BULETIN CYBERINT

SEMESTRUL I - 2024

VULNERABILITĂȚILE *0-day* - MADE IN CHINA

În ultimii ani, operațiunile cibernetice ofensive derulate de grupările din Republica Populară Chineză (RPC) s-au remarcat atât prin diversificarea țintelor, cât și prin creșterea nivelului de sofisticare al tacticilor, tehnicilor și procedurilor utilizate. Resursele de ordin financiar, uman și tehnologic mobilizate pentru derularea atacurilor relevă, cu un grad ridicat de probabilitate, implicarea autorităților chineze în aceste campanii.

Această ipoteză este susținută inclusiv de creșterea semnificativă, începând cu a doua jumătate a anului 2023, a numărului de vulnerabilități *0-day* descoperite de industria de securitate cibernetică. În acest sens, a fost observat faptul că actorii cibernetici chinezi au reușit să identifice și să exploateze breșe de securitate cibernetică existente la nivelul unor *software*-uri produse de companii cu notorietate la nivel mondial.

► 16 octombrie 2023 - Cisco a confirmat că peste 40.000 de dispozitive proprietare au fost exploatate prin intermediul unei vulnerabilități *0-day* de nivel critic, existentă la nivelul interfeței web de management a acestora. Documentată ulterior în mediul online drept CVE-2023-20198, vulnerabilitatea permitea atacatorului să creeze un utilizator cu toate privilegiile de administrare pentru dispozitivul compromis. Ipoteza referitoare la posibila exploatare de către actori cibernetici chinezi a acestei breșe de securitate este susținută de un comunicat public al autorităților din SUA și Japonia de la finalul lunii septembrie 2023 cu privire la operațiunile cibernetice ofensive ale grupării BlackTech, asociată RPC. Conform raportului respectiv, unul dintre elementele de *modus operandi* specifice operațiunilor cibernetice ofensive derulate de BlackTech este exploatarea dispozitivelor Cisco prin tehnici asemănătoare cu cele specifice CVE-2023-20198.

► 25 octombrie 2023 - VMware a publicat o serie de actualizări de securitate pentru remedierea vulnerabilității de nivel critic CVE-2023-34048, ce afecta *software*-ul vCenter Server. Ulterior, Mandiant și VMware Product Security au identificat că această vulnerabilitate a fost exploatată, încă din anul 2021, de către actorul cibernetic chinez UNC3886 pentru compromiterea sistemelor informatice ce rulau vCenter Server.

► 10 ianuarie 2024 - Ivanti a descoperit vulnerabilitățile CVE-2023-46805 și CVE-2024-21887, prezente la nivelul soluțiilor proprietare Connect Secure VPN și Policy Secure. Ulterior, investigațiile Mandiant au relevat că actorul cibernetic chinez UNC5221 a exploatat aceste vulnerabilități încă din decembrie 2023 pentru a obține acces în rețelele victimelor ce utilizau aplicațiile respective.

Companiile afectate de vulnerabilitățile *0-day* exploatate de actorii cibernetici chinezi sunt unii dintre principalii furnizori de echipamente și soluții IT&C din piață. Astfel, atacurile cibernetice pot afecta lanțuri întregi de distribuție, precum și entități guvernamentale din multiple state.

Obținerea acestor vulnerabilități (achiziționarea de pe *deep/ dark web* sau identificarea acestora prin mijloace proprii) și utilizarea lor presupune un proces costisitor, însă impactul exploatării acestora este unul semnificativ, afectând soluții *software* utilizate extensiv la nivel global pentru perioade îndelungate înainte de a fi descoperite. Disponibilitatea actorilor cibernetici chinezi de a întreprinde astfel de activități demonstrează faptul că aceștia dispun de capabilități avansate și de un „arsenal" impresionant de astfel de mijloace ofensive.

ATRIBUIREA PUBLICĂ A ACTIVITĂȚII *APT CALLISTO* CĂTRE FEDERAȚIA RUSĂ

La 7 decembrie 2023, Regatul Unit al Marii Britanii (UK) și SUA, alături de alți parteneri occidentali, au inițiat un demers comun de tip „*blame and shame*" la adresa Serviciului Federal de Securitate al Federației Ruse (FSB) pentru interferențele, prin operațiuni cibernetice ofensive, în procesele democratice din mai multe state. Ralierea țării noastre la expunerea publică și condamnarea Federației Ruse pe acest subiect a fost exprimată printr-un comunicat de presă publicat în aceeași zi pe site-ul Ministerului Afacerilor Externe.

Responsabilitatea pentru aceste activități revine Centrului 18 al FSB, care coordonează gruparea APT CALLISTO în derularea de atacuri cibernetice ce vizează influențarea proceselor electorale prin campanii de spionaj și influență. În acest sens, a fost documentată implicarea, încă din 2016, a ofițerului FSB Ruslan Aleksandrovich PERETYATKO și a lui Andrey Stanislavovich KORINETS în atacuri cibernetice ce au vizat:

- targetarea, inclusiv cu e-mailuri *spear-phishing*, a unor parlamentari din multiple partide politice;
- compromiterea și publicarea (campanii *hack and leak*), înainte de alegerile generale ce au avut loc în UK în 2019, a unor documente ce vizează comerțul între UK și SUA;
- compromiterea unui *think-tank* a cărui activitate viza apărarea democrației împotriva dezinformării;
- targetarea unor universități, jurnaliști, entități din sectorul public, ONG-uri și alte organizații ale societății civile ce susțin democrația în UK.

Conform investigațiilor derulate de autoritățile din UK și SUA, între 2016 și 2020, KORINETS a asigurat infrastructura necesară de atac pentru campaniile *spearphishing* ale FSB. În aceeași perioadă, PERETYATKO a folosit multiple adrese e-mail care impersonau reprezentanții unor companii IT&C pentru a obține credențiale de acces la diferite conturi ale victimelor, folosind inclusiv infrastructura pusă la dispoziție de KORINETS.

Cei doi indivizi au fost plasați pe lista de sancțiuni de către UK și SUA, Departamentul de Stat al SUA oferind inclusiv o recompensă de până la 10 milioane de dolari pentru orice informații ce pot ajuta la prinderea acestora.

RADIOGRAFIE A FENOMENULUI *RANSOMWARE*: TRENDURI, ATACURI ȘI RECOMANDĂRI

I. OVERVIEW AL FENOMENULUI RANSOMWARE ÎN 2023

Pe parcursul anului 2023, atacurile cibernetice cu *ransomware* au continuat să fie cea mai profitabilă formă de criminalitate cibernetică, motiv pentru care acestea rămân cea mai importantă amenințare cibernetică din sfera *cybercrime* pentru entitățile din sectorul public și privat la nivel global. Astfel, în cursul anului 2023 s-au remarcat următoarele caracteristici ale fenomenului *ransomware*:

► Principalul vector prin care s-a obținut accesul inițial nu a mai fost reprezentat de *botnet*-uri, ca în 2022, ci de exploatarea vulnerabilităților aplicațiilor și *software*-urilor legitime;

► Cu excepția etapei în care este descărcat *payload*-ul propriu-zis, majoritatea actorilor cibernetici care au instrumentat atacuri cu *ransomware* au evitat utilizarea altor tipuri de *malware*, folosindu-se în principal de aplicații *software* și instrumente legitime, cele mai comune fiind PsExec, PowerShell și WMI;

► Atacurile *ransomware* au înregistrat un vârf în octombrie 2023, numărul entităților publice și private compromise fiind cu 66% mai mare decât în octombrie 2022, conform rapoartelor companiei Chainalisys;

► Numărul companiilor victimă care au plătit răscumpărarea cerută a crescut de la 68% (în 2022) la 76% (2023), conform companiei de securitate cibernetică Delinea;

► Gruparea CL0P a dezvoltat un *pattern* eficient pentru atacurile de tip *double-extortion*, prin exploatarea vulnerabilității MOVEit. Identificând vulnerabilități de tip *zero-day*, gruparea a exfiltrat concomitent date de la o serie de multinaționale, obținând un număr semnificativ de victime într-o singură campanie de atac cu *ransomware*;

► Principalele entități vizate au fost corporațiile, instituțiile cu profil înalt, infrastructurile critice, inclusiv spitale, instituții de învățământ pre-universitar și universitar și, nu în ultimul rând, entitățile guvernamentale;

► În paralel cu creșterea numărului de atacuri *ransomware* față de anul 2022 (cu 68%), a crescut și media sumei de răscumpărare cerută. În acest context, se remarcă gruparea LockBit, care, în urma compromiterii infrastructurii informatice aparținând Royal Mail din UK, a cerut răscumpărare în valoare de 80 de milioane de dolari;

► În urma atacurilor de tip *supply-chain*, grupările de criminalitate cibernetică motivate financiar au atins un nou record în anul 2023, depășind 1 miliard de dolari obținuți din plata răscumpărărilor cerute, aproape dublu față de anul 2022;

► Deși au fost compromise infrastructurile informatice de la nivelul unor companii din peste 120 de țări, ținta principală a atacurilor este SUA, peste 47% dintre postările de la nivelul DLS-urilor grupărilor *ransomware* referindu-se la companii cu sediul în această țară, conform echipei de *Threat Intelligence* Unit 42 din cadrul Palo Alto Networks;

► Sistemul *Ransomware-as-a-Service* a rămas și în 2023 un element central al fenomenului ransomware, remarcându-se grupări precum LOCKBIT și ALPHV BlackCat;

► Numărul postărilor de victime pe DLS-urile (*Dedicated Leak Site*) conexate grupărilor *ransomware* a crescut cu 49% față de anul 2022 (de la 2679 la 3998), conform Unit 42;

► Popularizarea serviciilor oferite de *Initial Access Brokers* (IaBs) a condus la o înmulțire a atacurilor cu *ransomware* în 2023. Accesul comercializat de brokerii de acces inițial, împreună cu serviciile oferite în sistem *as-a-Service*, a permis unor actori cibernetici fără cunoștințe tehnice avansate să instrumenteze atacuri cibernetice complexe în 2023.

În 2023 au fost identificate peste 25 de grupări noi de *ransomware*, fapt care indică afinitatea actorilor cibernetici motivați financiar pentru atacurile cu *ransomware*. Cu toate acestea, multe dintre grupările nou înființate, cum ar fi Darkrace, CryptNet sau U-Bomb, au dispărut în a doua jumătate a anului 2023. Acest fapt poate fi conexat cu activitatea agențiilor internaționale de aplicare a legii și serviciilor de intelligence, care au depus eforturi semnificative pentru destructurarea grupărilor *cybercrime* și infrastructurilor de comandă și control utilizate.

> În 2023 au fost destructurate grupări de notorietate la nivel mondial, cum ar fi HIVE și Ragnar Locker.


RANSOMWARE

Având în vedere toate acestea, se conturează următoarele trenduri cu privire la fenomenul *ransomware* la nivel global pentru următoarea perioadă:

Exploatarea vulnerabilităților va continua să fie un element central în activitatea grupărilor *ransomware*, fie că este vorba despre vulnerabilitățile de tip *zero-day* sau a celor deja cunoscute.

Modernizarea codului sursă al aplicațiilor *ransomware* – din ce în ce mai mulți dezvoltatori de *ransomware* adoptă limbajul de programare Rust, care permite dezvoltarea de aplicații *malware* ce pot fi executate pe diferite sisteme de operare, cu utilizarea de secvențe de cod mai sigure (care îngreunează procesul de *reverse engineering* și de analiză a cercetătorilor din domeniul securității cibernetice).

Implementarea unor tactici, tehnici și proceduri avansate de atac – în următoarea perioadă, actorii *cybercrime* vor continua să-și îmbunătățească tacticile de atac implementate, folosind tehnici complexe de inginerie socială, campanii de *phishing*. Aceste metode devin din ce în ce mai potente prin integrarea soluțiilor de inteligență artificială, care vor permite o mai bună identificare a victimelor și vulnerabilităților sistemelor informatice.

În ciuda eforturilor de reglementare a domeniului specific criptoactivelor, actorii cibernetici motivați financiar vor continua să utilizeze criptomonedele în scopuri frauduloase. În context, o revenire a valorii criptomonedelor poate determina unele grupări care derulează atacuri cu *ransomware* să migreze către activități frauduloase de exfiltrare de credențiale/ portofele virtuale în detrimentul investițiilor în operațiuni de compromitere și criptare a datelor.

Va crește numărul de atacuri cu *ransomware* fără criptare sau cu criptare parțială – tendința este ca actorii *cybercrime* să se bazeze pe criptarea parțială (doar o parte a datelor este criptată) sau pe exfiltrarea de date, în detrimentul procesului clasic de criptare, care poate fi unul cronofag și complex. Astfel, au fost observate mai multe grupări *ransomware* cu notorietate, cum ar fi CL0P, ALPHV BlackCat, Rhysida, Avos sau BianLian, care au instrumentat atacuri cibernetice fără a executa procesul de criptare de date, acestea fiind doar exfiltrate și comercializate la nivelul platformelor de criminalitate cibernetică.

Cu toate că au fost înregistrate victorii relevante în procesul de combatere a fenomenului *ransomware*, acesta va continua să înregistreze schimbări și evoluții semnificative în 2024 și în perioada următoare, la nivel mondial, prin îmbunătățiri ale tacticilor, tehnicilor și procedurilor utilizate de grupările *ransomware*, precum și prin popularizarea serviciilor oferite în sistem *Ransomware-as-a-Service*.

II. ATACURI CU RANSOMWARE ÎN ROMÂNIA ÎN PERIOADA 2023-2024

La 20 februarie 2023, compania S.C. Transporturile Aeriene Române S.A. (TAROM) a fost victima unui atac cibernetic cu *ransomware*, care a criptat un număr limitat de date de la nivelul infrastructurii informatice aparținând acesteia. Nu au fost afectate operațiunile de zbor sau sistemul de rezervări al companiei, impactul atacului nefiind unul semnificativ.

La 17 octombrie 2023, infrastructura informatică aparținând certSIGN, furnizor de servicii de semnătură electronică, a fost compromisă în urma unui atac cu *ransomware*-ul Cactus. Urmare atacului, au fost afectate indirect inclusiv entități din administrația publică și servicii publice, respectiv Autoritatea pentru Digitalizarea României (ADR) și *ghișeul.ro*, care utilizau sisteme și produse gestionate de certSIGN. Daunele provocate de atacul cibernetic au fost semnificative, ADR suspendându-și temporar emiterea de certificate digitale prin soluția SEAP, oferită de certSIGN. La două zile după atac, pe 19 octombrie 2023, toate serviciile de semnătură electronică operate de certSIGN au redevenit funcționale.

Infrastructura informatică aparținând Camerei Deputaților – Parlamentul României a fost compromisă, la finalul lunii ianuarie 2024, în urma unui atac cibernetic cu *ransomware*. *Malware*-ul utilizat în cadrul atacului este dezvoltat de către gruparea *ransomware* KNIGHT și comercializat în sistem *Ransomware-as-a-Service* la nivelul forumurilor specializate de criminalitate cibernetică din *darkweb*. Datele exfiltrate au fost comercializate la nivelul DLS-ului grupării KNIGHT, însă postarea a fost ștearsă după 2 zile, întrucât gruparea care operează *ransomware*-ul nu le permite afiliaților să targeteze instituții guvernamentale.

În perioada 10-12 februarie 2024 a avut loc un atac cibernetic cu *ransomware* asupra infrastructurii informatice aparținând companiei care gestionează platforma Hipocrate, utilizată la nivel național de mai multe unități spitalicești. Atacul s-a răspândit și a compromis infrastructurile informatice aparținând unui număr de 26 de spitale, afectând activitatea acestora. *Malware*-ul utilizat în campania de atacuri este un *ransomware* din familia PHOBOS, care a vizat în perioada 2019-2021 exclusiv sectorul medical din România.

III. RECOMANDĂRI DE PROTECȚIE ȘI PREVENȚIE A INFECȚIEI CU MALWARE-URI DE TIP RANSOMWARE

În cursul anului 2023 s-a remarcat atât înmulțirea atacurilor cibernetice cu *ransomware*, îmbunătățirea tacticilor, tehnicilor și procedurilor utilizate de grupările *cybercrime*, cât și efectul acestora asupra entităților publice și private compromise. Toate acestea denotă amploarea fenomenului *ransomware* la nivel global, care se află, în continuare, pe un trend ascendent. Efectele atacurilor cibernetice cu *ransomware* conduc la compromiterea celor trei valori fundamentale ale datelor de la nivelul sistemelor informatice vizate, respectiv confidențialitatea, integritatea și disponibilitatea acestora. Astfel, impactul acestor atacuri poate cauza prejudicii de ordin reputațional, financiar sau legal entităților publice sau private afectate, motiv pentru care, la nivel strategic, sunt necesare politici publice în domeniul securității cibernetice și planuri de răspuns și reacție rapidă la atacuri cibernetice, împreună cu investiții în pregătirea specialiștilor în securitate cibernetică pentru combaterea fenomenului *ransomware*. La nivelul entităților publice și private sunt necesare, de asemenea, investiții pentru creșterea rezilienței cibernetice, prin securizarea infrastructurilor informatice și crearea unei culturi de securitate cibernetică.

Deși nu reprezintă o listă exhaustivă, următoarele măsuri sunt recomandate pentru protecția și prevenția infecțiilor cu *ransomware*:

1. Actualizarea și aplicarea *patch*-urilor disponibile pentru dispozitivele și soluțiile VPN (*Virtual Private Network*);

2. Actualizarea soluțiilor *software*, a serviciilor și sistemelor de operare;

3. Implementarea unei soluții de tip DLP (*Data Loss Prevention*) pentru prevenirea exfiltrării neautorizate de date;

4. Implementarea unor soluții de prevenire a intruziunilor (IPS) și sisteme de tip *Web Application Firewall* (WAF) ca protecție perimetrală aproape de serviciile Web expuse pe internet;

5. Implementarea unei platforme de securitate XDR (*Extended Detection and Response*);

6. Restricționarea accesului VPN doar pentru anumite categorii strict necesare de utilizatori (administratori, firme terțe) și folosirea unei scheme de adresare statice cu lista de control access și implementarea unui mecanism de autentificare 2FA (*Two-Factor Authentication*);

7. Monitorizarea execuției comenzilor și scripturilor Powershell, logarea execuției acestora și crearea de reguli pentru detecția execuției de comenzi cu conținut codificat;

8. Auditarea activităților neautorizate ale conturilor de utilizatori, administratori și servicii;

9. Limitarea capacității (permisiunilor) utilizatorilor de a instala și rula aplicații *software* și aplicarea principiului *least privilege* tuturor sistemelor și serviciilor;

10. Filtrarea cererilor de tip DNS (*Domain Name System*) pentru a bloca comunicațiile și exfiltrarea de date de la și către un server C2 (*command & control*);

11. Limitarea utilizării RDP (*Remote Desktop Protocol*) sau a altor servicii similare;

12. Oprirea serviciilor nefolosite pe toate stațiile/ serverele și eliminarea sistemelor neutilizate, neactualizate sau inactive din rețea, deoarece acestea pot constitui o vulnerabilitate și un punct de intrare pentru un posibil atacator;

13. Segmentarea rețelelor în funcție de necesități (restricționați accesul la Internet pe cât posibil) și instituirea unor politici de acces de tip *whitelist* / *blacklist* pentru permiterea sau blocarea accesului la anumite resurse din Internet;

14. Evitarea activării comenzilor macro din atașamentele de e-mail. Dacă un utilizator deschide atașamentul și activează comenzi macro, codul încorporat poate executa *malware* pe sistem;

15. Evitarea accesării *link*-urilor web din e-mailuri;

16. Separarea conturilor de administrator față de cele de utilizatori;

17. Utilizarea unui plan de *backup* și recuperare a datelor pentru toate categoriile de date esențiale. Realizarea și testarea *backup*-urilor în mod regulat pentru a limita impactul pierderii datelor sau a sistemului și pentru a accelera procesul de recuperare. Backup-urile conectate la rețea pot fi afectate de *ransomware*, de aceea e important ca *backup*-urile critice sa fie păstrate pe dispozitive de stocare *offline* sau pe sisteme izolate;

18. Crearea, menținerea și exersarea periodică a planului de răspuns rapid la incidente;

19. Realizarea periodică a unor teste de auditare a infrastructurilor, în vederea identificării și remedierii vulnerabilităților existente.

AMENINȚĂRI DIGITALE ÎN CONTEXT ELECTORAL

Conform ONU, anul 2024 poate fi privit ca un moment rar în istorie, întrucât aproximativ jumătate din populația globului va fi chemată la vot. Pe acest fond au crescut îngrijorările privind potențialul unor actori externi ostili de a afecta procesele electorale.

Printre țintele vizate s-ar putea număra atât electoratul, echipele implicate în campanii electorale, candidații sau trusturile media, cât și autoritățile implicate în organizarea proceselor electorale. Compromiterea dispozitivelor electronice și platformelor ori serviciilor online de centralizare și numărare a voturilor ar putea conduce la afectarea integrității listelor de alegători, alterarea parțială a rezultatului alegerilor ori crearea de prejudicii de imagine, în funcție de metoda aleasă.

În acest sens, în timpul desfășurării scrutinelor electorale, entități ostile ar putea aplica - în funcție de profilul țintei - atât metode „tradiționale", prin instrumentarea de atacuri cibernetice de tip APT, *ransomware* sau *DDoS*, cât și tehnici, tactici și proceduri specifice operațiunilor de influență sau campaniilor de dezinformare, ce au cunoscut o dezvoltare fără precedent în ultimii ani, mai ales în contextul integrării unor tehnologii emergente, precum inteligența artificială și *deepfake*.

PRINCIPALELE ȚINTE CARE AR PUTEA FI VIZATE

ELECTORAT

Principala amenințare care ar putea afecta electoratul o reprezintă operațiunile de propagandă și dezinformare, construite pentru a favoriza un anumit candidat și a denigra un altul, prin crearea și propagarea în mediul online a unor teorii conspiraționiste sau știri false, inclusiv cu ajutorul instrumentelor bazate pe IA, utilizând diverse metode tehnologice de amplificare a narativelor susținute.

Aceste acțiuni cu potențial subversiv sunt menite să polarizeze discursul public, să submineze adeziunea la valorile democratice, cu afectarea încrederii în procesul de votare și în instituțiile statului.

CANDIDAȚI SAU ECHIPE DE CAMPANIE ELECTORALĂ

Cel mai adesea, actorii cibernetici au intenționat să acceseze în mod neautorizat adresele de e-mail ale persoanelor implicate în mod direct, ca prim pas al unui atac cibernetic mai complex sau doar pentru a exfiltra date confidențiale, pe care să le publice ulterior în mediul online pentru deturnarea agendei electorale și compromiterea candidaților, element specific acțiunilor de tip „*hack and leak*".

Tehnicile de inginerie socială aplicate în campaniile de *phishing* au rămas o constantă în portofoliul capabilităților asociate actorilor cibernetici, reprezentând una dintre principalele metode de atac pentru obținerea accesului inițial în cadrul rețelelor informatice aparținând entităților implicate în procesele electorale. Acestea au evoluat permanent și s-au adaptat factorilor externi, devenind tot mai credibile cu ajutorul inteligenței artificiale. În ultimii ani au fost identificate următoarele campanii notabile de *phishing*/*spearphishing* în context electoral:

- 2015-2016: Activitatea actorilor cibernetici APT28 și APT29 (atribuiți Federației Ruse) a condus la compromiterea rețelei informatice aparținând Comitetului Național Democrat din SUA, înainte de alegerile naționale;
- noiembrie 2016: Actori cibernetici aflați în conexiune cu serviciile de informații militare rusești au instrumentat campanii de tip *spearphishing*, care au vizat administratorii alegerilor din Florida, obținând acces în cadrul rețelei informatice aparținând unui guvern al unui comitat din Florida;
- 2017: APT28 a compromis conturile profesionale și personale ale personalului campaniei prezidențiale franceze prin intermediul unor atacuri de tip *spearphishing*, urmărind exfiltrarea de credențiale;
- 2020: Actorii cibernetici conexați cu Coreea de Nord au instrumentat mai multe campanii de atacuri cibernetice de tip *phishing*, vizând organizațiile care au sprijinit candidații la președinția SUA;
- mai-august 2022: A fost observată o creștere semnificativă a atacurilor cibernetice bazate pe e-mailuri care au vizat lucrătorii electorali din SUA, înainte de alegerile naționale de la mijlocul mandatului. Atacatorii au trimis e-mailuri de *phishing* cu scopul exfiltrării de credențiale.

Cu toate acestea, specialiștii în domeniu au remarcat în 2023 apetența actorilor cibernetici de sorginte estică pentru campanii de atacuri de *tip brute* force sau *password spray*, care, deși vizează tot obținerea de credențiale sau asigurarea accesului inițial, diferă de campaniile de *phishing* prin faptul că atacatorul nu necesită o interacțiune directă cu ținta vizată prin intermediul unui fișier malware. Așadar, există posibilitatea ca, în 2024, metode complexe precum acestea să se numere printre cele mai utilizate căi de obținere a accesului.

SISTEME INFORMATICE UTILIZATE ÎN PROCESUL ELECTORAL

De-a lungul timpului, atacurile cibernetice de tip *defacement* sau *DDoS* au rămas printre cele mai utilizate mijloace de indisponibilizare a resurselor online. Afectarea infrastructurii IT&C implicate direct în procesul electoral reprezintă o amenințare serioasă din prisma impactului pe care l-ar putea avea manipularea directă a voturilor sau perturbarea rezultatelor.

ELEMENTE DE *MODUS OPERANDI* ÎN INTERFERAREA ASUPRA PROCESELOR ELECTORALE

Propaganda, dezinformarea, spionajul și atacurile cibernetice reprezintă instrumente utilizate, adesea împreună, în operațiuni de influență, care pot fi derulate de actori ostili în vederea afectării capacității operaționale a instituțiilor publice și alterării proceselor decizionale de nivel strategic, prin destabilizarea comunităților și scăderea încrederii populației în autorități.

În contextul proceselor electorale ce vor avea loc în Republica Moldova în 2024, prezintă relevanță analiza intitulată „*The Threat from Russia's Unconventional Warfare Beyond Ukraine, 2022-24*", care a fost publicată în februarie 2024, de *think tank*-ul britanic RUSI.

Aceasta notează o schimbare de strategie a Federației Ruse, începând cu 2023, în încercările sale de destabilizare a Republicii Moldova prin intensificarea campaniilor targetate de dezinformare.

În contextul în care Maia Sandu este acuzată de neajunsurile economiei, se urmărește ca percepția negativă asupra persoanei președintelui să fie transferată și asupra aspirațiilor R. Moldova de accedere în UE (Maia Sandu fiind principalul motor al acestor demersuri). În același timp, pentru crearea unor disensiuni la nivel societal, sunt targetați cetățenii moldoveni cu vederi favorabile asupra României în scopul amplificării mesajelor lor astfel încât populația vorbitoare de limbă rusă să resimtă o amenințare în creștere asociată cu integrarea în UE.

Viginum, agenția care asigură protejarea intereselor franceze față de interferențe externe în spațiul online, a publicat în februarie 2024 un raport care detaliază activitatea rețelei Portal Kombat, formată din cel puțin 193 website-uri, utilizată în vederea derulării de campanii informaționale ofensive în Ucraina și mai multe state vest-europene.

În general, articolele cu conținut pro-rus sunt preluate din postările unor personalități ruse sau pro-ruse ori din cadrul unor agenții de presă rusești sau locale, prezentând informații inexacte sau false cititorilor. Deși conținutul site-urilor din rețea a părut să fie apolitic, fiind teoretic axat în principal asupra unor date referitoare la evenimente sportive, festive sau instituționale, după ce Rusia a invadat Ucraina, rețeaua a început publicarea de articole prin care se urmărește prezentarea în registru pozitiv a „operațiunii militare speciale" și denigrarea Ucrainei și a liderilor acesteia. Portalurile din rețea care targetează Franța au publicat de asemenea și conținut care a contribuit direct la polarizarea discursului public din spațiul digital.

În urma investigațiilor s-a constatat că rețeaua Portal Kombat utiliza o serie de tehnici în scopul creșterii audienței: selectarea atentă a surselor pro-ruse utilizate în raport cu comunitatea locală, integrarea unor tehnici de automatizare în distribuirea conținutului, respectiv de optimizare a motoarelor de căutare pentru creșterea vizibilității.

RECOMANDĂRI GENERALE

În perspectiva combaterii efectelor campaniilor de dezinformare este necesară o abordare la nivel guvernamental și societal, câteva dintre recomandările generale fiind:

- creșterea nivelului de educație mediatică și digitală;
- consolidarea parteneriatelor cu organizațiile internaționale și locale;
- sprijinirea organizațiilor internaționale, regionale și locale în activitatea lor de combatere a dezinformării și pentru creșterea gradului de conștientizare a publicului.

Punctual, în vederea prevenirii materializării unor atacuri cibernetice, este oportună aplicarea următoarelor recomandări:

- utilizarea unor parole complexe la toate conturile utilizate în mediul online;
- evitarea deschiderii *link*-urilor sau fișierelor primite pe e-mail, verificarea și validarea adresei e-mail sursă în prealabil, dar și a extensiilor fișierelor atașate (de exemplu, denumirile de forma: *document.doc.rtf, document.pdf.exe, document.doc.exe* sunt suspecte pentru că au o dublă extensie);
- aplicarea unor politici de configurare a securității aplicațiilor *software* utilizate și actualizarea permanentă a acestora;
- efectuarea de back-up al datelor;
- verificarea autorilor și validarea conținutului prin intermediul mai multor surse de încredere;
- evitarea distribuirii imediate a știrilor cu titluri hiperbolice sau provocatoare.

OPORTUNITĂȚI ȘI PERSPECTIVE ÎN REGLEMENTAREA CRIPTOACTIVELOR – *REGULAMENTUL MiCA*

În 2024, Uniunea Europeană va deveni prima mare jurisdicție la nivel global care va adopta în mod oficial o serie de legi și norme care au ca scop reglementarea sectorului criptoactivelor.

> Criptoactivele sunt active digitale, care conform autorităților europene, sunt înregistrate pe un registru distribuit și securizate prin criptografie. Practic, acestea sunt o reprezentare digitală a valorii sau a drepturilor, care pot fi transferate și stocate electronic, utilizând registrul distribuit DLT (*Distributed Ledger Technology*) sau o tehnologie similară. Altfel spus, criptoactivele se referă la criptomonede, *token*-uri și valori mobiliare *crypto* (*crypto-securities*).

Regulamentul (UE) 2023/1114 al Parlamentului European și al Consiliului privind piețele criptoactivelor (MiCA – *Markets in Crypto-Assets*), este primul cadru de acest gen, oferind linii directoare și standarde clare pentru participanții din piața *crypto*, cu scopul de a asigura protecția consumatorilor și de a menține integritatea pieței.

Implementarea MiCA se concentrează în jurul următoarelor obiective:

- ► Înlocuirea reglementărilor individuale implementate sau în curs de dezvoltare din țările membre ale UE cu un cadru unificator și cuprinzător;
- ► Asigurarea certitudinii în ceea ce privește reglementarea criptoactivelor, în cazul în care acestea nu sunt acoperite de reglementările financiare existente;
- ► Stabilirea unor norme mai clare pentru furnizorii de servicii de criptoactive și pentru emitenții de *token*-uri.

> Conform MiCA, furnizorii de criptoactive sunt acele entități care furnizează servicii legate de domeniul *crypto*, cum ar fi administrarea platformelor de tranzacționare, schimbul acestora pentru fonduri bănești sau pentru alte criptoactive și furnizarea de servicii de custodie și administrare în numele clienților.

Propriu-zis, MiCA stabilește noi norme comune atât pentru emiterea de criptoactive și supravegherea acestora, protecția împotriva manipulării pieței *crypto* și delimitarea de activitățile specifice criminalității cibernetice, prin impunerea emitenților de criptomonede

stabile (*stablecoins*) să dețină o rezervă de active care să garanteze valoarea *token*-urilor. În plus, este impusă raportarea obligatorie a oricăror tranzacții suspecte. Cu toate acestea, MiCA nu reglementează industria financiară descentralizată (DeFi), *token*-urile non-fungibile (NFT-urile) și nici tranzacțiile de finanțare prin intermediul criptoactivelor.

Implementarea MiCA este programată pentru 30 decembrie 2024, ceea ce va poziționa Europa drept prima regiune care implementează un cadru de reglementare de acest tip.

În România, adoptarea Regulamentului MiCA va avea, cel mai probabil, un impact semnificativ asupra legislației financiare de reglementare, impunând entităților autohtone din sectorul privat care tranzacționează criptoactive să se înregistreze la autoritățile relevante și să implementeze măsuri de combatere a spălării banilor sau a finanțării terorismului. Mai mult, legislația din România va trebui să fie adaptată noilor reglementări, în special în ceea ce privește protecția consumatorilor și legislația specifică monedelor electronice (Lege nr. 127/2011), care se vor intersecta parțial cu Regulamentul MiCA.

Astfel, MiCA oferă numeroase potențiale beneficii pentru piața *crypto* națională și europeană, dintre acestea remarcându-se următoarele:

► Protecția consumatorilor – prin stabilirea unor reglementări clare și unor cerințe standardizate de divulgare, investitorii vor fi mai bine protejați de actorii cibernetici motivați financiar. O protecția mai bună a investitorilor poate duce la o încredere sporită în proiectele specifice pieței criptoactivelor, încurajând investițiile în acestea.

► Dezvoltarea unui mediu echitabil și competitiv – prin reglementarea și supravegherea participanților din piața *crypto*, transparența și integritatea pieței sunt îmbunătățite semnificativ.

► Investiții instituționale – securitatea juridică și cadrul de reglementare stabil și cuprinzător oferite prin Regulamentul MiCA pot conduce la atragerea mai multor investiții instituționale, care pot facilita creșterea și maturizarea domeniului *crypto* prin injectarea de mai mult capital pe piață.

► Legitimizarea pieței *crypto* – având o reglementare standardizată în vigoare, piața *crypto* europeană ar putea dobândi un nivel mai mare de legitimitate și, prin aceasta, crește posibilitatea de a fi sprijinită de sectorul guvernamental național/ european. La nivel global, un mediu de reglementare eficient și transparent în piața criptoactivelor poate încuraja inovarea și investițiile internaționale;

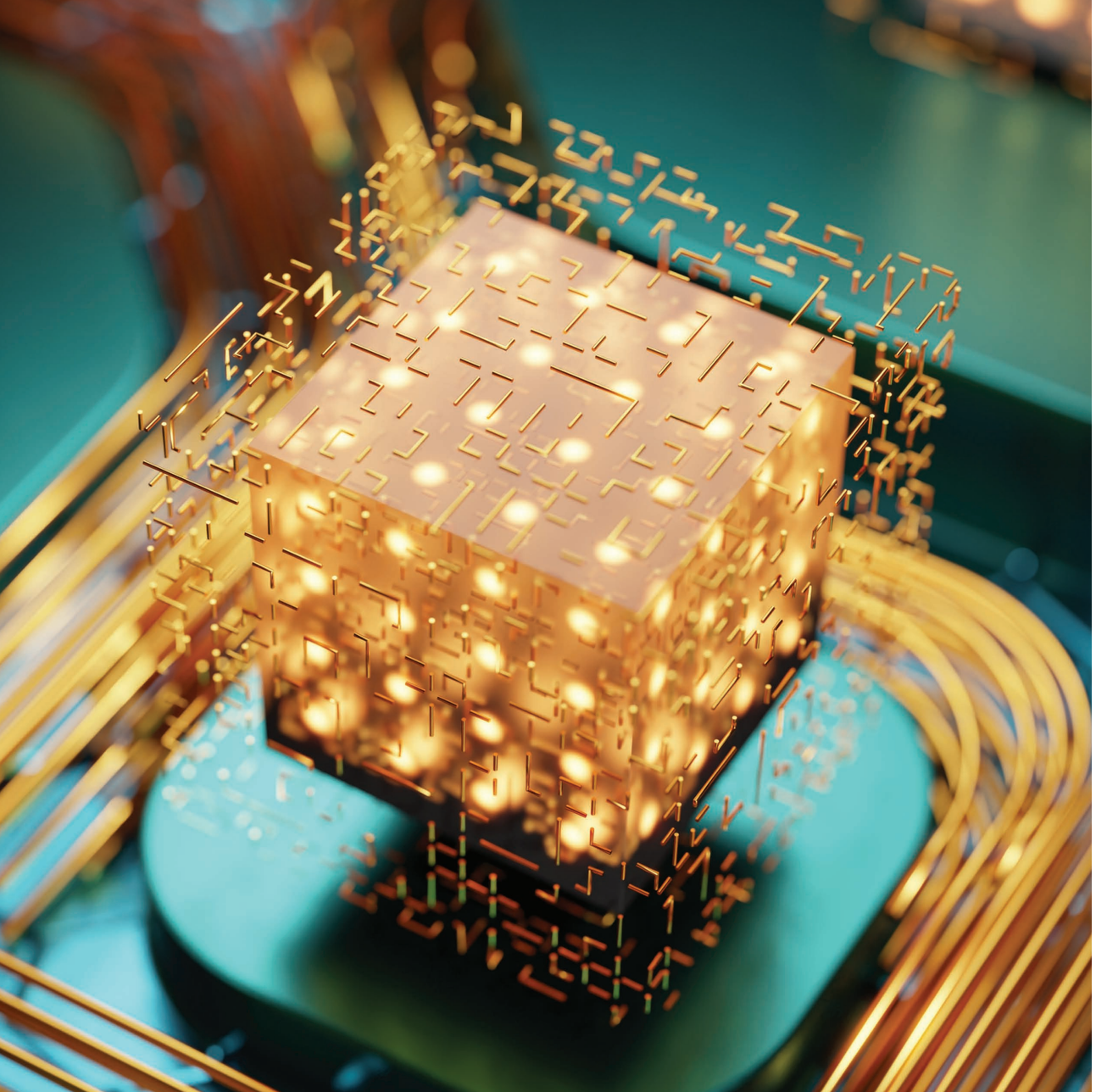
► Combaterea criminalității – obligația furnizorilor de servicii din sfera criptoactivelor de a detecta și raporta fluxurile ilicite de criptomonede, împreună cu standardele impuse prin programele de tipul *Know Your Customer* (KYC), vor susține eforturile organelor de aplicare a legii pentru destructurarea grupărilor de criminalitate cibernetică și informatică la nivel global, precum și pentru combaterea spălării de bani și finanțării terorismului.

Deși este așteptat ca Regulamentul MiCA să reprezinte un avans semnificativ în domeniul criptoactivelor, pot apărea eventuale limitări în ceea ce privește implementarea în România, precum:

► Costuri semnificative de conformitate – MiCA va impune proceduri suplimentare de conformitate pentru participanții la piața *crypto*, motiv pentru care, cel mai probabil, cheltuielile operaționale vor crește, în special pentru companiile mici și *start-up*-uri. Mai mult, necesitatea unor resurse semnificative pentru implementarea MiCA poate reprezenta o barieră pentru intrarea companiilor mici și *start-up*-urilor pe piață, astfel fiind redusă diversitatea din domeniul *crypto* și, implicit, îngreunând evoluțiile emergente.

► Pseudonimizare inconsistentă – implementarea unor prevederi stricte pentru a descuraja spălarea banilor (proceduri de tip AML – *Anti-Money Laundering*) și elementele de KYC pot conduce la reducerea pseudonimizării specifice mediului *crypto* pentru unii dintre participanții acestei piețe. Astfel, anumite entități private sau investitori interesați de aspectele care țin de confidențialitate ar putea fi descurajați să investească în piața *crypto* a Uniunii Europene.

Concluzionând, Regulamentul MiCA reprezintă un pas important în direcția reglementării pieței criptoactivelor din Uniunea Europeană. O bună implementare a acestui regulament ar putea sprijini consecvența necesară pentru dezvoltarea pieței *crypto* din Europa, devenind sigură și transparentă. Pe măsură ce adoptarea activelor digitale continuă să crească, este esențial ca autoritățile de reglementare și furnizorii de servicii de criptoactive să colaboreze pentru a implementa programe de tip KYC, având ca scop final menținerea integrității pieței *crypto* și protejarea tuturor participanților din acest domeniu.



O ALTĂ FAȚĂ A PROGRESULUI TEHNOLOGIC – *CALCULUL CUANTIC*

Tehnologiile cuantice marchează un salt important în domeniul calculului, fiind percepute drept o „industrie a industriilor", similar celor patru revoluții industriale, datorită plajei extinse de aplicabilitate. Printre domeniile cheie în care aceste tehnologii pot fi integrate, se numără: economie, agricultură, securitate și apărare, sănătate și biotehnologie, climă și mediu, transport și logistică, comunicații și rețele, educație și cercetare, societate și cultură. Astfel, tehnologiile cuantice vor contribui la o serie de progrese revoluționare:

- dezvoltarea unor sisteme de calcul avansate și rețele de comunicații militare securizate;
- detectarea și prevenirea amenințărilor cibernetice prin intermediul criptografiei cuantice;
- eficientizarea proceselor de analiză financiară, evaluare a riscului și optimizare a portofoliului financiar;
- accelerarea procesului de descoperire și dezvoltare a medicamentelor și îmbunătățirea simulărilor moleculare și a medicinei personalizate;
- dezvoltarea unor modele de predicție a schimbărilor climatice și reducerea amprentei de carbon;
- optimizarea fluxurilor de trafic în vederea îmbunătățirii mobilității urbane.

Considerând capacitatea remarcabilă a calculului cuantic de procesare – în doar patru minute – a unor seturi de date pe care calculul clasic le-ar parcurge în 10.000 de ani, această tehnologie este adesea prezentată drept următorul punct de referință în dezvoltarea inteligenței artificiale și a învățării automate, având capacitatea de a contribui la dezvoltarea unor variante mult mai performate ale celor existente deja. Totodată, tehnologiile cuantice sunt asociate cu o potențială revoluție tehnologică în ceea ce privește securitatea cibernetică, atât din perspectivă pozitivă – prin îmbunătățirea serviciilor de criptare a datelor și consolidarea capacității de detecție a intruziunilor *high level* în sistemele informatice – dar mai ales din perspectiva caracterului disruptiv pe

care acestea îl pot dobândi în momentul în care devin accesibile pentru actorii de criminalitate informatică și cibernetică (spargerea algoritmilor de criptare, spionaj cibernetic dificil de detectat datorită caracteristicilor superioare anti-interceptare sau generarea unor chei de criptare puternice pentru accesarea informațiilor sensibile).

* TOTODATĂ, TEHNOLOGIILE CUANTICE SUNT ASOCIATE CU O POTENȚIALĂ REVOLUȚIE TEHNOLOGICĂ ÎN CEEA CE PRIVEȘTE SECURITATEA CIBERNETICĂ

ADAPTAREA SECURITĂȚII CIBERNETICE LA AMENINȚAREA CUANTICĂ

Deși informatica cuantică este o tehnologie care poate oferi avantaje semnificative într-o multitudine de domenii, aceasta are potențialul de a deveni o tehnologie disruptivă odată ce ajunge la maturitate. Astfel, există o probabilitate crescută ca aceasta să devină o amenințare la adresa securității cibernetice, cu precădere la nivelul capabilităților actuale de criptare a datelor care trebuie să rămână secrete pe termen nelimitat, cum ar fi datele bancare, datele privind viața privată, datele cu importanță deosebită pentru securitatea națională etc.

În prezent, algoritmul de criptare cel mai utilizat pentru transferul de date sensibile pe Internet este RSA și se bazează pe numere de 2048 de biți. Conform unor descoperiri recente, s-a dovedit că un computer cuantic cu 20 de milioane de qubiți ar putea sparge această criptare în doar 8 minute și este estimat că va apărea în următorii 5-10 ani. Deși cel mai mare și performant computer cuantic disponibil în prezent – Advantage, dezvoltat de către compania D-Wave – este format din doar 5.000 de qubiți și este încă sensibil la cele mai mici interferențe de mediu – cum ar fi câmpul magnetic al Pământului, radiațiile locale și chiar razele cosmice – ceea ce face ca rezultatele acestuia să fie predispuse la erori, domeniul cercetării și dezvoltării acestor tehnologii a înregistrat o evoluție acerbă în ultima perioadă, aspect care împinge teoria spargerii algoritmului RSA din ce în ce mai mult în sfera viitorurilor concretizabile.

Probabilitatea tot mai ridicată de spargere a algoritmului de criptare RSA, a reclamat necesitatea conceperii de contramăsuri eficiente, inclusiv soluții criptografice cuantice (QC) și clasice (postcuantice).

Soluțiile criptografice cuantice joacă un rol crucial în asigurarea unei infrastructuri de comunicare securizate, cele mai importante fiind comunicarea cuantică și distribuția cuantică a cheilor (QKD) intrinsec sigure. Teoriile existente sugerează că fizica permite QKD sau QC să detecteze intruziunea unui actor cibernetic în cadrul unui sistem informatic, caracteristică indisponibilă la nivelul criptografiei standard.

Una dintre contramăsurile care beneficiază de o atenție sporită este dezvoltarea algoritmilor rezistenți la calculul cuantic. Acești algoritmi constau într-un sistem criptografic interoperabil cu protocoalele și rețelele de comunicații existente, care oferă mijloacele de asigurare a confidențialității, integrității și autentificării unei transmisii – chiar și împotriva unui potențial viitor calculator cuantic.

În prezent, Institutul Național de Standarde și Tehnologie (NIST) desfășoară un proces de selecție riguros pentru a identifica algoritmi rezistenți la tehnologiile cuantice (sau post-cuantice) în vederea standardizării. Conex, la finalul anului 2023 au fost lansate soluții *open-source* care oferă acces la algoritmii de criptografie post-cuantică și permit dezvoltatorilor să își creeze propria stivă, sau „sandwich", de protocoale și implementări care pot fi încorporate în aplicații fără a rescrie codul.

„CURSA ÎNARMĂRII" CUANTICE

Celeritatea progresului tehnologic și riscul de poziționare în incapacitate de răspuns a sectorului privat și guvernamental în fața unor amenințări necunoscute, a transformat procesul de construire a calculatoarelor cuantice într-o cursă globală. Este estimat că din această „cursă a înarmării" cu capabilități cuantice fac parte peste 600 de companii și mai mult de 30 de laboratoare naționale și agenții guvernamentale din întreaga lume.

Piața globală a calculatoarelor cuantice a fost evaluată în 2021 la 395 milioane USD și este preconizat că va crește la aproximativ 532 milioane USD până în 2028. În prezent, cu excepția Mexicului, Turciei și Indoneziei, țările ale căror PIB depășește 1 trilion de USD au lansat inițiative cuantice naționale iar jumătate dintre statele cu un PIB de peste 500 de miliarde de USD au început să investească în vederea atingerii unui astfel de deziderat național.

Preocuparea sporită a statelor asupra dezvoltării și deținerii de tehnologii cuantice a fost declanșată de potențialul pe care acestea îl pot avea în: realizarea unor sisteme de arme mai sofisticate, spargerea codurilor criptografice și crearea de aplicații care le-ar putea oferi avantaje militare.

În acest sens, impactul pe care tehnologiile cuantice îl poate avea în domeniile critice precum cel militar, de informații sau cibernetic, au determinat Statele Unite ale Americii să adopte în 2023 o politică limitativă asupra investițiilor americane în companii cu sediul în China, Hong Kong sau Macao care activează în domeniul tehnologiilor informaționale cuantice, al semiconductorilor, al microelectronicii și al inteligenței artificiale (AI).

Totodată, Parlamentul European și-a reiterat preocupările referitoare la finanțarea de către Republica Populară Chineză a unor proiecte de cercetare a tehnologiilor cuantice ale Uniunii Europene, conform Rezoluției Parlamentului European din 1 iunie 2023 referitoare la ingerințele externe în toate procesele democratice din Uniunea Europeană, inclusiv dezinformarea (2022/2075(INI)). Prin această rezoluție, Parlamentul European a îndemnat statele membre să ia măsuri de reevaluare a parteneriatelor, refuzare a finanțărilor și chiar revocare a licențelor institutelor asociate, cu scopul echilibrării polilor de putere la nivel global.

DIVERSIFICAREA INSTRUMENTARULUI CIBERNETIC – *DEEPFAKE AI*

Deep-learning Fake AI este o tehnologie derivată din inteligența artificială, care are la bază tehnici avansate de învățare automată, cum ar fi *deep-learning* și rețele generative adversariale (GAN), care pot fi antrenate pentru a genera conținut fals (imagini și videoclipuri) extrem de realist, pornind de la seturi de date existente. GAN utilizează *deep-learning* pentru a identifica tipare în imaginile reale, analizând comportamentul, mișcările și modurile de vorbire din videoclipul sau imaginea originală și le rulează de mai multe ori pentru a regla cu precizie realismul imaginii sau videoclipului final.

Materialele *deepfake* pot fi create în două moduri: prin utilizarea conținutului sursă original, în care ținta este reprezentată spunând și făcând ceva neconform cu realitatea; sau prin schimbarea feței unei persoane într-o înregistrare video a unei alte persoane. În dezvoltarea materialelor de impersonare sunt utilizate abordări specifice precum:

sursă video *deepfake* în care sunt analizate atributele relevante ale țintei – expresiile faciale și limbajul corpului – cu ajutorul rețelelor neuronale convoluționale (CNN), ulterior fiind filtrate printr-un autocodificator, format dintr-un codificator care codifică atributele relevante, și un decodificator, care impune aceste atribute în cadrul videoclipului țintă;

falsificări audio în cadrul cărora GAN clonează sunetul vocii unei persoane, creează un model bazat pe tiparele vocale – identificate cu ajutorul algoritmilor de programare neuro-lingvistică sau NLP – și folosește acest model pentru a face ca vocea să spună orice dorește creatorul. Această tehnică este întâlnită preponderent la nivelul dezvoltatorilor de jocuri video.

sincronizarea buzelor este o altă tehnică în care rețele neuronale recurente (RNN) mapează o înregistrare vocală pe un material video, făcând să pară că persoana din videoclip rostește cuvintele din înregistrare. Astfel, dacă sunetul în sine este un *deepfake*, componenta video reușește să adauge un nivel suplimentar de înșelăciune.

Astfel de *content* poate fi creat în doar câteva secunde cu ajutorul unor instrumente specifice, printre cele mai utilizate regăsindu-se: Deep Art Effects, Deepswap, Deep Video Portraits, FaceApp, FaceMagic, MyHeritage, Wav2Lip, Wombo și Zao.

Ca orice tehnologie emergentă, construită pe baza capabilităților aproape nelimitate ale inteligenței artificiale (IA), realității virtuale (RV), realității augmentate (AR) sau altor mijloace, *deepfake* poate avea dublă utilizare. În sens pozitiv, această tehnologie este utilizată în domeniile artelor și divertismentului, prin varietatea tipurilor de conținut multimedia pe care le poate produce, precum: jocuri video, muzică, satiră și parodie și chiar producții cinematografice, respectiv scene greu de filmat care sunt construite în post-producție prin clonarea și manipularea vocilor actorilor.

Totodată, *deepfake* a facilitat automatizarea serviciilor de apelare și asistență telefonică prin crearea de răspunsuri personalizate la solicitările telefonice, redirecționarea apelurilor și utilizarea de voci false pentru soluționarea unor sarcini simple, precum verificarea soldului bancar sau depunerea de reclamații.

Având în vedere caracterul de dublă utilizare și gradul minimal de conștientizare a populației asupra efectelor pe care acestea le pot produce, *deepfake* poate fi utilizat pentru activități de înșelătorie, pornografie infantilă, defăimare sau discurs instigator la ură. De asemenea, astfel de tehnologii pot face parte din instrumentarul hibrid utilizat de entități sau state ostile asupra unor state democratice, ceea ce poate reprezenta o amenințare la adresa securității naționale.

Cu toate acestea, tehnologia *deepfake* AI poate produce prejudicii considerabile datorită capacității sale de a răspândi informații false care par a proveni din surse legitime și de încredere. De exemplu, în anul 2022, în contextul războiului dintre Federația Rusă și Ucraina, a fost publicat un videoclip *deepfake* în care președintele ucrainean Volodimir Zelenski cere trupelor sale să se predea. De asemenea, au fost exprimate îngrijorări cu privire la potențialul unor actori ostili de a interfera în procesele electorale cu scopul de a influența rezultatele. Un exemplu în acest sens este reprezentat de materialele deepfake lansate în 2020 cu scopul discreditării președintelui SUA, Joe Biden, care a fost afișat în stări exagerate de declin cognitiv, vizându-se astfel influențarea alegerilor prezidențiale.

Variațiuni ale acestui tip de materiale au fost identificate și în activități ilicite precum: șantajarea și afectarea reputației unei persoane din motive vindicative sau pentru hărțuirea cibernetică a acesteia, fabricarea de dovezi, fraudă prin impersonare, manipularea parcursului tranzacțional al unor acțiuni, dezinformare și manipulare politică.

În vederea combaterii acestui fenomen au fost dezvoltate tehnologii pentru a detecta și bloca acest tip de materiale, precum și posibilități de atașare a unei semnături la nivelul videoclipurilor și fotografiilor în vederea îngrădirii capabilităților de perpetuare a acestora în materiale *deepfake AI*. Totodată, unele companii *social media* au început să utilizeze tehnologia *blockchain* pentru a verifica sursa videoclipurilor și a imaginilor înainte de a le permite accesul pe platformele lor, identificând astfel sursele de încredere în vederea prevenirii falsurilor.

Există totodată și modalități non-sistemice de detectare a acestor materiale, fiecare persoană fiind capabilă să combată aceste tehnici circumscrise activităților malițioase. Cele mai importante semne de urmărit în cazul materialelor audio și video sunt:

- poziționarea facială neobișnuită;
- mișcările faciale sau corporale nefirești;
- culoarea nefirească;
- comportament neobișnuit al videoclipului atunci când este aplicat zoom-in;
- sunetul inconsistent;
- persoanele care nu clipesc.

Și în cazul *deepfake*-urilor cu conținut text există câțiva indicatori, cei mai întâlniți fiind:

- greșelile de ortografie;
- propozițiile care nu curg natural;
- adresele de e-mail cu sursă suspectă;
- frazele care nu corespund cu stilul presupusului expeditor;
- mesajele în afara contextului, care nu sunt relevante pentru nicio discuție, eveniment sau problemă vizată.

În pofida numeroaselor măsuri de combatere a acestui fenomen, progresul tehnologic accelerat al inteligenței artificiale creează frecvent sincope în lupta sectorului privat și a celui guvernamental împotriva caracterului disruptiv al acestor tehnologii. Prin îmbunătățirea constantă a capabilităților de eludare a indicatorilor standardizați, respectiv prin instrumente precum cele care susțin clipitul natural și perfecționarea NLP, *deepfake*-ul va rămâne un mijloc predilect în orchestrarea campaniilor de criminalitate cibernetică.

DIRECTIVA (UE) 2022/2557 PRIVIND REZILIENȚA ENTITĂȚILOR CRITICE

La 14 decembrie 2022 a fost publicat în Jurnalul Oficial al UE textul final al *Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului* (Directiva CER).

Începând cu 16 ianuarie 2023, atât Directiva CER, cât și Directiva NIS 2 au intrat în vigoare la nivelul UE. Statele membre au obligația să transpună cerințele Directivei CER în legislațiile naționale proprii, până la 17 octombrie 2024, urmând ca din 18 octombrie 2024 să fie aplicate toate măsurile obligatorii din această directivă.

Conform Directivei CER, entitățile critice sunt acele instituții/ entități publice sau private care furnizează unul sau mai multe servicii esențiale, prin intermediul propriei infrastructuri critice existente pe teritoriul național care poate include și infrastructura critică națională, așa cum este definită aceasta în Ordonanța de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată prin Legea nr.18/2011.

Practic, domeniul de reglementare al Directivei CER este complementar domeniului protecției infrastructurilor critice reglementat prin OUG nr.98/2010. În calitate de furnizoare de servicii esențiale, entitățile critice joacă un rol indispensabil în menținerea funcțiilor societale sau a activităților economice vitale pe piața internă, într-o economie dinamică a UE, caracterizată de tot mai multe interdependențe sectoriale. Există 11 sectoare critice pentru care se va aplica Directiva CER: energie, transporturi, bancar, infrastructuri ale pieței financiare, sănătate, apă potabilă, ape uzate, infrastructură digitală, administrație publică, spațiu și producție, prelucrare și distribuție de alimente.

În contextul unei abordări exhaustive și al înțelegerii riscurilor asociate entităților considerate critice la nivelul UE, Directiva CER conturează un cadru cuprinzător prin care să fie asigurată reziliența acestor entități din toate perspectivele. Astfel, entitățile critice din statele membre trebuie să aibă permanent în vedere înțelegerea și evaluarea riscurilor la care sunt expuse, precum și obligațiile ce le revin astfel încât să poată asigura în mod optim furnizarea de servicii esențiale din domeniile referite.

În consecință, la nivel național urmează să fie stabilit un cadru național care va viza atât consolidarea rezilienței entităților critice prin stabilirea unor norme minime armonizate, cât și sprijinirea acestora prin intermediul unor măsuri specifice de sprijin și supraveghere.

ACCELERATORUL NATO PENTRU INOVARE – *DIANA*

MOTTO: „SUPREMAȚIA ÎN DOMENIUL TEHNOLOGIC INFLUENȚEAZĂ DIN CE ÎN CE MAI MULT SUCCESUL PE CÂMPUL DE LUPTĂ”.

Conceptul Strategic al NATO, 2022, punctul 17.

Acceleratorul NATO pentru Inovare (DIANA – în engleză: *Defense Innovation Accelerator for the North Atlantic*) reprezintă o inițiativă a Alianței Nord-Atlantice operaționalizată în vederea valorificării și dezvoltării de noi tehnologii în scopul asigurării securității și apărării membrilor acesteia. Inițiativa a fost lansată în anul 2021, la Summitul NATO de la Bruxelles, pentru consolidarea cooperării transatlantice în domeniul tehnologiilor critice, promovarea interoperabilității și valorificarea inovației civile prin crearea unui cadru de cooperare între mediul academic și sectorul privat.

Astfel, DIANA vizează consolidarea cooperării între mediul academic, comercial, și antreprenorial (atât *start-up*-uri, cât și companii cu grad ridicat de maturitate) pentru dezvoltarea de noi tehnologii cu uz dual (atât comercial, cât și de apărare), care să consolideze capacitățile de apărare și securitate, respectiv care să fie conectate cât mai rapid la cerințele operaționale ale utilizatorilor militari finali. Pentru susținerea acestui deziderat, sub egida DIANA au fost dezvoltate două rețele formate din 11 acceleratoare și 91 de centre de testare. Prin intermediul acestora este facilitată reunirea unor reprezentanți ai mediului universitar, guvernamental și ai diverselor industrii pentru a coopera cu *start-up*-uri și alți inovatori în vederea abordării unor provocări critice de securitate și apărare.

În cadrul Conceptului Strategic al NATO, adoptat de șefii de stat și de guvern în cadrul Summitului de la Madrid din anul 2022, a fost asumată accelerarea transformării digitale, adaptarea structurii de comandă la era informațională și consolidarea mijloacelor de apărare cibernetică, rețelelor și infrastructurii. De asemenea, este stipulată promovarea inovării și creșterea investițiilor pentru dezvoltarea tehnologiilor emergente și disruptive, pentru a menține interoperabilitatea și avantajul militar. Conform Conceptului Strategic, pentru atingerea acestor scopuri, NATO va colabora cu sectorul privat în vederea adoptării și integrării noilor tehnologii.

În acest sens, prin intermediul DIANA este vizată valorificarea oportunităților oferite de tehnologiile emergente și disruptive în vederea consolidării avantajului competitiv al NATO pentru susținerea și asigurarea apărării și securității colective. Practic, prin promovarea acestei direcții de acțiune, NATO urmărește să dezvolte capabilități noi de răspuns atât la amenințările convenționale, cât și la provocările viitoare care vor fi generate de acest tip de tehnologii. Această direcție de acțiune are un puternic caracter pragmatic întrucât, după cum este cuprins în Conceptul Strategic al NATO din 2022, „*tehnologiile emergente și disruptive aduc atât oportunități, cât și riscuri*", fiind previzionat un impact strategic ce va modifica natura conflictelor și a competiției globale.

Domeniile de interes relevante din perspectiva DIANA pentru susținerea activității de inovare din cadrul NATO sunt concentrate în jurul a nouă priorități:

- inteligența artificială;
- tehnologiile autonome;
- tehnologiile cuantice;
- biotehnologiile și îmbunătățirile umane (human enhancement);
- sistemele hipersonice;
- spațiul (aplicații spațiale);
- materialele noi (novel material and manufacturing);
- energia și tehnologiile de propulsie;
- rețelele de comunicații de ultimă generație (*next-gen*).

Concret, pentru susținerea avantajului strategic al NATO, DIANA identifică provocări competitive, în baza unei probleme critice de securitate și apărare, ulterior fiind transmise solicitări zonei de inovatori pentru a dezvolta tehnologii cu dublă utilizare. Inovatorii selectați în cadrul programelor DIANA primesc grant-uri non-dilutive (care nu implică oferirea unei cote de acțiuni ori drepturi de proprietate) și acces la cele două rețele de acceleratoare și centre de testare.

Din România au fost selectate două centre de testare: Institutul Național de Cercetare-Dezvoltare Aerospațială „Elie Carafoli" (INCAS), pentru domeniul hipersonic, și Centrul Internațional de Excelență în Inteligență Artificială din cadrul Universității Politehnica București, pentru inteligență artificială.

Suplimentar, prin intermediul DIANA este facilitat accesul la o rețea de oameni de știință, ingineri, diverși experți, utilizatori finali și la o comunitate de investitori de încredere. Astfel, DIANA intermediază oportunități de piață atât în cadrul NATO, cât și în relația cu aliații săi.

Plecând de la caracterul operațional puternic pronunțat al proiectelor dezvoltate în baza grant-urilor oferite prin intermediul DIANA, tehnologiile emergente și disruptive rezultate vor genera impact inclusiv la nivel macro și vor susține eforturile NATO în cadrul competiției tehnologice globale. În acest sens, suplimentar consolidării capacităților de apărare și de răspuns la provocări de securitate, DIANA va genera inclusiv implicații semnificative de ordin geopolitic, întrucât prin obținerea accesului la tehnologii emergente și disruptive se va consolida capacitatea competitivă a NATO față de adversarii existenți și potențiali.

În concluzie, DIANA reprezintă o inițiativă a cărei misiune este reprezentată de facilitarea cooperării dintre mediul academic și de cercetare cu cel comercial și cel guvernamental, în scopul dezvoltării de tehnologii cu uz dual, atât de apărare și securitate, cât și comercial. Astfel, prin intermediul DIANA vor fi dezvoltate tehnologii prin intermediul cărora vor fi rezolvate provocări critice de securitate și apărare colectivă a membrilor NATO și a aliaților săi.

APORTUL CENTRELOR DE INOVARE DIGITALĂ ÎN PROCESUL DE TRANSFORMARE DIGITALĂ A ROMÂNIEI

Transformarea digitală este o prioritate a Uniunii Europene, acesta fiind considerat unul dintre domeniile esențiale pentru consolidarea autonomiei strategice și a competitivității la nivel global. În acest sens, UE a definit cadrul „Deceniului Digital al Uniunii Europene", cu scopul de a ghida toate acțiunile corelate sectorului digital, în vederea pregătirii întreprinderilor și a cetățenilor UE pentru un viitor digital sustenabil, prosper și centrat pe factorul uman. Cadrul vizează dezvoltarea competențelor digitale, creșterea numărului de specialiști, încurajarea adoptării tehnologiei de către întreprinderi, dezvoltarea de infrastructuri digitale sigure și durabile și digitalizarea serviciilor publice.

În procesul de transformare digitală, Centrele Europene de Inovare Digitală (EDIH – în engleză: European Digital Innovation Hub) joacă un rol esențial, susținând integrarea soluțiilor digitale inovatoare, bazate pe noile tehnologii, în activitatea curentă a companiilor și administrațiilor publice. EDIH facilitează posibilitatea de a experimenta și testa aceste tehnologii (conform principiului „*testează înainte de a investi*"), în vederea identificării necesităților de aplicare specifice domeniului de activitate al fiecărei companii sau instituții din administrația publică. De asemenea, EDIH încurajează utilizarea la scară largă a noilor tehnologii într-o manieră care să respecte un nivel optim de securitate cibernetică și favorabilă inovării și dezvoltării digitale.

În România există o *Rețea națională de centre de inovare digitală*, formată din șapte EDIH, care au fost selectate de Comisia Europeană (COM), după cum urmează: **(1)** DIH4Society și **(2)** Transilvania DIH (Regiunea NV), **(3)** FIT EDIH (Regiunea Centru), **(4)** Wallachia eHub (Regiunea Sud-Muntenia), **(5)** CiTyInnoHub (Regiunea SE), **(6)** eDIH-DIZ (Regiunea NE), **(7)** DIGIVEST (Regiunea V). Astfel, rețeaua are reprezentativitate națională, având corespondent la nivelul majorității regiunilor de dezvoltare ale României. Obiectivul principal al acestora este accelerarea transformării digitale a României și susținerea eforturilor autorităților naționale în vederea creșterii competitivității și inovării în domeniul digital.

EDIH-urile au rolul de a sprijini obținerea de finanțare, facilitarea parteneriatelor și susținerea antreprenoriatului. Pentru susținerea acestor obiective, EDIH, în colaborare cu administrația publică și mediul de afaceri, organizează formate de lucru și colaborare

în vederea promovării oportunităților de finanțare pentru proiecte destinate accelerării procesului de transformare digitală.

Cu titlu de exemplu, la începutul lunii februarie 2024, EDIH-urile au realizat evenimente de promovare a portofoliilor de servicii pe care acestea pot să le ofere mediului de afaceri și instituțiilor administrației publice.

Astfel, în regiunea SE, EDIH CityINNOHub a organizat evenimente în colaborare cu mediul academic și cel al administrației publice locale, în cadrul cărora a fost prezentat portofoliul de servicii gratuite pe care entitatea le poate oferi IMM-urilor și instituțiilor din cadrul administrației publice locale ai căror reprezentanți și-au stabilit obiective privind transformarea digitală. CityINNOHub vizează crearea unui ecosistem prin care să fie identificate necesitățile de digitalizare ale IMM-urilor și instituțiilor publice din regiunea de sud-est a României. Astfel, entitățile interesate din regiunea de sud-est a României pot să apeleze la CityINNOHub în diverse domenii de interes precum training, consultanță pentru obținerea finanțării, soluții de securitate cibernetică și instrumente de digitalizare a activității, inclusiv prin integrarea inteligenței artificiale.

În regiunea NE, Transilvania DIH a organizat un eveniment de tip BOOTCAMP la care au participat reprezentanți ai IMM-urilor și ai organizațiilor din sectorul public care sunt beneficiari ai serviciilor de transformare digitală și inovare.

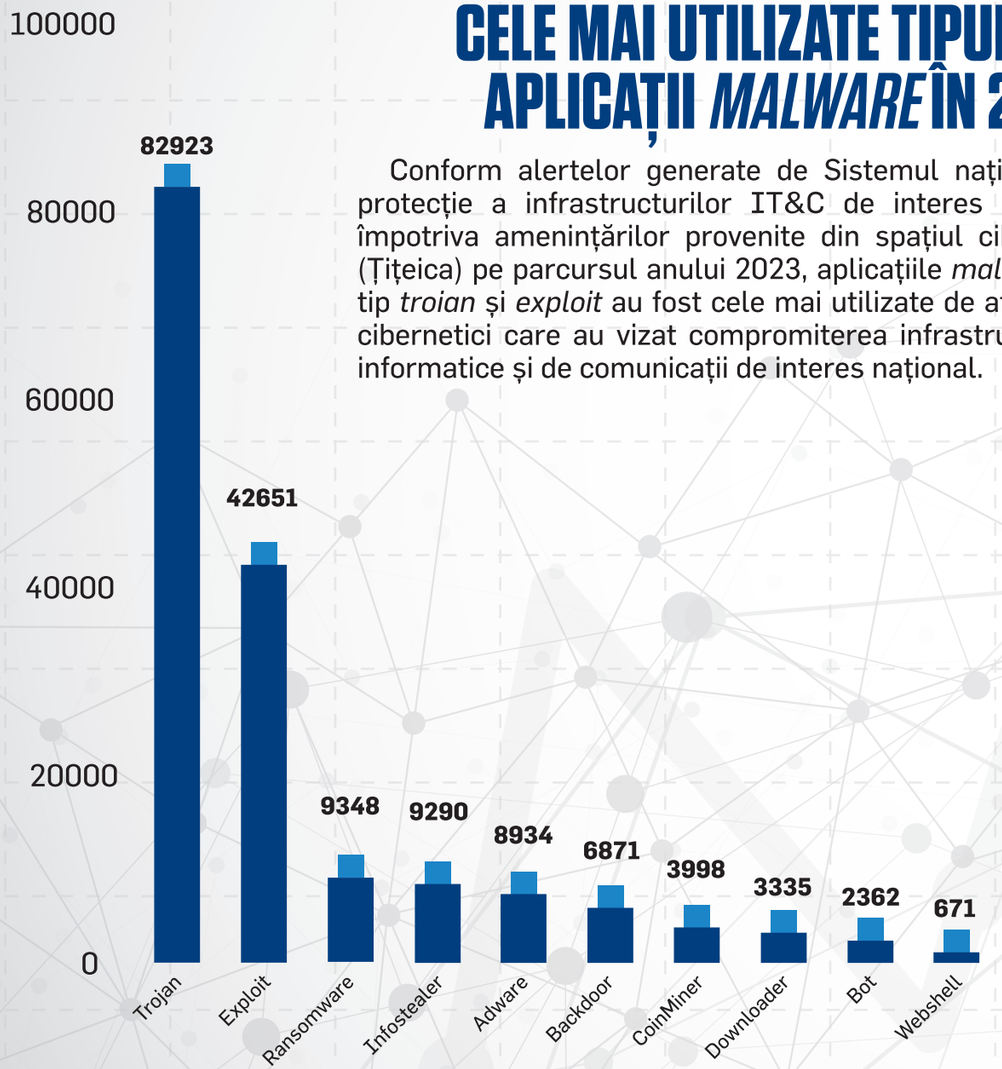
În regiunea Centru, FIT EDIH a organizat un eveniment în cadrul căruia a prezentat reprezentanților IMM-urilor și unităților administrativ teritoriale oportunități de transformare digitală din domeniile de producție, smart city și e-health. De asemenea, în a doua jumătate a lunii februarie a lansat un apel de proiecte competitiv, deschis în perioada 21.02.2024 – 20.02.2025, pentru selectarea de beneficiari din zona IMM-urilor și autorităților publice locale.

În regiunea NE, eDIH-DIZ a supus atenției un apel de selecție a beneficiarilor pentru servicii de transformare digitală și inovare de la nivelul IMM-urilor și administrației publice locale.

În regiunea Sud-Muntenia, la finalul anului 2023, Wallachia eHub a organizat la Sinaia un summit internațional (*InnopRo – Innovation Pathways Romania, towards Twin Transition. The Role of the European Digital Innovation HUB – WEH*). La eveniment au participat reprezentanți ai IMM-urilor din România, ai administrației publice și ai unor parteneri internaționali. În cadrul evenimentului au fost abordate aspecte privind promovarea unor proiecte de transformare digitală atât la nivelul României și UE, cât și oportunități de cooperare cu parteneri din afara UE. De asemenea, au fost prezentate oportunități de accesare a unor surse de finanțare din fondul european de apărare prin care este sprijinită dezvoltarea de tehnologii cu caracter dual, cu uz militar și civil.

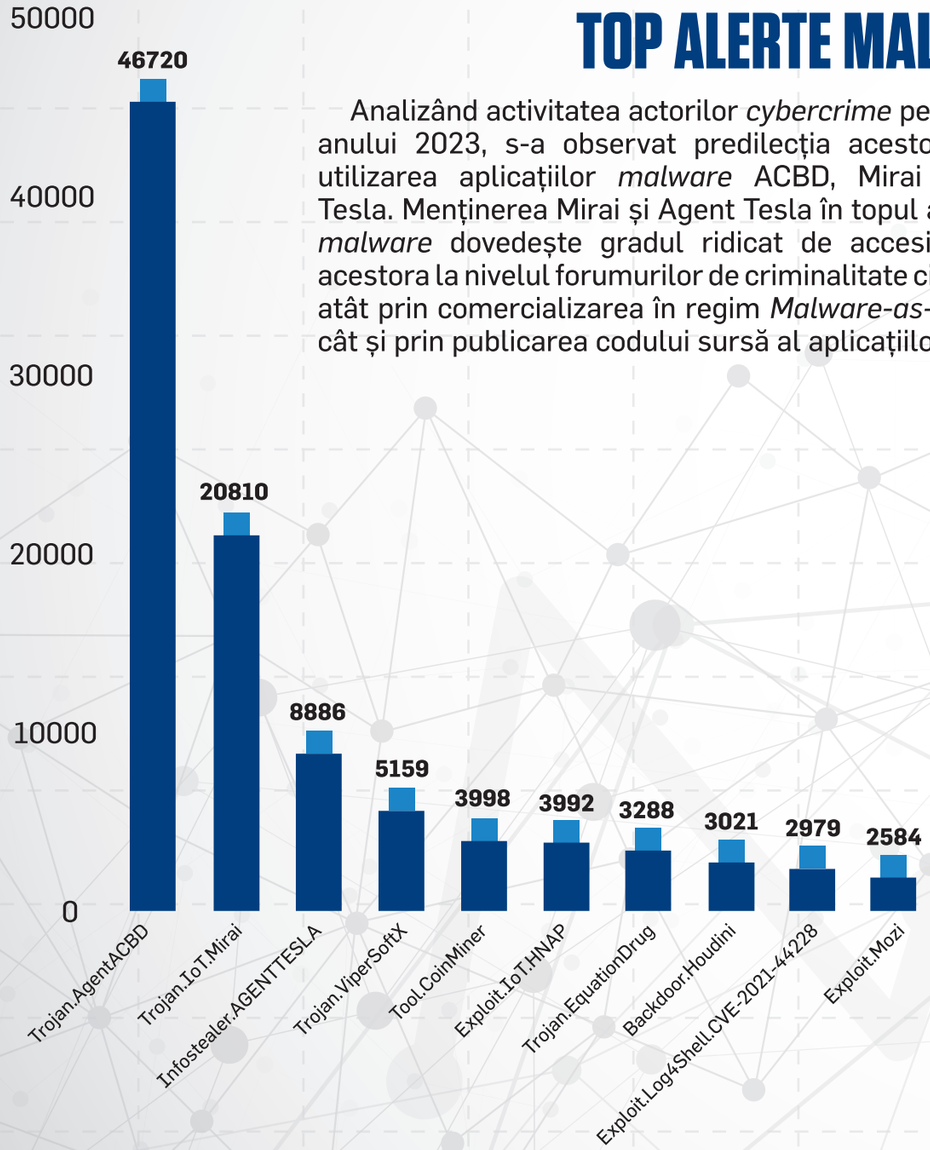
CELE MAI UTILIZATE TIPURI DE APLICAȚII *MALWARE* ÎN 2023

Conform alertelor generate de Sistemul național de protecție a infrastructurilor IT&C de interes național împotriva amenințărilor provenite din spațiul cibernetic (Țiței ca) pe parcursul anului 2023, aplicațiile *malware* de tip *troian* și *exploit* au fost cele mai utilizate de atacatorii cibernetici care au vizat compromiterea infrastructurilor informatice și de comunicații de interes național.

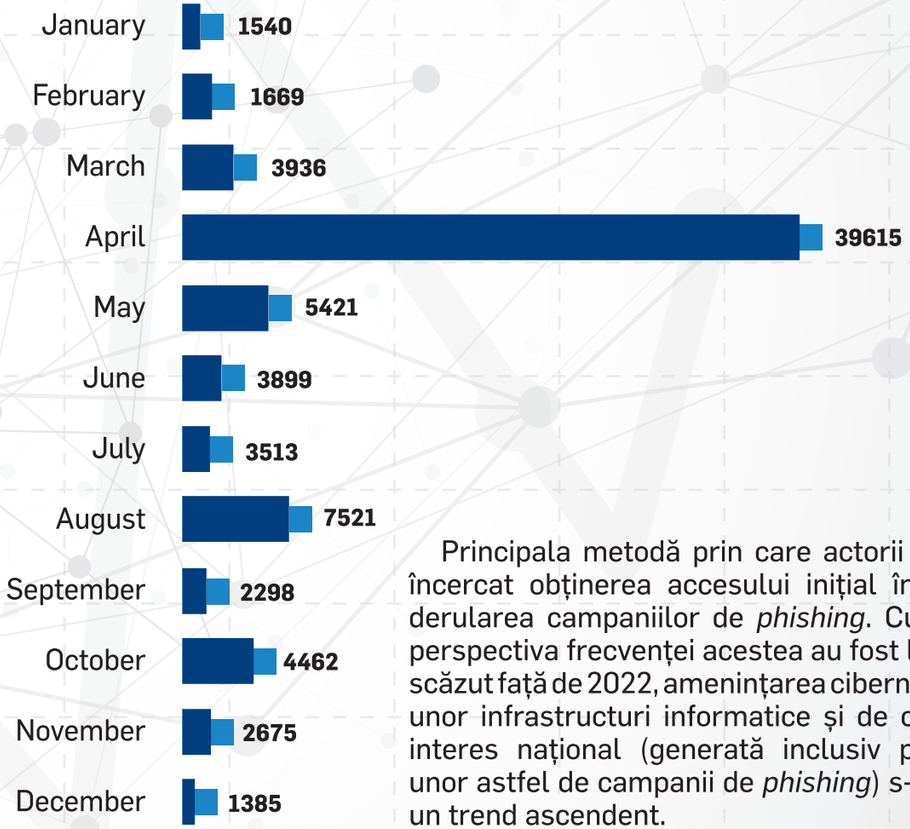


TOP ALERTE MALWARE

Analizând activitatea actorilor *cybercrime* pe parcursul anului 2023, s-a observat predilecția acestora pentru utilizarea aplicațiilor *malware* ACBD, Mirai și Agent Tesla. Menținerea Mirai și Agent Tesla în topul aplicațiilor *malware* dovedește gradul ridicat de accesibilitate al acestora la nivelul forumurilor de criminalitate cibernetică, atât prin comercializarea în regim *Malware-as-a-Service*, cât și prin publicarea codului sursă al aplicațiilor.



FRECVENȚA LUNARĂ A ACTIVITĂȚILOR DE *PHISHING*



Principala metodă prin care actorii cibernetici au încercat obținerea accesului inițial în 2023 a fost derularea campaniilor de *phishing*. Cu toate că din perspectiva frecvenței acestea au fost la un nivel mai scăzut față de 2022, amenințarea cibernetică la adresa unor infrastructuri informatice și de comunicații de interes național (generată inclusiv prin derularea unor astfel de campanii de *phishing*) s-a menținut pe un trend ascendent.

WWW.SRI.RO/CYBERINT