CENTRUL NAŢIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ

CERT-RO

RAPORT

cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2015

CUPRINS

1. Principalele constatări și concluzii

Obiectivul prezentului raport îl reprezintă **analiza alertelor de securitate cibernetică colectate și procesate de CERT-RO în anul 2015**, în vederea obținerii unei imagini de ansamblu asupra evenimentelor relevante pentru evaluarea riscurilor de securitate cibernetică la adresa infrastructurilor cibernetice de pe teritoriul României, aflate în aria de competență a CERT-RO.

În perioada de referință, respectiv 01.01.2015 – 31.12.2015, CERT-RO a colectat și procesat **68.206.856 de alerte de securitate cibernetică**, în scădere cu 13% față de anul 2014 (78.769.993), dintre care:

- alerte colectate și procesate automat (feed-uri): **68.205.633**;
- alerte colectate și procesate manual (email tiketing): **1.223**;

Prin **alertă de securitate cibernetică,** în contextul prezentului raport, înțelegem orice semnalare ce conține o adresă IP sau un domeniu web (URL), referitoare la un posibil incident sau eveniment de securitate cibernetică, ce implică sau poate implica sisteme informatice din spațiul cibernetic național deținute/administrate de persoane fizice sau juridice din România.

Un număr de 2.321.931 de adrese IP unice au fost vizate de alertele colectate de CERT-RO în anul 2015. Numărul total de IP-uri unice alocat organizațiilor din România este de **8.958.498**[1], în scădere față de anul 2014 (aprox. 10 mil.) și anul 2013 (aprox.13,5 mil.).

În urma analizării alertelor de securitate cibernetică colectate de CERT-RO în 2015, **au fost constatate următoarele:**

- **26% (2.3 mil.) din totalul IP-urilor** unice alocate spațiului cibernetic național au fost implicate în cel puțin o alerta de securitate cibernetica procesată de CERT-RO în anul 2015, față de **24% (2.4 mil.) în anul 2014** și **16% (2.2 mil.) în anul 2013**;
- **78% (53 mil.) din alertele colectate și procesate vizează sisteme informatice vulnerabile**, în sensul că sunt ne-securizate sau configurate necorespunzător. Unele dintre aceste sisteme informatice vulnerabile sunt utilizate de atacatori pentru lansarea de atacuri cibernetice asupra altor ținte și pentru mascarea identității, de cele mai multe ori ne-fiind necesară compromiterea acestora ci doar simpla utilizare a serviciilor disponibile (spre exemplu: servere DNS de tip „Open Resolver", servere Proxy fără autentificare, servere NTP configurate ne-corespunzător etc.);
- **20,78% (14 mil.) din alertele colectate și procesate vizează sisteme informatice infectate cu diferite variante de software malițios (malware) de tip botnet**, caracterizat prin faptul că dispune de mecanisme ce permit atacatorilor să controleze de la distanță sistemele informatice infectate;
- **64% (3 mil.) din numărul total de incidente rezultate din procesarea alertelor (secțiunea 3.2) reprezintă sisteme informatice ce fac parte din rețele de tip botnet,** acestea putând fi utilizate în derularea de atacuri cibernetice asupra unor ținte din România sau externe;
- **17.088 de domenii „.ro" au fost raportate la CERT-RO ca fiind compromise în anul 2015**, **în creștere cu aproximativ 58% față de anii 2014 (10.759) și 2013 (10.239)**. Din totalul de 855.997[2] domenii înregistrate în România în luna februarie 2015, numărul reprezintă aproximativ **2% din totalul domeniilor ".ro"** și aproximativ **6,5% din totalul domeniilor ".ro" active**.

[1] Conform datelor de la https://www.maxmind.com/en/allocation-of-ip-addresses-by-country.
[2] Conform datelor ICI-ROTLD.

În baza constatărilor de mai sus, **pot fi formulate următoarele concluzii:**

- amenințările și vulnerabilitățile de natură cibernetică la adresa spațiului cibernetic național continuă să se diversifice, aspect evidențiat prin faptul că în anul 2015, CERT-RO a introdus noi tipuri de alerte;
- majoritatea alertelor colectate se referă la sisteme informatice vulnerabile (configurate necorespunzător sau nesecurizate) și la sisteme informatice infectate cu diverse variante de malware de tip botnet;
- oricare dintre cele două tipuri de sisteme informatice menționate mai sus pot fi folosite ca interfață (proxy) pentru desfășurarea unor atacuri asupra unor ținte din afara țării, reprezentând astfel potențiale amenințări la adresa altor sisteme conectate la Internet;
- dispozitivele sau echipamentele de rețea de uz casnic (ex.: routere wireless), sau cele care fac parte din categoria Internet of Things (IoT) (camere web, smart TV, smartphone, imprimante etc.), odată conectate la Internet, devin ținta atacatorilor, iar vulnerabilitățile acestora sunt exploatate de către aceștia pentru a compromite rețeaua din care fac parte, sau pentru lansarea de atacuri asupra altor ținte din Internet;
- entități din România au fost ținta unor atacuri informatice direcționate și complexe, de tip APT (Advanced Persistent Threat), lansate de către grupări ce au capacitatea și motivația necesară pentru a ataca în mod persistent o țintă în scopul obținerii anumitor beneficii (de obicei acces la informații confidențiale);
- România este atât o țară generatoare de incidente de securitate cibernetică, cât și cu rol de proxy (de tranzit) pentru atacatori din afara spațiului național prin prisma utilizării unor sisteme informatice vulnerabile sau compromise, ce fac parte din spațiul cibernetic național.

În pofida aspectelor tehnice ce fac imposibilă identificarea numărului exact de dispozitive sau persoane afectate, din spatele celor peste 2,3 mil. de adrese IP, sau 68 mil. de alerte raportate la CERT-RO, este important de reținut că acestea acoperă aproximativ 26% din spațiul cibernetic național (raportat la nr. de IP-uri alocate RO) și ca urmare sunt necesare măsuri de remediere a situației, prin implicarea tuturor actorilor cu responsabilități de ordin tehnic sau legislativ.

2. Tipuri de alerte procesate de CERT-RO

CERT-RO procesează două tipuri de alerte de securitate cibernetică:

- ***Alerte colectate și transmise prin intermediul unor sisteme automate***. Aceste alerte sunt transmise de către organizații specializate, ce dețin sisteme de detecție a incidentelor de securitate cibernetică. Marea majoritate a acestor alerte (99%) sunt procesate automat de către CERT-RO și transmise către furnizorii de servicii Internet ce dețin/administrează infrastructurile vizate de alerte (IP, domeniu/URL etc.). În cazul acestui tip de alerte, CERT-RO nu deține date exacte despre utilizatorul adresei IP, identificarea acestuia putând fi făcută numai de către furnizorul de servicii internet (ISP), care de altfel ar trebui să retransmită și alerta către client;
- ***Alertele procesate manual*** sunt considerabil mai puține decât cele automate, dar conțin informații mult mai complete și mai relevante despre incident și despre organizația afectată, precum sursa atacului și metoda de atac. În majoritatea cazurilor datele sunt colectate de la entitățile afectate (persoane fizice sau juridice din țară sau străinătate), de către analiștii CERT-RO, odată cu raportarea incidentului.

Astfel, din punct de vedere al analizei securității cibernetice, aceste alerte sunt mult mai valoroase, reflectând mult mai bine evoluția unui incident de securitate.

3. Statistică pe baza alertelor primite

Numărul alertelor colectate de CERT-RO în anul 2015 a scăzut cu 13% (68.205.856) față de anul 2014 (78.769.993), după cum este evidențiat în Fig. 1.

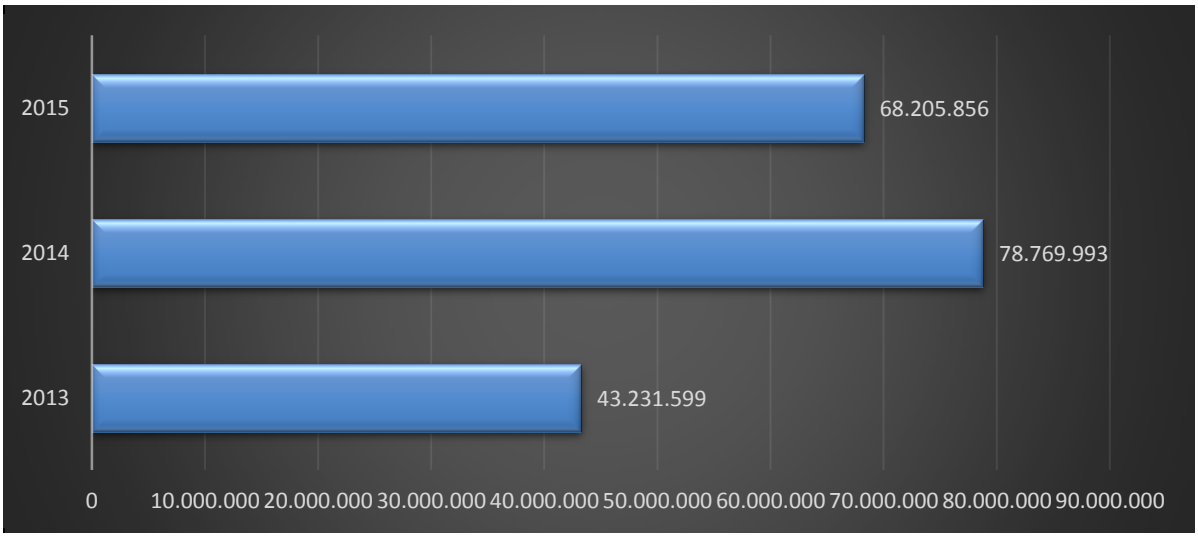

Fig. 1 – Evoluția numărului de alerte colectate în anii 2013, 2014 și 2015

Scăderea numărului de alerte colectate în anul 2015, față de anul 2014, poate fi explicată prin faptul că o parte din sistemele informatice vulnerabile (servere DNS de tip „Open Resolver", servere Proxy fără autentificare, servere NTP configurate ne-corespunzător etc.) au fost remediate în cursul anului trecut.

Numărul semnificativ de alerte prezentate în rapoartele CERT-RO evidențiază necesitățile instituției pentru asigurarea unui sistem performant, capabil să realizeze procesarea și diseminarea automată a unui volum mare de date.

3.1. Distribuția alertelor în funcție de clasă (categorie de alertă)

Alertele colectate și procesate de CERT-RO au fost clasificate în baza unei taxonomii în care au fost definite clase și tipuri de alerte (o clasă de alertă reprezentând o categorie generică ce poate îngloba mai multe tipuri specifice de alertă).

Tabelul și graficul de mai jos evidențiază distribuția celor mai întâlnite 5 categorii de alerte, în funcție de numărul acestora.

Nr.	**Clasă alertă**	**Număr alerte**	**Procent**
1	Vulnerabilities	53.424.880	78,33 %
2	Botnet	14.171.061	20,78 %
3	Malware	393.380	0,58 %
4	Information Gathering	102.167	0,15 %
5	Cyber Attacks	61.751	0,09 %

Tab. 1 – Top 5 al alertelor de securitate pe clase (categorii) de alertă

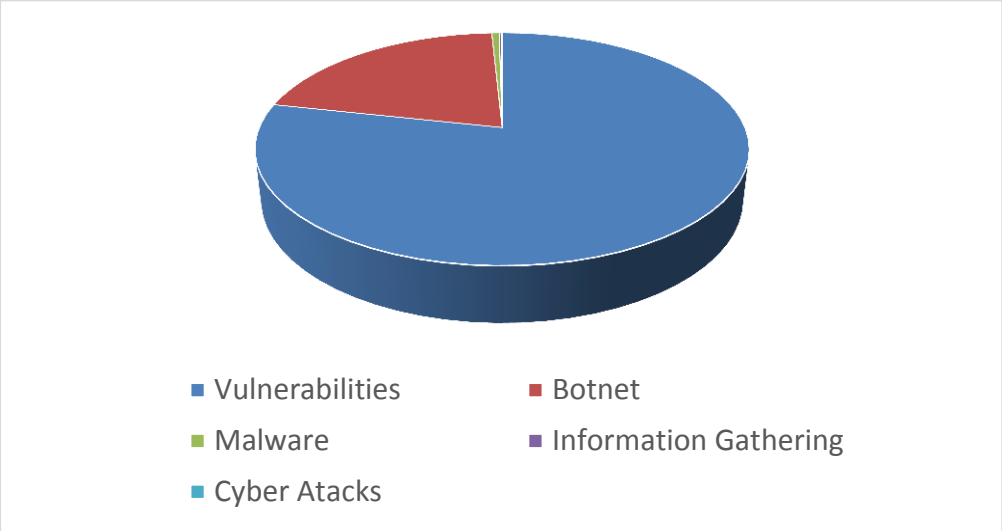

Fig. 2 – Distribuția alertelor pe clase (categorii)

3.2. Distribuția alertelor pe număr de incidente

Având în vedere faptul că unele alerte colectate de CERT-RO sunt repetitive, în sensul că mai multe alerte se referă la aceeași adresă IP și aceeași problemă (clasă/tip de alertă), s-a realizat o de-duplicare a alertelor prin gruparea acestora pe incidente.

Principul general care a stat la baza grupării alertelor pe incidente a fost acela de a agrega toate alertele care se referă la același sistem informatic și același tip de problemă (clasă/tip de alertă).

Având în vedere faptul că alertele colectate de CERT-RO se referă doar la adrese IP publice, este imposibil de determinat numărul exact de sisteme informatice afectate (victime), din cauza următoarelor 2 motive:

- Furnizorii de servicii de internet (ISP) alocă în mod dinamic (DHCP) adresele IP publice către clienții rezidențiali. Astfel că, în decursul unui an calendaristic, o adresă IP publică poate fi alocată mai multor clienți;
- O adresă IP publică poate să reprezinte un gateway de conectare la internet pentru o infrastructură formată din mai multe sisteme informatice. Astfel, în spatele unei adrese IP publice se pot afla mai multe sisteme informatice.

În acest context, gruparea alertelor pe incidente s-a realizat în baza următoarelor considerente:

1. Alertele referitoare la vulnerabilități au o pondere însemnată în numărul total de alerte (78,33%). Aceste vulnerabilități se referă la aplicații și servicii ce rulează pe platforme de tip server (servere web, servere de baze de date, servere de timp etc.), ale căror adrese IP nu sunt alocate dinamic și în general nici nu-și schimbă adresa IP prea des. În consecință, pentru alertele referitoare la vulnerabilități, am considerat că este suficient ca agregarea să se facă pe baza adresei IP și a clasei/tipului de alertă;
2. În cazul alertelor de tip botnet, a căror pondere este de 20,78%, se face referire la sisteme informatice ale utilizatorilor casnici care sunt infectate cu diferite variante de malware de tip botnet. În marea majoritate a cazurilor, pentru aceste sisteme informatice, alocarea adreselor IP se realizează dinamic. În consecință, pentru alertele de tip botnet, agregarea acestora în incidente s-a realizat pe baza adresei IP, a clasei/tipului de alertă și a perioadei de timp dintre 2 raportări (până la 14 zile).

În concluzie, realizând gruparea alertelor pe incidente, conform algoritmului și considerentelor precizate mai sus, au rezultă un număr de **4.900.651 de incidente în anul 2015**, distribuite conform tabelului și graficului de mai jos.

Nr.	**Clasă alertă**	**Nr. incidente**	**Procent**
1	Botnet	3.161.666	64,52 %
2	Vulnerabilities	1.729.042	35,28 %
3	Malware	5.847	0,12 %
4	Information Gathering	3.730	0,08 %
5	Cyber Attacks	366	0,01 %

Tab. 2 – Distribuția alertelor pe nr. de incidente

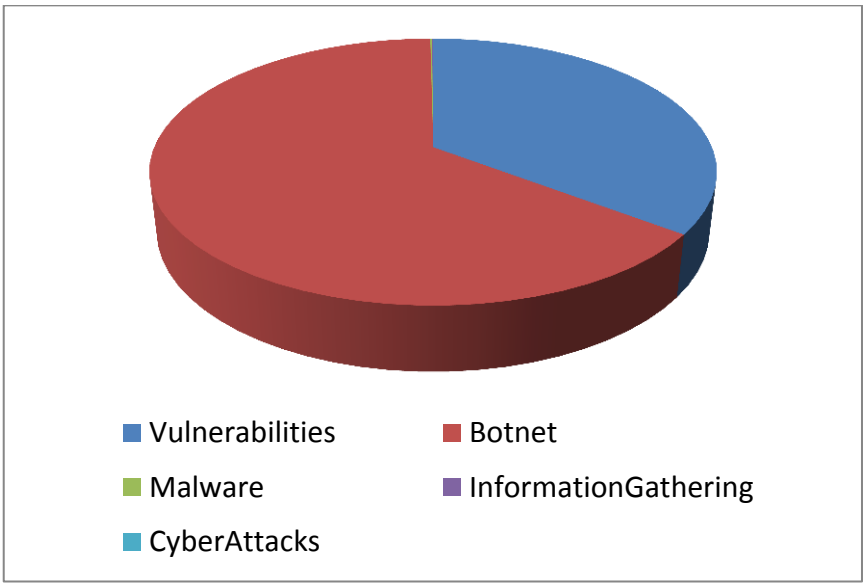

Fig. 3 – Distribuția alertelor pe incidente

Statistica bazată pe agregarea alertelor colectate în incidente arată faptul că principala problemă a spațiului cibernetic național o reprezintă sistemele informatice ce fac parte din rețele de tip botnet (64 %), deși statistica bazată pe nr. de alerte arată 78 % dintre acestea se referă la vulnerabilități și numai 20 % se referă la rețelele botnet. Acest aspect se datorează faptului ca alertele referitoare la vulnerabilități au un caracter de repetitivitate mult mai pronunțat, multe dintre sistemele vizate rămânând vulnerabile o perioadă îndelungată de timp și fiind astfel raportate de mai multe ori.

3.3. Tipuri de malware caracteristice spațiului cibernetic românesc

Un procent de 20% din totalul alertelor colectate și procesate de CERT-RO în anul 2015 conțin și informații referitoare la tipul de malware asociat alertei (precum alertele de tip botnet sau cele referitoare la URL-uri malițioase.

Nr. Crt.	Tip Malware	Procent (%)
1	Conficker	47,98 %
2	Sality	16,98 %
3	ZeroAccess	8,19 %
4	Ramnit	6,07 %
5	Tinba	3,00 %
6	Virut	2,82 %
7	StealRat	2,74 %
8	Pushdo	2,47 %
9	NivDort	1,71 %
10	Gameover ZeuS	0,99 %

Tabel 3 – Top 10 tipuri de malware România 2015

3.4. Tipuri de sisteme informatice afectate

Un procent de 23,87% din totalul alertelor colectate și procesate de CERT-RO în anul 2015 conțin și informații referitoare la sistemul de operare al sistemelor informatice vizate de alerte.

Nr. Crt.	Familie sistem de operare	Procent (%)
1	Network Devices Firmware/OS	32,51 %
2	Unix	28,13 %
3	Linux	25,83 %
4	UPnP OS	9,04 %
5	Windows	3,31 %

Tabel 4 – Distribuție alerte totale per tipuri de sisteme de operare afectate

3.5. Particularități ale alertelor procesate manual

Alături de alertele automate, în perioada de referință, analiștii CERT-RO au preluat o serie de alerte de securitate cibernetică raportate direct de către persoane sau organizații din țară sau străinătate, clasificate ca ***alerte procesate manual***.

Acestea sunt considerabil mai puține decât cele automate, dar conțin informații mult mai complete și mai relevante despre incident, despre organizația afectată, precum sursa atacului precum și metoda de atac. În

majoritatea cazurilor datele sunt colectate de la entitățile afectate (persoane fizice sau juridice din țară sau străinătate), de către analiștii CERT-RO, odată cu raportarea incidentului.

Astfel, în perioada de referință, CERT-RO a colectat **1.223 alerte procesate manual**, repartizate astfel:

Nr. Crt.	Clasa alerte	Tip alertă	Procent alerte
1	Malware	Infected IP	34 %
2	Malware	Malicious URL	25 %
3	Fraud	Phishing	16 %
4	Information Gathering	Scanner	11 %
5	Cyber Attacks	Exploit Attempt	6 %

Tabel 5 – Distribuție alerte individuale

Restul de 8% din alertele procesate manual, se încadrează în diferite clase și tipuri de alerte precum: botnet, spam, defacement, bruteforce, malware sau diseminare de date confidențiale etc.

În tabelul de mai jos regăsiți un top 5 al celor mai afectate tipuri de sisteme, extrase din alertele procesate manual de CERT-RO.

Nr. Crt.	Tipul sistemelor afectate	Procent alerte
1	Rețele/Sisteme informatice	34%
2	Site-uri web	32%
3	Stații de lucru	22%
4	Servicii de tip banking/payment	7%
5	Echipamente de rețea	5%

Tab. 6 – Repartiție alerte procesate manual pe tipuri de sisteme afectate

3.6. Domenii ".ro" compromise

Pentru perioada de referință, CERT-RO a primit alerte referitoare la **17.088** de domenii ".ro" compromise.

Din 855.997[3] domenii înregistrate în România, în luna februarie 2015, numărul reprezintă aproximativ 2% din totalul domeniilor ".ro" și aproximativ 6,5% din totalul domeniilor ".ro" active.

Distribuția domeniilor afectate, după tipul de incident, se regăsește în tabelul de mai jos.

[3] Conform datelor ICI-ROTLD

Nr. Crt.	Categorie	Nr. site-uri
1	Malicious URL	8.783
2	Phishing	7.846
3	Defacement	459
TOTAL		17.088

Tab. 7 – Domenii .ro compromise

3.7. Distribuția detaliată a alertelor pe clase și tipuri

În tabelul de mai jos se regăsesc toate tipurile de alerte colectate de CERT-RO în anul 2015.

Se remarcă faptul că, față de anul 2014, **CERT-RO a procesat 8 noi tipuri de vulnerabilități**: SSL_POODLE, FREAK, Open NAT PMP, Open MsSql, Netis Vulnerability, Open Mongodb, Open Redis și Open Elasticsearch.

Nr.	Clasa alerte	Tip alertă	Nr. alerte	Procent
1	Vulnerabilities	SSL_POODLE	15.910.893	23,33
2	Botnet	Botnet Drone	14.167.432	20,77
3	Vulnerabilities	Vulnerable NTP	12.743.539	18,68
4	Vulnerabilities	Open Resolver	11.239.636	16,48
5	Vulnerabilities	Open SSDP	5.567.411	8,16
6	Vulnerabilities	Open NetBIOS	2.615.348	3,83
7	Vulnerabilities	Open SNMP	2.221.945	3,26
8	Vulnerabilities	FREAK	943.198	1,38
9	Vulnerabilities	Open IPMI	747.316	1,10
10	Vulnerabilities	Open NAT PMP	655.291	0,96
11	Vulnerabilities	Open MsSql	536.055	0,79
12	Malware	Malicious Url	393.207	0,58
13	Information Gathering	Scanner	102.167	0,15
14	Vulnerabilities	Open Chargen	74.650	0,11
15	Cyber Attacks	Bruteforce	61.198	0,09
16	Vulnerabilities	Netis Vulnerability	52.457	0,08

17	Vulnerabilities	Open Mongodb	49.125	0,07
18	Abusive Content	Spam	40.854	0,06
20	Vulnerabilities	Open QOTD	35.252	0,05
21	Vulnerabilities	Open Redis	19.267	0,03
22	Fraud	Phising	11.538	0,02
23	Vulnerabilities	Open Proxy	7.132	0,01
24	Vulnerabilities	Open Elasticsearch	6.365	0,01
25	Botnet	Botnet C&C Server	3.629	0,01
26	Cyber Attacks	APT	553	0,00
27	Malware	Infected IP	173	0,00
28	Compromised Resources	Compromised Router	2	0,00
	TOTAL		**68.205.633**	**100,00%**

3.8. Descrierea (taxonomia) tipurilor de alerte procesate de CERT-RO

Clasa alerte	Tip alertă	Descriere
Abusive Content	**Spam**	Comunicări electronice (email) nesolicitate cu caracter comercial.
Botnet	**Botnet C&C Server**	Sisteme informatice utilizate pentru controlul victimelor (drone, zombie) din cadrul unei rețele de tip botnet.
	Botnet Drone	Rețea de sisteme informatice infectate controlate de alte persoane/organizații decât deținătorii acestora.
Compromised Resources	**Compromised Router**	Compromiterea unor echipamente de comunicații de tip router.
Cyber Attacks	**Bruteforce**	Metodă automată de spargere a parolelor, folosită în scopul aflării credențialelor legitime ale utilizatorilor unui sistem informatic. Practic, prin intermediul unor mecanisme automate, se generează și se testează un număr foarte mare de combinații de parole, până la aflarea credențialelor reale. Metoda garantează succesul dar este foarte mare consumatoare de timp și resurse.
	DDoS	Un atac de tip DDoS (Distributed Denial of Service) este un atac ce vizează afectarea sau chiar întreruperea unor servicii expuse în internet (site-uri web, servere etc.).

	APT	Atacuri cibernetice cu un grad ridicat de complexitate, lansate de către grupuri ce au capacitatea și motivația necesară pentru a ataca în mod persistent o țintă în scopul obținerii anumitor beneficii (de obicei acces la informații sensibile).
Fraud	**Phishing**	O formă de înșelăciune în mediul online care constă în folosirea unor tehnici de manipulare a identității unor persoane/organizații pentru obținerea unor avantaje materiale sau informații confidențiale.
Information Gathering	**Scanner**	Sisteme care scanează clase întregi de IP-uri din Internet, în scopul identificării sistemelor vulnerabile, asupra cărora poate fi lansat ulterior un atac cibernetic. Faza de scanare este faza incipientă în majoritatea atacurilor cibernetice.
Malware	**Infected IP**	Sisteme/servicii informatice cu rol de vector de infectare pentru alte sisteme informatice. Sistemele/serviciile practic găzduiesc, cu sau fără voia administratorului, diverse mostre de malware ce pot infecta alți utilizatori legitimi.
	Ransomware	Ransomware este un software care blochează accesul la fișierele stocate într-un sistem informatic, solicitând plata unei sume de bani în schimbul re-dobândirii accesului la acestea.
	Malicious URL	Site-uri compromise, de cele mai multe ori fără voia administratorului, ce găzduiesc diverse tipuri de malware, facilitând infectarea altor utilizatori legitimi ce vizitează linkurile respective.
	Dyre/Dyreza	Dyre este un malware asemănător cu bine-cunoscutul troian bancar Zeus. Acesta se instalează pe computerul utilizatorului și devine activ doar când utilizatorul își introduce credenţialele pe un site specific, de cele mai multe ori în pagina de autentificare a unei instituții bancare. Prin intermediul unui atac de tip man-in-the-browser, hackerii injectează cod Javascript malițios ce le permite să fure credenţialele de autentificare sau să efectueze operațiuni neautorizate în cont.
Vulnerabilities	**Open Proxy**	Servere/servicii proxy nesecurizate, ce pot fi folosite de către orice utilizator al Internet-ului. Astfel de servicii sunt deseori folosite de atacatori pentru lansarea de atacuri către diverse ținte din internet, păstrându-și astfel identitatea ascunsă. Serviciile de tip proxy sunt deseori folosite pentru accesarea Internet-ului, printr-o singură adresă IP, de către mai mulți utilizatori sau echipamente.
	Vulnerable PLC	Acest tip de alertă se referă la dispozitive de control industrial, de tip PLC (Programmable Logic ControlleR), pentru care au fost identificate diferite

	vulnerabilități de securitate.
Open Resolver	Servere DNS, nesecurizate, ce permit lansarea de solicitări DNS recursive pentru alte domenii decât cele deservite de serverul DNS. Sunt utilizate pentru atacuri de tip DNS Amplification.
Open SSDP	*Simple Service Discovery Protocol* (SSDP) face parte din protocolul *Universal Plug and Play* care a fost implementat pentru a permite PC-urilor să comunice cu echipamentele din rețea (routere, servere media, smart TV, WiFI access point etc.). Prin exploatarea vulnerabilităților tipurilor de transmisie *broadcast* şi *multicast* ale acestui serviciu, un utilizator malițios poate lansa atacuri precum furt de date, DDoS etc.
Open SNMP	*Simple Network Management Protocol* a fost dezvoltat și implementat pentru monitorizarea și managementul dispozitivelor din rețea. Vulnerabilitățile acestui serviciu se datorează îndeosebi setărilor implicite ale acestuia. Prin exploatarea vulnerabilităților specifice SNMP se pot lansa atacuri precum DoS și buffer overflow.
Open NetBIOS	NetBIOS reprezintă un API prin care dispozitivele conectate în rețea pot partaja fișiere și imprimante. *Open NetBIOS* reprezintă orice host pe care acest serviciu este funcționabil și exploatabil.
Open Chargen	*CHARGEN* reprezintă un serviciu pentru testare și debugging a suitei de protocoale din Internet. *Open Chargen* reprezintă orice host pe care acest serviciu este funcționabil și exploatabil.
Open IPMI	*Intelligent Platform Management Interface* reprezintă o interfață de sistem pentru management *out-of-band*. *Open IPMI* reprezintă orice host pe care serviciul *IPMU* este funcționabil și accesibil, care răspunde la ping-urile de tip *IPMI*.
Open QOTD	Orice host care prezintă un serviciu (port) *Quote Of The Day* funcționabil și exploatabil.
SSL_POODLE	Atacul POODLE folosește faptul că, atunci când o încercare de conexiune securizată eșuează, serverele vor negocia folosirea unor protocoale mai vechi, cum ar fi SSL 3.0. Un atacator care poate declanșa o eroare de conexiune, poate forța apoi utilizarea SSL 3.0 și exploatarea vulnerabilității.
FREAK	O nouă vulnerabilitate SSL/TLS - FREAK, acronim pentru Factoring RSA Export Keys. Această vulnerabilitate permite atacatorilor să intercepteze conexiuni de tip HTTPS între clienții vulnerabili și serverele web, forțându-i să utilizeze criptografia de tip „export-grade”.

Open NAT PMP	Identifică gazde care au protocolul NAT Port Mapping (NAT-PMP) activ și accesibil din internet. Aceste servicii au potențialul de a expune informații despre rețeaua clienților.
Open MsSql	Gazde (adrese IP) care au serviciul MS-SQL Server Resolution accesibil din internet. Acest serviciu are potențialul de a expune informații despre rețea și chiar poate facilita propagarea unor atacuri de tip UDP amplification.
Netis Vulnerability	Vulnerabilitate a router-ului NETIS, care permite unui atacator să obțină control asupra dispozitivului. Acesta poate avea succes în momentul în care află adresa IP externă a echipamentului și accesează portul 53413 UDP.
Open Mongodb	Vulnerabilitate de tip zero-day a uneltei de administrare MongoDb. Aceasta permite unui atacator să execute cod fără obligativitatea autentificării.
Open Redis	Gazde (adrese IP) care au stocarea de tip cheie valoare Redis accesibilă direct din internet. Serviciul nu deține proces de autentificare.
Open Elasticsearch	Orice gazdă (adresă IP) care pare că are serviciul Elasticsearch accesibil din internet. Elasticsearch nu deține proces de autentificare.
Vulnerable NTP	Orice host care prezintă un serviciu (port) *Network Time Protocol* funcționabil și accesibil, care răspunde la cereri de tipul *Mode 6*, respectiv *Mode 7*.

Notă: Tabelul de mai sus conține tipurile de alertele de securitate cibernetică raportate frecvent la CERT-RO. Deși gama de amenințări cibernetice este mult mai variată, nu toate se regăsesc în raportările primite de instituția noastră. Sunt menținute denumirile în limba engleză a claselor și tipurilor de alerte pentru a nu pierde sensul anumitor categorii prin traducere în limba română.