ROMANIA

SRI

SERVICIUL ROMAN DE INFORMATII

Patria a priori

BULETIN CYBERINT

SEMESTRUL I - 2023

CONJUGAREA ATACURILOR CIBERNETICE CU OPERAȚIUNILE MILITARE CONVENȚIONALE. LECȚII ÎNVĂȚATE ÎN URMA CONFLICTULUI MILITAR DIN UCRAINA

Strategia utilizării operațiunilor cibernetice ofensive în mod conjugat cu avansul trupelor militare reprezintă o tehnică aplicată cu succes de către Federația Rusă încă din 2008, din timpul războiului din Georgia. În prezent, la mai bine de un an de la începutul conflictului militar declanșat de Federația Rusă împotriva Ucrainei, am putut asista la o optimizare și o rafinare a acestei strategii, reflectate atât de numărul crescut de astfel de evenimente, cât și de impactul lor asupra ecuației conflictului.

În acest sens, au fost observate multiple situații în care ofensiva militară a fost corelată cu o serie de atacuri cibernetice ante/ post factum. Alinierea obiectivelor celor două câmpuri de luptă a putut fi observată încă din primele zile ale conflictului, când incursiunile militare ale trupelor ruse au fost dublate de o serie de atacuri cibernetice care au vizat afectarea comunicațiilor prin compromiterea rețelei satelitare a companiei Viasat.

Ulterior, în luna martie, sisteme informatice ale companiilor care asigură servicii de televiziune au fost ținta unor ample campanii de atacuri cibernetice, iar, în plan *offline*, armata Federației Ruse a distrus mai multe elemente de infrastructură de *broadcast* (spre ex. antene radio) de pe raza Kievului. Impactul acestor evenimente a fost sporit de campaniile de dezinformare lansate de vectorii de imagine pro-ruși prin intermediul unor aplicații precum Telegram, WhatsApp sau prin intermediul paginilor de pe rețelele de socializare.

În data de 13 mai, rețelele administrației locale din orașul ucrainean Liov au fost compromise în urma unor atacuri cibernetice care au vizat exfiltrarea de date cu caracter strategic, care, foarte probabil, au fost folosite în cadrul bombardamentelor care au avut loc în aceeași zi asupra mai multor puncte strategice ale orașului. Un *pattern* similar a putut fi observat și în data de 23 iunie, când serverul de e-mail al Administrației de Stat Regionale din Nicolaev a fost compromis, iar la scurt timp armata rusă a lansat atacuri masive cu rachete asupra infrastructurii civile și militare a orașului.

Cu toate că, până în prezent, atacurile cibernetice nu au provocat pierderi materiale sau de vieți omenești comparabile cu operațiunile militare convenționale, Federația Rusă acordă în continuare resurse considerabile pentru lansarea ofensivelor pe mai multe fronturi. Exemplele prezentate anterior fundamentează ideea că atacurile cibernetice pot crea un avantaj strategic major, indiferent dacă sunt realizate în mod individual sau ca elemente auxiliare ale unor operațiuni mai ample.

În acest context, este foarte probabil ca Federația Rusă să păstreze această abordare conjugată pe cele două planuri, dat fiind faptul că atacurile cibernetice necesită mai puține resurse și pot produce efecte mult mai rapid, în detrimentul operațiunilor militare convenționale. De asemenea, atacurile cibernetice implică riscuri diplomatice mai reduse, atribuirea publică a acestora fiind un demers complex și cronofag.

ATACURI CIBERNETICE CARE AU VIZAT COMPROMITEREA UNOR INFRASTRUCTURI IT&C DIN DOMENIUL ENERGETIC

De la începutul conflictului militar declanșat de Federația Rusă împotriva Ucrainei, entități asociate guvernului de la Kremlin au folosit retorica șantajului energetic pentru a influența atitudinea statelor occidentale cu privire la acțiunile armate. În vederea accentuării stării de insecuritate asociată crizei energetice anticipată pentru iarna anului trecut, grupările de atacatori cibernetici raliați intereselor Moscovei au vizat pe parcursul anului 2022 multipli operatori energetici de pe teritoriul european. Conform unor rapoarte realizate de industria globală de securitate cibernetică, în anul 2022 s-a înregistrat un număr record de atacuri cibernetice care au țintit infrastructuri IT&C din cadrul unor

companii de producție, transport sau distribuție a energiei electrice, gazelor naturale și petrolului.

În acest sens, s-a remarcat activitatea actorului cibernetic statal APT SANDWORM, care, începând cu luna februarie a anului 2022, a vizat în mod activ compromiterea sistemelor și rețelelor din cadrul unor entități din domeniul energiei din Ucraina. Prin intermediul unui *modus operandi* asemănător campaniei de atacuri cibernetice din 2015, denumită generic *Black Energy*, APT SANDWORM a urmărit întreruperea facilităților de producere a energiei electrice în mai multe centrale de pe teritoriul ucrainean.

> Responsabilitatea pentru atacurile cibernetice derulate de APT SANDWORM a fost atribuită public în 2020 de către Departamentul de Justiție din SUA serviciului militar de intelligence al Federației Ruse – GRU.

Atacatorul a încercat să răspândească în rețelele victimelor aplicații *malware* de tip *wiper*, prin intermediul cărora să compromită în totalitate datele entităților vizate. Conform autorităților ucrainene, în cazul unuia dintre atacuri, APT SANDWORM ar fi deținut acces în sistemele entității încă din luna februarie 2022. Ulterior, într-un comunicat public de la începutul lunii aprilie, echipa CERT-UA a susținut că a reușit să prevină materializarea atacului cibernetic.

Atacuri similare ale APT SANDWORM asupra unor operatori energetici ucraineni au fost observate și în octombrie 2022, când forțele armate ale Federației Ruse au intensificat operațiunile militare convenționale asupra centralelor din domeniul energetic. De asemenea, în cadrul acestei campanii au fost folosite din nou aplicații *malware* de tip *wiper*, dar și *ransomware*, având același scop final, compromiterea totală a datelor.

În același registru, site-urile *web* ale operatorului energetic de stat din Lituania, Ignitis, au fost victima unor atacuri cibernetice de tip DDoS care au condus, în luna iulie 2022, la afectarea temporară a serviciilor *online* oferite de compania în cauză. La scurt timp, atacurile au fost revendicate de gruparea hacktivistă pro-rusă KILLNET. Cu toate că nu au fost identificate infecții în cadrul rețelelor interne ale operatorului, reprezentanții companiei, care are peste 1.7 milioane de clienți, au declarat că este cel mai important atac cibernetic cu care s-au confruntat în ultima decadă. De menționat faptul că atacul cibernetic s-a petrecut la câteva luni de la decizia Lituaniei, prima de acest fel între statele europene, de a întrerupe exporturile de gaz natural din Federația Rusă.

RADIOGRAFIA FENOMENULUI *RANSOMWARE* ÎN 2022

În 2022, atacurile *ransomware* au continuat să aibă un impact economic și social ridicat, constatându-se diversificarea tehnicilor, tacticilor și procedurilor adoptate cu îngreunarea activităților preventive. Actorii cibernetici motivați financiar au vizat compromiterea unor servicii de acces la distanță (RDP), vulnerabilități *software* și aplicații de tip cloud. Principalele ținte ale campaniilor *ransomware* sunt: infrastructurile IT&C din sectorul public, entități private din domeniul financiar, sănătate și energie.

Repere ale evoluției fenomenului *ransomware* în 2022:

A) STATISTICI:

Cele mai relevante statistici ale fenomenului ransomware în 2022 sunt:

- *Ransomware*-ul a reprezentat aproximativ 20% din toate activitățile ilicite din ecosistemul cibernetic;
- Au existat peste 236 de milioane de atacuri *ransomware* la nivel mondial în prima jumătate a anului 2022;
- 71% din companiile din întreaga lume au fost afectate de atacuri de tip *ransomware* în 2022;
- 62,9% dintre victimele atacurilor *ransomware* au plătit răscumpărarea cerută;
- 54% dintre atacurile *ransomware* au avut ca vector de infecție campanii de tip phishing/ spear-phishing;
- Au fost identificate activități de comercializare/ publicare a informațiilor sensibile obținute în urma unor atacuri *ransomware* pentru peste 2.363 de victime (dintre acestea, 42% sunt entități din SUA și 28% din Europa);
- 93% din *ransomware*-uri sunt executabile bazate pe sistemul de operare Windows;
- **90% dintre atacurile ransomware au eșuat sau nu au avut vreun impact asupra victimelor.**

B) PRINCIPALELE ATACURI RANSOMWARE:

Atacurile *ransomware* cu un impact ridicat în 2022 au vizat sistemele informatice din cadrul administrației publice, entităților din domeniul financiar, sanitar, educațional și

entități private (cu impact asupra lanțului de aprovizionare), respectiv:

- CHI Health, subsidiară a celui de-al doilea cel mai mare lanț de spitale din SUA, a fost victima unui atac *ransomware*, care a afectat activitățile unităților sanitare și a compromis datele pacienților (octombrie 2022);
- În Marea Britanie, activitatea *Royal Mail* a fost afectată în urma unui atac *ransomware* (10 ianuarie 2022);
- Orașul Oakland a declarat stare de urgență locală din cauza unui atac *ransomware*, care a forțat deconectarea mai multor sisteme informatice de la internet, incluzând pe cele din cadrul operatorilor de telefonie mobilă (8 februarie 2022);
- Atacul asupra Districtului Școlar Unificat din Los Angeles (LAUSD), care a compromis sistemele informatice și a condus la publicarea datelor exfiltrate pe platforme specializate de criminalitate cibernetică de la nivelul *dark web*-ului (documente confidențiale, detalii bancare, evaluări psihologice etc.). Atacul a fost revendicat de gruparea Vice Society (septembrie 2022);
- Seria de atacuri *ransomware* asupra Republicii Costa Rica, care au afectat semnificativ economia acesteia, activitatea instituțiilor guvernamentale și pe cetățeni, în general. Atacurile au fost revendicate de gruparea pro-rusă Conti (aprilie 2022);
- Pe parcursul lunilor februarie și martie, mai mulți furnizori ai Toyota au fost atacați cibernetic cu *malware* de tip *ransomware*, atacuri care au avut repercusiuni la nivel mondial – fabricile din America de Nord, America Centrală și Japonia oprindu-și activitatea. Atacurile au fost revendicate de două grupări, Pandora și LockBit (februarie-martie 2022);
- Nvidia, cea mai mare companie de cipuri de *gaming* din lume, a fost victima unui atac *ransomware*, care a condus la compromiterea sistemelor informatice din cadrul companiei, fiind nevoie de două zile pentru reluarea parțială a activității. Gruparea care a revendicat atacul este Lapsu$ (23 februarie 2022);
- O serie de servicii critice din municipalitățile suedeze Borgholm și Mörbylånga au devenit indisponibile în urma unui atac *ransomware* (12 decembrie 2022).

C) A DOUA EDIȚIE A SUMMIT-ULUI *COUNTER-RANSOMWARE INITIATIVE* (CRI):

În perioada 31 octombrie – 1 noiembrie 2022 a avut loc cel de-al doilea Summit *Counter-Ransomware Initiative*, la care au participat reprezentanți ai celor 37 de țări membre. Împreună cu partenerii din sectorul privat, au fost abordate și dezvoltate acțiuni concrete de cooperare cu scopul contracarării răspândirii și ameliorării impactului atacurilor cibernetice cu *ransomware* la nivel global.

În ultimul an, activitatea CRI s-a concentrat pe următoarele aspecte: creșterea rezilienței cibernetice a membrilor CRI; combaterea activității actorilor cibernetici motivați financiar; construirea unor parteneriate cu sectorul privat și cooperarea la nivel global pentru o abordare eficientă a acestei provocări. Aceste eforturi au fost realizate sub auspiciile a cinci grupuri de lucru: *resilience* (condus de Lituania și India), *disruption* (condus de Australia), *counter illicit finance* (condus de Regatul Unit și Singapore), *public-private partnership* (condus de Spania) și *diplomacy* (condus de Germania).

Pentru a continua activitatea de combatere a fenomenului *ransomware*, CRI a stabilit pentru anul 2023 următoarele coordonate:

1. înființarea unui grup operativ internațional de combatere a *ransomware*-ului (ICRTF), condus de Australia, pentru a coordona grupurile de lucru *resilience, disruption* și *counter illicit finance*;
2. crearea Centrului Regional de Apărare Cibernetică (RCDC) din Kaunas, condus de Lituania, pentru a testa o versiune la scară mai mică a ICRTF și pentru a operaționaliza angajamentele de schimb de informații;
3. furnizarea unui set de instrumente pentru investigații, inclusiv lecții învățate și strategii de răspuns la evenimente *ransomware* semnificative, respectiv modalități de abordare proactivă în combaterea activității principalilor actorilor cibernetici motivați financiar;
4. instituirea unui angajament activ și durabil cu sectorul privat, bazat pe schimbul de informații de încredere și acțiuni coordonate;
5. publicarea unor materiale de informare despre TTP-urile actorilor cibernetici importanți;
6. dezvoltarea unui instrument pentru consolidarea capacității de a susține țările membre să inițieze și să utilizeze parteneriate public-private pentru a combate fenomenul *ransomware*;
7. coordonarea unor exerciții semestriale de combatere a *ransomware*-ului pentru a dezvolta, consolida și integra în continuare o abordare colectivă în acest scop.

D) ACȚIUNI PREVENTIVE CE DIMINUEAZĂ SEMNIFICATIV RISCURILE/ IMPACTUL ASOCIATE UNOR POTENȚIALE ATACURI DE TIP *RANSOMWARE*:

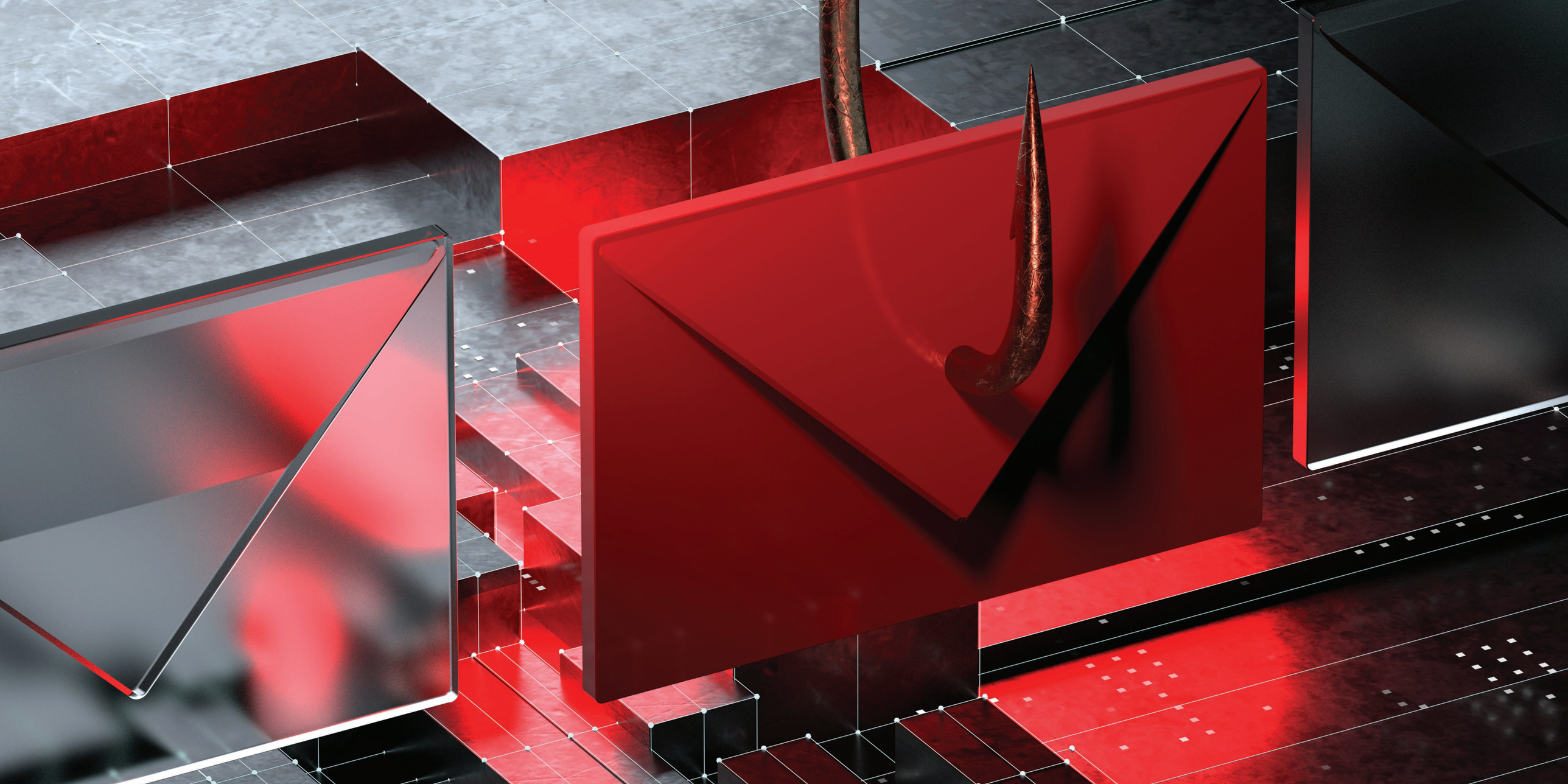
1. Păstrarea, în mod regulat, a unui *backup* al fișierelor (de preferat pe un spațiu de stocare extern, conectat la sistemul informatic doar pe durata *backup*-ului);
2. Folosirea soluțiilor de antivirus, anti-*malware*, *firewall* și scanarea regulată a sistemului informatic/ rețelei pentru a limita suprafața de atac;
3. Folosirea unui serviciu de VPN atunci când este accesată o rețea Wi-Fi publică;
4. Actualizarea regulată a sistemului de operare și aplicațiilor folosite;
5. Descărcarea, instalarea și folosirea doar a versiunilor oficiale ale programelor și întotdeauna de pe *site*-urile oficiale;
6. Dezvoltarea unei culturi cibernetice și respectarea bunelor practici în mediul online (neaccesarea *link*-urilor din mesajele *spam*, nesolicitate sau suspecte);
7. Utilizarea autentificării în mai mulți pași (unde este posibil);
8. Activarea funcțiilor de tip *System Restore*;
9. Stabilirea unui plan de răspuns la incidente cibernetice în vederea creșterii nivelului de reziliență a rețelelor și sistemelor informatice din cadrul instituției;
10. Raportarea oricărui incident autorităților competente.

ATACURILE SPEAR-PHISHING - PE CÂT DE RĂSPÂNDITE, PE ATÂT DE IGNORATE

Atacurile de tip *spear-phishing* continuă să reprezinte principalul vector de infecție al operațiunilor ofensive derulate de actori cibernetici. În cadrul unui atac de spear-phishing se folosesc informații specifice despre victimă pentru a trimite e-mailuri construite astfel încât să convingă utilizatorii să acceseze un *link* sau atașament care conține sau conduce la descărcarea unei aplicații *malware*. Scopul atacurilor este exfiltrarea de date cu caracter sensibil despre victime sau obținerea de acces în sistemele informatice.

În ultimii ani a fost identificată o nouă formă de *spear-phishing*, denumită ***whaling***, atac cibernetic care vizează persoane de rang înalt/ cu funcții importante dintr-o organizație/ instituție.

O caracteristică importantă a acestui nou tip de *spear-phishing* o reprezintă faptul că e-mailurile transmise sunt construite astfel încât să creeze impresia că sunt trimise tot de la o persoană importantă din cadrul organizației/ instituției vizate. Astfel, în cadrul atacului este adăugat un nou element de inginerie socială, persoanele-țintă fiind mai dispuse să acceseze un *link* sau atașament cu conținut *malware* de la o persoană cu credibilitate ridicată.



În general, *spear-phishing*-urile prezintă un nivel ridicat de adaptabilitate, fiind utilizate informații de actualitate cu privire la persoanele vizate, precum și subiecte de interes din plan geopolitic. De asemenea, există situații în care atașamentele *malware* nu sunt detectate de sistemele de securitate cibernetică.

Având în vedere că persoanele vizate în cadrul atacurilor de tip ***whaling*** sunt de rang înalt și prezintă interes ridicat pentru atacatori, aceștia alocă resurse importante pentru construirea e-mailurilor și includ elemente relevante care să convingă victima să acceseze conținutul *malware*. Atacurile de tip ***whaling*** conțin, de obicei, următoarele:

- informații personalizate despre organizația și persoana vizată;
- mesaje care induc ideea unei urgențe;
- cunoaștere aprofundată a limbajului folosit în cadrul unei organizații.

Având în vedere evoluția constantă a atacurilor de tip *spear-phishing* și adaptarea acestora atât la contextul geopolitic actual, cât și la noile sisteme de securitate cibernetică implementate, este necesară acordarea unei atenții sporite e-mailurilor primite pentru a identifica veridicitatea acestora. În acest sens, un utilizator trebuie să aibă în vedere următoarele aspecte:

- verificarea adresei de e-mail de pe care a fost transmis mesajul electronic și numele asociat;
- veridicitatea subiectului e-mail-urilor;
- conținutul e-mail-ului și identificarea greșelilor de scriere care pot apărea ca urmare a unei traduceri automate a textului;
- să nu acceseze link-urile sau atașamentele, decât în situația în care utilizatorul este sigur că e-mail-ul primit este unul autentic.

ÎNTĂRIREA PARTENERIATULUI UE – SUA ÎN DOMENIUL SECURITĂȚII CIBERNETICE

Subsumat *Dialogului Cyber UE-SUA (EU-US Cyber Dialogue)*, în data de 25 ianuarie 2023, a fost anunțată lansarea a trei fluxuri de lucru axate pe aprofundarea cooperării bilaterale, UE-SUA, în domeniul rezilienței cibernetice și consolidarea schimbului de informații cu privire la amenințările cibernetice.

Concret, Secretarul pentru Securitate Internă al SUA[1], **Alejandro MAJORKAS**, și Comisarul european pentru piața internă, **Thierry BRETON**, au emis o declarație comună privind cooperarea transatlantică în domeniul **rezilienței cibernetice**. Cei doi au subliniat importanța cooperării între aliați și creării unui cadru propice pentru ca oamenii, infrastructura critică și afacerile să fie protejate împotriva amenințărilor provenite din spațiul cibernetic.

Demersul implică Departamentul pentru Securitate Internă (DHS) al SUA și Direcția Generală pentru Rețele de Comunicații, Conținut și Tehnologie (DG CNECT) a Comisiei Europene și va viza:

- schimb de informații, *awareness* situațional și răspuns la situații de criză cibernetică;
- securitatea cibernetică a infrastructurilor critice și cerințe de raportare a incidentelor;
- securitatea cibernetică a echipamentelor *hardware* și a soluțiilor *software*.

În aceste formate de cooperare se așteaptă să fie implicate și alte instituții și agenții cu atribuții în domeniul securității cibernetice, precum Serviciul European de Acțiune Externă, Direcția Generală pentru Apărare, Industrie și Spațiu (DG GROW) și Departamentul de Stat al SUA. De asemenea, pe parcursul anului 2023, este așteptată lansarea, în regim pilot, a unei burse aflată sub coordonarea DHS și DG CNECT, care va reuni experți în securitate cibernetică.

Livrabilele asociate domeniilor de cooperare vor cuprinde:

- aprofundarea schimbului de informații cu privire la amenințări, actori, vulnerabilități și incidente de securitate cibernetică pentru a sprijini un răspuns colectiv de apărare împotriva amenințărilor globale, care să includă gestionarea crizelor și răspunsuri diplomatice;
- finalizarea unui acord de lucru între ENISA și CISA pentru a stimula cooperarea și schimbul de bune practici;
- colaborarea pe tema cerințelor de raportare a incidentelor de securitate cibernetică de la nivelul infrastructurilor critice, incluzând ghiduri și șabloane;

[1] *DHS: Department of Homeland Security.*

■ colaborarea în privința securității cibernetice a echipamentelor *hardware* și a soluțiilor *software*;
■ explorarea modului de colaborare în privința protejării sistemelor spațiale civile.

Primele rezultate sunt așteptate să fie raportate cu ocazia celei de-a noua ediții a „Dialogului Cyber UE-SUA" (*EU-USA Cyber Dialogue*), prevăzut pentru cea de-a doua jumătate a anului 2023.

IMPORTANȚA SECURIZĂRII SISTEMELOR DE TIP OPERATIONAL TECHNOLOGY

În ultimii anii, trendul de digitalizare accentuată în diverse sectoare industriale a transformat multe **sisteme de tip *Operational Technology* (OT)[2], din *sisteme închise*** (care nu comunică cu alte rețele), în ***sisteme semi-închise***, ca urmare a necesității administrării și calibrării acestora la nevoile actuale ale pieței și a conectării acestora la alte dispozitive sau rețele.

În consecință, **atacurile cibernetice lansate asupra sistemelor OT sunt în creștere și au devenit tot mai comune**. Impactul generat de acestea variază de la producerea unor disfuncții înregistrate în activitatea de prestare a serviciului sau a procesului OT până la compromiterea în totalitate a serviciului furnizat.

ATACATORII CARE VIZEAZĂ SISTEMELE OT AU CA PRINCIPALE OBIECTIVE:

■ indisponibilizarea serviciului furnizat cu efecte asupra vieții cetățenilor, dar și a societății, per ansamblu;
■ crearea unor disfuncții la nivelul sistemului, cu efect în planul activității/ producției;
■ generarea de prejudicii de imagine operatorului OT.

[2] *care sunt utilizate în administrarea proceselor industriale (monitorizare, comandă și control pentru activități din domeniul energetic: petrol, gaze, electricitate, încălzire, precum și pentru procese de producție din domeniul chimic, al mineritului, auto etc.).*

Din perspectiva gestionării amenințărilor, riscurilor și vulnerabilităților de securitate la nivelul sistemelor OT, responsabilii pe zona securității și a managementului de risc pentru aceste sisteme ar trebui să acorde o atenție ridicată **vulnerabilităților care țin de pregătirea resursei umane care operează sisteme OT**, precum și mediului/ cauzelor care generează astfel de vulnerabilități de securitate.

În vederea creșterii securității cibernetice a sistemelor OT, specialiștii în domeniu recomandă **măsuri de securitate** care vizează:

1. **Definirea de roluri și responsabilități pentru personal;**
2. **Pregătirea personalului;**
3. **Răspunsul la incidente de securitate;**
4. **Proceduri de *backup* și restaurare a sistemelor;**
5. **Proceduri de utilizare a mediilor de stocare;**
6. **Inventarierea activelor existente;**
7. **Segmentarea rețelei;**
8. **Colectarea de *log*-uri și detecție;**
9. **Configurarea securizată;**
10. **Actualizarea/ *patching*-ul.**

LEGEA NR. 58/2023 PRIVIND SECURITATEA ȘI APĂRAREA CIBERNETICĂ A ROMÂNIEI

Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României (LSACR) reglementează cadrul juridic și instituțional referitor la:

- organizarea și desfășurarea activităților din domeniile securitate cibernetică și apărare cibernetică;
- mecanismele de cooperare;
- responsabilitățile instituțiilor cu atribuții în domeniile menționate.

LSACR ia în calcul nevoile statului român de a gestiona toate amenințările de securitate națională provenite din spațiul cibernetic, așa cum sunt prevăzute în *Strategia Națională de Apărare a Țării*, precum și asigurarea rezilienței naționale a statului (în termeni de prevenție, răspuns, protecție etc.), armonizate inclusiv cu prevederile legislației UE în domeniul securității rețelelor și sistemelor informatice (precum *Directiva NIS 1*). Astfel, LSACR introduce și trei noi amenințări în Legea 51/1991 privind securitatea națională a României, art. 3, prin literele:

n) amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național;

o) acțiuni, inacțiuni sau stări de fapt cu consecințe asupra infrastructurilor informatice și de comunicații de interes național;

p) acțiuni derulate de către o entitate statală sau nonstatală, prin realizarea, în spațiul cibernetic, a unor campanii de propagandă și dezinformare, de natură a afecta ordinea constituțională.

Avem în vedere, în acest context, faptul că, prin ***Programul Național de Redresare și Reziliență (PNRR)***, **țara noastră și-a asumat implementarea** măsurii „*Asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice*" (Componenta 7 – Transformare digitală – Reforma 3). Indicatorul de implementare respectiv prevede dispoziția legală care indică necesitatea intrării în vigoare a **LSACR**.

LSACR vine în întâmpinarea satisfacerii unor nevoi de securitate și apărare cibernetică a statului român pe mai multe paliere, care țin de susținerea procesului de digitalizare a economiei și a serviciilor, prin asigurarea:

- unei capacități de reacție rapidă instituțională la incidente din spațiul cibernetic;
- unor capabilități robuste de apărare cibernetică, în cazul atacurilor cibernetice asupra rețelelor și sistemelor informatice de interes național.

De asemenea, **LSACR** reglementează atribuțiile instituțiilor publice în ceea ce privește asigurarea securității și apărării cibernetice, astfel:

- definește domeniile de activitate, atribuțiile și responsabilitățile fiecărei instituții/ autorități în domeniul securității și apărării cibernetice la nivel național;
- definește rolul, componența și atribuțiile Consiliului Operativ de Securitate Cibernetică, ca mecanism de coordonare a instituțiilor din domeniile apărare, ordine publică și securitate națională, precum și a DNSC;

- definește Sistemul Național de Alertă Cibernetică și atribuțiile instituțiilor/ autorităților în situații de alertă;
- stabilește responsabilitățile privind managementul incidentelor de securitate cibernetică adecvate fiecărei instituții din domeniul apărării, ordinii publice și securității naționale, precum și posibilitățile de cooperare interinstituțională, inclusiv cu DNSC;
- reglementează instituirea stării de urgență, în acord cu prevederea constituțională din art. 93 din Constituția României, republicată, pentru rațiuni de securitate cibernetică;
- reglementează aspecte privind asigurarea rezilienței rețelelor și sistemelor informatice la nivel național în spațiul cibernetic, precum și cu privire la domeniul cercetării, dezvoltării și inovării în domeniul securității cibernetice.

LEGEA NR. 354/2022

În 17 decembrie 2022 a intrat în vigoare **Legea nr. 354/2022** *privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei*.

Această lege are scopul de a preveni și contracara amenințările cibernetice derulate de actori statali și non-statali asupra infrastructurilor de comunicații și de tehnologia informației cu valențe critice pentru securitatea națională. Legea este aplicabilă **tuturor autorităților și instituțiilor publice de la nivel central și local** și **interzice achiziționarea și utilizarea de către acestea a produselor și serviciilor *software* de tip antivirus provenind din Federația Rusă.**

Legea definește o serie de criterii în baza cărora un operator economic este considerat ca fiind sub controlul direct sau indirect al unei persoane fizice ori juridice din Federația Rusă, tipurile de produse și servicii *software* pentru care sunt interzise achiziționarea, instalarea și utilizarea de către autoritățile și instituțiile publice, respectiv măsurile pe care acestea trebuie să le adopte.

Pentru punerea în aplicare a prevederilor Legii nr. 354/2022, Ministerul Cercetării, Inovării și Digitalizării (MCID) adoptă, prin ordin al ministrului: (1) **criteriile de stabilire** și **lista nominală** privind produsele, serviciile și entitățile producătoare și/ sau furnizoare interzise, care poate fi actualizată semestrial sau ori de câte ori este nevoie și (2) **procedura, metodele și instrumentele încetării utilizării** produselor și serviciilor prevăzute de lege.

DIRECTIVA NIS 2 (2022/2555)

La data de 14 decembrie 2022, Uniunea Europeană a aprobat **Directiva NIS 2 (2022/2555)** *privind măsuri pentru un nivel ridicat de securitate cibernetică în Uniune*, intrată în vigoare începând cu data de 16 ianuarie 2023. Scopul noii Directive este de revizuire a Directivei NIS[3], motiv pentru care statele membre au obligația de a aplica măsurile necesare pentru a se conforma directivei începând cu 18 octombrie 2024.

> Directiva NIS urmărește îmbunătățirea capabilităților naționale, consolidarea cooperării la nivelul UE și promovarea unei culturi a gestionării riscurilor și a raportării incidentelor în rândul principalilor actori economici care furnizează servicii esențiale și servicii digitale.

Cu toate că Directiva NIS a contribuit la creșterea capabilităților de securitate cibernetică, implementarea sa a înregistrat diverse **impedimente**, fapt care a condus la aplicarea sa în mod fragmentat la nivelul SM. De exemplu, în Directiva NIS 1 sunt definiți Operatorii de Servicii Esențiale (OSE) și Furnizorii de Servicii Digitale (FSD) care, în funcție de modul de reglementare de la nivelul fiecărui SM, pot să aibă obligații diferite.

Suplimentar, COM a realizat o evaluare a funcționării Directivei NIS, din perspectiva impactului, fiind identificate următoarele aspecte: **un nivel scăzut de reziliență cibernetică** a întreprinderilor care își desfășoară activitatea în UE; **reziliență inconsecventă** în toate SM și în toate sectoarele și **un nivel scăzut de conștientizare** comună a situației și lipsa unui răspuns comun în caz de criză.

Prin Directiva NIS 2 este **lărgită plaja de aplicabilitate a prerogativelor din Directiva NIS 1** și se **introduce o nouă abordare** cu privire la sectoarele și entitățile vizate, atât publice, cât și private, fiind aduse o serie de **modificări majore**, precum:

■ În Directiva NIS 2 fost schimbată taxonomia, fiind definite entități împărțite în două categorii: **esențiale** și **importante**. Diferența dintre acestea este dată de regimul de supraveghere la care sunt supuse, *ex-ante*, mai riguros, sau *ex-post*, mai permisiv.

■ A fost extins numărul de sectoare reglementate, de la 7 prevăzute în NIS 1 la 18 în NIS 2, defalcate în două categorii:

» **11 sectoare esențiale**: Energie; Transport; Bancar; Infrastructuri ale pieței financiare; Sănătate; Apă potabilă; Ape uzate; Infrastructură digitală; Administrație publică; Managementul serviciilor IT&C (B2B); Spațiu.

» **9 subsectoare**: Electricitate; Încălzire centralizată și răcire centralizată; Petrol; Gaze; Hidrogen; Transport aerian; Transport feroviar; Transport pe apă; Transport rutier.

» **7 sectoare importante**: Servicii poștale și de curierat; Gestionarea deșeurilor; Fabricarea, producția și distribuția de substanțe chimice; Producția, prelucrarea și distribuția de alimente; Fabricare; Furnizori digitali; Cercetare.

» **6 subsectoare**: Fabricarea de dispozitive medicale și de dispozitive medicale pentru diagnostic in vitro; Fabricarea computerelor și produselor electronice și optice; Fabricarea echipamentelor electrice; Fabricarea altor mașini și echipamente neclasificate în altă parte; Fabricarea autovehiculelor, remorcilor și semiremorcilor; Fabricarea altor echipamente de transport.

■ Prin Directiva NIS 2 sunt consolidate **cerințele de securitate cibernetică** impuse entităților vizate, organele de conducere ale acestora (managerii) **având responsabilitatea legală de implementare**. Aceste cerințe de securitate cibernetică includ, printre altele, răspunsul la incidente, criptarea și divulgarea vulnerabilităților de securitate cibernetică.

■ Au fost consolidate cerințele de securitate impuse întreprinderilor și sunt abordate securitatea lanțurilor de aprovizionare și relațiile cu furnizorii. În plus, sunt simplificate obligațiile de raportare și sunt introduse unele măsuri de supraveghere mai stricte pentru autoritățile naționale.

[3] *Directiva 2016/1148 – privind securitatea rețelelor și a sistemelor informatice, transpusă în legislația națională prin Legea nr. 362/2018.*

PAVING THE WAY FOR CLOUD

> **Proiectul de Cloud Guvernamental** se înscrie pe lista **obiectivelor de interes strategic** stabilite la nivel național în vederea asigurării procesului de **transformare digitală în cadrul serviciilor publice din România**.

Demersurile întreprinse în anul 2022 au poziționat statul român mai aproape de avantajele pe care le presupune o infrastructură digitală integrată la nivelul administrației publice. În prezent, eforturile partenerilor sunt concentrate asupra etapelor premergătoare lansării procedurilor de achiziții.

Descrierea tehnică a tuturor componentelor Cloudului Guvernamental, infrastructura de

bază, componentele de IaaS, PaaS și SaaS, precum și securitatea cibernetică a acestora sunt enunțate în cadrul documentației tehnice aferente proiectului, compusă din studiul de fezabilitate și proiectul tehnic. Cele două documente au fost înaintate spre consultarea publică în toamna anului 2022 și avizate în Comitetul Tehnico-Economic pentru Societatea Informațională (CTE) în luna noiembrie 2022.

Conform proiectului tehnic și în concordanță cu specificațiile existente în Planul Național de Redresare și Reziliență, structura cloudului va prezenta 3 niveluri: **intern, dedicat** și **extern**.

- **cloudul intern** – va consta în transpunerea soluțiilor existente în prezent în componenta IaaS și PaaS accesibile tuturor instituțiilor din administrația publică, cu posibilitatea dezvoltării de servicii SaaS, la nivelul căruia vor putea fi vehiculate date cu caracter personal;
- **cloudul dedicat** – va prezenta soluții de cloud disponibile în sectorul comercial, fiind dezvoltat în vederea asigurării funcționării integrate cu cloudul intern, la nivelul căruia vor fi vehiculate date cu un nivel de sensibilitate mai scăzut;
- **cloudul extern** – va fi constituit dintr-un catalog de soluții de cloud externe, generice, accesibile în Internet ca SaaS, ușor accesibile și intuitive.

> **Cloudul Privat Guvernamental (CPG)** va acoperi componenta internă și cea dedicată, ambele urmând a fi instalate și operaționalizate în cele patru centre de date construite la nivelul României.

Un pas important pentru implementarea acestui amplu proiect îl reprezintă data de 27 iunie 2022, în care s-a adoptat OUG nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice, acest act normativ fiind nominalizat inclusiv în numărul anterior al Buletinului CYBERINT (Semestrul II 2022).

Cadrul juridic necesar atât pentru implementarea și asigurarea furnizării serviciilor de cloud, cât și pentru dezvoltarea ulterioară a platformei a fost completat anul acesta de **Hotărârea de Guvern nr. 112 din 8 februarie 2023** privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental.

> Actul legislativ detaliază responsabilitățile instituțiilor partenere și ale utilizatorilor platformei menționate în OUG nr. 89/2022, tipurile de servicii de cloud furnizate, categoriile de date prelucrate în platformă și găzduite de CPG, cadrul de management și stocare a acestora, precum și politica ***cloud first***.

România se află în prezent printre primele state europene care reglementează politica de ***cloud first***, piatră de temelie în construirea infrastructurii de Cloud, promovând serviciile de ***cloud computing*** drept **tehnologie prioritară** pentru administrarea și furnizarea de servicii publice la nivel central și local.

CONFERINȚA BRAȘOV CYBERHUB 2023

Brașov CyberHUB își propune crearea unui ecosistem în domeniul securității cibernetice și tehnologiilor avansate, bazat pe utilizarea resurselor comune ale membrilor fondatori și pe atragerea, respectiv implicarea partenerilor strategici. Activitatea **Brașov CyberHUB** este axată pe două direcții: educația în domeniul securității cibernetice și promovarea conceptului de *cybersecurity* în companii private (inclusiv din domeniul industrial, automotive, dar și medical).

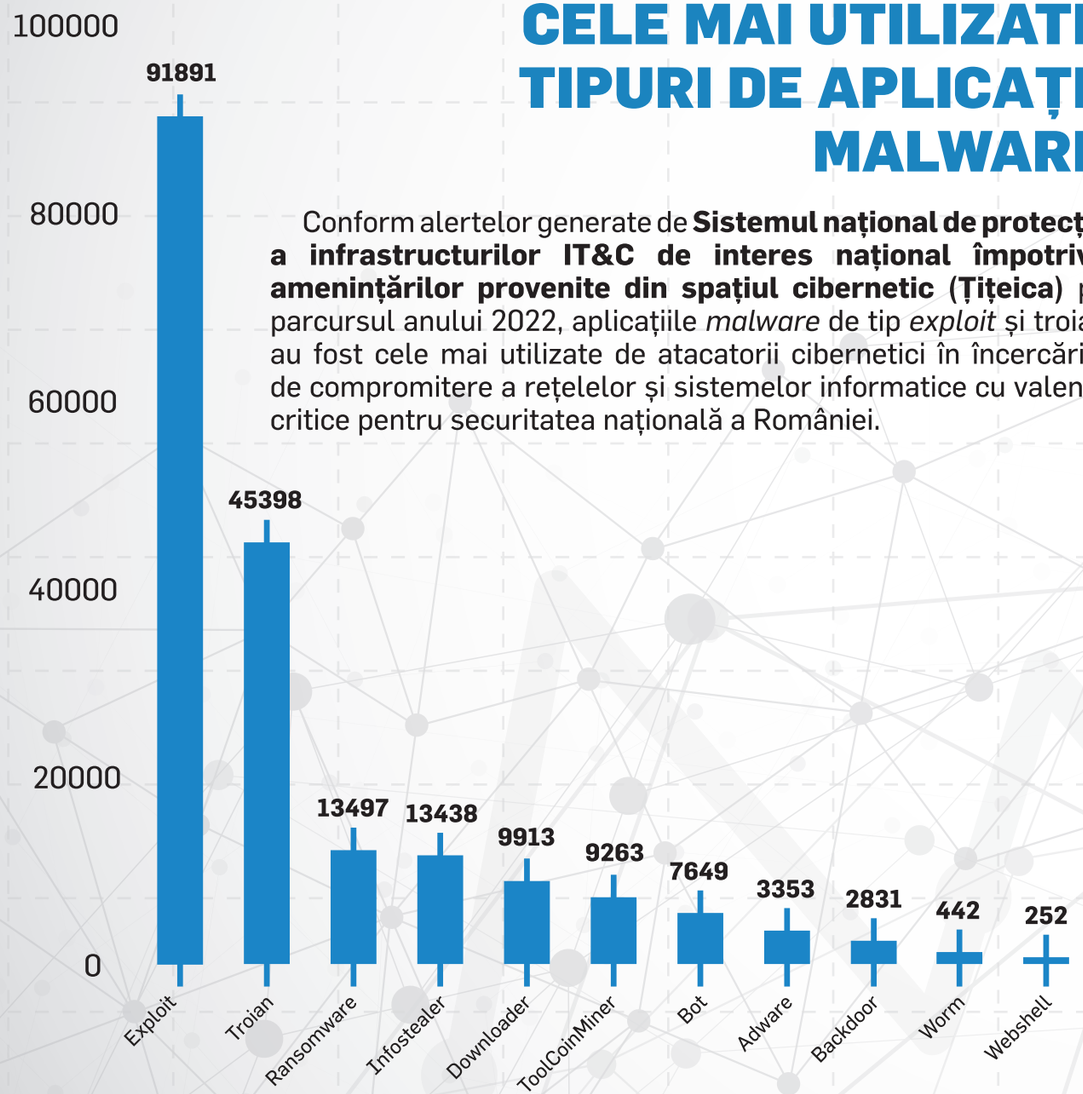
În acord cu misiunea și obiectivele proiectului, în data de 19 mai 2023, va avea loc a doua ediție a conferinței **Brașov CyberHUB**, în Aula principală a Universității Transilvania din Brașov.

Evenimentul concentrat pe teme de actualitate din domeniul securității cibernetice va întruni reprezentanți de rang înalt, precum directori de instituții cu atribuții în domeniul securității cibernetice, specialiști, profesori, furnizori de servicii, instituții, reprezentanți ai unor companii care activează în domeniile: IT, industrie, automotive și medical, având ca scop comun **identificarea de soluții noi în domeniul securității cibernetice**, adaptate specificului fiecărei instituții participante.

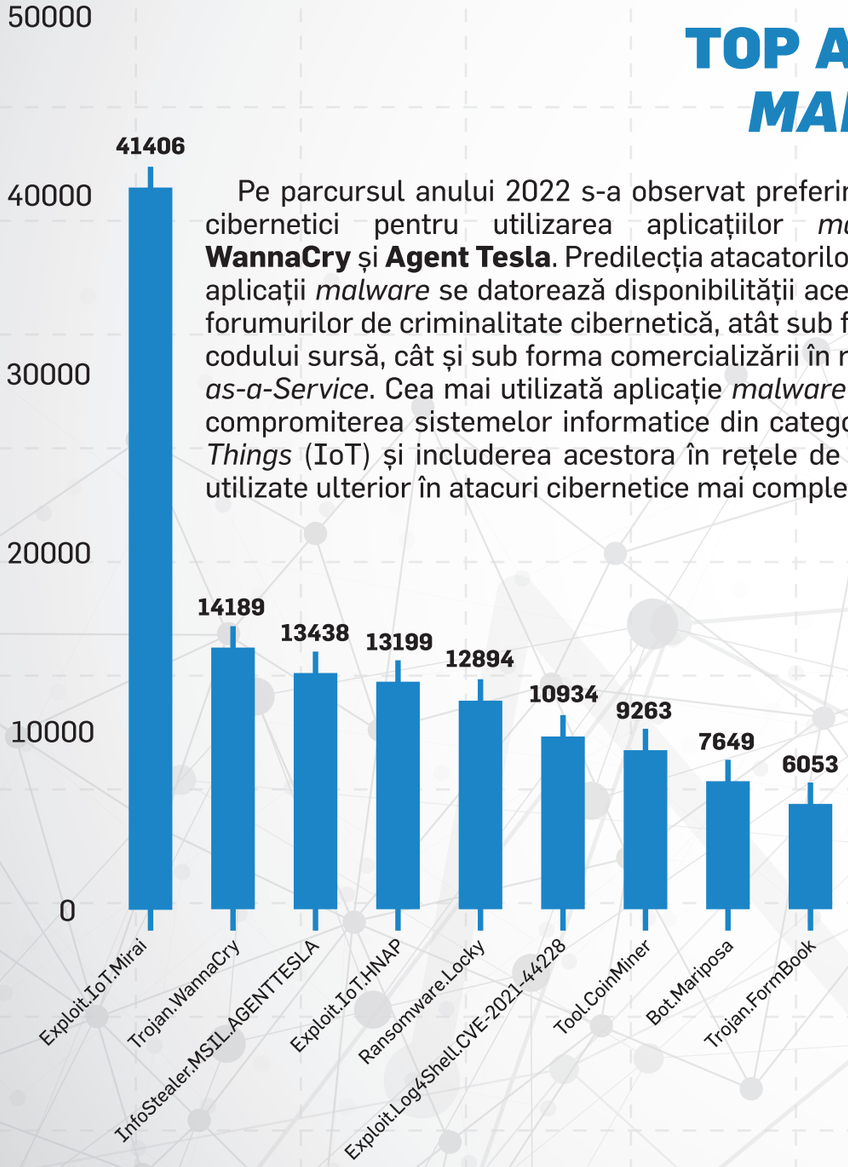
Evenimentul va fi organizat de Centrul Național CYBERINT, Agenția Metropolitană pentru Dezvoltare Durabilă Brașov – Primăria Municipiului Brașov, Universitatea Transilvania din Brașov și compania de securitate cibernetică ATOS Convergence Creators SRL.

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 2022, aplicațiile *malware* de tip *exploit* și troian au fost cele mai utilizate de atacatorii cibernetici în încercările de compromitere a rețelelor și sistemelor informatice cu valențe critice pentru securitatea națională a României.

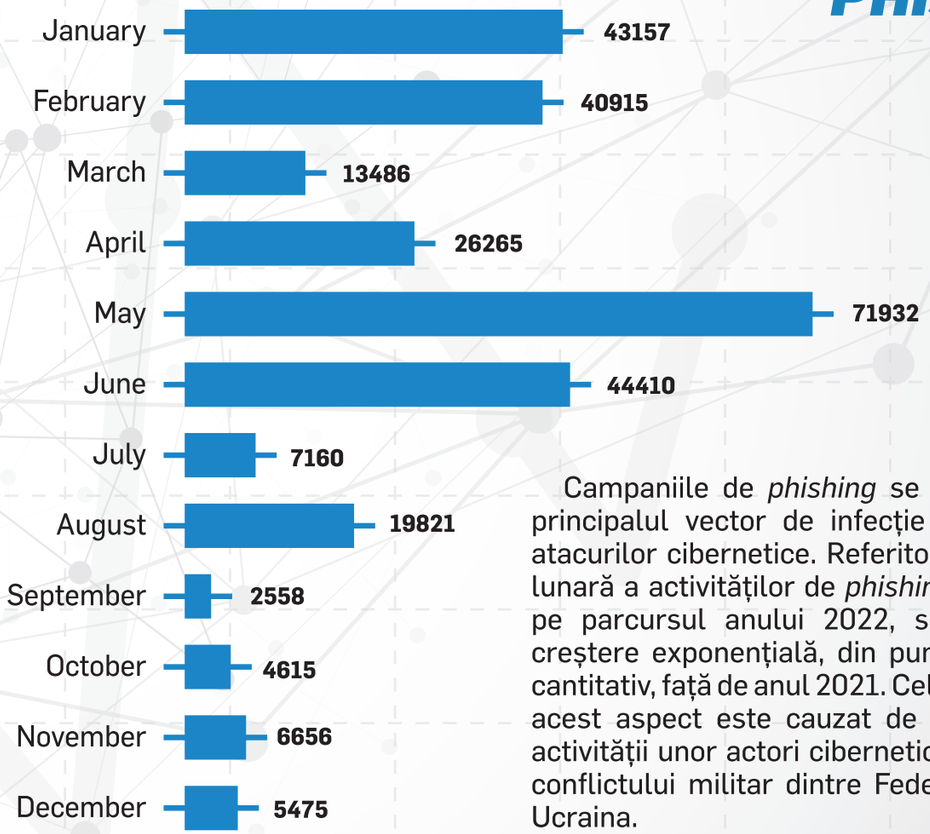


TOP ALERTE *MALWARE*



Pe parcursul anului 2022 s-a observat preferința atacatorilor cibernetici pentru utilizarea aplicațiilor *malware* **Mirai**, **WannaCry** și **Agent Tesla**. Predilecția atacatorilor pentru aceste aplicații *malware* se datorează disponibilității acestora la nivelul forumurilor de criminalitate cibernetică, atât sub forma publicării codului sursă, cât și sub forma comercializării în regim *Malware-as-a-Service*. Cea mai utilizată aplicație *malware*, **Mirai**, vizează compromiterea sistemelor informatice din categoria *Internet of Things* (IoT) și includerea acestora în rețele de boți, care sunt utilizate ulterior în atacuri cibernetice mai complexe.

FRECVENȚA LUNARĂ A ACTIVITĂȚILOR DE *PHISHING*



Campaniile de *phishing* se mențin drept principalul vector de infecție în derularea atacurilor cibernetice. Referitor la frecvența lunară a activităților de *phishing* identificate pe parcursul anului 2022, se remarcă o creștere exponențială, din punct de vedere cantitativ, față de anul 2021. Cel mai probabil, acest aspect este cauzat de intensificarea activității unor actori cibernetici în contextul conflictului militar dintre Federația Rusă și Ucraina.

ChatGPT – IMPACT ASUPRA SECURITĂȚII CIBERNETICE

ChatGPT (*Chat Generative Pre-trained Transformer*) este un program de Inteligență Artificială bazat pe un model complex de *machine learning*, care poate genera răspunsuri „umane", comprehensibile, la întrebările utilizatorilor. Deși există mai multe programe de IA asemănătoare (*Chatsonic, Chinchilla, Bloom, Megatron Turning NLG, Jasper, Replika, Elsa, Socratic* etc.), ChatGPT se diferențiază de acestea prin modalitatea în care „comunică".

Atractivitatea și facilitatea utilizării au determinat creșterea popularității acestui program de IA, din momentul lansării publice, la finalul lui noiembrie 2022, și până în ianuarie 2023, ChatGPT adunând peste 100 de milioane de utilizatori activi. În mediul online de specialitate s-a vehiculat inclusiv că ChatGPT are potențialul de a reconfigura semnificativ modelul de business al motoarelor de căutare.

ChatGPT se folosește de o rețea neuronală bazată pe un transformator pentru a oferi răspunsuri și date într-un model de scriere umană. Tehnologia include un model de limbaj pre-antrenat, care utilizează arhitectura GPT-3 (*un model de procesare a limbajului natural – natural language processing, NLP*) pentru a cerceta cantități imense de date și surse online și pentru a le folosi în generarea răspunsurilor.

OPORTUNITĂȚI, LIMITĂRI ȘI RISCURI ASOCIATE CHATGPT

Utilizarea ChatGPT în domeniul securității cibernetice poate îmbunătăți capabilitățile soluțiilor antivirus și poate crește reziliența sistemelor informatice și rețelelor, în următoarele moduri:

- identificarea și semnalarea e-mailurilor și mesajelor folosite în campanii de tip *phishing* sau *spear-phishing*, *spam* și *adware* (reclame nedorite);
- analizarea și clasificarea automată a diferitelor tipuri de *malware*;
- identificarea și semnalarea automată a traficului de rețea suspect sau modelelor neobișnuite de transfer de date;
- identificarea și raportarea vulnerabilităților sistemului informatic/ rețelei folosite;
- generarea de rapoarte și analize despre amenințările cibernetice, conținut care poate fi partajat, contribuind la creșterea conștientizării (*awareness*-ului) utilizatorilor.

Cu toate acestea, ChatGPT are o serie de limitări, menționate inclusiv de dezvoltatorii săi, compania OpenAI, precum incapacitatea de a răspunde la întrebările care sunt formulate într-un mod specific; răspunsurile slab calitative, lipsite de sens practic sau bazate pe informații false; datele pe care ChatGPT se bazează sunt limitate la nivelul anului 2021 etc.

În plus, instrumentele folosite de IA pot fi predispuse la *bias*-uri din cauza datelor folosite în dezvoltarea acestora, iar lipsa de transparență cu privire la această dezvoltare poate face dificilă înțelegerea modului în care programul a ajuns la o anumită concluzie. **Agenția Uniunii Europene pentru Drepturi Fundamentale** (FRA) a avertizat că **algoritmii bazați pe informații false ar putea cauza prejudicii** și că ar trebui să existe garanții pentru atenuarea discriminării. Acest lucru este potențat de faptul că programele de IA pot genera informații false pe care le prezintă ca faptice, proces cunoscut sub numele de *hallucination* și care, împreună cu fenomenul *deep fake*, poate potența semnificativ capabilitățile campaniilor cibernetice care folosesc tehnici de inginerie socială.

Astfel, la nivelul lunii decembrie 2022, diverși actori cibernetici s-au folosit de capabilitățile ChatGPT pentru a rafina mesajele folosite în campaniile de *phishing* și *spear-phishing*, iar în alt caz pentru dezvoltarea de cod *malware*, fără a avea cunoștințele tehnice necesare. În plus, la nivelul lunii ianuarie 2023, au fost identificate *thread*-uri pe forumurile specializate de *cybercrime* în care se discutau diferitele modalități de folosire a ChatGPT-ului în activități de criptare și exfiltrare de date.

Utilizarea ChatGPT-ului de către actori cibernetici rău intenționați, care dețin sau nu cunoștințe tehnice avansate, va conduce către **o înmulțire cantitativă și calitativă a amenințărilor din ecosistemul cibernetic**.

UTILIZAREA ChatGPT PENTRU A CREA *MALWARE*

Poate cel mai relevant exemplu, în acest sens, este faptul că, în ianuarie 2023, **ChatGPT a fost folosit pentru crearea mai multor tipuri de *malware***, prin exploatarea capacității sale de a genera acțiuni consistente, repetitive și de a ascunde cod *malware* în fișiere. Această metodă a fost folosită pentru dezvoltarea unui ***polymorphic malware***, cu scopul compromiterii sistemului informatic/ rețelei vizate, criptării datelor, dezvoltării de capabilități de *keylogger* și pentru exfiltrarea datelor.

Malware-ul polimorf este un tip de *malware* care este programat să-și modifice în mod repetat „aspectul” sau *signature files*-urile, prin noi rutine de decriptare. Această capabilitate face ca multe soluții tradiționale de securitate cibernetică, cum ar fi soluțiile antivirus sau anti-*malware*, care se bazează pe scanarea tiparelor cunoscute asociate *malware*-urilor, respectiv pe detectarea unei semnături, să nu recunoască și să nu poată bloca răspândirea *malware*-ului respectiv.

Primul pas în crearea *malware*-ului polimorf a fost **ocolirea filtrelor de conținut**, care împiedicau ChatGPT să creeze *tool*-uri care pot fi folosite în activități ilicite. Pentru a face acest lucru, utilizatorii au folosit versiunea API a ChatGPT, care, spre deosebire de versiunea *web*, nu avea filtru de conținut. Apoi, datorită capacității ChatGPT de a crea și modifica continuu injectoare (*injectors*), utilizatorii au reușit să creeze un program *malware* polimorf. În plus, conform specialiștilor în securitate cibernetică, capabilitățile de a genera diverse tehnici de persistență, module **Anti-VM (*Anti-Virtual Machine*)** și alte *payload*-uri, dar și posibilitățile de creare și dezvoltare *malware* ale programului de IA ChatGPT sunt vaste, motiv pentru care există deja îngrijorări legate de utilizarea inteligenței artificiale în viitoare campanii cibernetice, începând cu a doua jumătate a anului 2023.

Din acest motiv, devine din ce în ce mai stringentă **necesitatea unui cadru legal de reglementare pentru programele de Inteligență Artificială**, care să:

- asigure că sistemele de IA implementate sunt sigure și respectă drepturile fundamentale ale utilizatorilor și valorile democratice;
- faciliteze dezvoltarea unei piețe unice pentru sistemele de IA legale, sigure și de încredere și să prevină fragmentarea pieței;
- impună implementarea unor *watermark*-uri sau altor indicatori care să permită utilizatorilor să recunoască dacă un text sau o imagine a fost generată de IA etc.

Astfel de eforturi au fost demarate atât la nivel european - lansarea în 2021 a discuțiilor pentru elaborarea unui **regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind Inteligența Artificială**, cât și național, prin înființarea **Comitetului Român pentru Inteligență Artificială** și demararea unor demersuri de creare a unui cadru strategic național privind Inteligența Artificială.

WWW.SRI.RO/CYBERINT