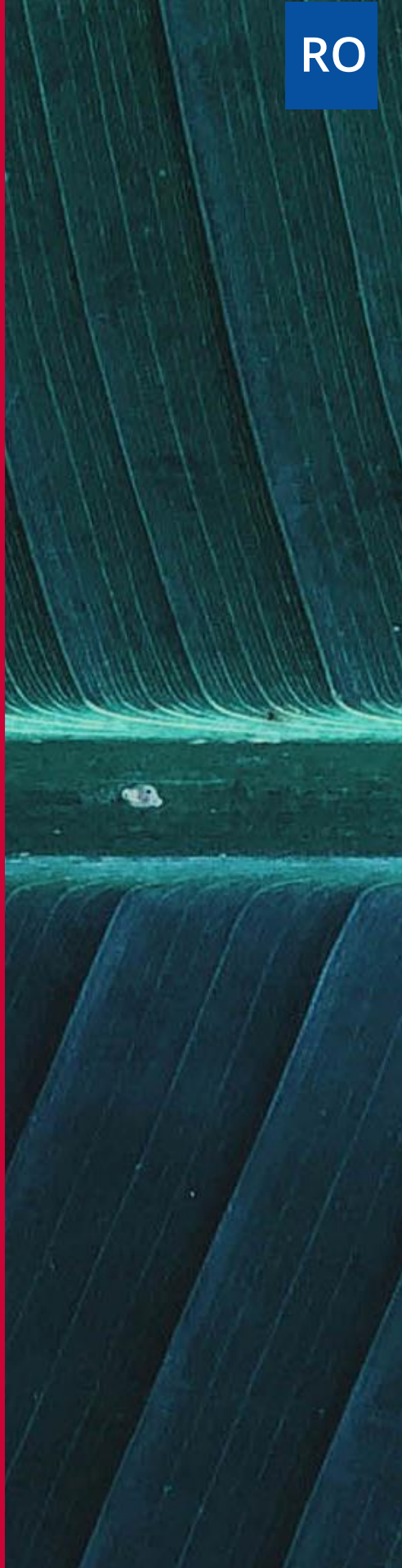
RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



Ianuarie 2019 – aprilie 2020

Spam

Raportul ENISA privind situația amenințărilor

Prezentare generală

Primul mesaj spam a fost trimis în 1978 de un manager de marketing la 393 de persoane, prin intermediul ARPANET. A fost o campanie de publicitate pentru un nou produs de la compania la care lucra, Digital Equipment Corporation. Pentru acele prime 393 de persoane vizate de spam, a fost la fel de iritant pe cât ar fi astăzi, indiferent de noutatea ideii[1]. Primirea de spam este un inconvenient, dar poate crea și o oportunitate pentru un actor rău intenționat de a fura informații cu caracter personal sau de a instala programe malware[2]. Spamul constă în trimiterea în bloc de mesaje nesolicitate. Spamul este considerat o amenințare la adresa securității cibernetice atunci când este utilizat ca vector de atac pentru a distribui sau a facilita alte amenințări.

Un alt aspect de remarcat este modul în care spamul poate fi uneori confundat sau clasificat greșit ca o campanie de phishing. Principala diferență dintre cele două constă în faptul că phishing-ul este o acțiune țintită care utilizează tactici de inginerie socială, urmărind în mod activ să fure datele utilizatorilor. În schimb, spamul este o tactică pentru trimiterea de e-mailuri nesolicitate către o listă în bloc. Campaniile de phishing pot utiliza tactici de spam pentru a distribui mesaje, în timp ce spamul poate trimite utilizatorului un link către un site compromis pentru a instala malware și a fura date personale.

Campaniile de spam din ultimii 41 de aniau profitat de numeroase evenimente sociale și sportive populare la nivel mondial, cum ar fi, printre altele, finala UEFA Europa League, US Open. Chiar și așa, nimic nu se compară cu activitatea de spam constatată anul acesta în contextul pandemiei de COVID-19[8].

Constatări

85 %_ din toate e-mailurile schimbate în aprilie 2019 au fost spam, un record pentru o perioadă de 15 luni[1]

14_ milioane de mesaje spam legate de extorcare sexuală au fost detectate în 2019[23]

58,3 %_ din conturile de e-mail din industria minieră au fost spamate[17]

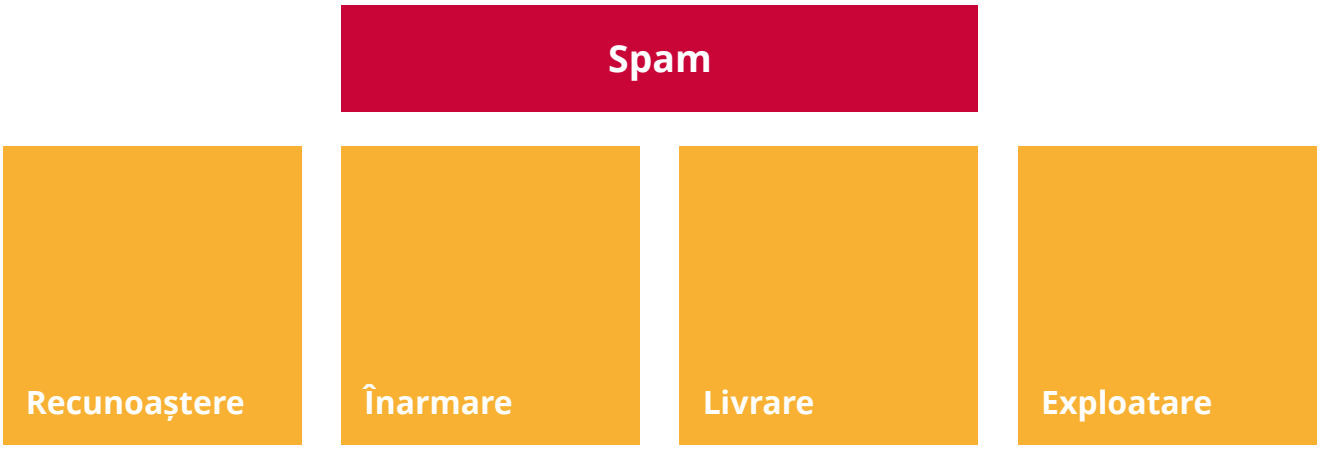
10 %_ din totalul detecțiilor de spam vizau conturile de e-mail germane[2,3]

13 %_ din încălcările securității datelor au fost cauzate de spam rău intenționat[16]

83 %_ din companii nu au fost protejate împotriva uzurpării mărcii prin e-mail[20]

42 %_ din responsabilii șefi pentru securitatea informațiilor (CISO) s-au ocupat de cel puțin un incident de securitate cauzat de spam[1]

Kill chain



Etapă din fluxul de activitate de atac

Amploarea scopului

Cadrul Cyber Kill Chain® a fost dezvoltat de Lockheed Martin, fiind adaptat după un concept militar legat de structura unui atac. Pentru a studia un anumit vector de atac, utilizați această diagramă kill-chain pentru a trasa fiecare etapă a procesului și a face referire la instrumentele, tehnicile și procedurile utilizate de atacator.

MAI MULTE INFORMAȚII

Descriere

_Avansat pentru vârsta lui

După 41 de ani de existență, spamul rămâne o amenințare notabilă pentru securitate, în ciuda tuturor celorlalte amenințări care sunt mult mai eficace. Cu toate acestea, și de această dată în perioada de raportare au apărut noi grupuri țintă, noi mijloace și noi câștiguri în campaniile de spam. De exemplu, în august 2019 au existat mesaje spam care au vizat mai multe conturi, încurajându-i pe deținătorii lor să divulge nu numai o copie scanată a actului lor de identitate, ci și un selfie, pentru a „câștiga" un dispozitiv smartphone gratuit. Într-o altă campanie de spam, utilizatorii au fost rugați să trimită o fotografie personală. Grupul-țintă al spammerilor a fost extins apoi pentru a include adresa de e-mail folosită de utilizator, în scopul de a activa serviciile de televiziune cu plată sau de transmisie în direct. Conturile respective au fost vizate de spam cu mesaje false de expirare sau reînnoire a licenței. Utilizatorii au fost rugați să răspundă și să introducă detaliile contului lor bancar și informații cu caracter personal pentru a reînnoi înregistrarea[2].

_Trimiterea de mesaje spam pentru a favoriza programe malware, ransomware și troieni de acces la distanță

În august 2019, s-au utilizat mesaje spam care conțineau fișiere de imagine de disc ISO dăunătoare pentru a răspândi malware-ul LokiBot și pentru a introduce troianul de acces la distanță (RAT) FlawedAmmyy. De asemenea, trimiterea de mesaje spam a fost utilizată pentru a răspândi troianul TrickBot, troianul-spion Negasteal (cunoscut și sub numele de Agent Tesla), RAT Ave Maria (cunoscut și sub numele de Warzone) și macro malware-ul notoriu, din 2018, Pawload. De asemenea, mai multe familii de ransomware au fost răspândite prin mesaje spam, cum ar fi Dharma, Crysis și Ryuk, toate fiind raportate a fi extrem de active în anul de raportare.[15,21]

SMS-uri spam

Anul acesta s-a desfășurat o operațiune de spam prin SMS, expunând datele personale a peste 80 de milioane de utilizatori. S-au trimis mesaje către foarte multe numere de telefon, care conțineau anumite expresii precum „bani oferiți gratuit” sau „pe bune” și linkuri către site-uri false. Din acel moment, oricine urma linkul era invitat să se înscrie, furnizând informații sensibile. S-a dovedit că baza de date utilizată de spammeri era deținută de compania ApexSMS, a cărei legitimitate este încă necunoscută. Deși cercetătorii în domeniul securității au accesat baza de date și au încercat să recupereze cât mai multe informații posibil, temându-se că operațiunea se va opri în mod neașteptat, încă nu se știe cine și din ce motiv poate accesa și utiliza aceste date, care sunt încă disponibile[4].

Formulare utilizate ca mijloace

Spammerii au manipulat formulare de feedback pe site-urile unor companii mari, care erau utilizate pentru adresarea de întrebări, exprimarea dorințelor sau abonarea la buletine informative. Totuși, în acest an de raportare, în loc să trimită spam către cutiile poștale legate de companie, spammerii au exploatat nivelurile scăzute de securitate a site-ului, au evitat orice teste reCAPTCHA și au înregistrat conturi multiple cu informații valide de e-mail. Drept urmare, victimele au primit un răspuns legitim de la companie, care includea mesajul spammerului.[2] În acest fel, chiar și Google Forms a fost manipulat pentru a prelua datele utilizatorilor și a trimite spam comercial. Un caz mai agresiv a fost atacul de spam vizând conturile companiei, prin care se solicita un transfer de bani către atacator. Pentru a convinge victima, spammerii au susținut că pot trimite mesaje abuzive în e-mailul victimei la mai mult de 9 milioane de adrese de e-mail, înscriind pe lista neagră adresa de e-mail a companiei[3].

Descriere

Spam cameleon

Diferite campanii din 2019 au folosit același sistem botnet pentru a distribui mesaje spam, deși au recurs la antete și șabloane aleatorii pentru formatarea conținutului. Din acest motiv, cercetătorii în domeniul securității au început să studieze aceste campanii ca un singur grup, sub numele de „spam cameleon”[5].

Mesajele de spam cameleon proveneau din țări diferite și includeau linkuri false către anunțuri de locuri de muncă sau oferte de locuri de muncă, site-uri de rezervare a biletelor de avion, oferte speciale la achiziționarea de produse sau chiar servicii simple bine cunoscute, toate false. Aceste mesaje spam foloseau un șablon similar cu cele utilizate de companii valide precum Google, Qatar Airways, FedEx, LinkedIn sau Microsoft, astfel încât destinatarul să nu observe diferența.[2]

La fel de dur ca boții vechi

În octombrie 2019, au fost trimise pe scară largă e-mailuri care foloseau șabloane în engleză, germană, italiană și polonă cu subiectul comun „Recomandări privind remiterea plăților”. Aceste mesaje includeau un document atașat care conținea o macrocomandă, iar destinatarilor li s-a cerut să o activeze la deschiderea documentului. Odată activată, macrocomanda putea începe procesul de infecție încercând să descarce troianul Emotet.[13]

Botnetul de spam Necurs a fost foarte activ în această perioadă, după o perioadă îndelungată de activitate redusă. Botnetul Gamut a fost al treilea cel mai activ botnet de spam în 2019. Mesajele Gamut sunt în mare parte legate de sugestii pentru întâlniri romantice sau întâlniri cu oameni, oferte de produse farmaceutice și oportunități de muncă.[1]

_Numărul de rețele botnet C2 asociate cu familiile de malware

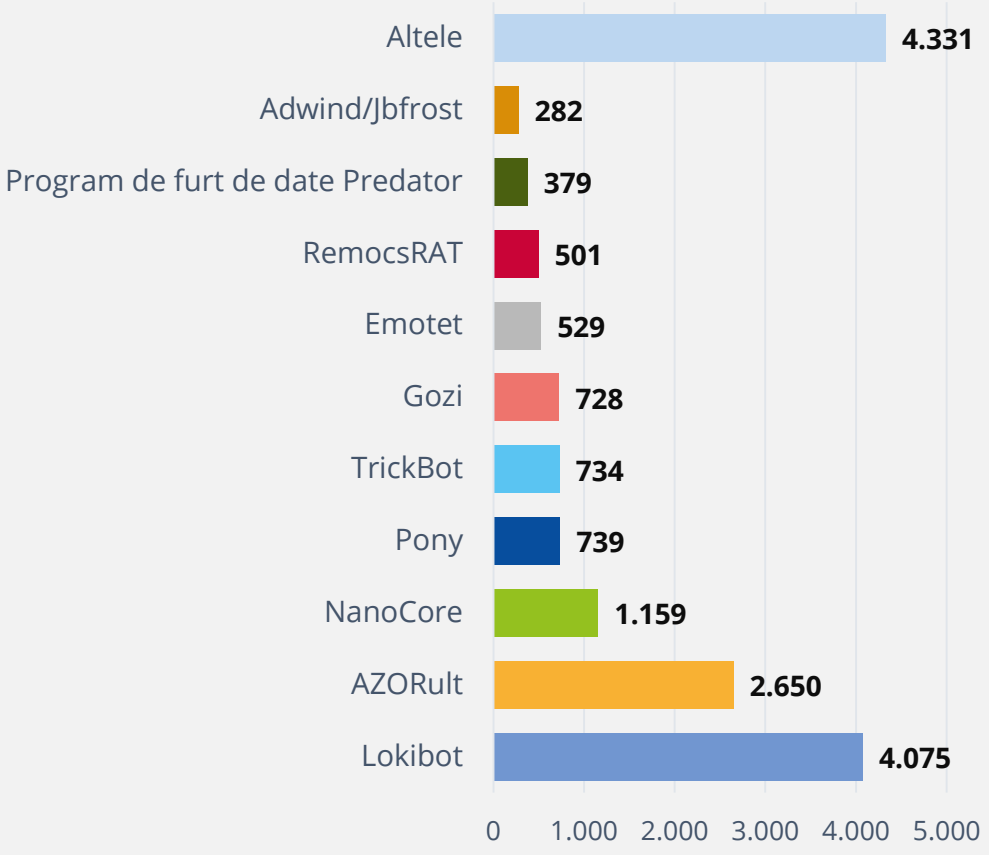


Figura 1 - Sursa: Spamhaus [14]

Descriere

_ COVID-19 a deschis noi uși

La scurt timp după începerea pandemiei de COVID-19, au apărut site-uri de phishing și fișiere rău intenționate livrate prin e-mail folosind termenii coronavirus sau COVID-19. S-a raportat că o campanie de trimitere de spam COVID-19 răspândea Eeskiri-COVID.chm19, un fișier keylogger deghizat. Numele fișierului poate sugera o origine estoniană a campaniei (și anume, eeskiri înseamnă „regulă" în estonă)[11]. La jumătatea lunii februarie 2020 erau înregistrate doar câteva sute de atacuri COVID-19 pe zi, dar în martie 2020 aveau loc peste 2 500 de atacuri în fiecare zi, promițând un an greu în ceea ce privește spamul.[12]

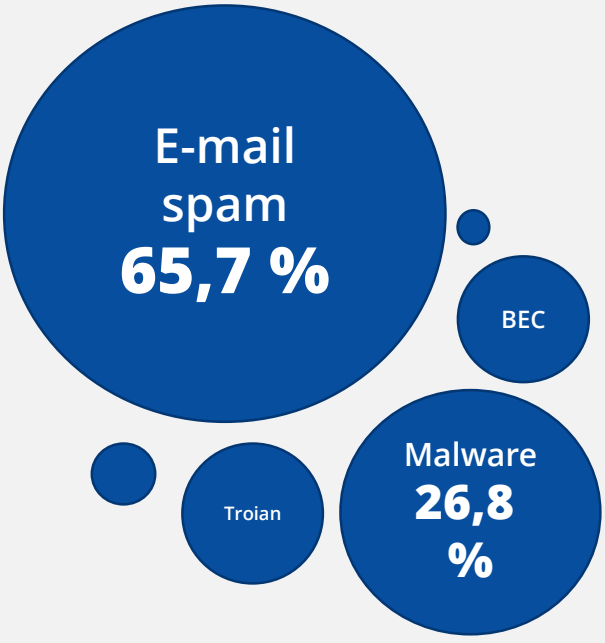


Figura 2: Amenințări provenite din contextul COVID-19. Sursa: Trend Micro[11]

_ Exemple

01_ Operațiunea de spam ApexSMS

ApexSMS, o companie de marketing prin SMS, a suferit o încălcare a securității datelor, expunând datele de contact a peste 80 de milioane de persoane.

02_ Campania de spam Chameleon

O campanie persistentă de spam de mare volum a provenit dintr-un sistem botnet care trimite mesaje cu anteturi randomizate și schimbă adesea șablonul.

03_ Campanie de distribuire a spamului Emotet

O campanie de spam care sprijină distribuția de malware Emotet.

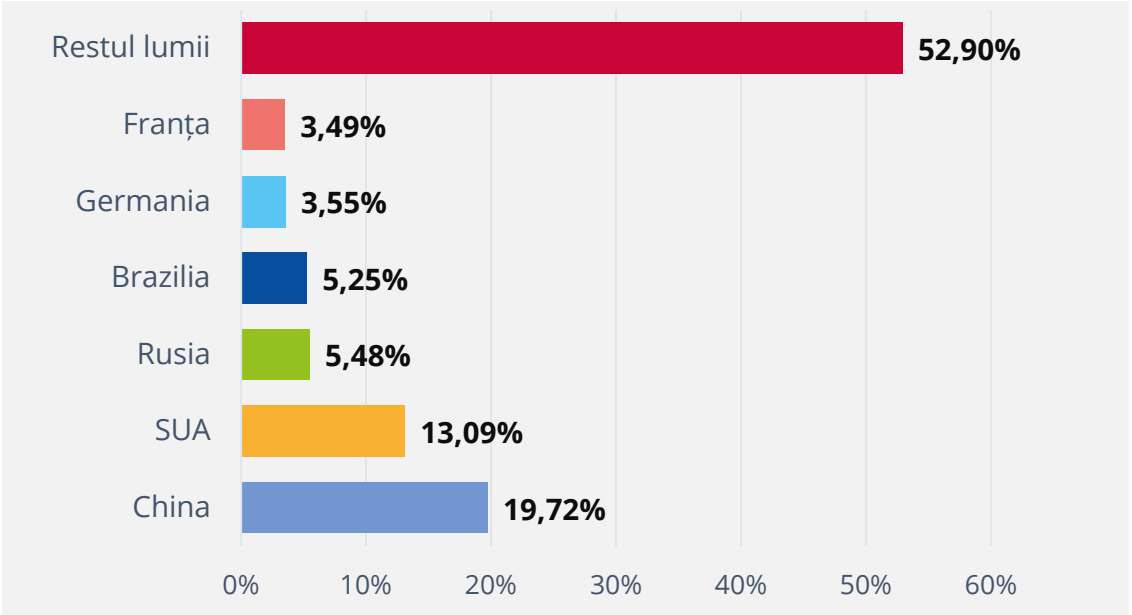
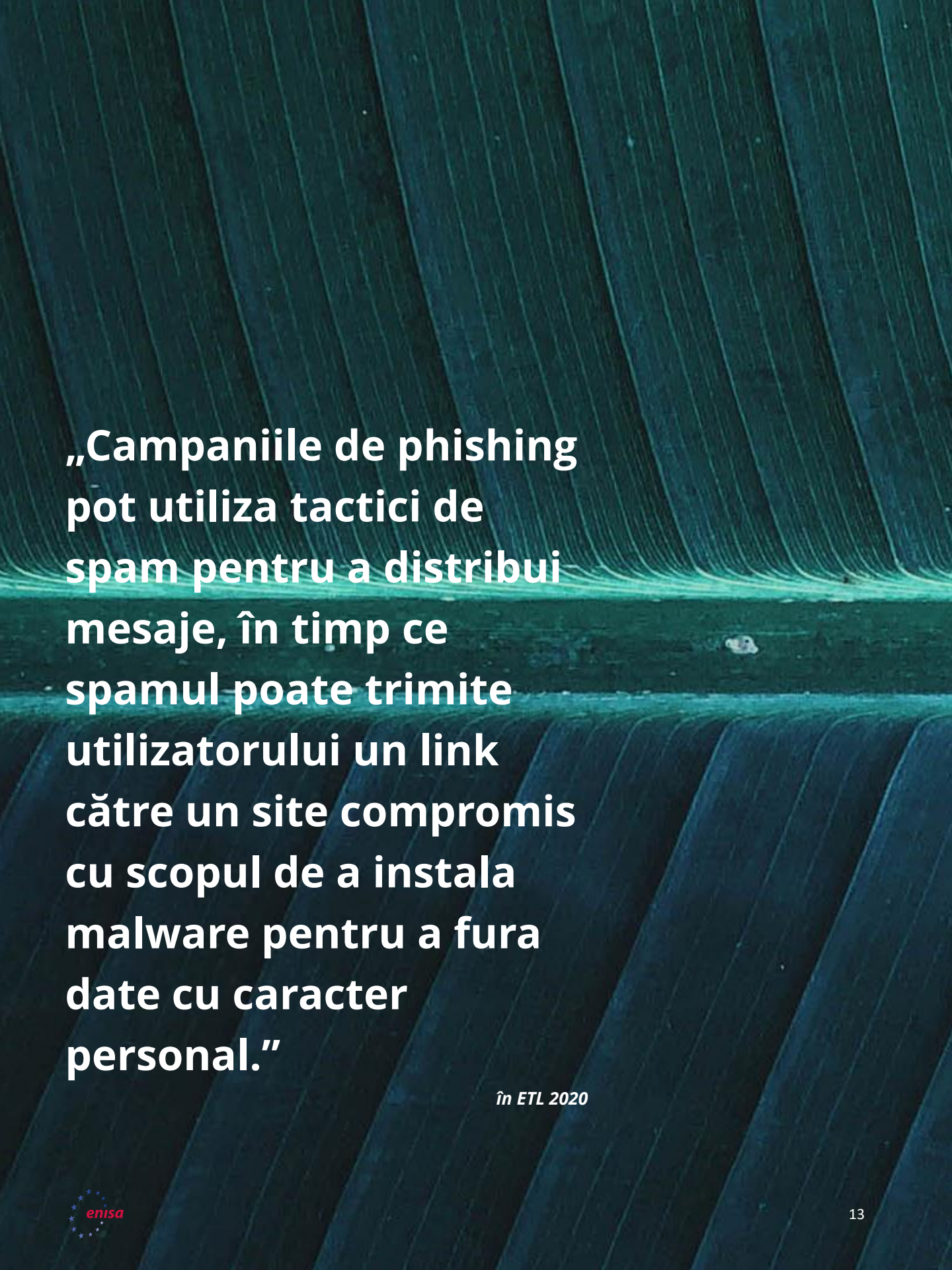


Figura 3: Cele mai comune surse de SPAM Surse multiple [17]

Măsuri de atenuare

Acțiuni propuse

- Aplicarea filtrării conținutului pentru a localiza atașamente nedorite, mesaje cu conținut rău intenționat, spam și trafic de rețea nedorit.
- Actualizarea periodică a hardware-ului, firmware-ului, sistemului de operare și a oricărui driver sau software.
- Utilizarea autentificării cu mai mulți factori pentru a accesa conturile de e-mail.
- Evitarea transferurilor de bani către conturi bancare neconfirmate.
- Evitarea conectării la linkuri noi primite în e-mailuri sau mesaje SMS.
- Elaborarea de proceduri și politici de operare standard pentru gestionarea datelor sensibile.
- Utilizarea unui gateway de e-mail securizat, dacă este posibil, cu întreținerea regulată și automată a filtrelor (anti-spam, anti-malware, filtrare bazată pe politici).
- Dezactivarea executării automate a codului, a activării macrocomenzilor și a preîncărcării graficelor și a linkurilor trimise prin poștă.
- Aplicarea de tehnici de securitate, cum ar fi cadrul de politică pentru expeditori (Sender Policy Framework –SPF), autentificarea, raportarea și conformarea mesajelor bazate pe domenii (Domain-based Message Authentication, Reporting & Conformance – DMARC) și e-mail identificat prin chei de domeniu (Domain Keys Identified Mail – DKIM).
- Actualizarea periodică a listelor albe, a filtrelor de reputație și a listei în timp real a găurilor negre (Real-time Blackhole List – RBS).
- Utilizarea inteligenței artificiale și învățarea automatizată pentru verificări de detectare a anomaliilor.



„Campaniile de phishing pot utiliza tactici de spam pentru a distribui mesaje, în timp ce spamul poate trimite utilizatorului un link către un site compromis cu scopul de a instala malware pentru a fura date cu caracter personal.”

în ETL 2020

Referințe

1. „Email: Click with Caution - How to protect against phishing, fraud, and other scams" (E-mail: faceți clic cu precauție – Cum să vă protejați împotriva phishingului, a fraudei și a altor escrocherii), iunie 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

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

3. „Spam and phishing in Q2 2019" (Spam și phishing în T2 2019), 28 august 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q2-2019/92379/

4. „SMS Spammers Doxxed" [Spammeri SMS discreditați (doxxed)], 9 mai 2019. Tech Crunch. https://techcrunch.com/2019/05/09/sms-spammers-doxxed/

5. „Tracking the Chameleon Spam Campaign" (Urmărirea campaniei de spam cameleon), 25 septembrie 2019. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracking-the-chameleon-spam-campaign/

6. „5 Biggest Cyberattacks of 2019 (So Far) and Lessons Learned" [Cele mai mari 5 atacuri cibernetice din 2019 (până acum) și lecțiile învățate], 7 iunie 2019. Gordon Flesch. https://www.gflesch.com/blog/biggest-cyberattacks-2019

7. „The world worst spammers" (Cei mai răi spammeri din lume). 2019. Spamhaus. https://www.spamhaus.org/statistics/spammers/

8. „Naming the coronavirus disease (COVID-19) and the virus that causes it" [Numirea bolii coronavirus (COVID-19) și a virusului care o provoacă]. 2020. OMS. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

9. „WHO Director-General's opening remarks at the media briefing on 2019 novel coronavirus" (Remarcile din deschidere ale Directorului General al OMS la informarea mass-media cu privire la noul coronavirus din 2019), 6 februarie 2020. OMS. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-2019-novel-coronavirus/

10. „COVID-19 situation update worldwide, as of 11 June 2020" (Actualizarea situației COVID-19 la nivel mondial, începând cu 11 iunie 2020), 2020. ECDC. https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

11. „Developing Story: COVID-19 Used in Malicious Campaigns" (Poveste în curs de desfășurare: COVID-19 utilizat în campanii rău intenționate), 24 aprilie 2020. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

12. „2019 Novel Coronavirus and COVID-19 Themed Attacks Dominate Threat Landscape" (Noul coronavirus din 2019 și atacurile tematice COVID-19 domină peisajul amenințărilor), 6 aprilie 2020. HIPAA Journal. https://www.hipaajournal.com/2019-novel-coronavirus-and-covid-19-themed-attacks-dominate-threat-landscape/

13. „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 Lab. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

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

15. „Evasive Threats, Pervasive Effects" (Amenințări evazive, efecte extinse), 27 august 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

16. „Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study" (Anticiparea necunoscutelor: studiul de referință CISO al Cisco 2019), 28 februarie 2019. Cisco. https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

17. „Internet Security Threat Report" (Raportul privind amenințările la adresa securității internetului), Volumul 24, februarie 2019. Broadcom. https://docs.broadcom.com/doc/istr-24-2019-en

18. „Spam and phishing in Q1 2019" (Spam și phishing în T1 2019), 5 mai 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q1-2019/90795/

19. „Total Global Email & Spam Volume for May 2020" (Volumul total de e-mail și spam global pentru luna mai 2020), mai 2019. Talos. https://talosintelligence.com/reputation_center/email_rep#global-volume

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

21. „The World's Most Abused TLDs" (Cele mai abuzate TLD-uri din lume), Spamhaus. https://www.spamhaus.org/statistics/tlds/

22. „Trend Micro Cloud App Security Report 2019" (Raportul Trend Micro privind securitatea aplicației cloud din 2019), 10 martie 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

23. „The Sprawling Reach of Complex Threats" (Abordarea extinsă a amenințărilor complexe). 2019. Trend Micro Research. https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf

24. „SONIC WALL Security Center Metrics" (Indici de cuantificare ai centrului de securitate SonicWall). SONIC WALL. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

Documente conexe

CITIȚI RAPORTUL

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

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

CITIȚI RAPORTUL

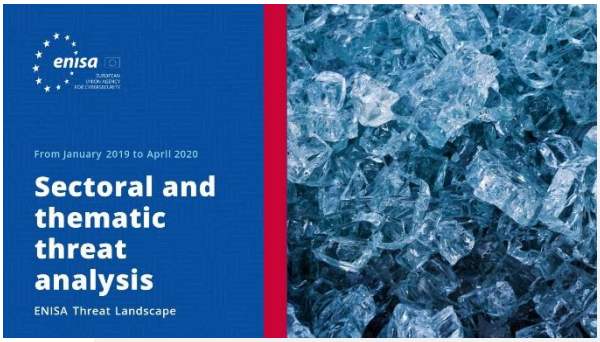
Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

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

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Teme de cercetare

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



CITIȚI RAPORTUL

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

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

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Tendințe emergente**

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

CITIȚI RAPORTUL

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

Situația actuală a informațiilor privind amenințările cibernetice în UE.

Despre

_ Agenție

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

Contribuitori

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

Editori

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

Date de contact

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

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

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

Aviz juridic

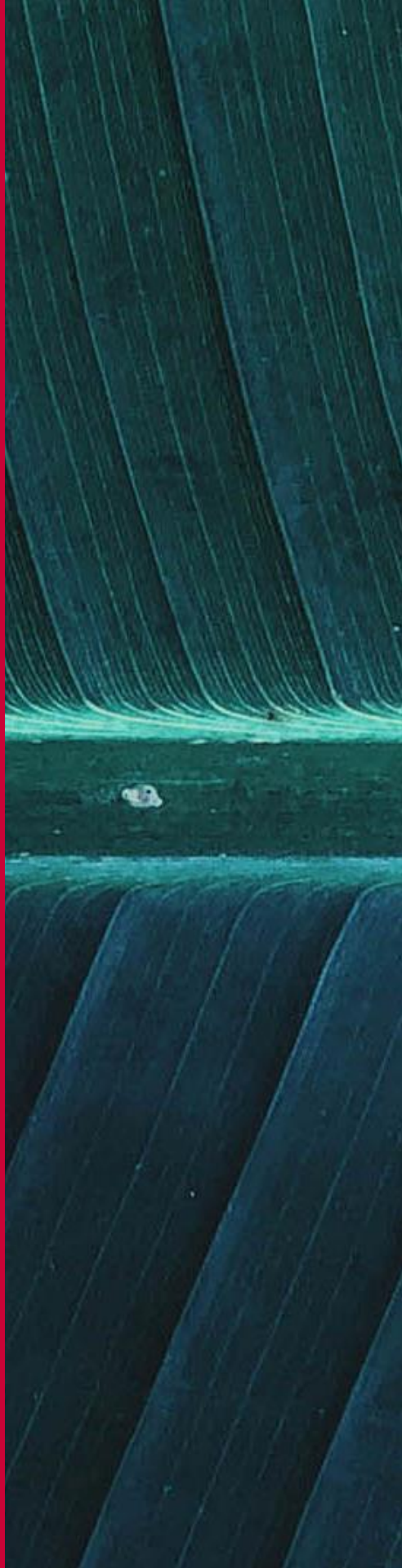
Trebuie luat în considerare faptul că această publicație reprezintă punctele de vedere și interpretările ENISA, cu excepția cazului în care se prevede altfel. Această publicație nu trebuie interpretată ca o acțiune juridică a ENISA sau a organismelor ENISA, cu excepția cazului în care a fost adoptată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

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

Această publicație are doar scop informativ și trebuie să fie accesibilă 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