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 2014

Pagină albă

CUPRINS

Pagină albă

1. Principalele constatări și concluzii

Obiectivul prezentului raport este analiza alertelor de securitate cibernetică colectate și procesate de CERT-RO în anul 2014, în vederea obținerii unei imagini de ansamblu asupra evenimentelor relevante pentru evaluarea riscurilor de securitate cibernetică la adresa infrastructurilor IT și de comunicații electronice de pe teritoriul României, aflate în aria de competență a CERT-RO.

În perioada de referință, respectiv 01.01 – 31.12.2014, la CERT-RO au fost primite sesizări (alerte), astfel:

1. **Număr total de alerte procesate: 78.769.993 (automate: 78.767.749, alerte colectate manual: 2.244)**
2. **număr total de IP-uri unice extrase din totalul alertelor: 2.481.648**

Numărul total de IP-uri unice alocat organizațiilor din România este de **10.021.888**[1], în scădere față de 2013 când numărul acestora era de 13,5 mil.

Prin **alertă de securitate cibernetică,** în contextul prezentului document, înțelegem orice semnalare ce conține o adresă IP sau o adresă URL (site), referitoare la un posibil incident sau eveniment de securitate cibernetică, de natură să afecteze securitatea cibernetică, ce implică sau poate implica sisteme informatice ce aparțin unor persoane juridice sau fizice ce aparțin spațiului cibernetic național.

Pe baza datelor colectate au fost **constatate** următoarele:

- 24% din totalul IP-urilor unice alocate spațiului cibernetic romanesc (2.4 mil) au fost implicate in cel puțin o alerta de securitate cibernetica procesata de CERT-RO. In anul 2013, 16% (2.2 mil) din IP-urile unice alocate spațiului cibernetic național au fost implicate în cel puțin o alerta de securitate cibernetică.
- 54% din alertele primite vizează sisteme informatice configurate necorespunzător (misconfigured), nesecurizate sau vulnerabile, ce oferă diverse servicii nesecurizate în Internet, folosite de atacatori pentru ascunderea identității și lansarea de atacuri cibernetice asupra altor ținte. De cele mai multe ori, aceste sisteme nu trebuie compromise, simpla folosire a acestora fiind suficientă (ex: DNS open resolver, open SNMP, open NTP etc.); acest trend se observă și prin creșterea numărului de alerte ce au vizat echipamente de rețea de tip business (routere, firewall, etc.) sau home user (routere wireless, camere web, smart TV, smartphone etc.), față de alte sisteme de operare, creștere evidențiată în subcapitolul 3.1.4.
- 46% din alerte vizează sisteme informatice din România, victime ale unor atacatori care au reușit preluarea de resurse în cadrul unor rețele de tip botnet (zombie) prin exploatarea unor vulnerabilități tehnice și infectarea sistemelor cu diverse tipuri de aplicații malware. Rețelele de tip botnet reprezintă cea mai importantă problemă existentă în spațiul cibernetic național deoarece aceste computere compromise pot fi utilizate în derularea de atacuri cibernetice asupra altor ţinte din România sau din spaţiul extern ţării noastre.
- 10.759 domenii .ro au fost raportate la CERT-RO ca fiind compromise în cursul anului 2014, cu 5% mai multe domenii decât în cursul anului 2013, perioadă în care au fost raportate

[1] Conform datelor http://www.ip-broker.uk din luna Ianuarie 2015.

10.239. Din 710.000[2] domenii înregistrate în România, în luna decembrie 2013, numărul reprezintă aproximativ 1,5% din totalul domeniilor ".ro".

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

- amenințările de natură informatică, asupra spațiului cibernetic național, continuă să se diversifice
- majoritatea alertelor primite se referă sisteme infectate cu diverse variante de malware, ce fac parte din diverse rețele de tip botnet, precum și la sisteme informatice configurate necorespunzător (misconfigured) sau nesecurizate.
- oricare dintre cele două tipuri de sisteme, menționate mai sus, pot fi folosite cu rol de „proxy" pentru desfășurarea altor atacuri asupra unor ținte din afara țării, reprezentând astfel potențiale amenințări la adresa altor sisteme conectate la Internet;
- dispozitive sau echipamente de rețea de uz casnic (routere wireless) sau 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 atacatori pentru a avea acces în rețeaua în care acestea sunt utilizate 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 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);
- România nu mai poate fi considerată doar o țară generatoare de incidente de securitate cibernetică, analiza datelor prezentate demonstrând caracterul intermediar/de tranzit al unor sisteme informatice conectate 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 2,4 mil. adrese IP sau 78 mil. alerte raportate la CERT-RO, este important de reținut că acestea acoperă aprox. 24% 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*** (ex: honeypots). Aceste alerte sunt transmise de către organizații specializate[3], ce dețin sisteme de detecție a incidentelor de securitate cibernetică. Marea majoritatea (99%) acestor alerte sunt procesate automat de către CERT-RO și transmise către furnizorul de servicii Internet în reţeaua căruia funcţionează sistemul informatic identificat prin IP-ul din cadrul alertei. 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),

[2] Conform datelor ICI-ROTLD.
[3] Precum alte CERT-uri sau companii de securitate.

care de altfel trebuie să retransmită și alerta către client. Deși aceste alerte nu conțin foarte multe detalii (ex: arhitectura sistemului informatic atacat, tipul organizației victimă, nivelul pagubelor produse etc.), ele oferă o imagine de ansamblu asupra tipului de amenințări ce afectează infrastructurile cibernetice din România, un procent de 90% din alertele transmise fiind confirmate de către furnizorii de servicii internet (ISP).

- ***Alertele procesate manual*** 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, 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 primite de CERT-RO în **2014**, a crescut cu **82%** (**78.767.749)** față de 2013 (43.231.149), creșterea fiind expusă în tabelul de mai jos.

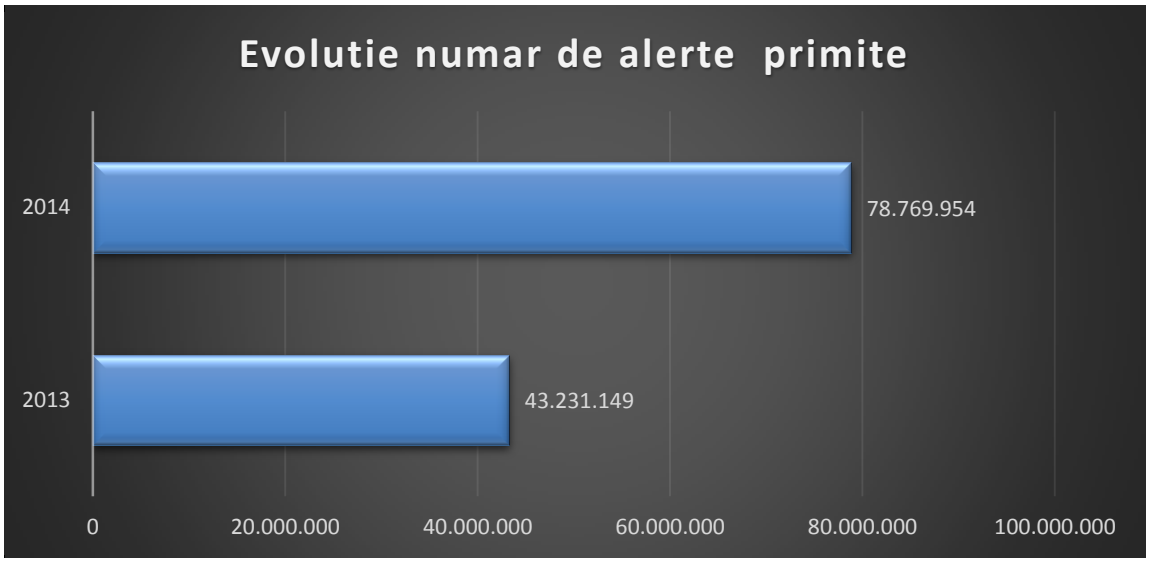

Fig. 1 – Evoluția numărului de alerte primite 2013/2014

3.1.1. Distribuția alertelor pe clase

Tabelul și graficul de mai jos redau distribuția primelor 5 tipuri de alertelor primite, pe clase de alerte.

Nr.	Clasă alerte	Număr alerte	Procent
1	Vulnerabilities	42.146.259	53,51%
2	Botnet	35.657.806	45,27%
3	Information Gathering	465.288	0,59%
4	Malware	284.158	0,36%
5	CyberAttacks	160.304	0,20%

Tabel 1 – Distribuția alertelor pe clase (categorii) de alerte

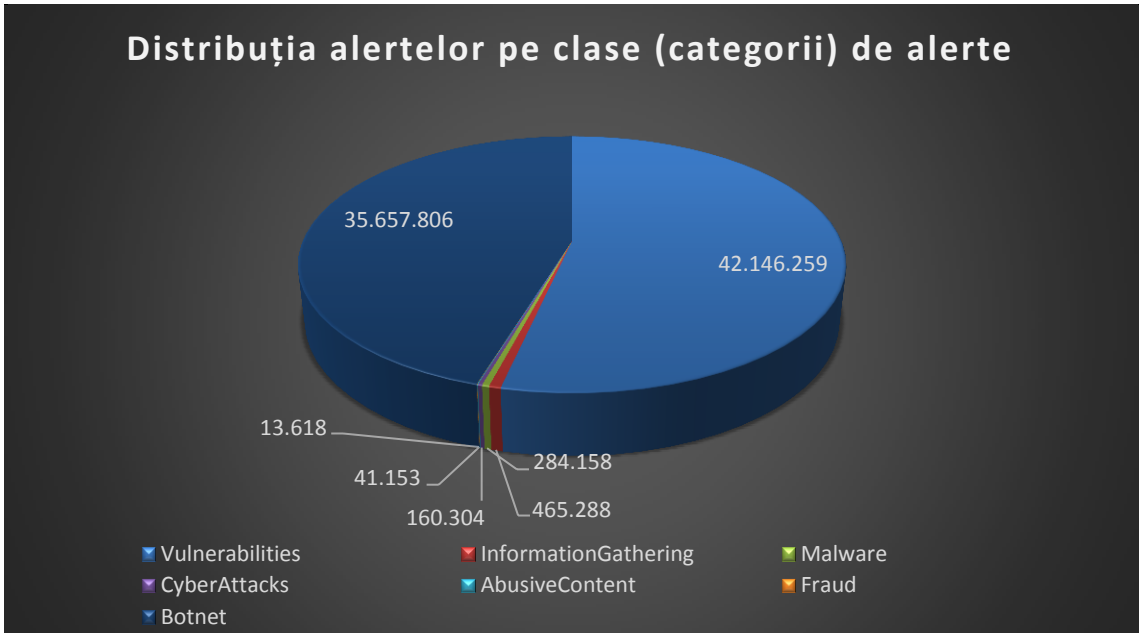

Fig. 2 – Distribuția alertelor pe clase (categorii)

Distribuția detaliată a alertelor, atât pe clase cât și pe tipuri, este disponibilă în anexa nr. 1 a prezentului raport.

3.1.2. Tipuri de malware caracteristice spațiului cibernetic românesc

Nr. Crt.	Tip Malware	Procent (%)
1	Downadup	10.79%
2	Zeus	8.73%
3	Sality	4.55%
4	Virut	3.30%
5	Zeroaccess	2.94%
6	Irc-bot	2.13%
7	Troj-bankpath	1.98%
8	Gameoverzeus	1.14%
9	Gamarue	0.94%
10	Dorkbot	0.89%

Tabel 2 – Top 10 tipuri de malware România 2014

Identificarea tipului de malware a fost posibilă în 37,5% din numărul alertelor primite.

3.1.3. Tipuri de sisteme afectate de alerte

Nr. Crt.	Familie sistem operare	Procent
1	Linux	8.68%
2	Cisco	5.69%
3	OS 1.0 UPnP (dispozitive casnice cu SSDP) (ex: routere, camere web, imprimante, smart TV etc.)	3.87%
4	Unix	3.53%
5	Windows	2.23%

Tabel 3 – Repartiție alerte totale per tipuri de sisteme de operare afectate

Identificarea familiei sistemului de operare a fost posibilă în aprox. 24,6% din totalul alertelor.

3.1.4. 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 2244 alerte procesate manual, repartizate astfel:

Nr. Crt.	Clasa alerte	Tip alertă	Procent alerte
1	Malware	Infected IP	40%
2	Malware	Malicious URL	22%
3	Fraud	Phishing	12%
4	Information Gathering	Scanner	11%
5	Cyber Attacks	Exploit Attempt	6%

Tabel 4 – Distribuție alerte individuale per tipuri

Restul de 9% din alertele procesate manual, se încadrează în diferite clase și tipuri de alerte precum: botnet, spam, defacement, bruteforce, mostre malware sau diseminare de date confidențiale (disclosure of confidential data).

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	28%
3	Stații de lucru	26%
4	Servicii de tip banking/payment	5%
5	Echipamente de rețea	3%

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

3.1.5. Domenii ”.ro” compromise

Pentru perioada de referință, CERT-RO a primit alerte referitoare la **10.759** domenii ”.ro” compromise.
Din 710.000[4] domenii înregistrate în România, în luna decembrie 2013, numărul reprezintă aproximativ 1,5% din totalul domeniilor ”.ro”.
Distribuția domeniilor afectate, după tipul de incident, se regăsește în tabelul de mai jos.

Nr. Crt.	Categorie	Nr. site-uri
1	Phishing	2164
2	Malicious URL	8037
3	Defacement	558
	TOTAL	10.759

Tab. 7 – Domenii .ro compromise

[4] Conform datelor ICI-ROTLD

Anexa 1 – Distribuția detaliată a alertelor pe clase și tipuri

Nr.	Clasa alerte	Tip alertă	Alerte manuale	Alerte automate	Total	Procent
1	**Botnet**	Botnet Drone	33	35.652.050	**35.652.083**	**45,26%**
2	**Vulnerabilities**	OpenResolver	1	13.694.039	**13.694.040**	**17,38%**
3	**Vulnerabilities**	OpenSSDP		12.462.475	**12.462.475**	**15,82%**
4	**Vulnerabilities**	Open NTP	1	8.905.805	**8.905.806**	**11,31%**
5	**Vulnerabilities**	OpenSNMP		2.622.503	**2.622.503**	**3,33%**
6	**Vulnerabilities**	OpenNetBIOS		2.262.387	**2.262.387**	**2,87%**
7	**Vulnerabilities**	SSL_POODLE		1.654.714	**1.654.714**	**2,10%**
8	**InformationGathering**	Scanner	256	465.032	**465.288**	**0,59%**
9	**Vulnerabilities**	OpenIPMI		404.208	**404.208**	**0,51%**
10	**Malware**	Malicious URL	482	283.993	**284.475**	**0,36%**
11	**Cyber Attacks**	Bruteforce	5	159.970	**159.975**	**0,20%**
12	**Vulnerabilities**	OpenChargen		83.171	**83.171**	**0,11%**
13	**Abusive Content**	Spam	15	41.129	**41.144**	**0,05%**
14	**Vulnerabilities**	OpenQOTD		36.479	**36.479**	**0,05%**
15	**Fraud**	Phishing	266	13.349	**13.615**	**0,02%**
16	**Vulnerabilities**	NetisVulnerability		12.485	**12.485**	**0,02%**
17	**Vulnerabilities**	OpenProxy		7.986	**7.986**	**0,01%**
18	**Botnet**	Botnet C&C Server	46	5.677	**5.723**	**0,01%**
19	**Malware**	Infected IP	896	165	**1.061**	**0,00%**
20	**Cyber Attacks**	APT	6	132	**138**	**0,00%**
21	**Cyber Attacks**	Exploit Attempt	135		**135**	**0,00%**
22	**Cyber Attacks**	DdoS	56		**56**	**0,00%**
23	**CompromisedResources**	Comprimised Application/Service	9		**9**	**0,00%**
24	**CompromisedResources**	Defacement	8		**8**	**0,00%**
25	**CompromisedResources**	Compromised Website	6		**6**	**0,00%**
26	**Vulnerabilities**	Other[5]	5		**5**	**0,00%**
27	**Abusive Content**	Disclosure of Personal Data	4		**4**	**0,00%**
28	**Abusive Content**	Disclosure of Confidential Data	3		**3**	**0,00%**
29	**Fraud**	Unlawful eCommerce/Services	3		**3**	**0,00%**
30	**Malware**	Malware Sample	3		**3**	**0,00%**
31	**Abusive Content**	Other[6]	2		**2**	**0,00%**
32	**CompromisedResources**	Compromised Router	2		**2**	**0,00%**
33	**CompromisedResources**	Compromised Network/System	1		**1**	**0,00%**
	TOTAL		2244	78.767.749	78.769.993	100,00%

[5] Vulnerabilities - Other – se referă la orice alte tip de alertă referitoare la vulnerabilități ce nu au fost definite până în prezent.

[6] Abusive content – Other - se referă la orice alte tip de alertă referitoare la conținut abuziv, ce nu a fost definită până în prezent.

Anexa 2 – Clasificarea tipurilor de alerte procesate de CERT-RO

Clasa alerte	Tip alertă	Descriere
Abusive Content	**Spam**	Comunicări electronice (mail) nesolicitate cu caracter comercial.
	Child Pornography	Distribuire materiale pornografice cu minori.
	Disclosure of Personal Data	Publicarea ilegală a datelor cu caracter personal.
	Disclosure of Confidential Data	Publicarea ilegală de date confidențiale. Compromiterea datelor prin încălcarea principiului confidențialității lor .
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	**Defacement**	Atac asupra unui site web, realizat prin diferite metode, ce are ca scop alterarea conținutului afișat în paginile web. De cele mai multe ori atacatorii înlocuiesc prima pagină a site-ului cu o altă pagină ce afișează informații false.
	Compromised Router	Compromiterea unor echipamente de comunicații de tip router.
	Compromised Network/System	Compromiterea unei rețele sau a unui sistem informatic.
	Compromised Application/Service	Compromiterea unor aplicații/servicii
	Compromised Website	Site web compromis
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	Afectarea disponibilității unor sisteme/servicii informatice sau de comunicaţii electronice. Sistemul țintă este atacat prin trimiterea unui număr foarte mare de solicitări nelegitime, ce consumă resursele hardware sau software ale acestuia, făcându-l indisponibil pentru utilizatorii legitimi.
	Exploit Attempt	Secvențe de cod ce exploatează erori de programare din sistemul de operare sau din orice alt program rezident în acel sistem. De cele mai multe ori, exploit-urile nu cauzează daune, ci doar permit unui atacator obținerea controlului asupra sistemului infectat creând

		posibilitatea instalării altor tipuri de malware.
	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.
	Unlawful eCommerce/Services	Activități ilegale de comerț de servicii sau produse pe internet.
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.
	Sniffer	Sistem ce interceptează pachetele de date transmise prin rețea permițând decodificarea ulterioară a acestora. Această metodă se folosește pentru aflarea parolelor sau a altor date senzitive despre anumiți utilizatori. Sniffing se referă la actul de interceptare a pachetelor TCP/IP.
	Social Engineering	Reprezintă un set de tehnici folosite pentru manipularea utilizatorilor sistemelor informatice, în scopul divulgării de informaţii confidenţiale, ce pot fi folosite ulterior pentru obținerea de foloase necuvenite sau acces fără drept la sistemul informatic.
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.
	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.
	Malware sample	Sample de malware transmis pentru analiză.
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.
	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 reţea (rutere, servere media, smart TV, WiFI access point etc.). Prin exploatarea vulnerabilităţilor tipurilor de transmisie *broadcast* şi *multicast* ale acestui serviciu, un utilizator maliţios poate lansa atacuri precum furt de date, DDoS etc.
	Open SNMP	*Simple Network Management Protocol* a fost dezvoltat şi implementat pentru monitorizarea şi managementul dispozitivelor din reţea. Vulnerabilităţile acestui serviciu se datorează îndeosebi setărilor implicite ale acestuia. Prin exploatarea vulnerabilităţilor specifice SNMP se pot lansa atacuri precum DoS, buffer overflow etc.
	Open NetBIOS	NetBIOS reprezintă un API prin care dispozitivele conectate în reţea pot partaja fişiere şi printere. *Open NetBIOS* reprezintă orice host pe care acest serviciu este funcţionabil şi exploatabil.
	Open Chargen	*CHARGEN* reprezintă un serviciu pentru testare şi debugging a suitei de protocoale din Internet. *Open Chargen* reprezintă orice host pe care acest serviciu este funcţionabil şi exploatabil.
	Open IPMI	*Intelligent Platform Management Interface* reprezintă o interfaţă de sistem pentru management *out-of-band*. *Open IPMI* reprezintă orice host pe care serviciul *IPMU* este funcţionabil şi accesibil, care răspunde la ping-urile de tip *IPMI*.
	Open QOTD	Orice host care prezintă un serviciu (port) *Quote Of The Day* funcţionabil şi exploatabil.
	Vulnerable NTP	Orice host care prezintă un serviciu (port) *Network Time Protocol* funcţionabil şi 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 instituţia noastră. Sunt menţinute denumirile în limba engleză a claselor și tipurilor de alerte pentru a nu pierde sensul anumitor categorii prin traducere în limba română.