CERT.RO

RAPORT
cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2016

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

CUPRINS

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

1. Principalele constatări și concluzii

Obiectivul prezentului raport îl reprezintă **analiza alertelor de securitate cibernetică colectate și procesate de CERT-RO în anul 2016**, 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 01.01.2016 – 31.12.2016, CERT-RO a colectat și procesat **110.194.890 de alerte de securitate cibernetică**, în creștere cu 61,55% față de anul 2015 (68.206.856), dintre care:

- alerte colectate și procesate automat (feed-uri): **110.193.527**;
- alerte colectate și procesate manual (email tiketing): **1.363**.

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 2.920.407 de adrese IP unice au fost vizate de alertele colectate de CERT-RO în anul 2016. Numărul total de IP-uri unice alocat organizațiilor din România este de **7.540.736**[1], în scădere față de anul 2015 (8.958.498), anul 2014 (aprox. 10 mil.) și anul 2013 (aprox.13,5 mil.).

În urma analizării alertelor de securitate cibernetică colectate de CERT-RO în anul 2016, **au fost constatate următoarele:**

- **38,72% (2,92 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 2016, față de **26% (2,3 mil.) în anul 2015**;

- **81,39% (89,68 mil.) din alertele colectate și procesate vizează sisteme informatice vulnerabile**, în sensul că acestea sunt nesecurizate 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;

[1] Conform datelor de la http://www.nirsoft.net/countryip/ro.html

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

- **12,81% (14,12 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;

- **58,98% (2.38 mil.) din numărul total de incidente rezultate din procesarea alertelor de securitate cibernetică reprezintă sisteme informatice vulnerabile**, acestea putând fi utilizate în derularea de atacuri cibernetice asupra unor ținte din Internet, existând posibilitatea ca unele dintre atacuri să fie realizate fără compromiterea sistemelor;

- **40,96% (1,65 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;

- **10,639 de domenii „.ro" au fost raportate la CERT-RO ca fiind compromise în anul 2016**, **în scădere cu aproximativ 40% față de anul 2015 (17.088)**. Din totalul de 896.726[2] domenii înregistrate în România în luna decembrie 2016 (421.973 fiind active[3]), numărul reprezintă aproximativ **1,19% din totalul domeniilor ".ro"** și aproximativ **2,52% din totalul domeniilor ".ro" active**.

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

- 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;

[2] Conform datelor ICI-ROTLD publicate la http://www.rotld.ro/
[3] http://viewdns.info/data/

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

- 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;

- amenințările și vulnerabilitățile de natură cibernetică la adresa spațiului cibernetic național continuă să se diversifice, aspect evidențiat prin faptul că în anul 2016, CERT-RO a introdus noi tipuri de alerte.

În pofida aspectelor tehnice ce fac imposibilă identificarea numărului exact de dispozitive sau persoane afectate, din spatele celor aproximativ 2,9 mil. de adrese IP, sau 110 mil. de alerte raportate la CERT-RO, este important de reținut că acestea acoperă aproximativ 38,72% 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.

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

3. Statistică pe baza alertelor primite

Numărul alertelor colectate de CERT-RO în anul 2016 (110.194.890) a crescut cu 61,55% față de anul 2015 (68.206.856). În figura de mai jos se regăsește evoluția numărului de alerte pe ani, începând cu 2013.

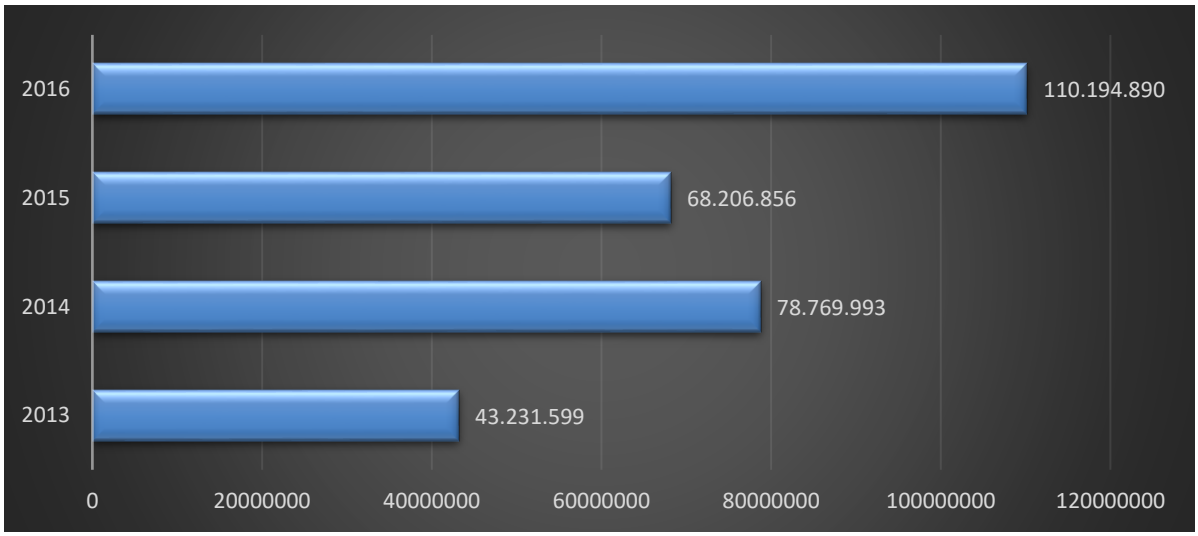

Fig. 1 – Evoluția numărului de alerte colectate în anii 2013, 2014, 2015 și 2016

Numărul semnificativ de alerte prezentate în rapoartele CERT-RO evidențiază necesitățile instituției pentru asigurarea unui sistem informatic performant capabil să realizeze colectarea, 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).

Descrierea (taxonomia) tipurilor de alerte procesate de CERT-RO se regăsește în secțiunea 3.8 de la finele prezentului raport.

Tabelul și diagrama de mai jos evidențiază distribuția celor mai întâlnite 5 categorii de alerte, în funcție de numărul acestora și distribuția grafică a alertelor în funcție de tipul acestora.

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

Nr. crt.	Clasă alertă	Număr alerte	Procent
1	Vulnerabilities	89.684.933	81,39 %
2	Botnet	14.121.119	12,81 %
3	Compromised Resources	5.902.174	5,36 %
4	Malware	454.807	0,41 %
5	Cyber Attacks	26.466	0,02 %

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

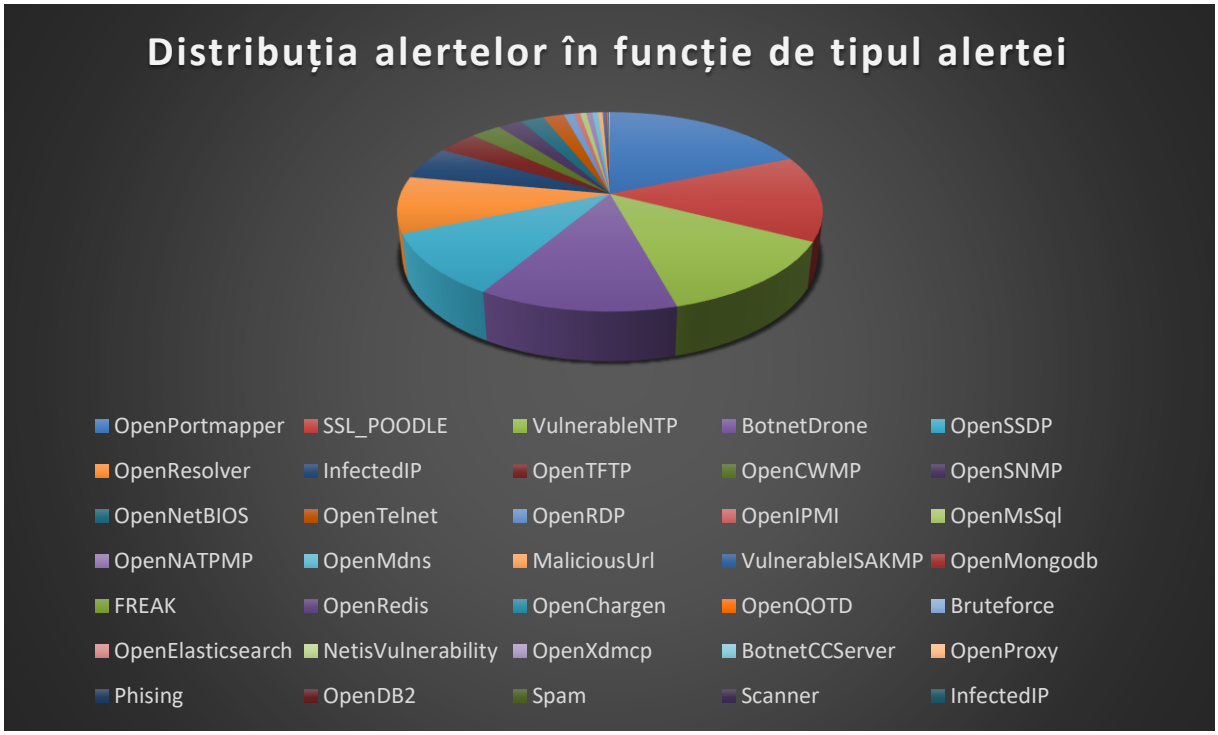

Fig. 2 – Distribuția alertelor în funcție de tipul acestora

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).

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

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 (81,39%). 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 12,81%, 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 **4.035.445 de incidente în anul 2016**, distribuite conform tabelului și graficului de mai jos.

Nr. crt.	Clasă alertă	Nr. incidente	Procent
1	Vulnerabilities	2.380.120	58,98%
2	Botnet	1.653.096	40,96%
3	Malware	2.071	0,05%
4	Altele	158	0,01 %

Tabelul 2 – Distribuția alertelor pe nr. de incidente

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

Statistica bazată pe agregarea alertelor colectate în incidente arată faptul că sistemele informatice ce fac parte din rețele de tip botnet (40,96 %) reprezintă în continuare o problemă principala a spațiului cibernetic național, alături de sistemele informatice vulnerabile (58,98%).

Agregarea alertelor pe incidente ne arată o pondere mult mai semnificativă a amenințărilor de tip botnet decât în cazul statisticii referitoarele numărul de alerte. 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 în mod repetat.

3.3. Tipuri de malware caracteristice spațiului cibernetic românesc

Un procent de 13% din totalul alertelor colectate și procesate de CERT-RO în prima anul 2016 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	Număr de alerte	Procent (%)
1	Sality	4.953.615	34,16%
2	Downadup	2.570.006	17,72%
3	Nivdort	1.979.510	13,65%
4	Ramnit	1.081.592	7,46%
5	Dorkbot	830.914	5,73%
6	Mirai	522.377	3,60%
7	Zeroaccess	312.785	2,16%
8	Virut	277.460	1,91%
9	Conficker	244.371	1,69%
10	Tinba	187.556	1,29%

Tabelul 3 – Top 10 tipuri de malware în România

3.4. Tipuri de sisteme informatice afectate

Un procent de 20,19% din totalul alertelor colectate și procesate de CERT-RO în anul 2016 conțin și informații referitoare la sistemul de operare al sistemelor informatice vizate de alerte.

Tabelul următor conține distribuția alertelor pe tipuri de sisteme de operare.

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

Nr. crt.	Familie sistem de operare	Procent (%)
1	Linux	42,96%
2	Network Devices Firmware/OS	22,91%
3	Unix	24,02%
4	UPnP OS	8,08%
5	Windows	0,57%

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

3.5. Particularități ale alertelor procesate manual

Alături de alertele automate, 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 **1.363 alerte procesate manual**, repartizate astfel:

Nr. crt.	Clasa alerte	Tip alertă	Număr de alerte	Procent alerte
1	Fraud	Phising	505	37,05 %
2	Malware	Malicious Url	363	26,63 %
3	Malware	Infected IP	256	18,78 %
4	Botnet	Botnet Drone	84	6,16 %
5	Botnet	Botnet CC Server	42	3,08 %
6	Cyber Attacks	Bruteforce	37	2,71 %
7	Information Gathering	Scanner	23	1,69 %
8	Vulnerabilities	Other	23	1,69 %
9	AbusiveContent	Spam	17	1,25 %
10	Compromised Resources	Infected IP	13	0,95 %

Tabelul 5 – Distribuția alertelor procesate manual

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

3.6. Domenii ”.ro” compromise

Pentru perioada de referință, CERT-RO a primit alerte referitoare la **10.639** de domenii ”.ro” compromise.

Din 896.726[4] domenii înregistrate în România, în luna decembrie 2016, numărul reprezintă aproximativ 1,19% din totalul domeniilor ”.ro” și aproximativ 2,52% din totalul domeniilor ‟.ro” active.

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

Nr. crt.	Clasă alerte	Nr. site-uri
1	Vulnerabilities	8202
2	Malware	1363
3	Botnet	677
4	Fraud	361
5	AbusiveContent	36
TOTAL		10.639

Tabelul 6 – 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 2016.

Se remarcă faptul că, față de anul 2015, **CERT-RO a procesat 11 noi tipuri de vulnerabilități**: Open Port Mapper, Open TFTP, Open CWMP, Open NetBIOS, Open Telnet, Open RDP, Vulnerable ISAKMP, Open Redis, Open mDNS, Open XDMCP și Open DB2.

Nr. crt	Clasa alerte	Tip alertă	Nr. alerte	Procent
1	Vulnerabilities	Open Portmapper	20.539.496	18,63925 %
2	Vulnerabilities	SSL_POODLE	15.358.349	13,93744 %
3	Vulnerabilities	Vulnerable NTP	14.493.897	13,15297 %
4	Botnet	Botnet Drone	14.117.097	12,81103 %

[4] Conform datelor ICI-ROTLD publicate la http://www.rotld.ro/

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

Nr. crt	Clasa alerte	Tip alertă	Nr. alerte	Procent
5	Vulnerabilities	Open SSDP	11.177.596	10,14348 %
6	Vulnerabilities	Open Resolver	10.107.848	9,17270 %
7	CompromisedResource	Infected IP	5.902.187	5,35613 %
8	Vulnerabilities	Open TFTP	4.027.012	3,65445 %
9	Vulnerabilities	Open CWMP	3.026.661	2,74664 %
10	Vulnerabilities	Open SNMP	2.430.907	2,20601 %
11	Vulnerabilities	Open NetBIOS	2.306.809	2,09339 %
12	Vulnerabilities	Open Telnet	2.116.736	1,92090 %
13	Vulnerabilities	Open RDP	981.330	0,89054 %
14	Vulnerabilities	Open IPMI	626.050	0,56813 %
15	Vulnerabilities	Open MsSql	615.636	0,55868 %
16	Vulnerabilities	Open NAT-PMP	604.933	0,54897 %
17	Vulnerabilities	Open mDNS	575.435	0,52220 %
18	Malware	Malicious Url	455.169	0,41306 %
19	Vulnerabilities	Vulnerable ISAKMP	309.947	0,28127 %
20	Vulnerabilities	Open Mongodb	143.375	0,13011 %
21	Vulnerabilities	FREAK	73.748	0,06693 %
22	Vulnerabilities	Open Redis	60.093	0,05453 %
23	Vulnerabilities	Open Chargen	48.781	0,04427 %
24	Vulnerabilities	Open QOTD	33.792	0,03067 %
25	CyberAttacks	Bruteforce	26.503	0,02405 %
26	Vulnerabilities	Open Elasticsearch	12.677	0,01150 %
27	Vulnerabilities	Netis Vulnerability	6.003	0,00545 %
28	Vulnerabilities	Open Xdmcp	4.162	0,00378 %
29	Botnet	Botnet CC Server	4.148	0,00376 %
30	Vulnerabilities	Open Proxy	2.685	0,00244 %
31	Fraud	Phising	3.062	0,00278 %
32	Vulnerabilities	Open DB2	975	0,00088 %
33	AbusiveContent	Spam	911	0,00083 %
34	InformationGathering	Scanner	600	0,00054 %
35	Malware	Infected IP	257	0,00023 %

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

Nr. crt	Clasa alerte	Tip alertă	Nr. alerte	Procent
36	Vulnerabilities	Other	23	0,00002 %
	TOTAL		**110.194.89**	**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.
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.
	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.).
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.

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

Clasa alerte	Tip alertă	Descriere
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.
Vulnerabilities	**Open Protocols and Services:** *Portmapper, NTP, SSDP, TFTP, CWMP, SNMP, NetBIOS, Telnet, RDP, IPMI, MsSql, NAT-PMP, mDNS, ISAKMP, Mongodb, Redis, Chargen, QOTD, Elasticsearch, Xdmcp, DB2*	Protocoale sau servicii care rulează pe diferite sisteme informatice, adesea servere, care nu sunt configurate corespunzător sau reprezintă versiuni neactualizate și cu probleme de securitate cunoscute. Aceste sisteme informatice sunt vulnerabile la diferite amenințări ce pot exploata vulnerabilitățile respective.
	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.
	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.

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455

Clasa alerte	Tip alertă	Descriere
	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”.
	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.

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.

www.cert.ro office@cert.ro +4031-6202187 Bd. Mareșal Averescu 8-10, Sector 1, București, 011455