CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ

EVOLUȚIA AMENINȚĂRILOR ÎN SPAȚIUL CIBERNETIC ROMÂNESC ÎN ANUL 2018

BUCUREȘTI, 2019

[ABSTRACT]

Analiza CERT-RO privind evoluția amenințărilor cibernetice în spațiul cibernetic românesc este rezultatul unui proces de prelucrare a informațiilor colectate și procesate de instituție pe parcursul anului 2018. Un element de noutate față de rapoartele din anii anteriori îl reprezintă trecerea la un nou concept ”particularizat-global”, datorat în principal intrării în vigoarea a Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

CERT-RO a trecut la o nouă paradigmă de lucru, pe domeniile de competență, prin inițierea unui proces de redefinire a fluxurilor de lucru, astfel încât să fie asigurată o reacție proporțională la incidentele de securitate cibernetică, în funcție de impactul incidentului și de amploarea acestuia. De asemenea, au fost dezvoltate surse proprii de date referitoare la incidentele de securitate cibernetică, respectiv senzori, mecanisme Darknet, honeypots.

Ca rezultat al acestei noi abordări, în anul 2018 au fost identificate atacuri provenite de pe toate continentele din peste 190 de state/teritorii comparativ cu 60 de state/teritorii identificate în cursul anului 2017, element ce reflectă ”lipsa frontierelor” în spațiul cibernetic precum și caracterul de universalitate a atacurilor cibernetice.

Au fost identificate noi tipuri de malware în spațiul cibernetic românesc, Monerominer, VPNFilter și Eitest. De asemenea, nu au mai fost identificate indicii de activitate pentru alte tipuri de malware care au acționat în anul 2017, Palevo.

România este generatoare de incidente de securitate cibernetică, dar este și țintă.

În ceea ce privește atacurile cibernetice de tip malware, poziția #1 este deținută de malware Andromeda.

* * *

EVOLUȚIA AMENINȚĂRILOR LA NIVEL NAȚIONAL

Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, ca structură independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice, este o instituție publică cu personalitate juridică, în coordonarea Ministerului Comunicațiilor și Societății Informaționale. CERT-RO își desfășoară activitatea în conformitate cu legislația în vigoare și cu regulamentul propriu de organizare și funcționare, în scopul realizării prevenirii, analizei, identificării și reacției la incidente în cadrul infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale.

CERT-RO organizează și întreține sistemul de baze de date privind amenințările, vulnerabilitățile și incidentele de securitate cibernetică, identificate sau raportate.
CERT-RO, conform Legii nr. 362/2018 prin care este transpusă, în totalitate, Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, a devenit și Autoritate Națională pentru Securitatea Rețelelor și Sistemelor Informatice, Punct Național Unic de Contact și CSIRT Național în domeniul de aplicare al Directivei NIS.

În acest context, pentru realizarea analizei s-au utilizat cu prioritate rezultatele obținute prin intermediul surselor proprii, precum și notificările primite de CERT-RO prin intermediul surselor clasice.

Raportul prezintă o viziune de ansamblu asupra amenințărilor și vulnerabilităților din spațiul cibernetic național, precum și recomandări pentru consolidarea capacităților de prevenire și reacție, care pot fi utilizate atât în procesul de definire a politicilor publice în domeniu, al politicilor organizaționale, cât și la nivel individual.

Pentru evaluarea stării de securitate a spațiului cibernetic național, CERT-RO a inițiat procesul de transfer de la analiza de securitate ce utiliza *sintagma* ”*general-particular*” la analiza de securitate ce utilizează *sintagma* ”*particularizat-global*”. Prin implementarea noului concept se urmărește identificarea, în principal din surse proprii (senzori, mecanisme Darknet, honeypot etc.), a evenimentelor/incidentelor specifice spațiului cibernetic național, care au impact global și în care România este, inclusiv, o țintă a atacurilor cibernetice.

Etape abordate în atingerea țelului propus (noului concept):

- Implementarea unor senzori proprii pe sectoare/domenii de activitate.
  - Pentru identificarea celor mai recente incidente/evenimente cibernetice, s-a demarat o procedură de implementare a unor senzori proprii prin care sunt colectate și corelate date privind alertele de securitate cibernetică, în funcție de sectoarele/domeniile stabilite prin Directiva (UE) 2016/1148.
- Implementarea unor mecanisme complexe de securitate cibernetică.
  - Pentru identificarea și cercetarea incidentelor de securitate care vizează spațiul cibernetic național, s-au implementat mecanisme de securitate cibernetică de tip honeypot, precum și mecanisme de tip telescop de rețea (Darknet).
- Identificarea și implementarea de noi feed-uri de date de tip OSINT.

Ca o primă observație a noii abordări analitice, putem constata scăderea alertelor de securitate cibernetică procesate automat provenite de la furnizori globali (*informații cu caracter general*), în paralel cu o creștere semnificativă a volumului de date colectate din surse proprii (*informații cu caracter particularizat*).

O analiză specifică și corectă se va putea efectua la finalul anului 2019, când se preconizează ca noul concept ”particularizat-global” să fie implementat în totalitate, iar analiza statistică să se bazeze, în principal, pe datele colectate din surse proprii.

Tendința globală cu privire la diversificarea amenințărilor și vulnerabilităților de natură cibernetică s-a reflectat pe parcursul anului 2018 și în spațiul cibernetic național, prin apariția de noi tipuri de atacuri cibernetice și dispariția altora.

În timp ce majoritatea alertelor procesate automat de CERT-RO (alte surse decât cele proprii) se referă la sisteme informatice vulnerabile (*neactualizate*, *nesecurizate sau configurate necorespunzător*), compromise sau infectate cu diverse variante de malware, ceea ce poate indica inclusiv un nivel redus al culturii de securitate cibernetică în rândul utilizatorilor din România, majoritatea alertelor provenite din surse proprii – *mecanisme complexe de securitate* se referă la atacuri de tip *Information Gathering*, prin care sunt trimise cereri către un sistem pentru a descoperi punctele slabe și se încearcă colectarea informațiilor despre gazde, servicii și conturi.

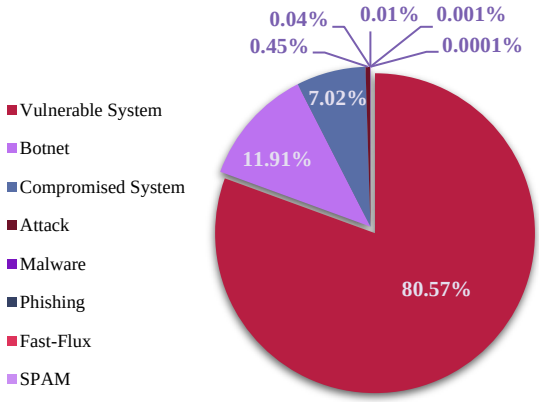
DATE STATISTICE

1. ALERTE PROCESATE AUTOMAT
2. ALERTE PROCESATE MANUAL
3. MECANISME COMPLEXE DE SECURITATE – DARKNET
4. SURSE/SENZORI PROPRII

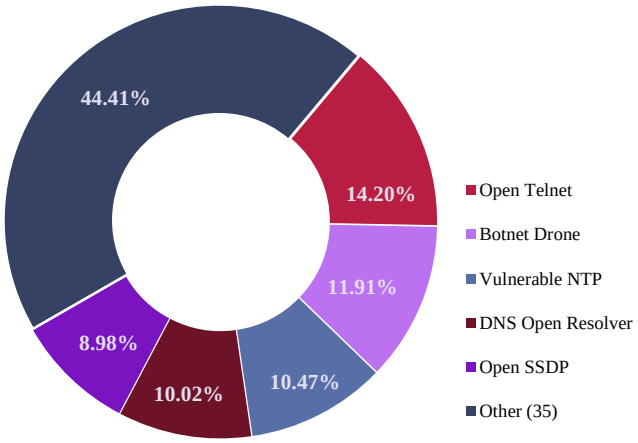
1. ALERTE PROCESATE AUTOMAT

Distribuția amenințărilor în funcție de clasa alertei/incidentului

Principala clasă de incidente -> Vulnerabilități: 80,57%.



Distribuția amenințărilor în funcție de tipul alertei/incidentului



«Top 5 tip incidente» au reprezentat: 55,59%.

În anul 2018, s-au identificat atacuri/alerte din toate tipuri de incidente predefinite: 40.

Ca și în anul precedent, prima poziție este ocupată de atacurile de tip Open Telnet.

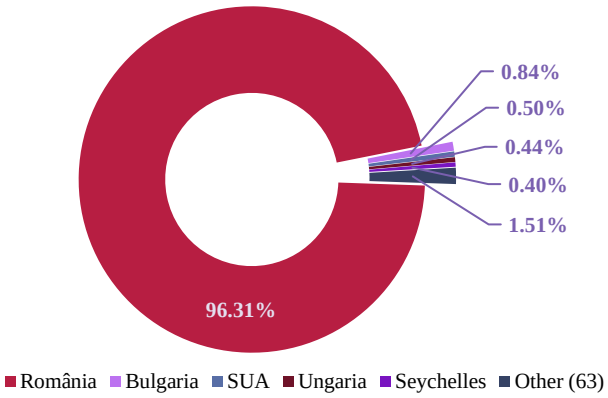
Distribuția amenințărilor în funcție de țara de proveniență a alertei/incidentului

«Top 5 țari sursă atacuri» au reprezentat: 98,49%.

Număr total al statelor de proveniență a atacurilor: 68.

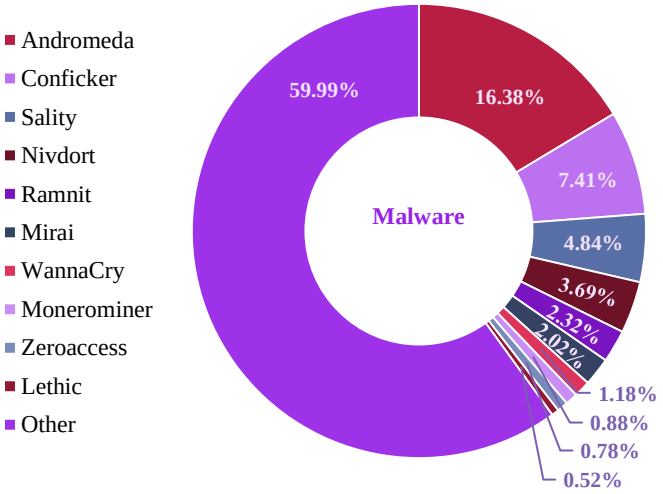
Ca o particularitate, s-au identificat pentru prima dată atacuri provenite din 25 state noi față de anul 2017 (exemple: Afganistan, Armenia, Aruba, Algeria, Estonia, Filipine, Indonezia, Siria etc.).

De asemenea, comparativ cu anul 2017, s-au diminuat atacurile provenite din: China, Belgia, Israel și Japonia.



Se observă că, în cazul vechiului concept *"general-regional"*, impactul amenințărilor pe spațiul cibernetic românesc are un puternic caracter zonal. Lipsa sistemelor și a mecanismelor complexe de securitate cibernetică nu poate genera o analiză corectă a amenințărilor din spațiul cibernetic național, fapt ce a dus la trecerea la noul concept analitic "particularizat-global" în scopul creșterii nivelului de securitate cibernetică la nivel național.

Distribuția atacurilor de tip malware



Alertele procesate la nivelul CERT-RO, au conținut informații referitoare la tipul de malware asociat (*alerte de tip botnet sau URL-uri malițioase*).

Poziția #1 este deținută de malware Andromeda

Poziția #1 din Top10/Malware Downadup (Conficker), a coborât pe poziția #2.

Au fost identificate noi tipuri de malware: **Monerominer, VPNFilter** și **Eitest**; dar și dispariția altora: **Palevo**.

În anul 2018 a cunoscut o creștere semnificativă fenomenul atacurilor de tip **cryptojacking**, la nivelul României fiind identificate cu preponderență aplicațiile malițioase de tip MoneroMiner (*0,88% din totalul malware asociat*), CoinMiner (*0,015%*) și BitcoinMiner (*0,007%*).

EITest. Una dintre cele mai vechi rețele de malware din lume, rețeaua de infecții EITest a fost închisă în anul 2018 (după ce a fost descoperită în anul 2011). Malware-ul era distribuit printr-un kit privat de exploatare și avea drept scop direcționarea traficului web de pe serverul infectat către site-uri malware și înșelătorie. Deși rețeaua de răspândire EITest este închisă, infecția este încă activă și poate afecta serverele vulnerabile și care rulează cod malițios.

WannaCry încă nu a murit. Deși la începutul anului se părea că WannaCry a devenit istorie, în anul 2018 au fost identificate IP-uri din România infectate cu acest tip de malware.

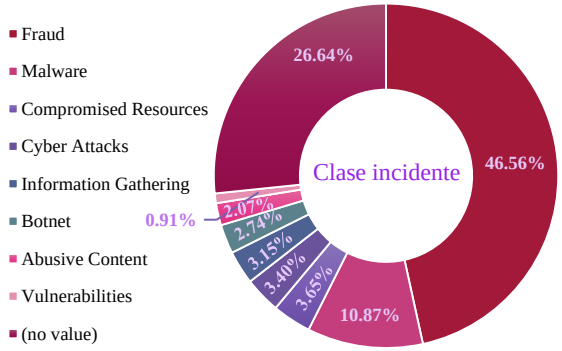
Cum statisticile provin de la furnizori globali de informații, nu s-au identificat dacă au avut loc daune reale la nivelul României. Cu toate acestea, numărul de încercări de infectare a calculatoarelor cu acest malware, în 2018, sugerează că, în continuare, WannaCry este activ. Deci, computerele pot fi infectate cu acest ransomware.

Locky. Dacă la sfârșitul anului 2017, se previziona că ransomware-ul Locky va fi abandonat de către creatorii săi și va dispărea, în anul care a trecut el a fost dezvoltat în continuare și s-au observat noii campanii, fiind identificate IP-uri, inclusiv din România.

VPNFilter. În luna mai 2018, Cisco Systems anunța faptul că peste 500.000 de routere și dispozitive de stocare au fost infectate de hackeri în 54 de țări. La nivelul României, au fost identificate IP-uri implicate, atât în atacuri, cât și victime.

2. ALERTE PROCESATE MANUAL

Date reprezentative privind alertele colectate manual

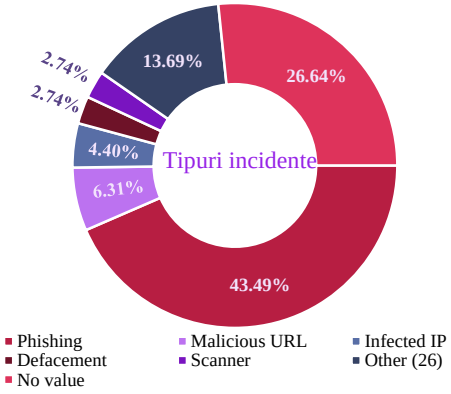


În anul 2018, s-au identificat atacuri/alerte pentru toate clasele de incidente utilizate de CERT-RO pentru clasificarea acestora. Evenimentele au fost gestionate cu ajutorul **Request Tracker for Incident Response (RTIR)**.

Cea mai răspândită clasă de incidente: **Fraud (561)**

În funcție de tipul de incidente, au fost identificate/colectate 31 tipuri de alerte (*din 36 de tipuri definite în RTIR*).

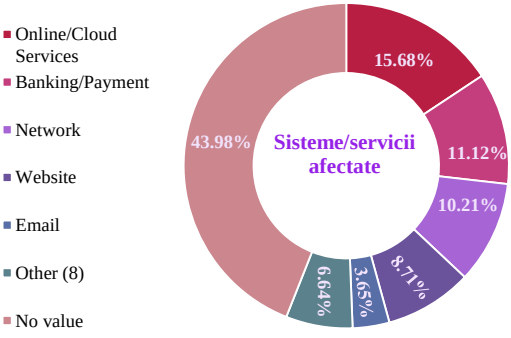
Cel mai răspândit tip de incident rămâne în anul 2018 cel de tip Phishing (524), din clasa de incidente de tip Fraud.



În ceea ce privește serviciile/sistemele afectate, au fost identificate 13 tipuri (din cele 14 tipuri predefinite).

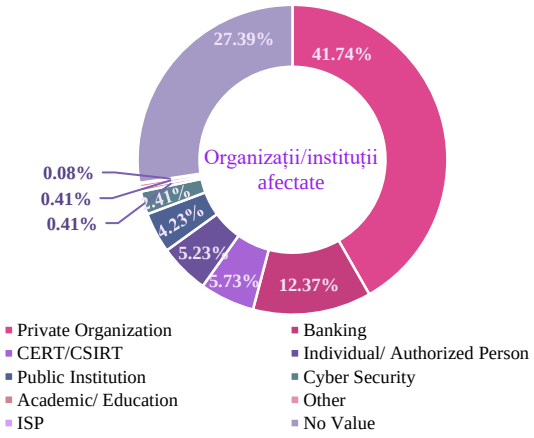
Poziția #1 sisteme/servicii afectate se află *Online/Cloud Services*.

Pentru prima dată au fost identificate alerte care au afectat servicii de tip *ERP/CRM* și *Database*.



În ceea ce privește organizații/instituții afectate, au fost identificate 9 tipuri (din cele 10 tipuri predefinite).

Pe prima poziție se află firmele private (503).



Alertele/tichetele procesate au implicat un număr de 107.430 IP-uri unice și au fost emise 175.890 alerte/informări.

3. MECANISME COMPLEXE DE SECURITATE - DARKNET.

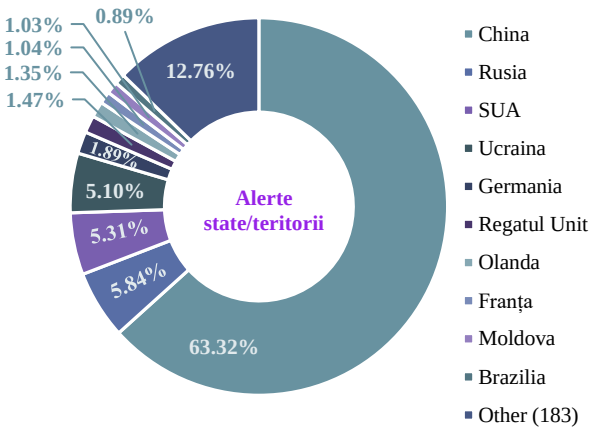
Toate atacurile detectate prin intermediul acestui mecanism au făcut parte din clasa de alerte *Information Gathering* și au fost de tip *Scanning*.

Au fost identificate atacuri din 193 state/teritorii, inclusiv din România (0,28% din totalul atacurilor).

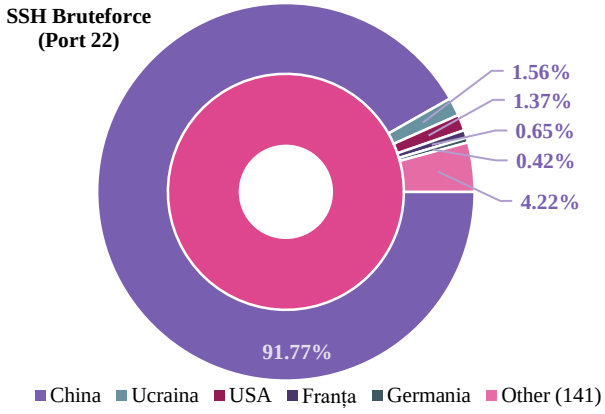
Poziția #1 este deținută de China (63,32% din totalul atacurilor).

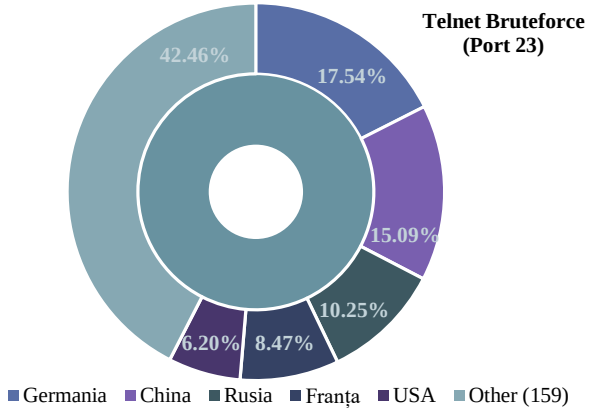
Dacă în cazul surselor/feed-urilor externe (la care CERT-RO este abonat) se observă că atacurile identificate au impact zonal, în cazul surselor proprii se identifică că impactul este unul global.

Datele colectate fiind doar pentru anul 2018, nu se poate efectua o analiză comparativă, dar acest fapt va duce în anul viitor la o interpretare mai corectă a fenomenului.



Pentru primele două tipuri de atac (SSH Bruteforce și Telnet Bruteforce) identificate, în funcție de proveniența surselor de atac, situația se prezintă astfel:





4. SURSE/SENZORI PROPRII

Analiza datelor colectate prin intermediul acestor mecanisme prezintă **starea de securitate a spațiului cibernetic național aferent domeniului Administrație Publică Locală** (domeniul aflat în responsabilitatea CERT-RO în conformitate cu HG nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO).

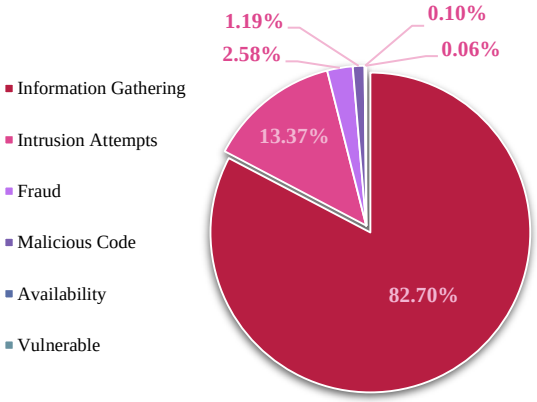
Distribuția amenințărilor în funcție de clasa și tipul incidentului

Principala clasă de incidente -> Information Gathering[1]: **82,70%**.

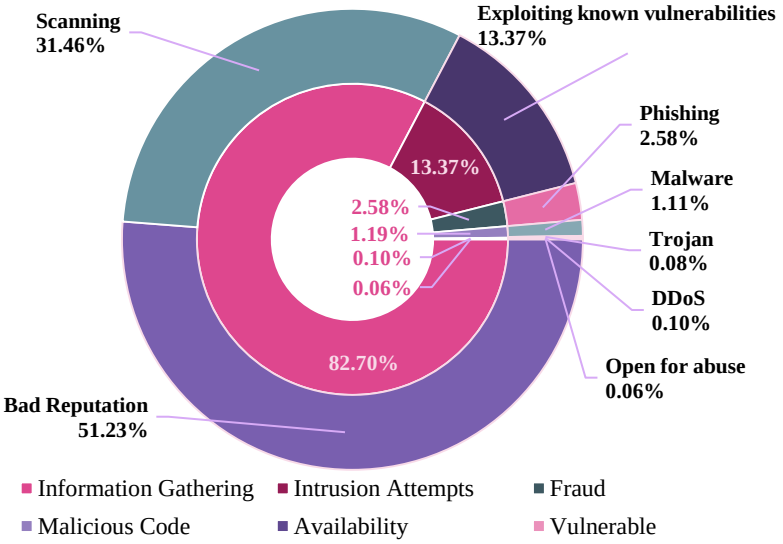
Atacuri cibernetice: 3,87% .

Comparativ cu datele colectate din surse externe se poate observa: clasa Vulnerable este plasată pe ultima poziție (0,06%).

Deci datele obținute din surse proprii oferă informații mai relevante despre starea de securitate a spațiului cibernetic național.



Situația privind repartiția tipurilor de atacuri în funcție de clasa acestora.



Peste jumătate din datele colectate au reprezentat atacuri de tip *Bad reputation*[2] (*51,23%*).

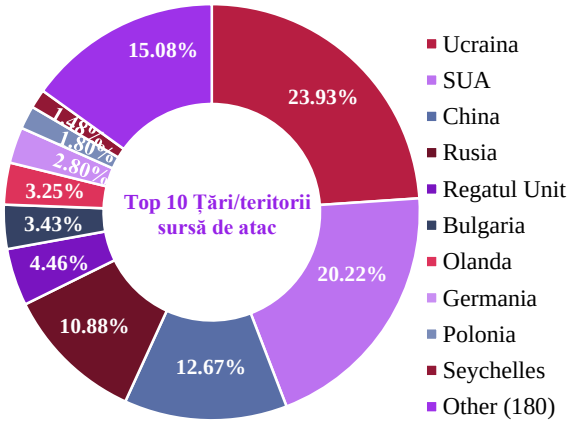
2,58% au fost atacuri de tip Phishing, 1,11% atacuri de tip Malware și 0,08% de tip Trojan.

De asemenea, atacurile de tip DDoS au reprezentat 0,1% din totalul atacurilor cibernetice desfășurate asupra administrației publice locale.

Distribuția amenințărilor în funcție de țara/teritoriu de proveniență a atacurilor

Din analiza atacurilor desfășurate pe domeniul administrației publice locale se desprind următoarele:

- Marea majoritate a atacurilor provin din China (12,67%) și fostul spațiu sovietic, în principal din Ucraina (23,93%) și Rusia (10,88%).
- Atacurile au provenit din 190 state/teritorii, iar cele provenite din primele 10 țări *(«Top 10»)* au reprezentat un procent de 84,92%.

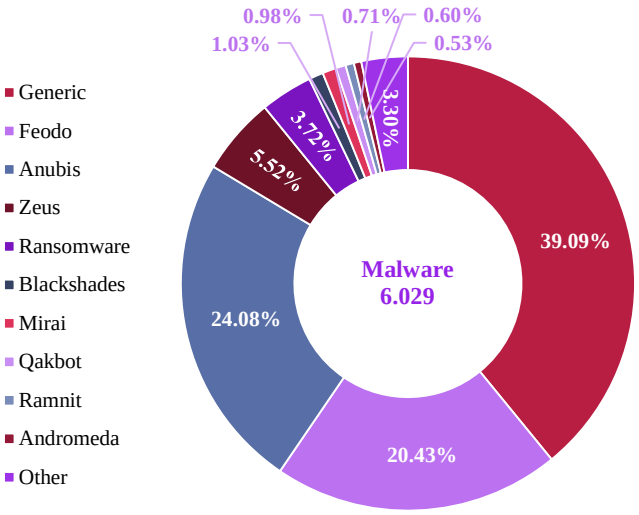


[1] Information Gathering - Atacurile care trimit cereri către un sistem pentru a descoperi puncte slabe, incluzând și procese de testare pentru a culege informații despre gazde, servicii și conturi. Exemple: fingerd, interogare DNS, ICMP, SMTP (EXPN, RCPT, ...), scanare port.

[2] Bad reputation – prin intermediul senzorilor au fost identificate conexiuni din rețelele informatice în care acești sunt plasați către adrese IP cunoscute a fi implicate în activități malițioase.

De asemenea, bazându-ne pe informațiile furnizate de senzori estimăm că un procent de aproximativ 20% dintre echipamentele IT din zona administrației publice locale sunt afectate de diferite aplicații malițioase.

Distribuția atacurilor de tip malware



6,82% din alerte procesate la nivelul CERT-RO, au conținut informații referitoare la tipuri de malware.

Poziția #1 este deținută de aplicații malware care încă nu au fost incluse într-o categorie dedicată (malware Generic).

Comparând datele colectate din surse externe și interne, în «Top 10 Malware» se identifică unele tipuri comune de malware, Mirai, Ramnit și Andromeda.

CONCLUZII

Analiza datelor colectate și procesate a presupus o comparație a surselor externe vs surse interne (proprii), respectiv caracter regional vs. caracter global.

În timp ce în primul caz au fost identificate atacuri provenind din 68 de state/teritoriu, în cel de al doilea caz (Darknet, respectiv senzori) au fost identificate atacuri provenite din 193 de state/teritorii inclusiv din România.

În aceste condiții, orientarea analizei de securitate spre conceptul ”particularizat-global” și, în principal, pe datele provenite de la senzorii proprii creează premisele unei abordări aprofundate și extinse a problematicii de securitate cibernetică aflate în competența CERT-RO.

În cazul noului concept *”particularizat-global”*, se constată că **impactul amenințărilor pe spațiul cibernetic românesc are un puternic caracter global, iar atacurile provin aproape din toate statele/teritoriile lumii**. Deci, în era digitală ”distanța nu primează”, iar atacurile sunt efectuate din orice punct al Terrei.

În concluzie, **viitorul apărării cibernetice este ”*cooperarea la nivel global*”** pentru asigurarea unui spațiu cibernetic sigur, caracterizat prin lipsa frontierelor, dinamism și anonimat.

Prin implementarea de senzori și sisteme de detecție proprii, analiza CERT-RO este mult mai precisă, scoțând în evidență specificitatea spațiului cibernetic național.

Asigurarea securității informatice presupune o serie de măsuri, cum ar fi: conștientizarea și instruirea utilizatorilor, analiza și evaluarea riscurilor, managementul vulnerabilităților și alertelor de securitate, managementul drepturilor de acces, managementul configurațiilor rețelelor și sistemelor informatice și realizarea planurilor de securitate la nivelul acestora, conformitatea cu standardele europene și internaționale.

În acest sens, în calitate de Autoritate națională în domeniul securității cibernetice, CERT-RO susține demersul de creare a unui cadru național de cooperare între instituțiile de stat, mediul privat și mediul academic care să contribuie, în mod real, atât la schimbul de informații și bune practici, cât și la consolidarea măsurilor de securitate cibernetică.

Pentru acest motiv, am considerat oportună schimbarea modului de abordare a raportului anual astfel încât acesta să poată oferi date specifice referitoare la nivelul de securitate existent în România, pentru a încuraja atât raportarea către CERT-RO, cât și schimbul de bune practici în ceea ce privește măsurile de securitate cibernetică.

Apreciem, de asemenea, că în perioada imediat următoare, pe lângă activitățile specifice implementării Directivei NIS, un rol important îl vor juca activitățile de conștientizare și educație pe care ne-am propus să le derulăm pe categorii de vârstă și sociale, astfel încât să ne asigurăm că securitatea cibernetică este din ce în ce mai bine și mai mult înțeleasă de toți utilizatorii internetului din țara noastră, întrucât SECURITATEA CIBERNETICĂ A ROMÂNIEI ESTE RESPONSABILITATEA TUTUROR.