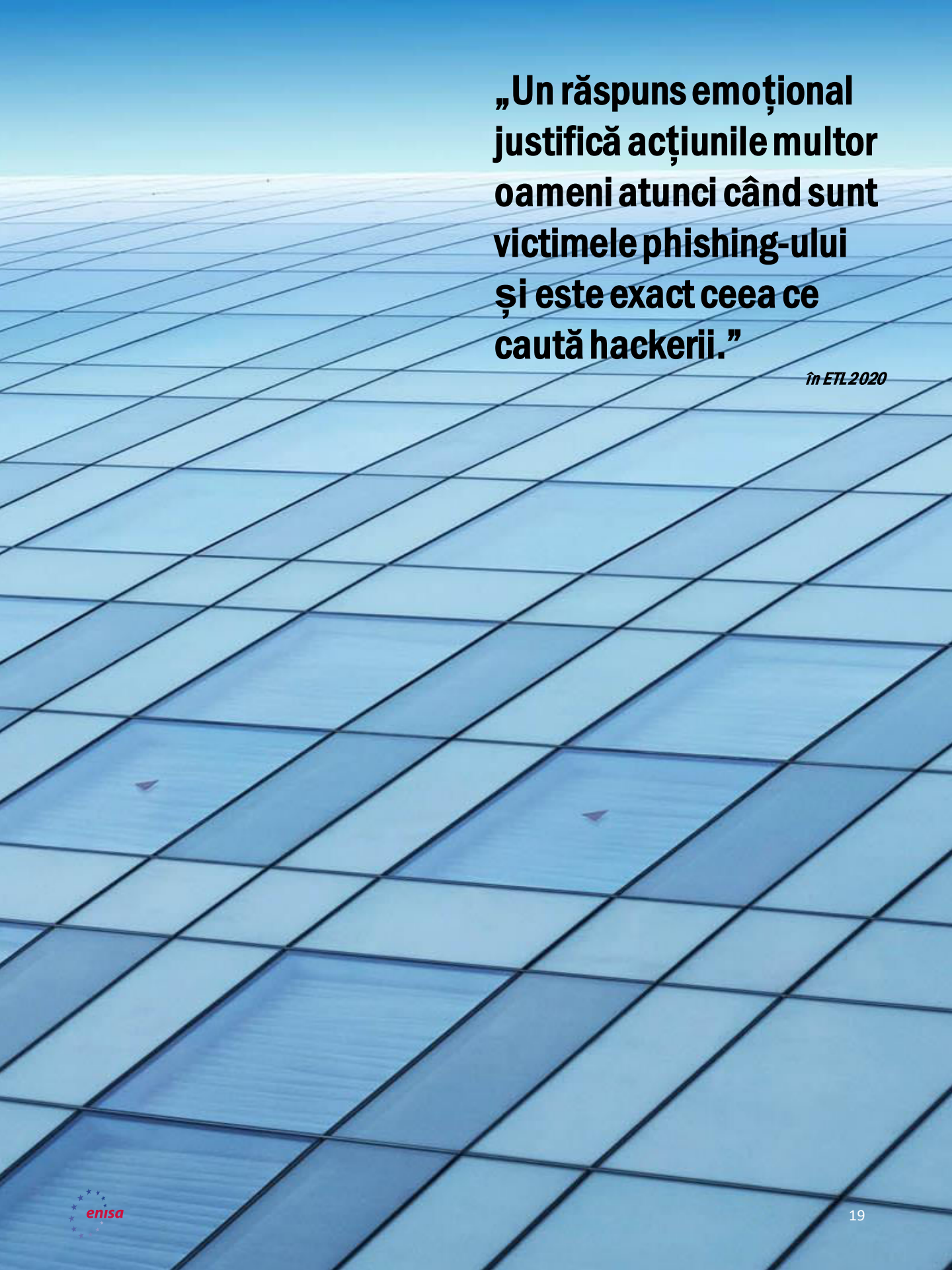
42. „Cybercrime Tactics and Techniques: the 2019 state of healthcare" (Tacticile și tehnicile de criminalitate informatică: situația asistenței medicale în 2019). 2019. Malwarebytes. https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-the-2019-state-of-healthcare/

43. „Significant Cyber Incidents" (Incidente cibernetice semnificative). 2019. CSIS. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

44. „More Than 99% of Cyberattacks Need Victims' Help" (Peste 99 % dintre atacurile cibernetice au nevoie de ajutorul victimelor). 9 septembrie 2019. Dark Reading. https://www.darkreading.com/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769

45. „office-365-phishing-attacks-deconstructed" https://dropsuite.com/office-365-phishing-attacks-deconstructed/

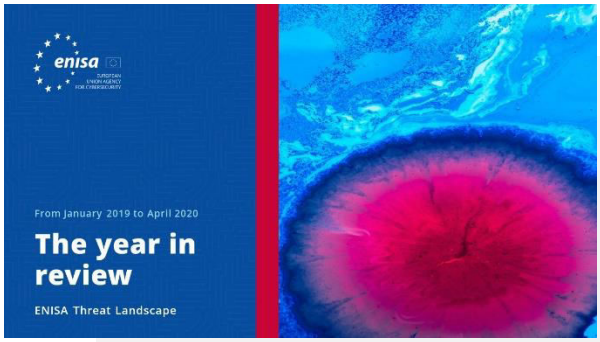
46. ENISA. https://www.enisa.europa.eu/topics/wfh-covid19



„Un răspuns emoțional justifică acțiunile multor oameni atunci când sunt victimele phishing-ului și este exact ceea ce caută hackerii.”

în ETL 2020

Documente conexe



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

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

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

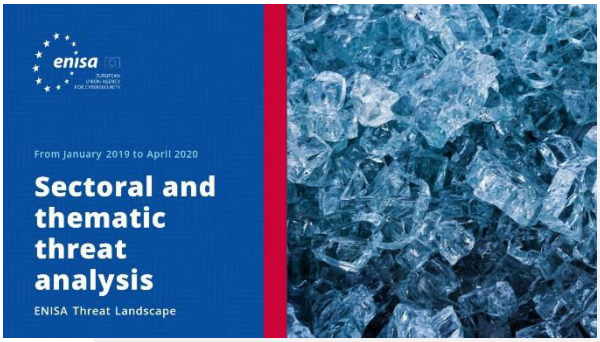
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Teme de cercetare

Recomandări privind teme de cercetare în diferite sectoare din securitatea cibernetică și informațiile privind amenințările cibernetice.

CITIȚI RAPORTUL



CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Analiza sectorială și tematică a amenințărilor**

Analiza contextualizată a amenințărilor în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Tendințe emergente**

Principalele tendințe în securitatea cibernetică observate în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Prezentare generală a informațiilor privind amenințările cibernetice**

Situația actuală a informațiilor privind amenințările cibernetice în UE.

Despre

_Agenție

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică
contribuie la politica cibernetică a UE, sporește credibilitatea produselor, serviciilor și proceselor TIC cu ajutorul sistemelor de certificare a securității cibernetice, cooperează cu statele membre și organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu părțile interesate cheie pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, în cele din urmă, pentru a menține securitatea digitală a societății europene și a cetățenilor. Mai multe informații cu privire la ENISA și activitatea sa sunt disponibile la adresa www.enisa.europa.eu.

Contribuitori

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

Editori

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

Date de contact

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

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

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

Aviz juridic

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

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

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

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Telefon: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu