BULETIN CYBERINT

SEMESTRUL I - 2026

ATRIBUIREA PUBLICĂ A ACTIVITĂȚII DERULATE DE ACTORI CIBERNETICI ASOCIAȚI/ATRIBUIȚI GRU

La 18 iulie 2025, Regatul Unit al Marii Britanii (UK), alături de alți parteneri occidentali, inclusiv Consiliul Nord Atlantic și Înaltul Reprezentant al UE, au inițiat un demers comun de tip *blame and shame* privind activitățile ostile din spațiul cibernetic derulate de Direcția Principală a Forțelor Armate Ruse – serviciul militar de informații al Federației Ruse (GRU).

UK a acuzat GRU de instrumentarea unor operațiuni cibernetice ostile timp de mai mulți ani, derulate în special de trei unități militare - U.M. 29155, U.M. 26165 și U.M. 74455. Totodată, statul britanic a impus sancțiuni asupra 18 ofițeri de informații, angajați în cadrul unităților menționate, implicați în derularea atacurilor cibernetice.

Astfel, a fost denunțată implicarea celor trei unități GRU, precum și ofițerilor acestora, în acțiuni ostile precum:

► în 2022, U.M. 26165, a cărei activitate este asociată cu actorul cibernetic APT28, a realizat activități de *reconnaissance* online pentru a sprijini atacul Federației Ruse cu rachete împotriva orașului Mariupol, inclusiv distrugerea Teatrului de artă dramatică al oblastului Donețk;

► targetarea cu aplicația *malware* X-Agent a dispozitivelor personale ale Yuliei Skripal, fiica fostului ofițer GRU Sergei Skripal, relocați pe teritoriul britanic, înainte de tentativa din 2018 de asasinare a acestora;

► targetarea unor trusturi media, furnizori de telecomunicații, instituții politice și democratice și infrastructuri energetice din UK;

► derularea de operațiuni cibernetice în sprijinul războiului de agresiune rus împotriva Ucrainei.

România a susținut demersul UK, prin publicarea, în aceeași zi, de către MAE român a unui comunicat care a condamnat activitățile cibernetice ostile desfășurate de unitățile GRU îndreptate împotriva mai multor state membre NATO și UE, inclusiv țara noastră.

Atribuirea publică a actorilor cibernetici este utilă pentru descurajare, setarea unor norme cibernetice, promovarea cooperării în spațiul cibernetic și creșterea rezilienței cibernetice. Prin atribuirea publică se fac cunoscuți actorii cibernetici ostili, amenințările cibernetice devin tangibile și sunt semnalate posibile metode de rezolvare a unor incidente. De asemenea, atribuirile publice reprezintă prima etapă în condamnarea și aplicarea de măsuri suplimentare, inclusiv sancțiuni economice aplicate statelor care finanțează grupările cibernetice.

APTs INTO THE CLOUD

În ultimii ani, tot mai multe entități publice/private își mută infrastructurile și resursele informaționale în cloud, datorită accesibilității, eficienței și a costurilor semnificativ mai reduse comparativ cu utilizarea unor infrastructuri informatice proprii, aspecte ce au determinat remodelarea fundamentală a peisajului amenințărilor cibernetice statale. Cu toate acestea, cloudul prezintă multiple breșe de securitate ce pot fi exploatate de grupările de tip APT (*Advanced Persistent Threat*) în cadrul operațiunilor derulate.

În acest sens, actorii cibernetici asociați/atribuiți Federației Ruse (FR) și Republicii Populare Chineze (RPC) și-au rafinat elementele de *modus operandi* și TTP-urile (tactici, tehnici și proceduri) pentru a eficientiza rata de succes a atacurilor derulate asupra infrastructurilor ce funcționează în mediul cloud.

Actorii cibernetici de sorginte rusă, în special grupări precum APT28/FANCY BEAR sau APT29/COZY BEAR, dețin resurse și capabilități consistente pe care, începând din 2019, le folosesc în manipularea și exploatarea platformelor Microsoft 365 și Azure. *Modus operandi*-ul lor nu mai vizează neapărat infectarea cu *malware* a unei stații de lucru sau a unei rețele interne, ci compromiterea conturilor de utilizator din cloud.

O tehnică utilizată intens este compromiterea cheilor de validare (*token*-uri) pentru a genera permisiuni de acces. Prin această metodă, atacatorii pot crea „legitimații de acces" false ale oricărui angajat, permițându-le să acceseze direct resursele infrastructurii ce rulează în cloud, fără a fi detectați de sistemele de securitate cibernetică. În plus, grupările APT au început să exploateze serviciile de autentificare legitime, precum OAuth, prin care solicită permisiuni pentru accesarea și copierea datelor utilizatorului, fără a fi necesară parola. Mai precis, odată ce un angajat cu drepturi de administrator este determinat să utilizeze un astfel de serviciu, atacatorii obțin acces permanent la e-mailuri și fișiere, fără a mai avea nevoie de parola victimei.

Pe de altă parte, grupările APT de sorginte chineză, cum sunt grupările APT41/Brass Typhoon sau Storm-0558, prioritizează exploatarea breșelor de securitate ale platformelor cloud concomitent cu asigurarea unui nivel cât mai ridicat de anonimizare a activităților ostile încă din anul 2023, când au fost identificate primele campanii de targetare a furnizorilor mari de servicii cloud, precum Microsoft.

O tehnică des întâlnită este exfiltrarea unor chei de semnătură electronică de nivel înalt de la furnizorii de servicii cloud, fapt care le permite atacatorilor să obțină accesul ilegitim

la conturile de e-mail ale unor oficiali din plan guvernamental, fără ca aceștia să sesizeze activitatea suspectă. O altă tehnică preferată de atacatori este utilizarea instrumentelor legitime ale platformelor cloud pentru a exfiltra date de interes. Astfel, în loc să folosească programe *malware* convenționale, care pot fi detectate cu ușurință, actorii cibernetici chinezi folosesc comenzile interne ale mediului cloud pentru a realiza *backup*-uri ale întregului volum de date stocate. Ei realizează o copie de rezervă instantanee a întregului *hard disk* virtual și o distribuie către propriile servere externe, astfel transferând volume mari de informații, fără a lăsa urme în sistemul compromis.

Atât actorii cibernetici de origine rusă, cât și cei de origine chineză profită de erorile de configurare făcute de utilizatorii legitimi. Aceștia caută în permanență conturi folosite pentru realizarea de sarcini automate, care beneficiază de permisiuni prea mari, pe care le utilizează ca punct inițial de acces pentru preluarea controlului asupra întregii infrastructuri.

Noile elemente de *modus operandi* utilizate de actorii cibernetici statali asupra mediului cloud indică o evoluție și o maturizare tehnică rapidă, adaptate la noile medii în care entitățile de interes pentru aceștia își gestionează resursele informatice și informaționale. Cu toate că mediul cloud atrage cu sine multiple beneficii din perspectivă de securitate cibernetică, acesta nu este lipsit de vulnerabilități care pot oferi atacatorilor acces la datele și informațiile de interes.

OPERAȚIUNI INTERNAȚIONALE DE DESTRUCTURARE A UNOR INFRASTRUCTURI INFORMATICE ASOCIATE CRIMINALITĂȚII CIBERNETICE ÎN 2025

În cursul anului 2025 s-a observat o intensificare semnificativă a operațiunilor coordonate ale autorităților la nivel internațional, ce au avut ca obiectiv indisponibilizarea infrastructurilor informatice utilizate de exponenții mediului *cybercrime*. Ca parte a eforturilor de cooperare transfrontalieră între organe de aplicare a legii, servicii de informații și parteneri din sectorul privat, aceste acțiuni au vizat ecosisteme complexe de tip *Cybercrime-as-a-Service* (CaaS), platforme specializate de criminalitate cibernetică, infrastructuri de comandă și control, servicii de anonimizare utilizate pentru mascarea activităților ilegale și alte instrumente/ servicii utilizate de grupările *cybercrime*.

1. SCATTERED SPIDER

La 18 septembrie 2025, autoritățile din Marea Britanie au pus sub acuzare doi membri ai grupării Scattered Spider, pentru derularea de atacuri cibernetice împotriva mai multor infrastructuri critice la nivel global.

> Scattered Spider este o grupare *cybercrime* activă din 2022, care realizează atacuri cibernetice de tip *ransomware* asupra unor organizații mari și furnizori de servicii, urmărind obținerea de beneficii materiale ilicite prin criptarea/ exfiltrarea datelor sensibile de la nivelul infrastructurilor informatice vizate. Gruparea a revendicat peste 47 de atacuri cibernetice și a obținut peste 115 milioane de dolari din răscumpărările achitate.

Operațiunea a fost susținută inclusiv de autoritățile din România, care au jucat un rol esențial în obținerea datelor despre unul dintre membrii grupării Scattered Spider. Departamentul Justiției din SUA a mulțumit public autorităților române implicate (DIICOT, BCCO Târgu-Mureș, Poliția Română) pentru contribuțiile semnificative în cadrul acestei operațiuni.

2. OPERATION TALENT

În perioada 28–30 ianuarie 2025, sub coordonarea autorităților germane și Europol, organele de aplicare a legii, inclusiv din România, au desfășurat „Operation Talent", care a vizat destructurarea forumurilor Nulled și Cracked, considerate unele dintre cele mai mari și influente comunități *cybercrime* la nivel global, care aveau împreună peste 10 milioane de utilizatori.

Platformele facilitau comercializarea de date exfiltrate, aplicații *malware*, servicii dedicate fraudelor online, acces inițial în cadrul unor sisteme informatice și alte servicii specifice CaaS.

În urma acțiunii, infrastructura informatică a forumurilor a fost preluată de autorități, fiind confiscate mai multe dispozitive, servere și domenii asociate acestora. Autoritățile implicate au anunțat arestarea a doi suspecți, inclusiv unul dintre administratorii forumului Nulled.

3. OPERATION PHOBOS AETOR

La data de 10 februarie 2025 a avut loc operațiunea internațională „Phobos Aetor", care a avut ca obiectiv destructurarea infrastructurii informatice asociate *ransomware*-ului Phobos și grupării *cybercrime* 8Base. Acțiunea a fost realizată prin cooperarea structurilor naționale de aplicare a legii din 14 țări, cu sprijinul Europol și Eurojust.

Ransomware-ul Phobos, comercializat în regim *Ransomware-as-a-Service* (RaaS), a fost utilizat de afiliați pentru derularea de atacuri cibernetice de tip *double extortion*, constând în criptarea datelor sistemelor compromise și exfiltrarea datelor sensibile în vederea exercitării de presiuni suplimentare asupra victimelor pentru a plăti răscumpărarea cerută.
În România, *malware* din familia PHOBOS a fost observat exclusiv în cazul atacurilor cibernetice derulate asupra sistemului medical: (1) compromiterea platformei Hipocrate, care a afectat activitatea a 26 de spitale din România (10-12.02.2024), (2) atac cibernetic asupra infrastructurii informatice aparținând Spitalului Clinic „CF Witting" din București (22.07.2021), (3) compromiterea infrastructurilor IT&C asociate spitalelor „Victor Babeș", București și celor din Huși, Dorohoi și Cărbunești (20.06.2019).

În urma operațiunii, autoritățile au arestat patru cetățeni ruși, implicați în administrarea și operarea *ransomware*-ului Phobos și au indisponibilizat serverele utilizate pentru atacuri și publicarea datelor exfiltrate.

Informațiile obținute în urma arestărilor au permis autorităților de aplicare a legii să avertizeze proactiv peste 400 de entități publice și private la nivel global cu privire la atacuri *ransomware* aflate în desfășurare sau iminente asupra infrastructurilor informatice ale acestora.

4. OPERATION CHECKMATE

La 24 iulie 2025, o inițiativă comună a organelor de aplicare a legii la nivel internațional, condusă de U.S. Homeland Security Investigations și susținută de entități private, inclusiv de compania autohtonă Bitdefender, a desfășurat „Operation Checkmate", care a vizat neutralizarea infrastructurii informatice a grupării *ransomware* BlackSuit.

> BlackSuit este o grupare *ransomware* activă din 2023, cunoscută anterior sub denumirile Quantum și Royal, fiind formată din foști membri ai grupării CONTI, care a fost asociată public serviciului de informații rus FSB. Gruparea a revendicat peste 180 de atacuri, obținând peste 370 de milioane de dolari din răscumpărări.

Ca urmare a operațiunii, autoritățile au sechestrat și indisponibilizat infrastructura site-urilor, preluând controlul asupra mai multor servere și domenii utilizate pentru facilitarea campaniilor *ransomware*, inclusiv pentru negocierea răscumpărărilor și publicarea victimelor/ datelor exfiltrate. O parte din activele digitale ale grupării – criptomonede estimate la peste 1 milion de dolari – au fost confiscate sau blocate pentru a diminua capacitatea operațională a BlackSuit.

5. OPERATION OLYMPIA

În perioada 24–28 noiembrie 2025, Europol, în cooperare cu autoritățile din Germania și Elveția, a derulat „Operation Olympia", vizând un serviciu de mixing de criptomonede (cryptomixer.io), utilizat pentru spălarea de fonduri ilicite provenite din atacuri cibernetice, fraude financiare și alte activități specifice mediului *cybercrime*.

> Un *crypto mixer* este un serviciu care amestecă fondurile provenite de la mai mulți utilizatori și le redistribuie către alte adrese, în tranșe și la intervale diferite, cu scopul de a afecta trasabilitatea tranzacțiilor pe *blockchain* dintre sursa inițială și destinația finală a fondurilor. În mediul *cybercrime*, aceste servicii sunt frecvent utilizate pentru a masca proveniența criptomonedelor obținute din *ransomware*, fraude online sau alte activități ilicite, îngreunând semnificativ procesul de atribuire. De la înființarea sa în 2016, cryptomixer.io a procesat peste 1.3 miliarde EUR în criptomonede.

Ca urmare a operațiunii, autoritățile au întrerupt serviciul, blocând accesul la servere și identificând principalele conturi asociate activităților ilegale, ceea ce a redus semnificativ posibilitatea spălării de fonduri pentru numeroase grupări cibernetice.

Analiza operațiunilor desfășurate în 2025 indică o intensificare a acțiunilor internaționale coordonate împotriva criminalității cibernetice, cu rezultate concrete în destructurarea infrastructurilor informatice asociate *malware*-urilor, platformelor *cybercrime* specializate și serviciilor/ instrumentelor subsumate *Cybercrime-as-a-Service*. Operațiunile au permis reducerea capacității operaționale a mai multor grupări *cybercrime*, identificarea și arestarea unor operatori cheie, precum și întreruperea fluxurilor financiare ilegale, concretizându-se într-un factor esențial pentru descurajarea acestor activități ilegale.

DE LA DDOS LA INFLUENȚĂ STRATEGICĂ: PROFILUL OPERAȚIONAL AL NoNAME057(16)

În ultimii ani, activitatea entităților hacktiviste proruse a cunoscut o intensificare semnificativă, iar în acest context, NoName057(16) a devenit una dintre cele mai influente grupări motivate ideologic.

NoName057(16) este o grupare hacktivistă activă încă din martie 2022, imediat după invazia rusă în Ucraina. Aceasta derulează atacuri cibernetice, în special de tip Distributed Denial of Service/DDoS, iar motivația grupării este centrată pe factori politici și ideologici, acționând în sprijinul intereselor geopolitice ale Federației Ruse.

Gruparea a revendicat atacuri asupra website-urilor guvernamentale, instituțiilor media, companiilor private și structurilor critice din state membre NATO și UE, în special pe fondul sprijinului oferit Ucrainei.

NoName057(16) își coordonează activitatea prin canale de Telegram, la nivelul cărora revendică atacurile și gestionează proiecte ostile precum DDoSia.

> DDoSIA este o platformă distribuită de atac, destinată coordonării acțiunilor cibernetice la scară largă. Proiectul permite implicarea unui număr ridicat de participanți care, prin instalarea unei aplicații dedicate, contribuie cu resurse de calcul la generarea traficului necesar indisponibilizării temporare a infrastructurilor vizate.

Proiectul a fost utilizat în campanii susținute împotriva instituțiilor guvernamentale, serviciilor publice și entităților private din state care nu se aliniază intereselor Federației Ruse, devenind un exemplu relevant de activism în spațiul cibernetic. Atacurile lansate de grupare sunt prezentate drept forme de protest politic și represalii cibernetice, indicând folosirea spațiului cibernetic ca o extensie a confruntării militare.

Industria de securitate cibernetică consideră că, la nivel internațional, NoName057(16) desfășoară una dintre cele mai persistente activități din sfera hacktivistă, gruparea fiind implicată în mii de atacuri *DDoS*, ale căror impact variază de la perturbări temporare ale serviciilor online până la blocări extinse ale accesului populației la paginile web vizate.

Gruparea a desfășurat atacuri de tip *DDoS* care au coincis cu perioade electorale sau alte evenimente sociale de interes major în mai multe state europene, precum Republica

Cehă, Belgia, Suedia și România. Aceste atacuri au vizat în principal *website*-uri ale autorităților electorale, instituțiilor publice și actorilor politici, fără a avea capacitatea de a compromite integritatea sistemelor de vot.

Aceste acțiuni derulate la nivel global reflectă natura repetitivă și geopolitică a atacurilor, sens în care, activitatea grupării a impus reacții coordonate din partea autorităților europene. Astfel, în iulie 2025, Europol și Eurojust au coordonat operațiunea internațională „Eastwood", ce a vizat destructurarea NoName057(16). Autorități judiciare și de aplicare a legii din 11 țări europene și SUA au desfășurat acțiuni simultane împotriva infrastructurii asociate grupării. Ca urmare, au fost scoase din uz peste 100 de servere utilizate de grupare și au fost emise mandate de arestare pentru membrii acesteia. În contextul extinderii conflictelor globale în spațiul cibernetic, operațiunea a marcat reușite semnificative în combaterea atacurilor cibernetice la nivel internațional.

De asemenea, în contextul „Eastwood" au fost evidențiate legături ale membrilor grupării cu organizația guvernamentală *Centre for the Study and Network Monitoring of the Youth Environment/CISM*, subordonată direct Administrației Prezidențiale de la Kremlin.

> CISM este o organizație responsabilă pentru monitorizarea mediului online, în scopul „protejării" tinerilor ruși.

Prin activitățile derulate de gruparea hacktivistă NoName057(16) și existența conexiunilor membrilor cu aparatul de stat rus este relevată tranziția de la hacktivismul simbolic la utilizarea capabilităților deținute pentru atingerea unor scopuri geopolitice.

AMENINȚĂRI LA ADRESA SPAȚIULUI INFORMAȚIONAL LA NIVEL EUROPEAN

Începând cu 2020, spațiul informațional european a fost marcat de o serie de evenimente, precum pandemia de COVID-19 și declanșarea conflictului din Ucraina, care au restructurat viața economică și socială, redefinind contextul geopolitic. Acestea au condus la normalizarea unui climat de volatilitate socială și politică și au creat un mediu informațional fragmentat, în care nemulțumirile populației sunt instrumentalizate sistemic.

Actori ostili intereselor naționale și comunitare pot exploata aceste tensiuni prin campanii de tip *Foreign Information Manipulation and Interference* (FIMI) cu scopul intensificării polarizării și a diviziunilor sociale și politice, atât în interiorul Uniunii Europene, cât și în afara acesteia.

Conform *European Union External Action* (EEAS), FIMI desemnează un tipar de comportament care, deși, în majoritatea cazurilor, nu este ilegal, reprezintă o amenințare sau are potențialul de a afecta negativ valorile fundamentale, capacitatea instituțională și procesele decizionale. Astfel de campanii sunt caracterizate de un grad ridicat de manipulare, fiind desfășurate în mod coordonat, și au ca obiectiv subminarea poziției internaționale a Uniunii Europene, precum și diminuarea capacității acesteia de a-și promova interesele și obiectivele de politică publică.

Prin proliferarea dezinformării, a conținutului fals generat în mod automatizat și prin crearea unor bule informaționale, se accentuează clivajele sociale, cu efecte precum: subminarea coeziunii comunitare, erodarea încrederii în instituțiile publice și promovarea unor agende politice situate la marginea consensului democratic.

În ultima perioadă, se remarcă implicarea în derularea sau susținerea unor astfel de operațiuni informaționale de către entități statale, narativele de dezinformare și conspiraționiste devenind complementare cu retorica oficială a statelor, acest lucru fiind observat pe parcursul anului 2025 inclusiv în contextul scrutinelor electorale din Germania, Polonia, România, Republica Cehă sau Republica Moldova.

Operațiunile informaționale derulate în aceste state întrunesc elemente de *modus operandi* comune, atât din perspectiva TTP-urilor utilizate, cât și a narativelor promovate în mediul online.

ELEMENTE COMUNE DE MODUS OPERANDI LA NIVEL EUROPEAN

În ceea ce privește TTP-urile utilizate de actori toxici în vederea manipulării și/sau intoxicării spațiului informațional european au fost identificate similarități pe următoarele coordonate:

► Clonarea site-urilor ce aparțin unor surse legitime de informare, prin asumarea identității vizuale, structurii și numelui trusturilor media cunoscute, cu scopul distribuirii de știri false prin intermediul acestora și manipulării opiniei publice;

> În acest sens, cea mai relevantă operațiune a fost *Doppelgänger*, atribuită în mod public de Franța și Statele Unite ale Americii către entități din Federația Rusă, observată în contextele electorale din 2025 în state precum Germania, Republica Moldova, Polonia.

► Operaționalizarea unor rețele de site-uri dedicate producerii, replicării și (re) distribuirii de conținut propagandistic, cu scopul modelării mediului informațional într-o manieră favorabilă unor interese ostile, respectiv normalizării unor narative recurente;

> În 2025, cea mai activă rețea la nivel internațional a fost Pravda (cunoscută inclusiv sub denumirea de *Portal Kombat*), descrisă de VIGINUM drept o rețea de dezinformare cu orientare prorusă. Modul de operare al acesteia presupune distribuirea descentralizată a aceloraşi narative și știri false, prin adaptarea minimă a conținutului la contextul local (inclusiv prin traducerea unor articole și/sau transmiterea de știri false cu privire la evenimente sociale la nivel național), respectiv amplificarea știrilor false prin intermediul *social media*. Rețeaua activează în 19 state europene, fiind activă inclusiv în Germania, Republica Cehă, Republica Moldova, România și Polonia.

► Manipularea algoritmilor platformelor de social media prin utilizarea unor rețele de conturi neautentice coordonate, în special cu scopul creșterii vizibilității unui conținut, fapt ce contravine politicilor stabilite de platforme;

> Rețelele de conturi care prezentau comportamente neautentice coordonate au fost instrumentalizate diferit la nivel european, modul de operare fiind adoptat în funcție de specificul țărilor cu privire la utilizarea celor mai populare rețele sociale.

► Utilizarea inteligenței artificiale (IA) pentru generarea de conținut fals sau distorsionat, inclusiv în presupuse articole de știri sau pentru a crea aparența unor persoane reale.

> Acest mod de operare a cunoscut o amplificare exponențială odată cu creșterea diversității și disponibilității, la nivelul publicului larg, a instrumentelor bazate pe IA care creează automat conținut digital, în special a celor dedicate creării de materiale foto/video. Astfel de instrumente au fost utilizate la scară largă inclusiv în contextele electorale din Germania, România, Republica Moldova, Polonia și Republica Cehă.

ELEMENTE COMUNE DE MODUS OPERANDI LA NIVEL EUROPEAN

În contextul proceselor electorale recente la nivel european s-a observat o recurență a unor narative/ teme diseminate în spațiul public cu scopul de a manipula opinia publică și de a promova interese anti-occidentale, conspiraționiste și proruse adaptate specificului fiecărui stat:

► Promovarea curentului eurosceptic – au urmat un tipar discursiv convergent în care Uniunea Europeană a fost acuzată de subminarea suveranității și/sau a valorilor naționale ale statelor membre/candidate. Tema s-a remarcat preponderent în Republica Moldova, Polonia, Republica Cehă sau România, unde actorii informaționali ostili au pretins că instituțiile europene au interferat în procesele electorale atunci când rezultatele nu au fost favorabile intereselor acestora.

► Contestarea solidarității transnaționale față de Ucraina – au fost lansate idei conform cărora: (1) refugiații ucraineni exploatează sistemele de asistență socială; (2) refugiații ucraineni sunt membri ai mafiei; (3) familia Zelensky are un stil de viață luxos.

► Subminarea încrederii în instituțiile naționale – s-a manifestat printr-un set de teme care susțineau următoarele: (1) guvernele și elitele politice sunt slabe; (2) guvernele vor frauda/manipula alegerile; (3) guvernele nu servesc interesele cetățenilor sau sunt subordonate intereselor străine; (4) politicienii lucrează în interes personal. Suplimentar, au fost aduse acuzații false la adresa liderilor.

► Contestarea integrității electorale – narativul a fost adaptat la contextele naționale având scopul de a submina încrederea societății în mecanismele democratice și de a descuraja prezența la vot prin inducerea sentimentului de inutilitate a procesului electoral: (1) în Germania au fost propagate informații despre nesiguranța votului prin corespondență; (2) în Republica Moldova au fost diseminate informații privind ilegitimitatea votului diasporei; (3) în Republica Cehă serviciile de informații au fost acuzate de favoritism politic; (4) în Polonia au fost distribuite mesaje care invocau riscul unor atacuri teroriste la urne; (5) iar în România au circulat sfaturi înșelătoare privind buletinele de vot și modul de imprimare al ștampilei pe acestea.

CONCLUZIE

Spațiul informațional european se confruntă cu o normalizare a unui climat volatil în care nemulțumirile înregistrate la nivel societal sunt instrumentalizate de actori externi ostili și integrate într-un cadru operațional suficient de flexibil pentru a fi calibrat la specificul fiecărui stat. Recurența unor mecanisme similare aplicate în contexte electorale diferite relevă o arhitectură informațională bine organizată ce urmărește degradarea progresivă a rezilienței democratice și a coeziunii sociale în interiorul Uniunii Europene.

Eficiența operațiunilor FIMI constă în convergența dintre infrastructura tehnologică, narațiunile cu grad ridicat de adaptabilitate în funcție de contextul social al fiecărui stat și o strategie de creștere a vizibilității. Narativele identificate funcționează ca multiplicatori de neîncredere, generând sentimente de incertitudine și anxietate. Astfel, acest tip de amenințări ce se înscriu în sfera hibridă necesită o abordare integrată la nivel european, bazată pe anticipare și descurajare, concomitent cu eforturi susținute de consolidare a culturii de securitate și de creștere a nivelului de alfabetizare media.

ÎNFIINȚAREA UNUI SOC ÎN DOMENIUL SĂNĂTĂȚII

La nivelul lunii decembrie 2024, Ministerul Sănătății a emis Ordinul nr. 5933, cu scopul de a include printre investițiile finanțate prin intermediul Planului Național de Redresare și Reziliență (PNRR) proiectul unei platforme naționale pentru securitate cibernetică în domeniul sănătății – un *Security Operations Center* (SOC), care să deservească cele mai importante unități spitalicești la nivel național, ce vor fi selectate pe baza numărului de pacienți tratați și a importanței la nivel regional.

Această structură vine în întâmpinarea necesităților crescute privind asigurarea securității cibernetice, ridicate atât de investițiile realizate prin PNRR în domeniul digitalizării și retehnologizării sectorului sănătății, cât și de avansul tehnologic intens al industriei TIC din ultimii ani.

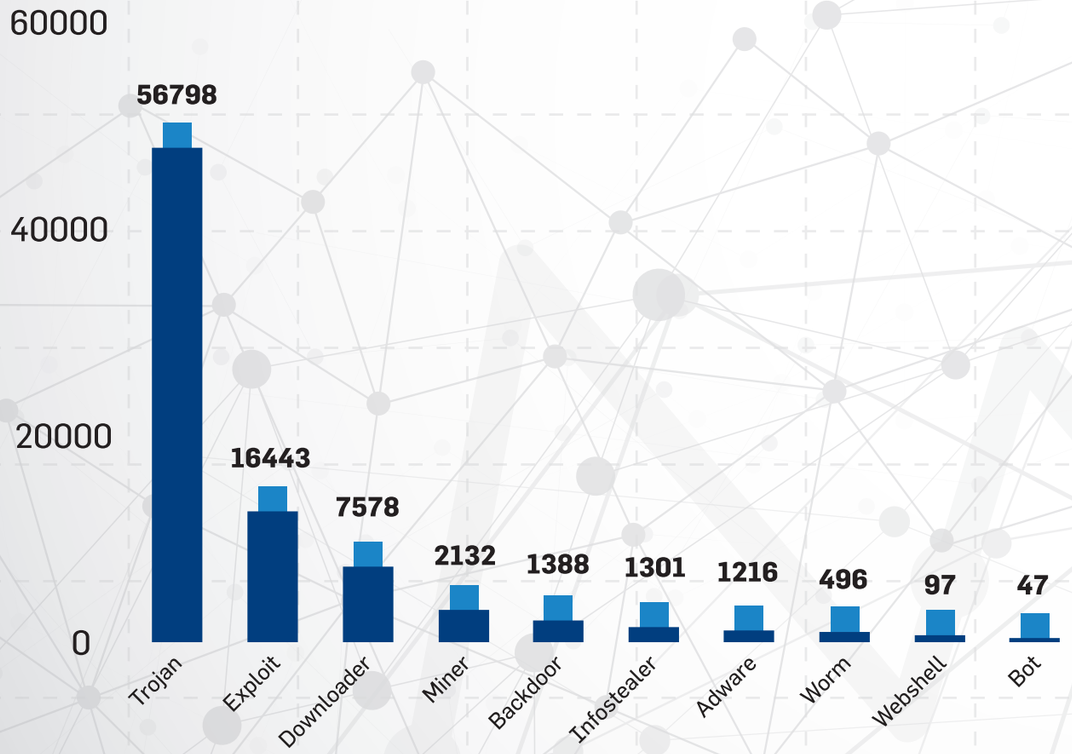
> Un SOC este o structură specializată al cărei obiectiv este monitorizarea continuă a unei anumite infrastructuri IT, cu scopul detectării și analizării oricăror incidente de securitate cibernetică și asigurării unor răspunsuri imediate cu privire la potențiale amenințări cibernetice. Alături de aceste funcții, un SOC asigură, de asemenea, și funcțiile de Threat Hunting – caută proactiv amenințări ascunse în rețea, și de vulnerability assessment – identificarea și remedierea continuă a vulnerabilităților de securitate cibernetică ale infrastructurii pe care o deservește.

Proiectul acestui SOC include investiții suplimentare pentru achiziționarea și instalarea de echipamente *hardware*, identificarea și achiziționarea/ dezvoltarea de soluții *software* de securitate cibernetică adaptate specificului și realităților sistemului de sănătate din România, recrutarea de personal calificat pentru această activitate (și remunerarea sa la standardele pieței), dar și identificarea unui spațiu fizic care să găzduiască structura.

De la momentul decembrie 2024, Ministerul Sănătății a susținut permanent desfășurarea proiectului, existând toate premisele implementării sale cu succes înainte de finalizarea oficială a PNRR, de la sfârșitul lunii august a acestui an.

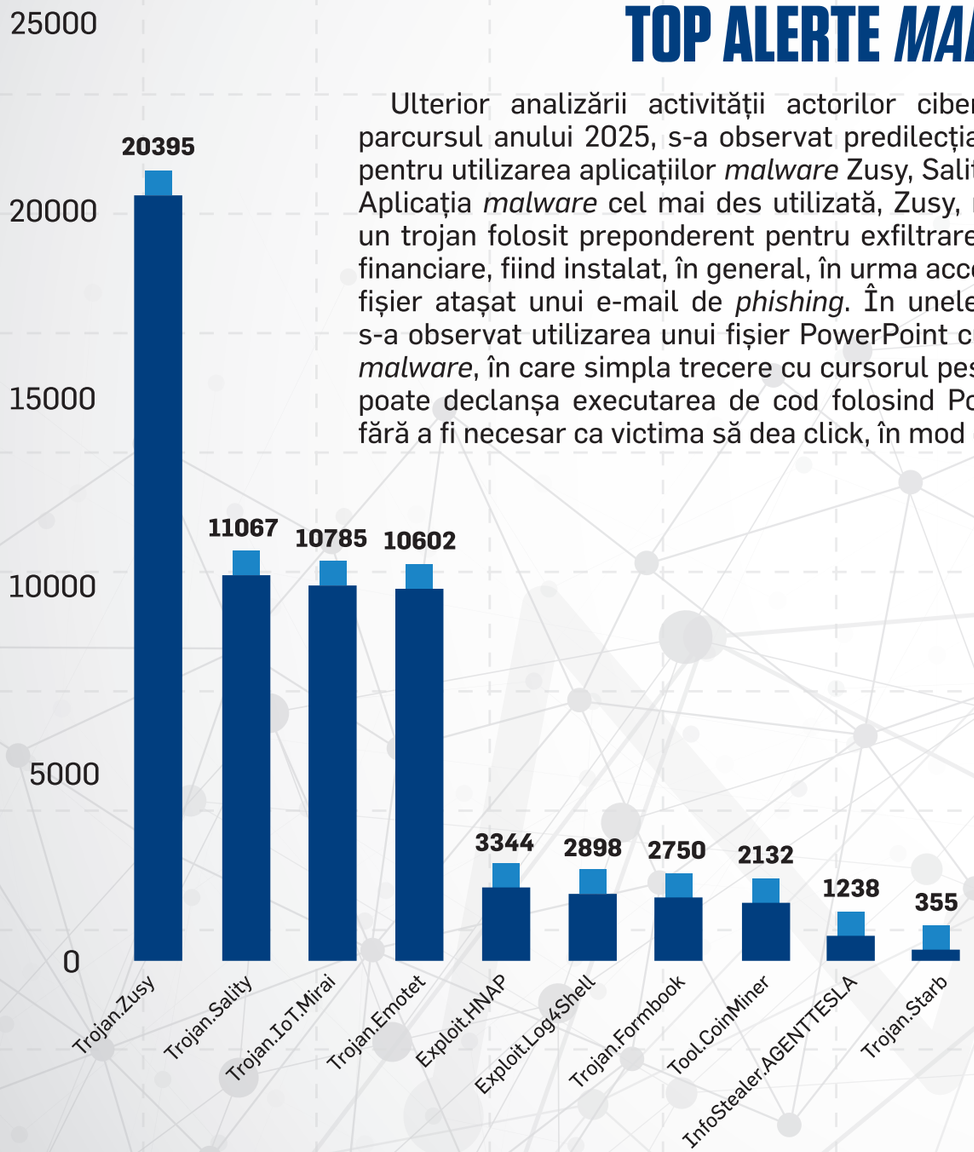
CELE MAI UTILIZATE TIPURI DE APLICAȚII *MALWARE*

Conform alertelor generate de Sistemul național de protecție a infrastructurilor IT&C de interes național împotriva amenințărilor provenite din spațiul cibernetic (Țițeica) pe parcursul anului 2025, aplicațiile *malware* de tip Trojan și Exploit au fost cele mai utilizate de actorii cibernetici care au vizat compromiterea infrastructurilor informatice și de comunicații de interes național.

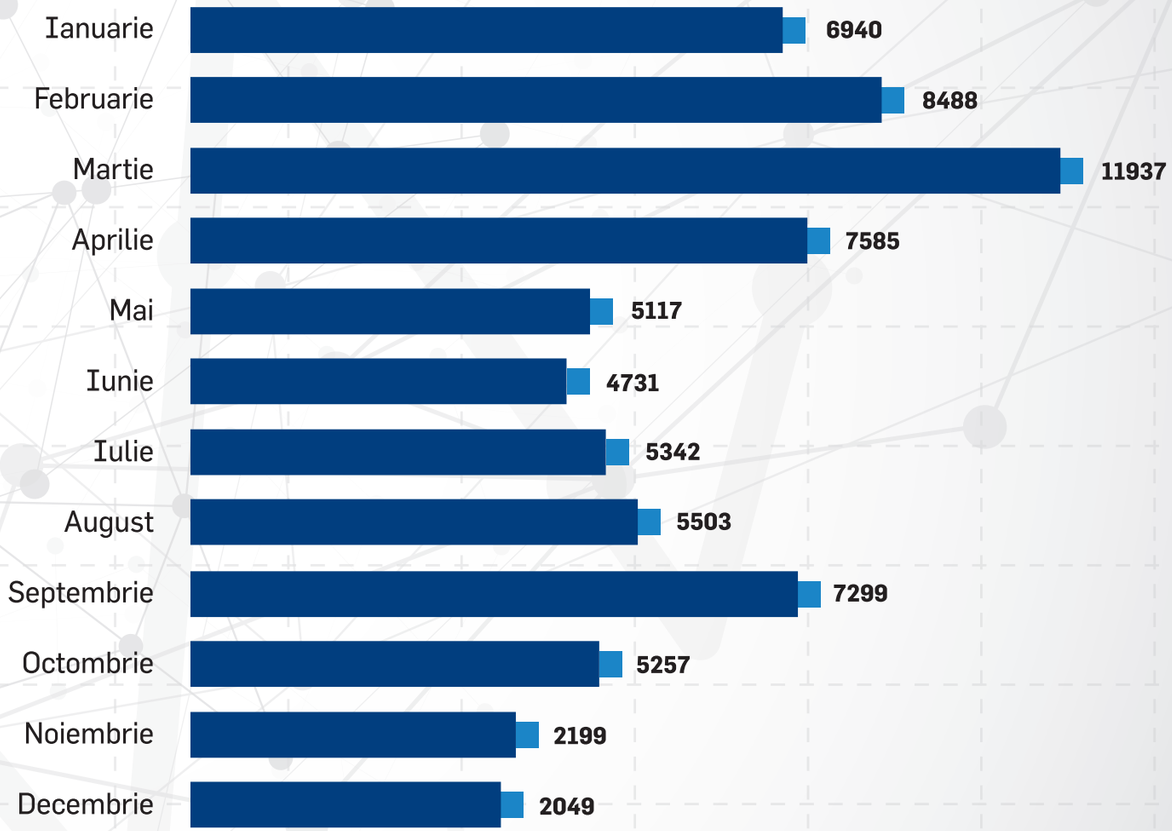


TOP ALERTE *MALWARE*

Ulterior analizării activității actorilor cibernetici pe parcursul anului 2025, s-a observat predilecția acestora pentru utilizarea aplicațiilor *malware* Zusy, Sality și Mirai. Aplicația *malware* cel mai des utilizată, Zusy, reprezintă un trojan folosit preponderent pentru exfiltrarea de date financiare, fiind instalat, în general, în urma accesării unui fișier atașat unui e-mail de *phishing*. În unele instanțe, s-a observat utilizarea unui fișier PowerPoint cu conținut *malware*, în care simpla trecere cu cursorul peste un link poate declanșa executarea de cod folosind PowerShell, fără a fi necesar ca victima să dea click, în mod explicit.

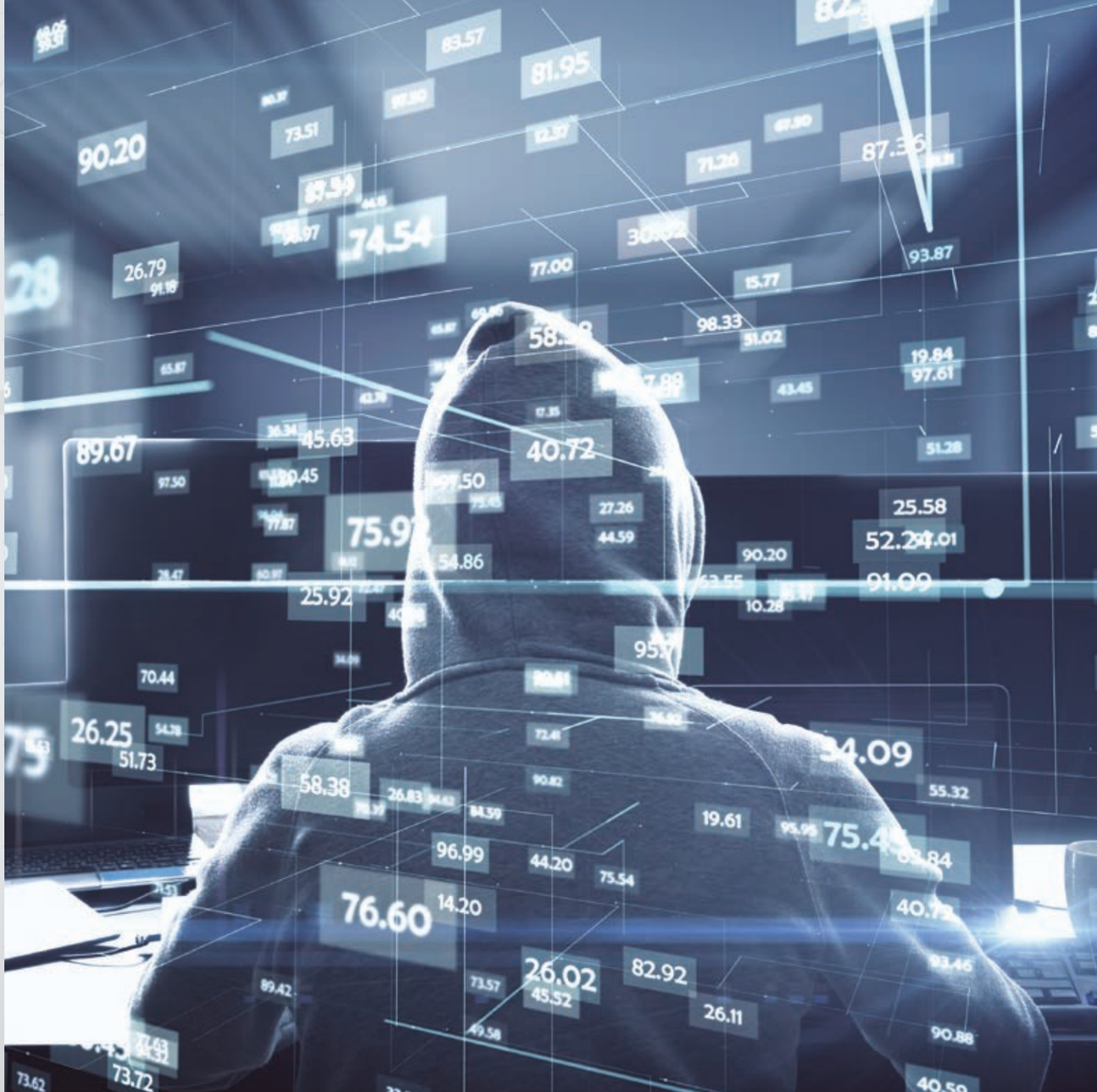


FRECVENȚA LUNARĂ A ACTIVITĂȚILOR DE *PHISHING*



Principala metodă prin care actorii cibernetici au încercat obținerea accesului inițial în 2025 a fost derularea campaniilor de *phishing*. Frecvența acestor campanii se menține pe un trend ascendent, cu o activitate mai intensă în prima parte a anului ce se diminuează pe parcursul lunilor de vară și ulterior atinge cel mai scăzut nivel în luna decembrie.

Acest tipar este similar celor observate în anii anteriori.



DIGITAL OMNIBUS – NORME DIGITALE MAI SIMPLE, ECONOMII DE MILIARDE DE EURO ȘI STIMULAREA INOVĂRII

Digital Omnibus reprezintă o propunere a Comisiei Europene de a simplifica legislația Uniunii Europene (UE) prin adoptarea unor amendamente la adresa actelor normative care reglementează securitatea cibernetică, inteligența artificială și circulația datelor.

Principalele beneficii sunt (1) simplificarea cadrului normativ pentru eliminarea suprapunerilor din reglementările aflate în aplicare; (2) stimularea competitivității și inovației, însă fără a compromite norme fundamentale privind datele personale și drepturile cetățenilor și (3) reducerea efortului administrativ pentru companii și autorități – aspecte aflate în concordanță cu obiectivele asumate de Ursula von der Leyen și rapoartele emise de Mario Draghi și Enrico Letta.

În măsura în care se va reuși implementarea sa completă până în 2027, pachetul de măsuri va genera economii de aproximativ 5 miliarde de EUR pentru companii și 1 miliard de EUR pentru autoritățile publice, până la finalul mandatului Comisiei Europene din 2029.

Concret, Digital Omnibus modifică următoarele:

1. DATA ACT (secțiunea 1.1)

În prezent, în UE există trei legi care reglementează circulația datelor: *Free Flow of Non-Personal Data Regulation* (FFDR), *Data Governance Act* (DGA) și *Open Data Directive* (ODD). Deși, sunt acte normative distincte, acestea nu interacționează coerent și au suprapuneri de prevederi.

Principala problemă resimțită prin acest *status-quo* este confuzia generată de suprapunerile reglementărilor. Printre entitățile afectate se regăsesc și IMM-urile, care reclamă costuri mari pentru a atinge standardele de conformitate și efort administrativ crescut.

Propunerea Digital Omnibus vizează crearea Data Act, sub forma unui singur set de reguli și a unei proceduri unitare de acces la date.

2. GDPR (secțiunea 1.2)

În prezent, normele impun notificarea fiecărei persoane ale cărei date personale sunt procesate, indiferent de nivelul de risc. Totodată, GDPR reglementează definiția și portabilitatea doar a datelor cu caracter personal, fără a le include pe cele non-personale sau provenite din „*Internet of Things*".

Inițiatorii proiectului au argumentat necesitatea adoptării Digital Omnibus pentru eliminarea dificultăților reclamate precum efortul administrativ ridicat și risipa de resurse, generate de caracterul repetitiv al informărilor transmise manual către fiecare persoană.

Propunerea Digital Omnibus elimină notificările pentru prelucrări de rutină, pe care le înlocuiește cu notificări automate și obligatorii în situații cu risc ridicat, ce implică date personale sau cu un impact crescut asupra individului. Conform inițiativelor stipulate în noul proiect, operatorii vor continua să notifice autoritățile pentru situațiile cu probabilitate ridicată de a afecta drepturile persoanelor, însă se va operaționaliza un mecanism unic de raportare, evitând dublarea raportărilor.

3. COOKIES + ePRIVACY (secțiunea 1.3)

În prezent, accesarea celor mai multe *website*-uri presupune acceptarea unui număr crescut de „*cookies*" (fișiere pe care website-urile le salvează pe dispozitivul utilizatorului pentru a îmbunătăți experiența și pentru urmărirea activității sale în scop de marketing), fapt ce s-a transpus în apăsarea butonului de „*Accept cookies*" în mod mecanic, fără a evalua informațiile prezentate.

Digital Omnibus susține că normele actuale au alterat dezideratul inițial al bannerelor *cookie*, de a obține consimțământul liber și informat al utilizatorilor, și l-au transformat într-o formalitate („*consent fatigue*"). Ca soluție, documentul propune modificarea conținutului *cookies*-urilor și simplificarea procesului de acceptare a acestora prin setări centralizate ale *browser*-ului de internet sau ale aplicației.

4. INCIDENT REPORTING (secțiunea 2)

În prezent, companiile raportează incidentele prin multiple canale separate: NIS2 (securitate cibernetică), GDPR (protecția datelor), DORA (reziliență operațională), eIDAS (identitate digitală) și CER (entități critice).

Astfel, nu de puține ori apare necesitatea raportării aceluiași incident către mai multe autorități, cu termene și *template*-uri diferite. Principalele dificultăți generate de aceste situații sunt cele de procesare și prelucrare, resimțite de autorități, mai ales în situații de criză.

Digital Omnibus propune introducerea unui mecanism de raportare unic prin crearea *Single-Entry Point* (SEP), un portal european administrat de ENISA. Concret, o companie se conectează o dată, la un singur portal, raportează o dată, într-un format standardizat, iar notificarea ajunge la autoritățile relevante.

5. ARTIFICIAL INTELLIGENCE (AI) ACT (secțiunea 3)

În prezent, companiile reclamă dificultăți în a aplica AI Act din cauza lipsei unor standarde tehnice de implementare, precum explicarea rolurilor actorilor, dar și din cauza incertitudinii în ceea ce privește interacțiunea AI Act cu alte legi, în special Data Act.

Digital Omnibus implementează modificări ce facilitează aplicarea corectă, uniformă și alinierea AI Act cu restul reglementărilor. Modificările vizează simplificarea sarcinilor pentru companii, ca efect al elaborării unor ghiduri de aplicare coerentă.

6. PLATFORM-TO-BUSINESS (P2B) REGULATION (secțiunea 4)

Regulamentul (UE) 2019/1150 (P2B), care reglementează relația dintre platforme online și comercianți, a devenit parțial depășit și se suprapune cu cadre mai noi precum *Digital Markets Act* (DMA) și *Digital Services Act* (DSA). În anul 2019, nu erau în atenția centrală aspecte precum accesul la datele comercianților, transparența algoritmilor utilizați și auditarea acestora sau publicarea costurilor legate de publicitatea online, aspecte care, recent, s-a dovedit că necesită reglementare.

Digital Omnibus propune abrogarea P2B, fiind deja în mare măsură acoperit de DMA și DSA într-o notă mai actuală și cuprinzătoare, în special în ceea ce privește provocările privind transparența și echitatea în relația dintre platforme și comercianți.

Toate actele prezentate reglementează domenii aflate într-o dinamică crescută, marcate de evoluții tehnologice rapide, care solicită un răspuns la fel de prompt din partea autorităților responsabile de legiferarea acestora. Astfel, timpul avut la dispoziție pentru evaluarea măsurilor este redus, situație ce poate avea ca efect reglementări stricte care pot inhiba dezvoltarea în domeniu, din aceste considerente uneori fiind necesară perfecționarea și uniformizarea actelor, pentru a acoperi în întregime noile provocări generate de progresul tehnologic.

VULNERABILITĂȚILE DISPOZITIVELOR MOBILE, FUNCȚIONALITĂȚILE UNUI MALWARE ȘI METODE DE APĂRARE RECOMANDATE PENTRU UTILIZATORI

În epoca digitală actuală, dispozitivele mobile au evoluat din simple gadgeturi de consum în hub-uri digitale, precum: portofele de plată, instrumente de autentificare, platforme de comunicare, având un rol important inclusiv în infrastructurile organizaționale. Însă, această transformare funcțională a atras atenția actorilor rău intenționați și a făcut din dispozitivele mobile ținta predilectă de atac în peisajul amenințărilor cibernetice.

Conform raportului ENISA Threat Landscape 2025, dispozitivele mobile reprezintă o suprafață semnificativă de expunere la amenințările cibernetice desfășurate la nivel global. Datele din raport arată că amenințările mobile reprezintă 42,4% din totalul înregistrat, fapt care evidențiază rolul central al acestora în arhitectura generală a riscurilor. De asemenea, raportul evidențiază faptul că exploatarea vulnerabilităților continuă să fie modul principal de acces inițial, responsabil pentru 21,3% dintre cazurile de intruziune.

Sistemele de operare ale dispozitivelor mobile sunt complexe, integrate cu numeroase componente *software* și împart interfețe comune cu multiple aplicații. Această complexitate generează inevitabil puncte slabe: mecanisme privind permisiunile acordate, erori de logică provenite din greșeli în scrierea limbajului de programare și implementări defectuoase de *Aplication Programming Interface*.

Exploatarea acestora permite atacatorilor să obțină controlul asupra dispozitivului, să extragă date confidențiale sau să compromită sistemele.

Pentru a înțelege mai bine riscurile la care utilizatorii sunt expuși, vom lua ca exemplu capabilitățile *malware*-ului Rafel RAT, utilizat în 120 de campanii extinse prin care a afectat dispozitivele mobile care rulează sistemul de operare Android.

Prin funcționalitățile Rafel RAT, atacatorii pot accesa, modifica sau exfiltra date precum: contacte din agenda telefonică, mesaje SMS, jurnalul apelurilor telefonice, mesajele de tip *Two Factor Authentification* (2FA), dar și informații despre dispozitiv precum: modelul,

memoria RAM, operatorul de telefonie mobilă, țara, limba, locația live a dispozitivului și starea bateriei. De asemenea, atacatorul poate obține privilegii de administrator asupra dispozitivului, fiind astfel capabil să cripteze datele stocate pe acesta, urmând să solicite recompense în schimbul cheii de decriptare. Pentru intimidarea utilizatorului pot fi folosite tactici de distragere prin redarea unor mesaje vocale. Totodată, pentru a preveni dezinstalarea *malware*-ului, atacatorul are posibilitatea de a modifica parola de acces și poate bloca ecranul gadgetului, oprind încercările de intervenție ale unui utilizator care deține cunoștințe de bază privind utilizarea unui dispozitiv mobil.

Toate aceste elemente arată nivelul de complexitate a malware-urilor și plaja extinsă a posibilităților de acțiune ale atacatorilor în cadrul sistemelor informatice.

Exemple de practici fundamentale esențiale pentru securitatea dispozitivelor mobile:

1. ACTUALIZĂRI PERIODICE ALE SISTEMULUI DE OPERARE ȘI APLICAȚIILOR

Una dintre cele mai eficiente măsuri de protecție este efectuarea actualizărilor la ultima versiune oferită de dezvoltator a sistemului de operare și a aplicațiilor instalate.

Producătorii de dispozitive și dezvoltatorii de software lansează în mod regulat patch-uri de securitate care remediază vulnerabilitățile cunoscute. Acestea elimină vulnerabilitățile exploatate de malware sau de instrumente automatizate folosite de atacatori și reduc semnificativ posibilitatea compromiterii dispozitivului.

2. DESCĂRCAREA APLICAȚIILOR DOAR DIN SURSE DE ÎNCREDERE

Instalarea aplicațiilor trebuie realizată exclusiv din magazine oficiale, precum Google Play sau Apple App Store, unde procesele de verificare sunt stricte. Sursele neoficiale sau APK-urile descărcate din surse nesigure reprezintă o poartă de intrare pentru *malware*-urile care imită aplicații legitime.

3. SOLUȚII DE SECURITATE MOBILE ȘI MONITORIZARE

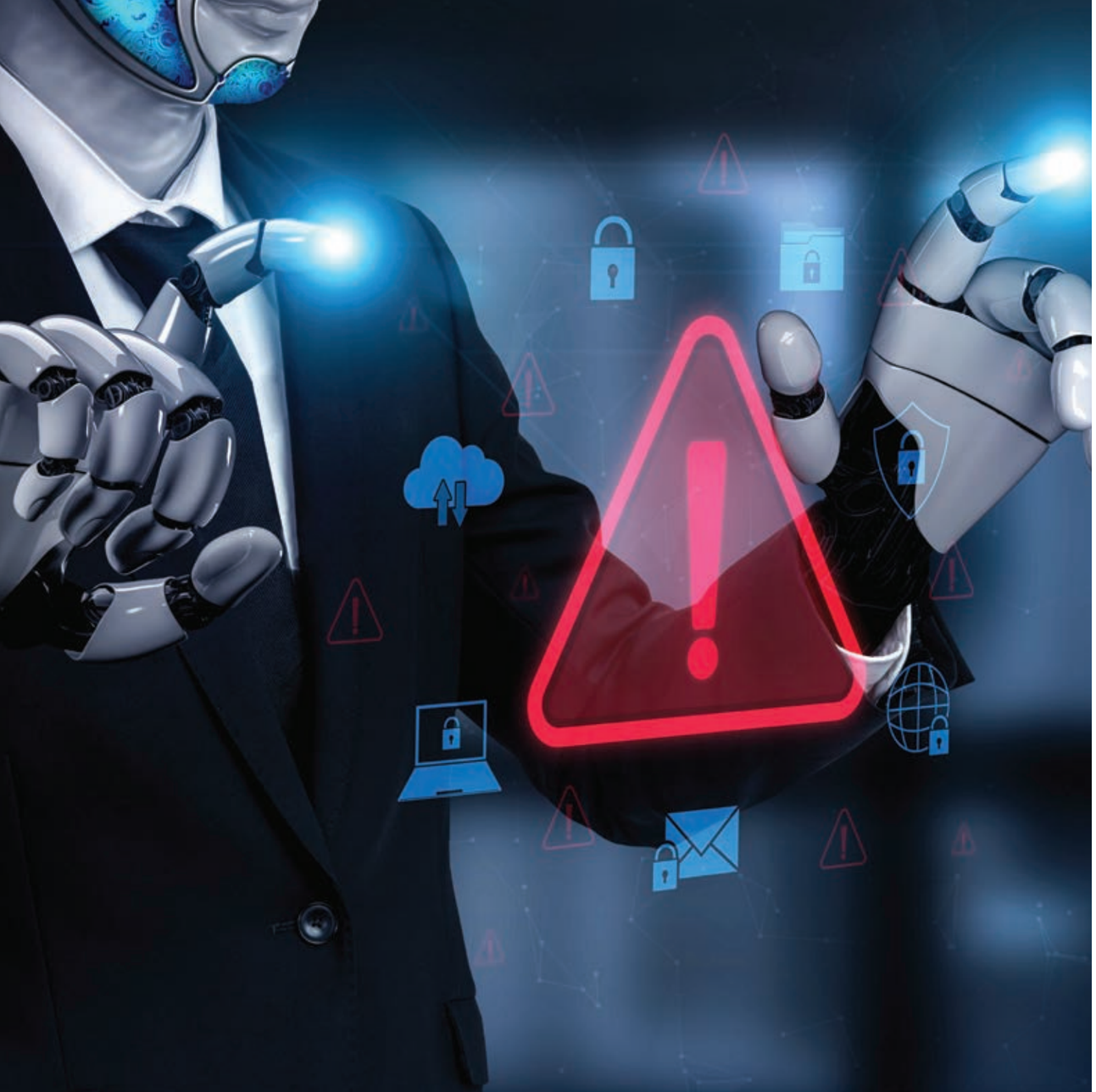
Implementarea unor soluții dedicate de securitate mobilă (*Mobile Threat Defense*) și integrarea acestora în programele de gestionare a dispozitivelor mobile (*Mobile Device Management* – MDM) oferă vizibilitate și protecție împotriva comportamentelor suspecte, detectând și blocând *malware*-ul înainte ca acesta să devină activ.

4. PERMISIUNI MINIMALE ȘI REVIZUIREA REGULATĂ A SETĂRILOR

Aplicațiile nu ar trebui să solicite mai multe permisiuni decât sunt strict necesare pentru funcționarea lor. Atunci când o aplicație solicită acces la SMS-uri, apeluri, contacte sau funcții suplimentare, utilizatorul trebuie să evalueze dacă această cerere este justificată și să refuze permisiunile excesive.

5. AUTENTIFICARE MULTIFACTOR (MFA)

MFA adaugă un nivel suplimentar de securitate care poate proteja conturile chiar dacă credențialele sau codurile de autentificare de tip SMS sunt compromise de un malware. Utilizarea unei aplicații de autentificare sau a unui token hardware oferă o funcție suplimentară de securitate, fiind mai dificil de evitat.



INTELIGENȚA ARTIFICIALĂ ȘI AMPLIFICAREA AMENINȚĂRILOR CIBERNETICE

În spațiul cibernetic, soluțiile de Inteligență Artificială (IA) au îmbunătățit exponențial tehnicile de inginerie socială utilizate în campaniile de *phishing/ spearphishing/ vishing* sau *smishing*, amplificând și mai mult impactul acestor amenințări cibernetice. De asemenea, IA generativă a fost exploatată pentru dezvoltarea aplicațiilor *software* de tip *malware*, în special prin folosirea soluțiilor IA pentru automatizarea și scalarea procesului de scriere a codului *malware*, rafinarea capabilităților aplicațiilor *malware* și creșterea eficienței în dezvoltarea scripturilor de atac.

UTILIZAREA SOLUȚIILOR IA PENTRU RAFINAREA ATACURILOR DE TIP PHISHING/ SPEARPHISHING

Folosind modele antrenate pe seturi mari de date lingvistice, IA poate genera conținut care este atât corect din punct de vedere gramatical, cât și din punct de vedere contextual. Acest lucru elimină indicatorii obișnuiți ai campaniilor de înșelătorie, cum ar fi greșelile de ortografie sau formularea atipică, care în mod obișnuit ar ridica suspiciuni. În plus, IA poate genera mesaje de *phishing* personalizate pe baza informațiilor colectate de pe platformele sociale, din bazele de date publice sau din breșe de securitate publicate, sporind credibilitatea mesajelor de *phishing/ spearphishing*. IA poate genera mesaje adaptate pentru fiecare victimă în parte, scrise într-un anumit ton sau folosind expresii specifice unui anumit domeniu (oficial, corporativ, IT etc.), făcând mult mai dificilă diferențierea între mesajele legitime și cele frauduloase.

Un alt avantaj semnificativ al utilizării AI în campaniile de *phishing* este capacitatea sa de a automatiza întregul proces de generare, trimitere și gestionare a e-mailurilor de *phishing* la scară mare. Această automatizare facilitează accesul infractorilor cibernetici la un număr semnificativ de victime potențiale, fără intervenție manuală.

INTENSIFICAREA ATACURILOR DE TIP VISHING PRIN CLONAREA VOCII APELANTULUI

IA generativă este, de asemenea, utilizată de actori cibernetici pentru a crea clone vocale realiste, care imită aproape perfect vocea unor persoane de încredere pentru victime, cum ar fi membrii familiei, colegii de muncă sau reprezentanți ai autorităților. Folosind modele avansate de *speech synthesis*, atacatorii pot genera conversații personalizate, dinamice, care sună natural și se adaptează pe baza răspunsurilor victimei. IA permite interacțiunea în timp real, în ambele sensuri, unde IA poate ghida conversația, determinând victima să dezvăluie informații sensibile sau să realizeze transferuri către conturi controlate de atacatori.

Similar modului în care soluțiile de IA amplifică și potențează atacurile de tip *phishing*, IA poate fi utilizată de exponenții mediului *cybercrime* pentru automatizarea și scalarea campaniilor de tip *vishing*, vizând simultan un număr semnificativ de victime și menținând în același timp un nivel ridicat de personalizare și sofisticare a mesajelor transmise.

IA este utilizată inclusiv în atacurile cibernetice de tip *honeypot*, în care actorii cibernetici utilizează conturi false pentru a manipula victimele, de obicei pentru câștiguri financiare sau pentru a obține informații sensibile. Instrumentele de IA permit criminalilor cibernetici să creeze profiluri false pe rețelele sociale, care prezintă fotografii, date biografice și conversații care par autentice. De asemenea, *chatbot*-urile bazate pe IA pot angaja victimele în conversații convingătoare pe o perioadă de timp îndelungată, obținând încrederea victimelor și manipulându-le emoțiile și acțiunile de-a lungul timpului.

DEZVOLTAREA UNOR NOI APLICAȚII MALWARE PRIN UTILIZAREA UNOR INSTRUMENTE IA

Instrumentele bazate pe IA, cum ar fi WormGPT, HackerGPT sau FraudGPT sunt utilizate pentru a automatiza și a îmbunătăți procesul de dezvoltare a aplicațiilor *malware*. Aceste modele avansate de IA generativă pot fi utilizate pentru a crea malware cu un grad foarte ridicat de sofisticare și cu capabilități complexe de eludare a soluțiilor de securitate cibernetică, inclusiv de actori cibernetici care nu dețin abilități tehnice avansate.

WormGPT a fost utilizat pentru a genera automat cod *malware* care exploatează vulnerabilitățile în aplicații *software*, sisteme sau rețele informatice, ceea ce conduce la o extindere semnificativă a plajei de atac pe care actorii cibernetici o pot exploata. WormGPT și instrumentele similare pot fi utilizate în moduri din ce în ce mai sofisticate, în special pentru atacurile cibernetice de tip DDoS – acestea pot automatiza crearea de *botnet*-uri - rețele de dispozitive compromise care generează trafic masiv pentru a indisponibiliza serviciile sau accesul în cadrul unei infrastructuri țintă. În plus, WormGPT poate identifica și exploata vulnerabilitățile din infrastructura țintei, făcând atacul de tip DDoS mai eficient și mai greu de mitigat.

WormGPT poate fi utilizat pentru a dezvolta boți capabili să ocolească inclusiv protecțiile CAPTCHA. Prin utilizarea algoritmilor de tip *machine learning*, IA poate fi instruit să recunoască modele și să rezolve testele CAPTCHA de validare, care sunt concepute pentru a diferenția între accesul uman și accesul automat. Acest lucru permite *chatbot*-urilor să obțină acces la site-uri și servicii restricționate, contribuind semnificativ la scalarea atacurilor cibernetice automate.

Un alt instrument utilizat de criminalii cibernetici este HackerGPT, soluție IA creată în mod oficial pentru a asista în sarcinile de securitate cibernetică și în *hacking*-ul etic. Cu toate acestea, instrumentul a fost exploatat pentru a oferi acces la diferite tipuri de aplicații *malware*, făcându-le disponibile pentru un număr considerabil de utilizatori. Mulți dintre utilizatori au fost neexperimentați (așa-numiții *script kiddies*), care folosesc aplicații *malware* pentru a derula atacuri cibernetice, fără însă a înțelege pe deplin modul în care acestea funcționează. Acest fenomen reprezintă un aspect important în ceea ce privește creșterea semnificativă a volumului atacurilor cibernetice din ultimii ani.

DEZVOLTAREA *MALWARE*-ULUI POLIMORF, CARE SE ADAPTEAZĂ ÎN TIMP REAL PENTRU A ELUDA DETECTAREA ȘI MĂSURILE DE SECURITATE

Nu în ultimul rând, modelele de IA generative pot crea *malware* polimorf, care își schimbă în mod continuu codul (modificându-și structura, comportamentul și *payload*-ul de fiecare dată când *malware*-ul este utilizat) pentru a evita detectarea de către sistemele de securitate tradiționale. Instrumentele AI pot modifica semnătura codului *malware* prin criptare, obfuscare sau reordonare, asigurându-se că *malware*-ul „arată" diferit de fiecare dată când compromite un sistem informatic.

Aceste modele de IA pot, de asemenea, să automatizeze crearea de aplicații de tip *ransomware, infostealer*, troieni și alte tipuri de *malware* prin utilizarea algoritmilor de învățare automată pentru a analiza și a se adapta la un mediu țintă, ajustând automat strategia de atac a *malware*-ului. Acest lucru permite *malware*-ului să fie mai rezistent la măsurile standard de securitate cibernetică, permițându-i să mențină accesul persistent în cadrul sistemelor informatice compromise.

WWW.SRI.RO/CYBERINT