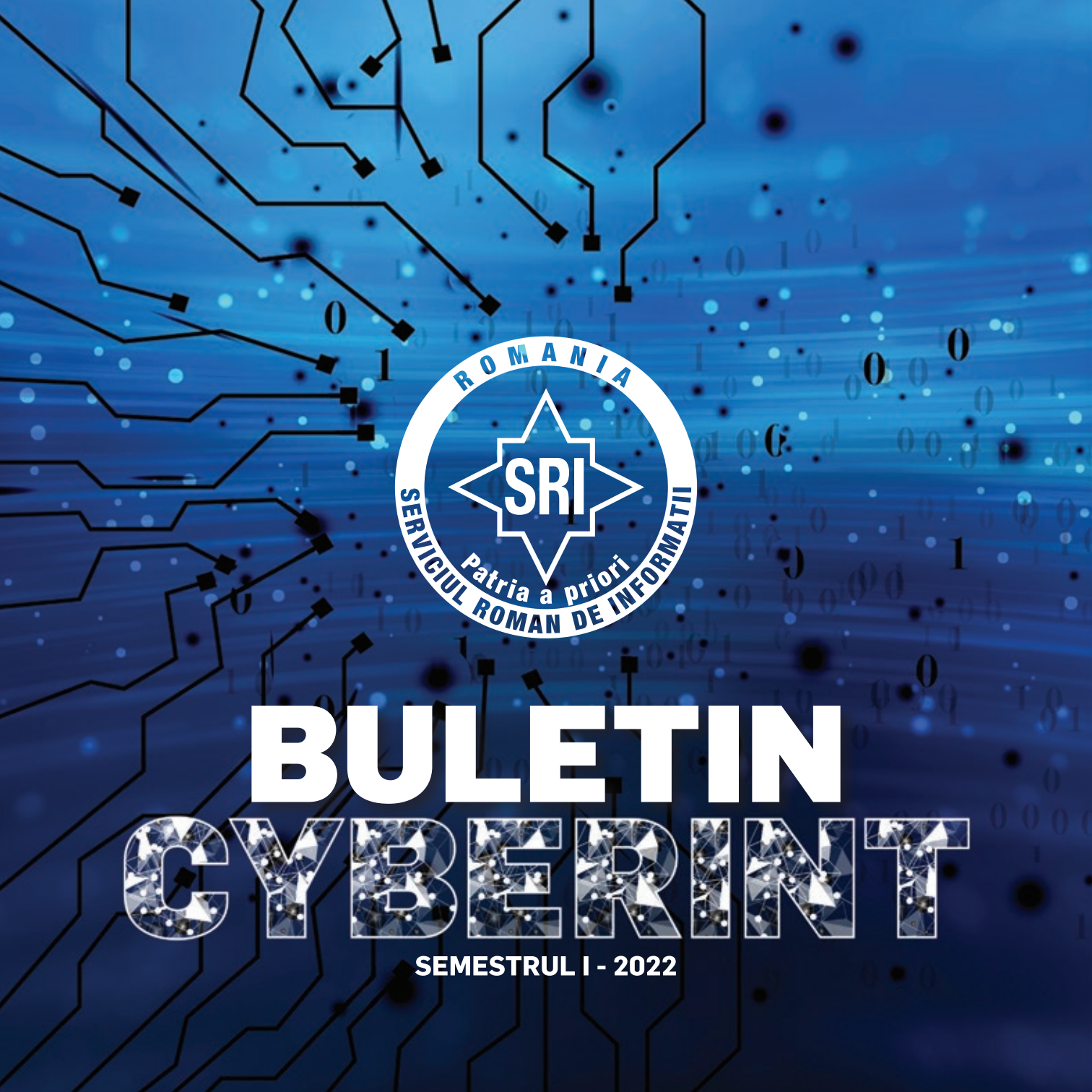


BULETIN CYBERINT

SEMESTRUL I - 2022

RETROSPECTIVA ANULUI 2021 ȘI TRENDURI PENTRU 2022

PRINCIPALELE AMENINȚĂRI CIBERNETICE CU IMPACT LA NIVEL NAȚIONAL

Atacurile cibernetice de tip APT provenite din Federația Rusă și Republica Populară Chineză au reprezentat principala amenințare cibernetică la adresa securității naționale a României, acestea continuând să deruleze atacuri cibernetice asupra infrastructurilor IT&C cu valențe critice.

Ca răspuns la activitățile ostile derulate de acești actori, România s-a raliat unor inițiative de tip ***blame and shame***, prin care au fost atribuite atacuri cibernetice unor entități ruse (cele instrumentate de Serviciul de Informații Externe al Federației Ruse asupra platformei Orion a Companiei SolarWinds), respectiv chineze (cele instrumentate de actorul ATP40 și Ministerul Securității Statului al Republicii Populare Chineze în cadrul campaniei cibernetice HAFNIUM).

Atacurile cibernetice de tip ransomware s-au menținut la un nivel ridicat în 2021, continuând să exploateze contextul pandemic pentru asigurarea succesului atacurilor derulate și pe parcursul anului 2021. Atacurile de tip *ransomware* au rămas una din principalele forme de amenințare și au vizat preponderent instituții din domeniul sănătății, în special prin utilizarea de aplicații malware din familia ***Phobos*** (ex. Spitalul Clinic Numărul 1 CF Witting din București).

În ceea ce privește **atacurile cibernetice cu *infostealer***, aplicațiile malware au fost distribuite prin campanii care au utilizat elemente de inginerie socială (ex. phishing, smishing) și au targetat, în mod nediscriminatoriu, instituții și indivizi din toate domeniile de activitate. Atacatorii au vizat în principal obținerea de date bancare, atât de la nivelul sistemelor informatice (calculator, laptop etc.) prin intermediul ***Agent Tesla***, cât și de la nivelul dispozitivelor de tip smartphone prin intermediul ***FluBot***.

Atacurile cibernetice de tip *defacement* și SQL *Injection* sunt în continuare instrumentate cu scopul de a afecta disponibilitatea și integritatea datelor de la nivelul unor infrastructuri IT&C cu valențe critice. Impactul acestor atacuri rămâne unul scăzut, cele mai relevante pe parcursul anului 2021 fiind atacurile de tip *defacement* instrumentate de grupările de hackeri provenite din spațiul MENA, care au avut drept ținte atât entități private, cât și instituții publice, inclusiv unități spitalicești de la nivel național. Scopul hackerilor a fost distribuirea în mediul virtual a unor mesaje de promovare a grupărilor din care fac parte.

Pe parcursul anului 2021, continuă să persiste o serie de **disfuncții și vulnerabilități de securitate cibernetică la nivelul infrastructurilor IT&C cu valențe critice pentru securitatea națională**, precum: 1) încadrare redusă cu specialiști IT, unii dintre aceștia fără a deține calificările profesionale corespunzătoare; 2) proceduri și politici de securitate ineficiente, nefiind implementate reguli stricte de creare a parolelor sau filtre de restricționare a accesării anumitor domenii din Internet; 3) utilizarea unor echipamente hardware și soluții software pentru care producătorii nu mai asigură suport tehnic sau actualizări de securitate.

În contextul eforturilor de digitalizare desfășurate la nivelul multor instituții ale statului, implementarea acestor proiecte trebuie să se desfășoare în parametri de securitate cibernetică, inclusiv prin integrarea, încă din procesul de dezvoltare, a măsurilor adecvate, conform principiului *secure-by-design*.

PRINCIPALELE TRENDURI PENTRU 2022

1 Dispozitivele inteligente devin tot mai mult parte integrată a vieții noastre, fapt ce atrage interesul atacatorilor cibernetici. **Securitatea cibernetică, de cele mai multe ori precară, a dispozitivelor IoT face ca acestea să reprezinte puncte inițiale de acces**, atacatorii având posibilitatea de a escalada privilegiile și compromite și alte dispozitive din aceeași rețea (dispozitive mobile, laptop-uri, stații de lucru etc).

2

Anul 2021 ne-a demonstrat că atacurile de tip *supply chain* au o eficiență considerabil mai crescută (șantajarea victimelor prin indisponibilizarea unor servicii care duc la pierderi financiare masive), context în care, anul acesta, ne putem aștepta la **creșterea numărului de atacuri pe lanțul de aprovizionare la nivel global**, cu precădere asupra unor companii private.

3

Este de așteptat ca **amenințarea proiectată de entitățile sponsorizate de Federația Rusă să se manifeste la un nivel mai ridicat**, mai ales în actualul context politic și militar din Ucraina. Vor fi vizate instituțiile la nivelul cărora sunt vehiculate informații de interes în vederea obținerii unor avantaje strategice. În eventualitatea impunerii unor sancțiuni, este de așteptat ca răspunsul cibernetic ofensiv să fie unul direct proporțional, fiind vizate companii din mai multe sectoare de activitate și instituții financiare.

4

Campaniile *ransomware* vor continua să reprezinte una dintre principalele provocări, având în vedere succesul pe care l-au avut în anul precedent. Ne putem aștepta ca focusul atacatorilor să nu mai fie în principal pe criptarea datelor, ci, mai degrabă, pe exfiltrarea acestora și șantajarea victimelor cu publicarea lor. În acest context, în 2022, este de așteptat ca eforturile instituțiilor cu atribuții în domeniul securității cibernetice de combatere a criminalității cibernetice și de destructurare a unor grupări cybercrime să se intensifice, în vederea reducerii impactului generat.

5

În prezent, **atacul cibernetic de tip DDoS devine una din componentele războiului hibrid**, aspect confirmat de contextele în care acesta a fost utilizat în ultima perioadă (la adresa statelor, infrastructurilor critice și marilor companii). Astfel, în 2022 este posibil să asistăm la lansarea unor atacuri DDoS menite să genereze indisponibilizări masive sau să creeze diversiuni, în vederea lansării altor atacuri (cu scopul de exfiltra date sau sume de bani).

6

Campaniile de tip „*ransom DDoS*" au devenit tot mai populare în ultimii doi ani. Acestea au ca scop șantajarea victimelor, sub amenințarea unor atacuri cibernetice de tip DDoS, în vederea obținerii de venituri. În ultimul an, grupările de hackeri s-au axat din ce în ce mai mult pe instrumentarea unor atacuri cibernetice de tip DDoS, vizând în principal entități din sectorul privat, în special din domeniul financiar. Este de așteptat ca fenomenul să înregistreze o creștere, atât în frecvență, cât și în complexitate, în 2022.

7

Având în vedere popularitatea crescută a criptomonedelor și gradul de utilizare a acestora, în anul 2022, estimăm că **atacatorii cibernetici vor derula campanii pentru obținerea credențialelor de acces la portofele electronice** sau conturi pe platforme de tranzacționare, cu scopul final de a fura activele digitale ale victimelor.

STRATEGIA DE SECURITATE CIBERNETICĂ A ROMÂNIEI 2.0

2022-2027

Amenințările provenite din spațiul cibernetic sunt într-o continuă transformare, evoluând în acord cu creșterea nivelului de utilizare a resurselor IT&C la nivelul societății și dezvoltarea noilor tehnologii la nivel internațional. O condiție esențială în vederea asigurării unui răspuns eficient la adresa acestor provocări este consolidarea unui cadru normativ la nivel național, aflat în concordanță atât cu evoluțiile tehnologice, cât și cu reglementările în domeniu la nivel internațional.

Demersurile privind reglementarea domeniului securității cibernetice în România au început în anul 2013, prin adoptarea *Hotărârii de Guvern nr. 271/2013*[1] *pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică.*

Adoptată prin *Hotărârea de Guvern nr. 1321/30 decembrie 2021*, noua Strategie de Securitate Cibernetică a României (SSCR) reprezintă o actualizare a cadrului normativ existent, în vederea racordării acestuia la amenințările cibernetice care se pot răsfrânge asupra tuturor domeniilor economice și sociale la nivel național. În acest sens, SSCR 2.0 este un act cu un grad ridicat de aplicabilitate la nivelul tuturor actorilor existenți în viața socială: cetățeni, entități publice, private sau instituții din mediul academic.

Pentru asigurarea securității rețelelor și sistemelor informatice, aceștia trebuie să deruleze acțiuni conjugate, care să vizeze atât dezvoltarea continuă a capabilităților de detecție, combatere și investigare a atacurilor cibernetice, cât și dezvoltarea rezilienței acestora prin:

- implementarea unor programe educaționale în domeniu;
- asigurarea unui buget dedicat securității cibernetice;
- susținerea și încurajarea cercetării și inovării în domeniu;
- asigurarea cooperării atât la nivel național, cât și la nivel internațional.

[1] *Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013*

Viziunea Strategiei este de a promova un cadru național competent, complex, care să consolideze capabilitățile României de a preveni, descuraja și a răspunde amenințărilor provenite din spațiul cibernetic. În vederea realizării acestui deziderat, este necesar ca România să adopte inclusiv o abordare proactivă, în conformitate cu arhitectura internațională de cooperare în domeniu.

OBIECTIVELE SSCR 2.0

1 REȚELE ȘI SISTEME INFORMATICE SIGURE ȘI REZILIENTE

SSCR vizează asigurarea funcționalității și continuității în parametrii optimi a confidențialității, integrității și disponibilității datelor gestionate la nivelul rețelelor și sistemelor informatice cu valențe critice pentru securitatea națională, îndeosebi a celor din domenii aferente serviciilor esențiale.

2 CADRU NORMATIV ȘI INSTITUȚIONAL CONSOLIDAT

Dezvoltarea și eficientizarea cooperării la nivel interinstituțional este o condiție esențială pentru gestionarea amenințărilor generate de atacurile cibernetice. Astfel, toți actorii implicați trebuie să relaționeze eficient și să asigure un cadru normativ și instituțional capabil să consolideze securitatea cibernetică a rețelelor și sistemelor informatice de la nivel național.

3 PARTENERIAT PUBLIC-PRIVAT PRAGMATIC

Consolidarea unei cooperări eficiente și sustenabile între mediul public și cel privat contribuie semnificativ la creșterea capacităților naționale de detecție, investigare și contracarare a amenințărilor provenite din spațiul cibernetic. Astfel de parteneriate pot genera inclusiv beneficii socio-economice (resursă umană calificată, creșterea contribuției industriei IT&C și securitate cibernetică la PIB-ul național etc.).

4 REZILIENȚĂ PRINTR-O ABORDARE PROACTIVĂ ȘI DESCURAJARE

Complexitatea amenințărilor cibernetice la adresa României impune necesitatea pregătirii instituțiilor abilitate de a pune în aplicare orice măsură proactivă în vederea asigurării rezilienței rețelelor și sistemelor informatice. Concomitent, acestea trebuie să dețină capabilități și mecanisme care să descurajeze derularea unor atacuri cibernetice împotriva țintelor sau obiectivelor naționale.

5 ROMÂNIA – ACTOR RELEVANT ÎN ARHITECTURA INTERNAȚIONALĂ DE COOPERARE

Având în vedere lipsa granițelor din spațiul cibernetic, SSCR își propune angajarea României în activități de cooperare internațională, care să asigure inclusiv rolul României ca actor relevant în arhitectura internațională de cooperare.

Așadar, adoptarea Strategiei de Securitate Cibernetică 2.0 (2022-2027) și a Planului de Acțiune aferent reprezintă o adaptare importantă la nivel național a cadrului normativ, care nu doar asigură reziliența rețelelor și sistemelor informatice, dar și aliniază România la standardele internaționale de pregătire și răspuns împotriva amenințărilor cibernetice.

LOG4SHELL
O VULNERABILITATE CU IMPACT RIDICAT

La sfârșitul lunii noiembrie - începutul lunii decembrie 2021, cercetătorii din domeniul securității cibernetice au identificat pentru prima dată semne de exploatare a unei vulnerabilități care indica a fi una dintre cele mai de impact din ultima perioadă.

Vulnerabilitatea este prezentă la nivelul aplicației de tip *logging framework* Log4j, care este utilizată pe scară largă în cadrul serverelor web Apache pentru înregistrarea și indexarea mesajelor de tip *log*. Exploatarea acesteia permite atacatorului să execute cod de la distanță la nivelul serverului țintă prin înregistrarea unui cod nelegitim de la nivelul unui server de tip *Lightweight Directory Access Protocol* (LDAP) controlat de către acesta.

Din punctul de vedere al severității, vulnerabilitatea denumită ***Log4Shell*** **(CVE-2021-44228)** este una de nivel critic maxim (scor CVSS 10), valoarea fiind stabilită pe baza următoarelor caracteristici identificate:

- complexitatea atacului cibernetic este una scăzută, în timp ce impactul asupra confidențialității, integrității și disponibilității este unul ridicat;

Este necesară doar deținerea unui server de tip LDAP, pentru exploatarea unui număr ridicat de servicii vulnerabile, pe baza unui PoC disponibil public în mediul online.

- aplicațiile afectate de această vulnerabilitate sunt populare și utilizate la scară largă;

Au fost identificate peste 250 de servicii unice care sunt afectate de această vulnerabilitate.

- codul de exploatare este disponibil public;

Conform *Proof of concept*-ul exploatării vulnerabilității publicat la nivelul mai multor platforme online, atacatorul poate exploata vulnerabilitatea prin transmiterea unei cereri către serverul țintă, utilizând un server de tip LDAP.

- exploatarea vulnerabilității permite compromiterea serverelor și posibilitatea executării de cod;

Introducerea *codului nelegitim* la nivelul aplicațiilor care utilizează librăria log4j va avea ca efect încărcarea în memorie și execuția unui cod arbitrar, pus la dispoziție de atacator prin intermediul unui server de tip LDAP controlat, drept răspuns la solicitarea transmisă. În aplicație, codul respectiv va fi descărcat și executat în mod automat, moment în care sistemul este compromis.

Riscurile proiectate de această vulnerabilitate pot fi mitigate sau eliminate, prin:

- Actualizarea aplicației la versiunea 2.16.0, furnizată de Apache, care elimină complet parametrii vulnerabili (Message Lookups și JNDI);

- În cazul în care nu poate fi realizată actualizarea aplicației, este necesară configurarea / eliminarea parametrilor vulnerabili pentru versiunile anterioare.

ATACURI CIBERNETICE ASUPRA SISTEMELOR INFORMATICE GUVERNAMENTALE DIN UCRAINA

La începutul anului 2022, infrastructurile IT&C din Ucraina au fost vizate de o serie de campanii cibernetice cu moduri diferite de operare, cele mai relevante în acest sens fiind un atac de tip *defacement* și un atac distructiv.

ATACUL CIBERNETIC DE TIP *DEFACEMENT*

În intervalul 13 - 14 ianuarie 2022, infrastructurile IT&C guvernamentale din Ucraina au fost ținta unui atac cibernetic, care a **modificat conținutul paginilor principale** a peste 70 de website-uri aparținând unor instituții publice ucrainene și companii private.

Conținutul paginilor web ale instituțiilor publice a fost modificat cu textul *„Ucraineni! Toate datele personale au fost încărcate în mediul online. Toate datele de pe computere sunt distruse, este imposibil să le recuperați...Toate informațiile despre voi au devenit publice, temeți-vă și așteptați-vă la ce este mai rău. Acesta este trecutul, prezentul și viitorul vostru."* Mesajul a fost tradus în 3 limbi: **rusă, poloneză** și **ucraineană**.

Conform CERT Ucraina (CERT-UA), bazele de date asociate website-urilor **nu au fost modificate și nu au fost exfiltrate date**. Totodată, în vederea limitării efectelor atacului și identificării sursei compromiterii, **CERT-UA a oprit temporar funcționarea și altor website-uri guvernamentale.**

Rezultatele investigațiilor primare realizate de autoritățile ucrainene au indicat drept variante posibile de compromitere a website-urilor **exploatarea de către atacatori a vulnerabilităților CVE-2021-32648[2] și Log4Shell[3]**, ambele utilizate frecvent atât la nivel guvernamental, cât și în mediul companiilor private.

Ulterior, Serviciul de Securitate al Ucrainei (SSU) a publicat un comunicat prin care a afirmat că există indicii noi cu privire la modul în care a fost realizat atacul de *defacement*, menționând faptul că este foarte probabil ca atacatorul să fi reușit compromiterea companiei KITSOFT, care se ocupă de administrarea paginilor web afectate. De asemenea, SSU a afirmat că deține date care indică drept autori ai atacului de *defacement* hackeri asociați serviciilor secrete ruse.

ATACUL CIBERNETIC DISTRUCTIV

Autoritățile ucrainene au publicat o serie de rapoarte tehnice cu privire la un atac cibernetic distructiv, care a avut loc concomitent cu atacul cibernetic de tip *defacement* descris anterior.

Atacul distructiv a fost disimulat sub forma unuia cu motivație financiară, atacatorul atașând un mesaj de răscumpărare cu textul *„Hard-drive-ul a fost compromis. Dacă dorești să îți recuperezi hard-drive-urile organizației tale, trebuie să ne plătești 10.000$ în portofelul electronic de Bitcoin (...) și să ne dai mesaj prin intermediul TOX (ID...) cu numele organizației tale. Te vom contacta ca să îți dăm instrucțiuni suplimentare."*. Cu toate acestea, investigațiile tehnice au relevat o serie de date care indică faptul că **atacul cibernetic nu a fost motivat financiar**, ci doar configurat astfel încât să creeze această aparență și, implicit, să indice drept autori ai atacului grupări independente, neasociate vreunui stat.

Scopul final al atacului a fost acela de a distruge datele utilizatorilor (aspect necaracteristic campaniilor motivate financiar), iar aplicațiile malware utilizate au funcționat în 2 etape:

1. SUPRASCRIEREA MASTER BOOT RECORD[4] (MBR) PENTRU A AFIȘA UN MESAJ FALS DE RĂSCUMPĂRARE

Aplicația malware a fost instalată de atacator în diverse locații din cadrul sistemelor compromise (precum C:\PerfLogs, C:\ProgramData etc.) și a fost denumită **stage1.exe**.

---

[2] *Vulnerabilitate critică ce afectează platformele web de tip Content Management System/ CMS prin intermediul cărora sunt realizate platforme web.*
[3] *Vulnerabilitate care afectează utilitarul Log4J, prin intermediul căruia sunt gestionate evenimente de securitate cibernetică, a cărei exploatare permite executarea unor comenzi în sistemele vizate de către atacator și, în final, preluarea sub control a acestora.*

[4] *MBR reprezintă o componentă a hard drive-ului care indică sistemului informatic cum să inițializeze sistemul de operare.*

În urma execuției aplicației malware, atacatorul a suprascris MBR din cadrul sistemelor victimă cu un mesajul de răscumpărare precizat anterior, care conținea adresa unui portofel electronic de Bitcoin și instrucțiuni de plată, creând astfel aparențele unei campanii cibernetice motivate financiar.

2. CORUPEREA FIȘIERELOR

În a doua etapă a atacului, o aplicație malware denumită **stage2.exe** descarcă din cadrul unui canal de **Discord** componenta malware finală, care sortează fișierele din sistemele informatice în funcție de extensia acestora. În final, aplicația suprascrie fișierele, le redenumește aleatoriu extensia, situație în care acestea devin **inutilizabile și nerecuperabile**.

Astfel, deși atacul cibernetic a creat aparența unui ransomware, scopul real a fost compromiterea sistemelor informatice guvernamentale ucrainene și distrugerea datelor din cadrul acestora, indicând astfel că motivația reală a fost afectarea capacității de funcționare a statului ucrainean.

Atât, suprascrierea MBR, cât și coruperea fișierelor sunt similare **modului de operare al APT SANDWORM[5] observat în cadrul campaniei cibernetice motivate strategic NotPetya[6], derulată în anul 2017**. Campania cibernetică a fost inclusiv atribuită public, în anul 2020, de SUA către Serviciul Militar de Informații al Federației Ruse (GRU) și către actorul cibernetic APT SANDWORM.

[5] *În data de 28 octombrie 2019, APT SANDWORM a derulat atacuri cibernetice complexe asupra unor infrastructuri din instituții politice, sectorul neguvernamental și sectorul media din Georgia. Actorul cibernetic a reușit compromiterea a mii de site-uri georgiene și scoaterea din funcțiune pentru câteva ore a două posturi TV. În urma atacurilor lansate asupra Georgiei,* ***SUA și Marea Britanie au atribuit în mod public gruparea cibernetică APT SANDWORM către Serviciul Militar de Informații al Federației Ruse/GRU****, acest demers fiind susținut inclusiv de România.*

[6] *În anul 2017, atacul cibernetic NotPetya (asociat unor entități statale de origine rusă) a vizat compromiterea unor sisteme informatice la nivel mondial, fiind concentrat în special asupra Ucrainei. Finalitatea atacului cibernetic a constat în ștergerea sau suprascrierea fișierelor stocate în cadrul sistemelor informatice compromise. Modul de operare al NotPetya a inclus afișarea unui mesaj de răscumpărare a datelor, cu instrucțiuni de plată, însă adresa portofelului electronic de Bitcoin transmisă de atacator era falsă, aspect care a relevat faptul că interesul real al atacatorului nu a fost unul financiar, ci unul distructiv.*

ATACURI CIBERNETICE DE TIP BRUTE FORCE REALIZATE ÎN ANUL 2021

Anul 2021 a fost marcat, la nivel internațional, de derularea mai multor campanii de atac cibernetic de tip *brute-force*, scopul principal al acestora fiind **obținerea accesului la sisteme și date sensibile de către actori cibernetici**.

Conform companiilor de securitate cibernetică, atacurile de tip ***brute-force*** au înregistrat o creștere de până la 600% la mijlocul anului 2021, față de aceeași perioadă a anului 2020. Atacul cibernetic de tip *brute-force* reprezintă o metodă de acces neautorizat la un sistem IT&C sau de decodare a conținutului criptat folosind „*forța brută*" de calcul, prin programe care aplică metoda încercare-eroare (trial and error) a unui număr cât mai mare de combinații de credențiale de acces.
Actorii cibernetici folosesc *brute-force* încă de la începutul utilizării credențialelor de acces (combinație utilizator - parolă), însă acest tip de atac cibernetic a luat amploare din momentul adoptării regimului de muncă *work-from-home* în contextul pandemiei COVID-19.

Pentru derularea atacurilor cibernetice de tip *brute-force*, actorii ciberneticii folosesc tool-uri specializate de automatizare, care pot fi realizate *in-house* sau cumpărate din mediul *darkweb*. Atacatorii utilizează inclusiv baze de date ce conțin credențiale exfiltrate anterior de alți actori cibernetici, precum și sisteme informatice compromise (*botnet)* care oferă puterea de calcul necesară pentru derularea de atacuri cibernetice.
Cu toate că atacurile de tip *brute-force* presupun alocarea de resurse semnificative din partea atacatorilor, acestea sunt eficiente, mai ales ca parte a unor atacuri cibernetice complexe. Aceste atacuri sunt de mai multe tipuri:

ATACURI BRUTE-FORCE SIMPLE

Un astfel de atac utilizează scripturi și procese de automatizare pentru „a ghici" parolele utilizatorilor. În mod uzual, în cadrul unui atac *brute-force* sunt încercate sute de combinații de credențiale de acces pe secundă, iar în cazul parolelor simple (de exemplu „123456" sau „password") acestea sunt compromise în câteva minute.

ATACURI BRUTE-FORCE DICȚIONAR

În derularea atacului sunt utilizate combinații de cuvinte și fraze comune, dar și parole care au fost obținute anterior (în cadrul altor campanii de atac) sau disponibile în mediul darkweb.

CREDENTIAL STUFFING

În acest caz un actor cibernetic folosește doar credențiale de acces valide, exfiltrate în urma derulării altor atacuri cibernetice. Acest atac are o rată ridicată de succes, deoarece oamenii au tendința de a refolosi parolele în cadrul mai multor platforme/ conturi pe care le utilizează.

REVERSE BRUTE-FORCE

Într-un atac de tip brute-force normal, atacatorii cunosc conturile pe care doresc să le compromită și utilizează combinații de parole în acest sens. În cazul reverse brute-force, atacatorii cunosc parole utilizate în cadrul unei organizații și încearcă compromiterea oricărui cont în baza acestor parole.

PASSWORD SPRAYING

Acest tip de atac este des întâlnit și presupune încercarea unei parole comune (de exemplu „password") asupra unei multitudini de conturi.

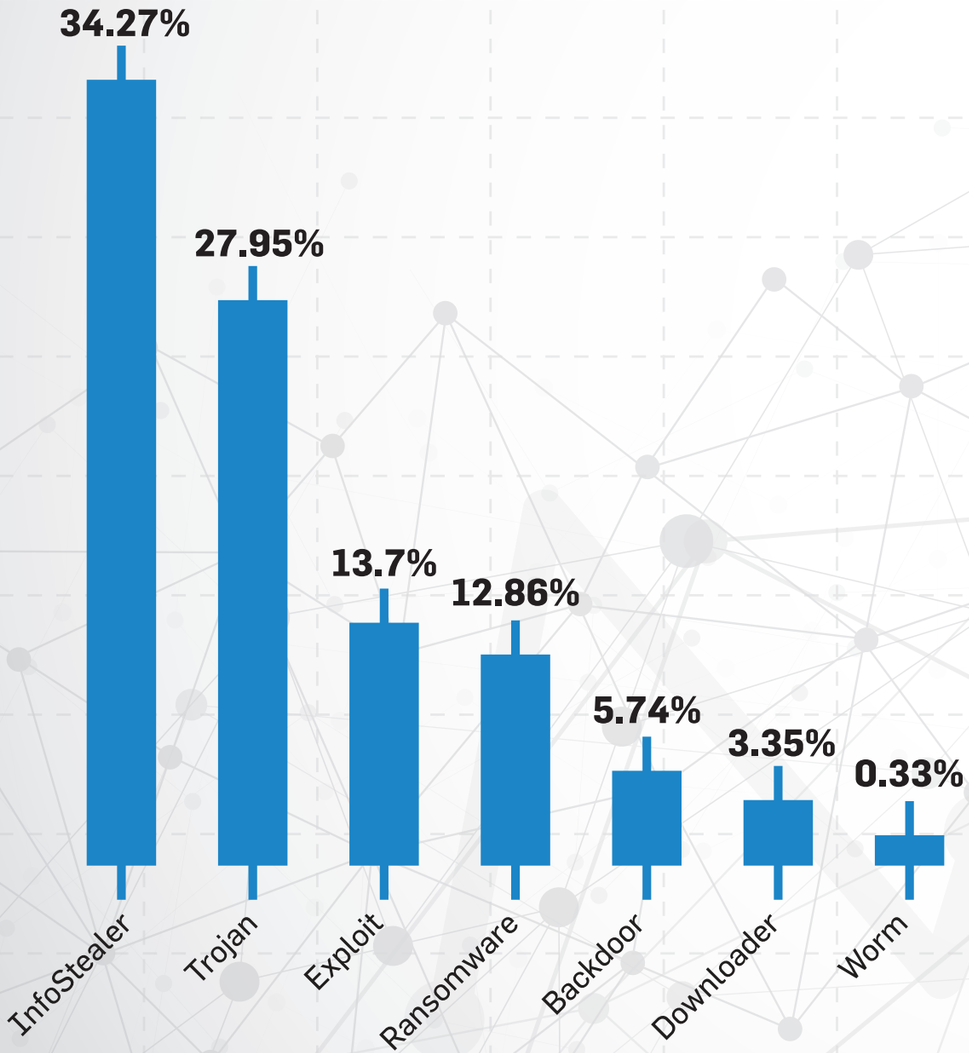
Având în vedere numărul ridicat de atacuri de tip *brute-force*, precum și impactul pe care îl pot avea asupra unor organizații private sau instituții de stat, agențiile de securitate cibernetică guvernamentale din SUA și Marea Britanie **au atribuit public o serie de atacuri cibernetice de tip brute-force către Serviciul de Informații Militare al Federației Ruse/ GRU**, precum și către **APT 28/SOFACY**, actor cibernetic atribuit public către acest serviciu de informații.

În vederea limitării ratei de succes a atacurilor de tip brute-force este recomandată implementarea de măsuri precum:

- **Utilizarea autentificării în mai mulți pași** – presupune utilizarea mai multor forme de autentificare concomitent, de exemplu parolă și amprentă;

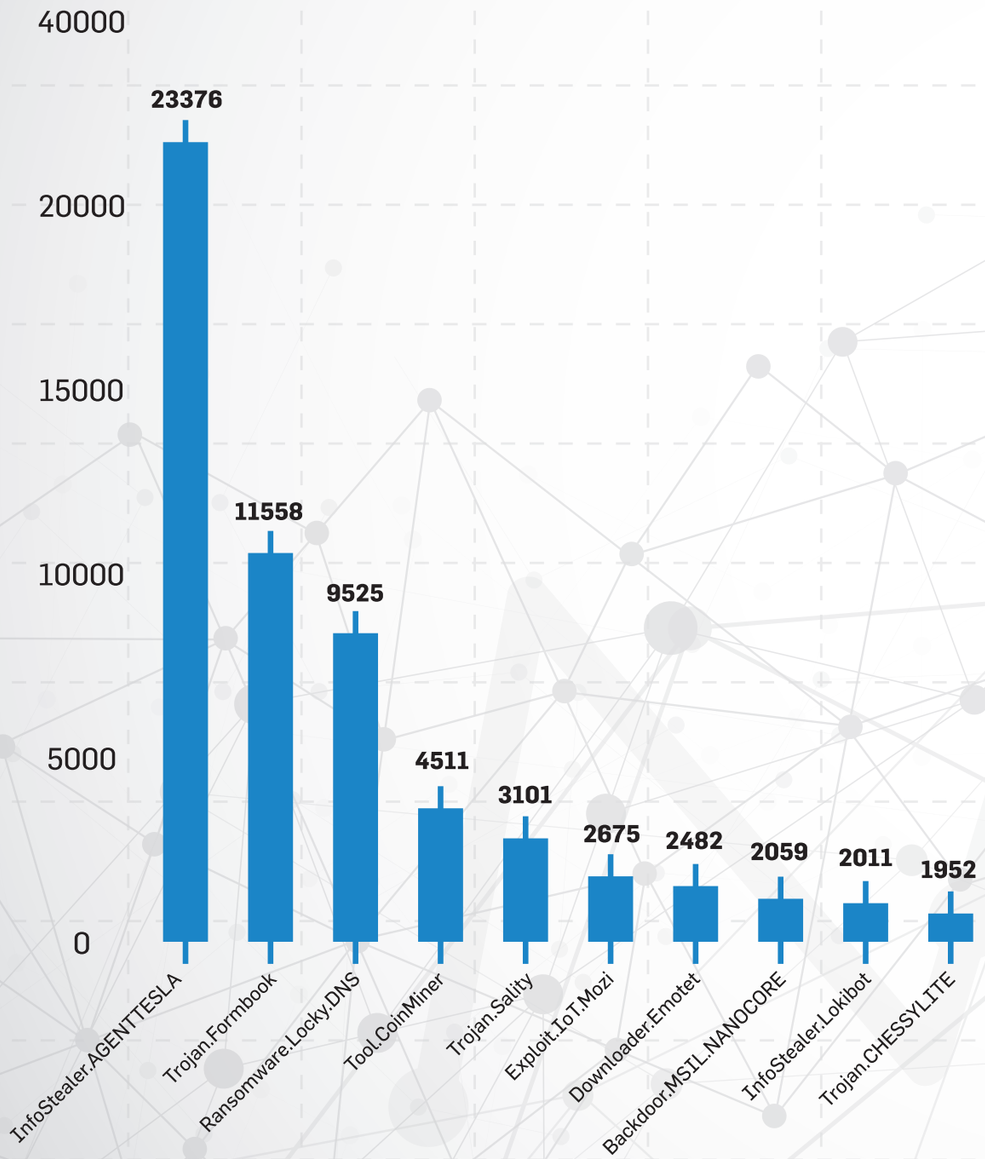
- **Adoptarea de politici de securitate cibernetică stricte** – în acest sens este utilă introducerea unor reguli care să reglementeze folosirea unor parole complexe (combinații de litere, cifre, simboluri speciale, cel puțin 8 caractere etc.) sau care să oblige utilizatorii să schimbe parolele la un interval de timp cât mai scurt.

STATISTICI
PENTRU ANUL 2021



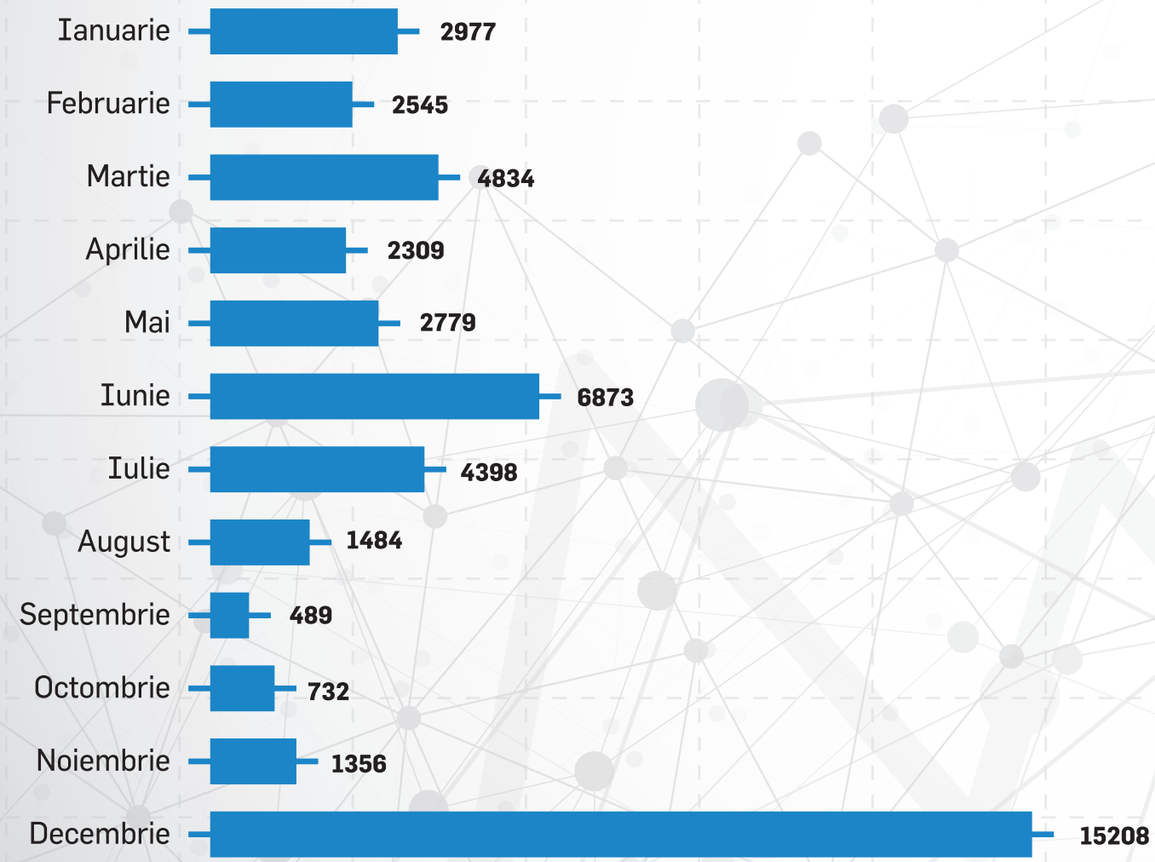
TOP 10 ALERTE MALWARE

Conform alertelor generate de sistemul Țițeica pe parcursul anului 2021, aplicațiile malware de tip infostealer și troian au fost cele mai utilizate de atacatorii cibernetici în încercările de compromitere a infrastructurilor IT&C cu valențe critice pentru securitatea națională a României. Acest comportament indică intenția atacatorilor de a fura date în vederea comercializării acestora pe forumuri de criminalitate cibernetică, respectiv pentru facilitarea unor atacuri ulterioare.



CELE MAI UTILIZATE TIPURI DE APLICAȚII MALWARE

Pe parcursul anului 2021, s-a observat preferința atacatorilor cibernetici pentru utilizarea aplicațiilor malware Agent Tesla, Formbook și Locky, pentru a compromite sistemele vizate. Cea mai utilizată dintre acestea, aplicația malware Agent Tesla, este un Remote Access Trojan, disponibil pentru achiziționare în format Malware-as-a-Service de pe forumuri de criminalitate cibernetică. Aceasta are capabilități ce permite atacatorului preluarea controlului total și de la distanță asupra unui sistem informatic sau asupra unei rețele: controlul sistemului de operare și al soluțiilor antivirus, rulare/blocare/oprire procese, exfiltrare de fișiere, credențiale de acces și date sensibile, captarea șirurilor de caractere introduse de la tastatură și realizarea de capturi de ecran.



FRECVENȚA LUNARĂ A ACTIVITĂȚILOR DE PHISHING

Campaniile de phishing rămân principalul vector de infecție în derularea atacurilor cibernetice. Referitor la frecvența lunară a activităților de phishing identificate pe parcursul anului 2021, s-a remarcat tendința atacatorilor de a crește exponențial numărul atacurilor în luna decembrie. Cel mai probabil, intensificarea activității pe parcursul acestei luni a fost generată de exploatarea contextelor oferite de perioada de sărbători și apariția variantei Omicron a virusului SARS-CoV-2.

INIȚIATIVA DE COMBATERE A RANSOMWARE

Pandemia COVID-19 a determinat intensificări și diversificări ale fenomenului atacurilor cibernetice de tip *ransomware*, îndreptate atât asupra instituțiilor publice, cât și asupra companiilor private și utilizatorilor individuali. Aceste activități din sfera criminalității cibernetice au reprezentat bazele ***Inițiativei de Combatere a Ransomware (Counter Ransomware Initiative – CRI)***, propusă de Statele Unite ale Americii.

Ransomware – aplicație care criptează fișierele din cadrul sistemelor informatice infectate, afectând integritatea și disponibilitatea datelor stocate la nivelul acestora. Scopul actorilor cibernetici care derulează atacuri de tip *ransomware* este obținerea de beneficii financiare, pentru decriptarea datelor fiind solicitată plata unei răscumpărări în criptomonedă.

ATACURI RANSOMWARE DE AMPLOARE	
Colonial Pipeline	*Kaseya*
În luna mai 2021, compania americană **Colonial Pipeline**, cel mai mare operator al conductelor de petrol din Statele Unite ale Americii, și-a oprit activitatea din cauza unui atac cibernetic de tip *ransomware* cu aplicația malware **DarkSide**, care le-a afectat infrastructura IT&C principală. Timp de 5 zile, transportul produselor petroliere prin conductele Colonial Pipeline a fost întrerupt, ceea ce a destabilizat economia SUA.	În luna iulie 2021, compania americană **Kaseya**, care oferă servicii de management IT în întreaga lume, a fost victima unui atac cibernetic de tip ransomware cu aplicația malware **Revil**. Atacul a fost unul de tip supply-chain, întrucât a afectat aplicația dezvoltată de Kaseya și a avut impact asupra activității a peste 1500 de companii la nivel mondial care o utilizau.

România este unul dintre cele 31 de state care au participat la reuniunea multilaterală pe tema atacurilor cibernetice de tip ransomware, organizată în perioada 13 – 14.10.2021 de Consiliul Securității Naționale din SUA (NSC), sub coordonarea Casei Albe. Evenimentul s-a desfășurat în sistem videoconferință, România fiind reprezentată de Directorul Centrului Național CYBERINT, Anton Rog, în cadrul panelului „Securitatea rețelelor și reziliență".

Reuniunea multilaterală s-a încheiat prin publicarea unei declarații comune, prin care statele participante au agreat concentrarea eforturilor pe următoarele coordonate:

- cooperarea, inclusiv cu sectorul privat, pentru creșterea nivelului de cultură de securitate cibernetică, în scopul consolidării rezilienței și mitigării riscului atacurilor de tip ransomware;

- creșterea capacității autorităților naționale de a identifica, preveni și combate activitățile de spălare de bani asociate activităților cu ransomware, inclusiv prin implementarea de acte legislative în acest scop;

- crearea unui mecanism de schimb de date și informații care să susțină activitățile de destructurare a infrastructurilor de atac utilizate în derularea de atacuri cibernetice de tip ransomware;

- reglementarea criptomonedelor și abordare holistică a acestora, ținând cont că majoritatea plăților realizate ca urmare a unor atacuri de tip ransomware sunt efectuate prin acest mijloc de plată;

- stabilirea unor metode de sancționare a infracțiunilor/criminalității cibernetice, respectiv a persoanelor/ actorilor cibernetici implicați.

INTERVIU
cu directorul Oficiului pentru Informații Integrate, domnul Consilier de Stat CONSTANTIN IONESCU

DIRECTORUL
OFICIULUI PENTRU INFORMAȚII INTEGRATE
CONSTANTIN IONESCU

CARE ESTE VIZIUNEA EXISTENTĂ LA NIVELUL OII ÎN CEEA CE PRIVEȘTE DOMENIUL SECURITĂȚII CIBERNETICE?

Multiplicarea exponențială a amenințărilor cibernetice, utilizarea capabilităților *cyber* de către actori statali și non-statali ca instrumente de putere moderne, impactul deosebit al atacurilor cibernetice, sub aspectul incapacitării rețelelor informatice și al exfiltrării de date din domenii strategice, precum și acțiunile malițioase specifice criminalității cibernetice afectează interesele strategice ale statului român și produce consecințe negative asupra politicilor sale la toate nivelurile.

Multitudinea domeniilor afectate, a țintelor vizate de amenințări (instituții civile și militare, mediul privat, societatea civilă și, nu in ultimul rând, cetățeanul) relevă dimensiunea strategică a amenințării și reclamă un răspuns integrat, coordonat și calibrat pe proporția și impactul exercitate de acest tip de amenințări.

Expresie a unor modele conceptuale recunoscute în lumea intelligence-ului modern, precum *need to share* și *responsability to provide*, Comunitatea Națională de Informații/ CNI oferă mecanisme și modele de acțiune adecvate gestionării amenințărilor contemporane. La acest nivel, amenințările cibernetice sunt gestionate în format inter-agenții atât prin instrumentele specifice fiecărei instituții componente, cât și prin demersuri integrate la nivelul comunității. Cunoașterea, prevenirea și contracararea amenințărilor cibernetice prin intermediul CNI se realizează, astfel, integrat.

În plan analitic, în calitate de structură de analiză integrată cu caracter permanent la nivelul CNI, Oficiul pentru Informații Integrate/ OII funcționează în baza unei Viziuni ce asigură aliniamentele conceptuale specifice unei organizații adaptate profilului problematicilor actuale de securitate. OII are ca misiune planificarea nevoilor de informații pentru securitate națională și analiza integrată la nivel strategic a informațiilor furnizate de instituțiile din CNI și elaborarea unor produse analitice de nivel strategic, în scopul fundamentării strategiilor și politicilor naționale de securitate. Dincolo de valorificarea cunoașterii și expertizei în cadrul Comunității de Informații, OII depune eforturi pentru captarea cunoașterii și din alte sectoare guvernamentale, zona ONG, precum și din mediile de expertiză privat și academic.

Raportate la amenințările cibernetice, aceste priorități acționale permit o bună cunoaștere a amenințării, prin integrarea aspectelor militare și civile specifice și sprijinirea procesului de decizie strategică.

OII a identificat o serie de trenduri majore în domeniul securității. Printre acestea se numără emergența noilor tehnologii (IA, 5G, IoT), care pot oferi un avantaj competitiv utilizatorilor/ actorilor geopolitici în competiția pentru resurse, influență și, nu în ultimul rând, control al noilor realități/ teritorii reale și/ sau virtuale, dar care pot, în egală măsură, reprezenta un risc la adresa securității cibernetice. În aceste condiții, reziliența și capacitatea de adaptare a sistemelor critice față de acțiunile disruptive și capacitatea de răspuns/ refacere în raport cu diverse tipuri de crize, inclusiv generate de atacuri cibernetice, devine esențială pentru orice entitate statală în actualul context de securitate.

Pe aceste aliniamente, OII a acționat pentru informarea beneficiarilor și orientarea procesului informativ la nivelul CNI, un accent deosebit fiind pus pe trinomul amenințare/ securitate/ dezvoltare cibernetică. Atribuțiile OII prevăzute in HCSAT 146/2005 legate de planificarea demersului informativ național prin intermediul Planului Național de Priorități Informative/ PNPI și informarea integrată de nivel strategic a beneficiarilor legali au asigurat și asigură CNI și, implicit, CSAT pârghii importante prin care domeniul securității cibernetice este abordat la adevărata sa dimensiune strategică.

PNPI identifică și prioritizează resursele informative ale CNI pentru gestionarea amenințărilor cibernetice. Totodată, surprinde ca tendință majoră și provocare semnificativă a mediului de securitate prevalența atacurilor cibernetice derulate ori coordonate de către entități statale/ non-statale, ce vizează sectoare

guvernamentale sau companii private. Informările curente și cele de nivel strategic abordează prevalent tematica amenințărilor cibernetice (atacuri cyber, criminalitate informatică, amenințări hibride cu utilizarea instrumentului cibernetic etc.).

În accepțiunea noastră, amplitudinea și impactul amenințărilor cibernetice trebuie relaționate cu necesitatea dezvoltării la nivel decizional a unei viziuni în măsură să permită: **a)** înțelegerea modului și a cauzelor pentru care acest fenomen poate produce mutații în plan intern/ internațional; și **b)** creșterea capacității de a răspunde adecvat noilor provocări din spațiul cibernetic.

Inclusiv în acest scop, pe viitor, OII are în vedere participarea, împreună cu instituțiile din CNI, ministere, alte instituții guvernamentale și societatea civilă, la proiecte de securitate în domeniul cyber și al noilor tehnologii menite să asigure materializarea viziunii și a obiectivelor strategice ale României, cel puțin în ce privește managementul cunoașterii strategice în domeniu.

Cum evaluați amenințările cibernetice din România, inclusiv prin raportare la contextul pandemic?

Pentru evaluarea corectă a amenințărilor cibernetice la adresa României, trebuie luat în considerare faptul că acest tip de acțiuni cu valențe agresive/ ostile pot fi derulate de entități interesate, statale ori non-statale, atât de sine stătător, cât și în mod conjugat/ inter-conexat (și deseori sincronizat), cu alte pârghii de putere. Unii actori statali cu regimuri autoritare, precum Rusia, sunt percepuți în spațiul euro-atlantic ca principali generatori de amenințări, riscuri și/ sau provocări, deoarece:

- vizează: promovarea propriilor obiective; afectarea democrației și subminarea coeziunii euro-atlantice;

- angrenează o varietate de resurse și instrumente, a căror utilizare și-a pus amprenta asupra dinamicii/ dimensiunii acțiunilor asimilabile spectrului hibrid.

Un loc important în tot acest angrenaj este ocupat de instrumentele cyber (însoțite de componente de ordin politico-diplomatic, de intelligence, economic, militar), devansate totuși de pârghiile informaționale (propagandă, dezinformare și *fake-news*), care sunt cele mai uzitate. Este cunoscut că Rusia derulează operațiuni cibernetice complexe în spațiul euro-atlantic, regiunile din proximitatea acestuia și alte zone de interes strategic.

De altfel, pe parcursul anului 2021 au fost identificate campanii derulate de actori cibernetici asociați Moscovei, care au avut drept scop obținerea accesului în cadrul unor sisteme informatice pentru exfiltrarea de informații sensibile/ confidențiale.

Prin prisma apartenenței la Spațiul Comunitar și Alianța Nord-Atlantică, dar și a rolul strategic deținut pe flancul estic al NATO și în zona Mării Negre, România a reprezentat și va continua să reprezinte pentru Rusia o țintă a campaniilor cibernetice. Asemenea acțiuni sunt puse în practică prin intermediul unor actori cibernetici (asociați/ atribuiți *intelligence-ului* rus), care au capabilitățile necesare compromiterii unor infrastructuri IT&C cu valențe critice pentru securitatea națională.

Deși riscurile asociate agresiunilor cibernetice s-au menținut la un nivel relativ ridicat (în strânsă corelare cu tendințele la nivel european și global, favorizate de proliferarea tehnologiilor emergente), contextul pandemic a favorizat manifestarea secvențială a unor tendințe ascendente asociate utilizării acestui instrument, pe fondul măsurilor restrictive (distanțare fizică, restrângerea unor activități sociale) adoptate de autorități pentru limitarea răspândirii virusului SARS COV-2.

Operațiunile cibernetice vizează și influențarea opiniei publice, în sensul scăderii încrederii populației în autorități, prin accesarea platformelor de social-media, dar și afectarea bunei funcționări a entităților care asigură servicii publice vitale, inclusiv obstrucționarea eforturilor autorităților în gestionarea pandemiei. Pe viitor, este de așteptat că atât România, cât și statele UE și NATO să constituie ținte ale unor campanii cibernetice (cu scopul exfiltrării de informații strategice), însoțite de operațiuni informaționale, inițiate de actori ostili, mai ales în contextul intervenției militare ruse în Ucraina.

Care sunt principalele obiective pe care România ar trebui să și le propună pentru a deveni un stat rezilient din punct de vedere cibernetic?

Pentru asigurarea unui grad sporit al rezilienței statului și societății în fața amenințărilor de orice tip (o atenție deosebită trebuind a fi acordată celor hibride), este dezirabilă o abordare integrată de tip "*whole of government*" și "*whole of society*". Raportat la amenințările cibernetice, este necesar a fi avute în vedere și provocările asociate dezvoltării societății informaționale și a

economiei digitale, întrucât:

■ preconizata creștere a nivelului de digitalizare a administrației ar putea să nu producă (toate) efectele scontate, pe fondul unor (posibile) inacțiuni/ acțiuni deficitare ale factorilor responsabili cu privire la: identificarea nevoilor reale ale cetățenilor și prioritizarea acestora; configurarea unor sisteme/ aplicații care să contribuie la creșterea eficienței administrației;
■ gestionarea proiectelor majore informatice ar putea fi afectată de (in) acțiuni ale unor paliere decizionale din instituții ori ale unor operatori economici și/ sau entități externe. Legat de acest subiect, *Platforma națională de cloud guvernamental* este un proiect de importanță strategică pentru modernizarea activităților instituționale, subsumat procesului de transformare digitală a serviciilor publice din România. Medii avizate susțin că o soluție de cloud eficientă pentru România ar trebui să fie una de tip multi-platformă (neutră tehnologic, scalabilă, cu disponibilitate înaltă și redundanță superioară).
■ funcționarea în condiții de disponibilitate, continuitate și integritate a sistemelor informatice/ rețelelor poate fi periclitată de vulnerabilități tehnologice și procedurale la nivelul infrastructurilor IT&C, având în vedere și faptul că sporirea volumului operațiunilor *online* va alimenta riscurile la adresa confidențialității datelor și a vieții private. În paralel, pot persista provocări/ dificultăți legate de digitalizarea economiei, dobândirea de competențe pentru a crea forță de muncă digitalizată și creșterea gradului de inter-operabilitate a sistemelor IT dedicate furnizării de servicii publice integrate, rapide și sigure către cetățeni.

Demersurile de creștere a rezilienței țării noastre în raport cu amenințările cibernetice trebuie susținute prin acțiuni de comunicare publică (inclusiv de nivel strategic - STRATCOM).

O abordare integrată în domeniu ar presupune eficientizarea cooperării inter-instituționale pentru armonizarea intervențiilor și racordarea cât mai bună a României la evoluțiile curente din domeniu în plan extern, dar și la pozițiile adoptate, unitar, consensual și coeziv, la nivelul UE și NATO.

Care credeți că ar trebui să fie rolul României în arhitectura internațională de securitate cibernetică?

Un nivel ridicat de securitate cibernetică în plan intern alături de susținerea, dezvoltarea și promovarea valorilor securității cibernetice la nivel internațional sunt principalele aliniamente care trebuie să ghideze poziția, acțiunea și imaginea României în peisajul internațional al securității cibernetice.

Continuarea eforturilor de dezvoltare instituțională pe plan intern și a investițiilor în tehnologii avansate și cercetare, extinderea cooperării cu mediul privat și societatea civilă și promovarea culturii de securitate reprezintă demersuri necesare pentru consolidarea nivelului intern de securitate cibernetică.

Cunoașterea amenințării, reducerea vulnerabilităților și promovarea conceptului de reziliență sunt repere ale unui *modus operandi* prin care România își asigură securitatea cibernetică proprie și poate să demonstreze valoarea sa în cadrul arhitecturii internaționale de securitate cibernetică. Aceste direcții de acțiune, consonante cu reperele trasate prin Strategia Națională de Apărare a Țarii 2020-2024, Strategia de Securitate Cibernetică și alte documente programatice consolidează profilul României în plan extern.
Consolidarea parteneriatelor și a cooperărilor la nivel european și euroatlantic este esențială pentru orice demers al României care vizează asigurarea propriei securități cibernetice, precum și a celei a partenerilor. Înființarea la București a Centrului Euroatlantic pentru Securitate Cibernetică reprezintă un semnal al încrederii partenerilor occidentali în potențialul României și o confirmare a eforturilor întreprinse până acum. Prestația și performanța României la acest nivel pot reprezenta puncte forte, dar și o provocare pentru rolul asumat de Romania de actor credibil și important la nivel aliat.

Alinierea la normativele europene în domeniu, susținerea inițiativelor și proiectelor partenerilor consacrați, rolul activ jucat de instituțiile și organizațiile de profil (Centrul Național Cyberint, Directoratul de Securitate) în acțiunile și planurile privind consolidarea securității cibernetice la nivel internațional sunt jaloane importante care oferă României un profil bazat pe expertiză și predictibilitate.

Cum apreciați că se realizează cooperarea în cadrul Comunității Naționale de Informații pe subiecte referitoare la amenințarea cibernetică?

În fața provocărilor de ordin tehnologic, Comunitatea Națională de Informații analizează pericolele generate de

agresiunile cibernetice asupra funcționării statului și instituțiilor, bunului mers al societății, bunăstării cetățeanului și, nu în ultimul rând, asupra deciziei strategice în statul român. La nivelul CNI sunt discutate necesitățile de ordin legislativ, al resurselor și instrumentelor necesare structurilor și instituțiilor pentru desfășurarea misiunilor specifice în contextul evoluțiilor generate de noile tehnologii.

La modul general, discuțiile și analizele abordează riscurile și oportunitățile generate de acțiunile din spațiul cibernetic – așa cum sunt acestea percepute la nivelul instituțiilor din CNI – și conțin aspecte legate de susținerea deciziei strategice în diferite contexte, uneori legate de medii de manifestare cibernetice.

Pe fond, se valorifică instrumentele de cooperare și se acționează pentru consolidarea expertizei în domeniul prevenirii și combaterii riscurilor și amenințărilor (inclusiv) cibernetice, dar și pentru susținerea deciziilor de nivel strategic în cazul unor manifestări cu caracter ostil sau perturbator în spațiul cibernetic.

Prezența experților Comunității la formate de lucru inter-instituțional, interacțiunea acestora în grupuri de lucru tehnice confirmă rolul serviciilor de informații în gestionarea proceselor de prevenire, limitare și contracarare a agresiunilor din spațiul cibernetic. Suportul tehnic și de specialitate oferite de aceștia întregesc un întreg tablou al arhitecturii de securitate care prinde coerență în cadrul Comunității.

Care au fost provocările adoptării Strategiei de Securitate Cibernetică a României?

Deși nu a fost un proces facil, adoptarea Strategiei de Securitate Cibernetică a României vine pe un teren fertil. Securitatea cibernetică face și obiectul ultimelor două Strategii Naționale de Apărare a Țării. Încă de la implementarea Strategiei Naționale de Apărare a Țării, în 2015, au fost introduse concepte novatoare pentru acel moment (securitate extinsă, amenințări cu caracter hibrid etc.) care au constituit baza teoretică, tehnică și normativă pentru alte strategii naționale și sectoriale.

Mai mult, având în vedere interesul general al unor factori politici, al mediului academic și societății civile pentru clarificarea unor concepte, precum și implicațiile lor asupra securității naționale, din perspectiva ghidării și orientării politicilor din domeniu, la nivelul CSAT au fost inițiate procese de reflecție strategică privind modul de realizare al securității cibernetice concomitent cu derularea unor programe de conștientizare a populației, a administrației publice și a sectorului privat cu privire la vulnerabilitățile, riscurile și amenințările specifice utilizării spațiului cibernetic.

De asemenea, diferiți decidenți au fost preocupați de menținerea unui dialog deschis cu societatea civilă și cu experții în domeniu, prin platforme de dialog și campanii *awareness*, și s-a încercat în permanență depășirea limitelor de ordin tehnic, legislativ și normativ. Asigurarea coerenței de ordin legislativ și tehnic, buna înțelegere a fenomenului de la expert și decident la cetățean a devenit o necesitate pe parcursul întregului proces de adoptare a noii Strategii.


LOADING KEYPASS

WWW.SRI.RO