CENTRUL NAŢIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO

Raport
cu privire la alertele de securitate cibernetică primite de CERT-RO în primele 6 luni ale anului 2013

Pagină albă

CUPRINS

1. Rezumatul raportului 5
2. Ce este CERT-RO? 6
3. Scopul prezentului raport 7
4. Despre sursele de date ale CERT-RO 8
5. Statistică pe baza alertelor primite 9
   5.1. Alerte colectate și transmise prin intermediul unor sisteme automate 9
   5.1.1. Repartiția alertelor pe tipuri de incidente 9
   5.1.2. Repartiția alertelor pe Autonomous System Number (ASN) 10
   5.1.3. Repartiția geografică a IP-urilor raportate 11
   5.1.4. Statistică domenii ”.ro” compromise 12
   5.2. Alerte individuale 13
   5.3. Amenințări de tip Advanced Persistent Threath (APT) 15
6. Concluzii și comentarii 16

Anexa 1 – Termeni și definiții 17

Pagină albă

1. Rezumatul raportului

Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO este o structură independentă de expertiză şi cercetare-dezvoltare în domeniul protecţiei infrastructurilor cibernetice, care dispune de capacitatea necesară pentru prevenirea, analiza, identificarea şi reacţia la incidentele de securitate cibernetică ale sistemelor informatice ce asigură funcţionalităţi de utilitate publică ori asigură servicii ale societăţii informaţionale. CERT-RO se află în coordonarea Ministerului pentru Societatea Informațională și este finanțat integral de la bugetul de stat.

În calitate de punct național de contact cu privire la incidente de securitate cibernetică, în perioada de referință, respectiv 01.01 – 30.06.2013, CERT-RO a fost sesizat de către diverși parteneri interni sau internaționali, cu referire la incidente de securitate cibernetică, prin:

1. Alerte colectate și transmise prin intermediul unor sisteme automate: 17.511.109
    - număr total de IP unice compromise, extrase din totalul alertelor: 1.716.278
2. Alertele individuale precum și cele constituite pe baza informațiilor colectate de CERT-RO: 140.

Scopul prezentului raport este de a realiza analiza incidentelor de securitate cibernetică colectate/gestionate la nivelul CERT-RO pe o perioadă relevantă de timp şi obţinerea unei viziuni de ansamblu asupra naturii şi dinamicii acestor tipuri de evenimente relevante pentru evaluarea riscurilor de securitate cibernetică la adresa infrastructurilor IT şi de comunicaţii electronice de pe teritoriul naţional al României, aflate în aria legală de competență a CERT-RO.

Pe baza datelor colectate au fost constatate următoarele:

- ameninţările, de natură informatică, asupra spațiului cibernetic național s-au diversificat, fiind relevate tendinţe evolutive, atât din perspectivă cantitativă, cât şi din punct de vedere al complexităţii tehnice;
- majoritatea incidentelor analizate de CERT-RO se referă la entități din România, victime ale unor atacatori care, de regulă prin exploatarea unor vulnerabilităţi tehnice, au vizat infectarea unor sisteme informatice cu diverse tipuri de aplicaţii malware, în scopul constituirii unor reţele de tip botnet (zombie);
- peste 12,5% din plaja de IP-uri alocată României este infectată cu diverse variante de malware, majoritatea alertelor de tip botnet vizând utilizatori de tip rezidențial (home user).
- prin calculatoarele unor victime din România, folosite ca proxy, sunt desfășurate atacuri asupra unor ținte din afara țării, identitatea reală a atacatorului rămânând ascunsă;
- România nu mai poate fi considerată doar o ţară generatoare de incidente de securitate cibernetică, analiza datelor prezentate demonstrând caracterul intermediar/de tranzit al unor resurse informatice semnificative conectate la reţeaua Internet în România;
- amenințările de tip APT, specifice campaniilor de spionaj cibernetic, au devenit o realitate și în România;
- aproximativ 90% din alertele primite de CERT-RO vizează computere din România, infectate cu diverse variante de malware, ce fac parte din rețele de tip botnet;
- 5.678 domenii ”.ro” au fost compromise, reprezentând mai puțin de 1% din totalul domeniilor existente; dintre acestea peste 51% au suferit atacuri de tip defacement, iar 43% au fost infectate cu diverse variante de malware.

Pentru detalii suplimentare, precum și interpretări ale unor rezultate, vă rugăm citiți întregul raport de analiză.

2. Ce este CERT-RO?

Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO este o instituție publică aflată în coordonarea Ministerului pentru Societatea Informațională și finanțată integral de la bugetul de stat.[1]

Printre atribuțiile CERT-RO, regăsim:

- organizează şi întreţine un sistem de baze de date, la nivel naţional, privind ameninţările, vulnerabilităţile şi incidentele de securitate cibernetică identificate sau raportate, tehnici şi tehnologii folosite pentru atacuri, precum şi bune practici pentru protecţia infrastructurilor cibernetice;
- asigură cadrul organizatoric şi suportul tehnic necesar schimbului de informaţii dintre diverse echipe de tip CERT, utilizatori, autorităţi, producători de echipamente şi soluţii de securitate cibernetică, precum şi furnizori de servicii în domeniu;
- asigură puncte de contact pentru colectarea sesizărilor şi a informaţiilor despre incidente de securitate cibernetică atât automatizat, cât şi prin comunicare directă securizată, după caz;
- elaborează propuneri pe care le înaintează către MSI sau Consiliului Suprem de Apărare a Ţării, denumit în continuare CSAT, privind modificarea cadrului legislativ în vederea stimulării dezvoltării securităţii infrastructurilor cibernetice ce asigură funcţionalităţi de utilitate publică ori asigură servicii ale societăţii informaţionale;
- constituie ”Sistemul de alertă timpurie şi informare în timp real” privind incidentele cibernetice în scopul avertizării în timp real şi emiterii de rapoarte cu privire la distribuţia şi natura incidentelor precum și al colaborării cu autorităţile naţionale responsabile în asigurarea securităţii cibernetice, în vederea prevenirii şi înlăturării efectelor incidentelor de securitate cibernetică;
- oferă servicii publice de tip ***preventiv*** (anunţuri privind ameninţări sau vulnerabilități noi-identificate pe plan naţional şi internaţional; realizarea, la cerere, de auditări şi evaluări de securitate sau teste de penetrare; situații actualizate asupra incidentelor de securitate cibernetică ce afectează sau implică entități din România), ***reactiv*** (alerte şi atenţionări privind apariţia unor activităţi premergătoare atacurilor; gestiunea incidentelor de securitate cibernetică la nivel naţional;) și de ***consultanță*** în domeniul securității cibernetice (pregătire echipe de tip CERT, analize de risc aplicate la nivel local şi la nivel naţional privind infrastructurile cibernetice).

CERT-RO colectează din surse naționale sau internaționale, date referitoare la incidente sau evenimente de securitate cibernetică ce afectează sau implică entități din România. Astfel, odată identificat un incident, în baza unei proceduri interne, CERT-RO declanșează o serie de acțiuni ce asigură activitatea de răspuns. În majoritatea cazurilor, activitatea de răspuns la incidentele de securitate cibernetică urmărește atingerea următoarelor obiective:

1. stoparea imediată sau reducerea la minimul posibil a efectelor incidentului;
2. stabilirea preliminară a impactului incidentului/evenimentului;
3. identificarea si alertarea tuturor părților afectate sau care pot fi afectate de incidentul/evenimentul de securitate precum și a celor responsabile de remedierea situației;
4. identificarea si alertarea tuturor instituțiilor sau autorităților publice responsabile de gestionarea situației;

[1] Conform H.G. 494/2011, http://www.cert-ro.eu/files/doc/HG_494-2011_CERT-RO.pdf

5. diseminarea de documente de natură tehnică referitoare la metode de detecție și tratare ale incidentul/evenimentul de securitate, pentru alte entități ce pot fi vizate de un incident similar.

NOTĂ:
Conform atribuţiilor legale, CERT-RO îndeplinește un rol de coordonator al activității de răspuns la incidente de securitate cibernetică, asigurând cooperarea între părțile implicate.
De asemenea, nu orice fel de incidente de securitate din mediul online intră în atribuțiile CERT-RO. De exemplu, incidentele de securitate cibernetică care au rezultat în urma săvârşirii unor infracţiuni circumscrise criminalităţii informatice, sunt investigate de organele de aplicare a legii, conform competenţelor legale. De asemenea, incidentele de securitate cibernetică care se pot constitui în ameninţări la adresa securităţii naţionale sunt gestionate la nivelul instituţiilor cu competenţe în domeniul de referinţă, conform legii.

3. Scopul prezentului raport

Scopul raportului este de a prezenta o analiză a incidentelor de securitate cibernetică raportate la CERT-RO în perioada 01.01 – 30.06.2013 şi obţinerea unei viziuni de ansamblu asupra naturii şi dinamicii acestor tipuri de evenimente/incidente, relevante pentru evaluarea riscurilor de securitate cibernetică la adresa infrastructurilor IT şi de comunicaţii electronice de pe teritoriul naţional al României, aflate în aria de competență a CERT-RO.
În acest sens, pe baza datelor colectate, respectiv incidentele semnalate la CERT-RO de către diferite persoane fizice sau juridice, precum și alte date colectate din Internet de către specialiștii Centrului, prezentul document cuprinde principalele categorii de incidente ce au afectat spațiul cibernetic românesc în primele 6 luni ale anului 2013.
Pentru evaluarea conţinutului prezentului document, prezintă relevanţă faptul că la nivelul CERT-RO nu au ajuns toate datele referitoare la incidente de securitate cibernetică ce au afectat sau au implicat resurse ale spațiului cibernetic românesc, însă volumul de date analizat este reprezentativ pentru nivelul de dezvoltare al infrastructurilor cibernetice pe teritoriul României în prezent.
În principal valorile statistice ale prezentului raport reprezintă date referitoare la diferite resurse limitate (URL-uri, adrese IP), detectate în Internet ca efectuând trafic suspect sau malițios.
Pentru rigurozitate considerăm necesare lămuriri asupra termenilor folosiți. Astfel, pe parcursul documentului ne vom referi la următoarele:

- **Eveniment de securitate cibernetică** - orice fapt sau situație relevantă din punct de vedere al securității cibernetice, ce poate produce o schimbare a stării de normalitate în cadrul unui sistem informatic, poate indica o posibilă încălcare a politicii de securitate sau o eroare a măsurilor de protecție și poate fi pusă în evidență și documentată corespunzător;
- **Incident de securitate cibernetică** – eveniment survenit în spaţiul cibernetic a cărui consecinţe afectează securitatea cibernetică sau orice acțiune, contrară oricăror reglementări în vigoare, în legătură cu un sistem informatic, a cărei consecință poate afecta sau a afectat securitatea cibernetică a acestuia, sau a dus la compromiterea informațiilor procesate de acesta.
- **Alertă de securitate cibernetică** – orice semnalare a unui incident sau eveniment de securitate cibernetică ce implică, poate implica sau afectează entități de pe teritoriul României.

4. Despre sursele de date ale CERT-RO

CERT-RO colectează date despre incidente, evenimente sau alerte de securitate cibernetică, din mai multe tipuri de surse, respectiv:

1) ***Alerte colectate și transmise prin intermediul unor sisteme automate*** (ex: honeypots). Acest tip de alerte sunt transmise numai de către organizații specializate, precum alte CERT-uri sau companii de securitate, ce dețin sisteme de detecție a incidentelor de securitate cibernetică. Numărul acestora este semnificativ mai mare decât al altor tipuri de alerte, putând ajunge la valori de aprox. 500.000 alerte zilnice.
2) ***Alerte individuale***, transmise de diverse entități, persoane fizice sau juridice din țară sau străinătate, referitoare la anumite incidente de securitate cibernetică. Numărul acestui tip de alerte se ridică la aproximativ 5-10 alerte zilnice.
3) ***Informații colectate de către CERT-RO***, din diverse surse. În această categorie intră diverse informații colectate din surse publice sau cu acces reglementat (ex: site-uri de profil, companii de securitate etc.) referitoare la anumite vulnerabilități, amenințări sau chiar incidente de securitate cibernetică.

Natura alertelor primite precum și categoriile de date disponibile pentru fiecare din categorii, impun tratarea acestora diferit.

Alertele transmise prin sisteme automate impun procesarea automată. În acest caz, datele primite se rezumă la liste de IP-uri detectate cu activități malițioase sau suspecte în Internet, precum și câteva alte detalii referitoare la activitatea suspectă (ex: timestamp, tip incident, porturi folosite, ținte atacate etc.). Majoritatea acestor alerte sunt procesate automat de către CERT-RO și transmise către furnizorul de servicii Internet în reţeaua căruia funcţionează sistemul informatic identificat în cadrul alertei. În cazul acestui tip de alerte, de cele mai multe ori CERT-RO nu deține date reale despre utilizatorul real al adresei IP, identificarea acestuia căzând în sarcina furnizorului de servicii internet (ISP). Tot în sarcina ISP cade și transmiterea mai departe a alertei de securitate. Deși acest tip de alerte nu oferă detalii asupra tipologiei țintei, ele oferă o imagine de ansamblu asupra tipului de amenințări ce afectează infrastructurile cibernetice din România.

Alertele individuale precum și cele constituite pe baza informațiilor colectate de CERT-RO, sunt în număr considerabil mai mic, 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, de către analiștii CERT-RO, odată cu raportarea incidentului. Dată fiind natura lor, respectiv faptul că, de regulă, sunt evenimente deja petrecute care au produs potenţiale pagube, iar părțile implicate sunt clar identificabile, aceste tipuri de alerte reprezintă, în majoritatea cazurilor, incidente de securitate cibernetică. Astfel, din punct de vedere statistic, aceste tipuri de alerte sunt mult mai valoroase, reflectând mult mai bine evoluția stării de securitate cibernetică la nivel național.

5. Statistică pe baza alertelor primite

5.1. Alerte colectate și transmise prin intermediul unor sisteme automate

În perioada de referință, respectiv 01.01 – 30.06.2013, la CERT-RO au fost colectate date, astfel:

1. număr total de alerte automate primite: 17.511.109
2. număr total de IP unice extrase din totalul alertelor: 1.716.278

În funcție de conținutul fiecărei alerte, respectiv problema semnalată, acestea au fost împărțite pe clase și tipuri de alerte, conform tabelului 1.

5.1.1. Repartiția alertelor pe tipuri de incidente

Tabelul și graficul de mai jos redau repartiția alertelor primite, precum și a IP-urilor unice extrase din acestea, pe clase și tipuri de alerte. O parte din IP-urile unice raportate se regăsesc în mai multe categorii de alerte.

Clasa alerte	Tip Alertă	Număr alerte	IP-uri unice
Botnet	Botnet drone	15.577.697	1.546.472
Spam	Spam	1.797.158	456.270
Malware infected resource	Malicious URL	46.332	2.258
Scanners	Scanners	39.732	3.627
Open resources	Openresolver	33.165	28.035
Intrusion attempts	Bruteforce	8.439	47
Open resources	Open-proxy	4.931	191
Malware infected resource	Infected machine	1.704	264
Phishing	Phishing URL	1.669	276
Botnet	Botnet C&C	282	85
TOTAL		**17.511.109**	**2.037.525**

Tabel 1 – Repartiția alertelor pe tipuri de incidente

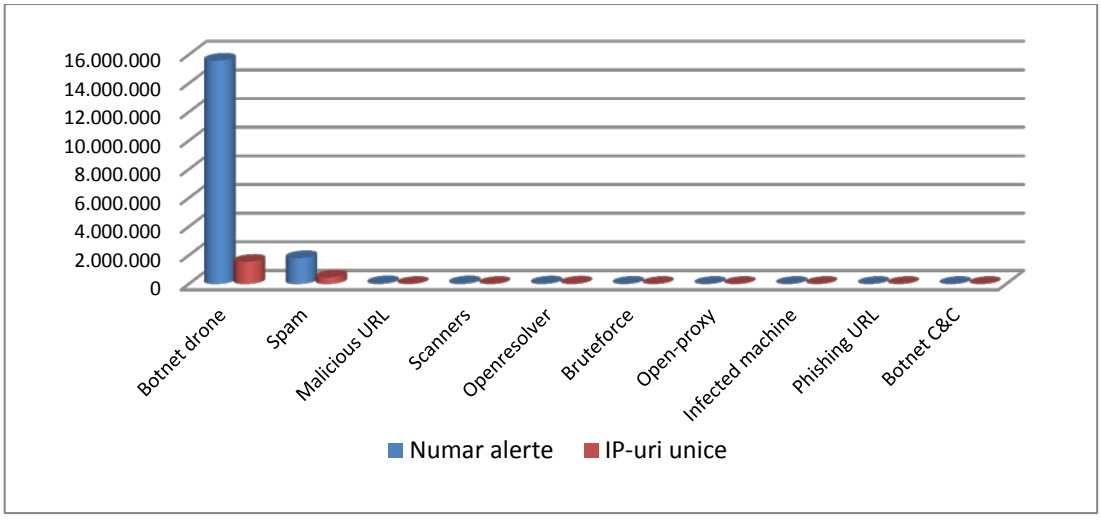

Fig. 1 – Repartiția alertelor pe tipuri de incidente

5.1.2. Repartiția alertelor pe Autonomous System Number (ASN)

În baza alertelor primite, acestea au fost repartizate pe ASN[2]-uri, după IP-ul conținut de fiecare alertă.
Astfel, alertele primite vizează 797 ASN-uri din România, dintr-un total de 1117 (conform http://bgp.he.net/country/RO). În tabelul și graficul următor sunt prezentați 20 de furnizori de servicii internet (ISP), în rețelele cărora au fost detectate IP-uri care generează trafic malițios, vizibil în internet (sortat după numărul de IP-uri compromise găzduite).

AS Name	ASN	Nr. alerte	Nr. IP-uri
RCS-RDS RCS & RDS SA	8708	6.850.688	878.117
RTD ROMTELECOM S.A	9050	5.307.494	569.852
LGI-UPC Liberty Global Operations B.V.	6830	1.608.905	93.863
ASEVERHOST S.C. Everhost S.R.L.	50915	62.121	31.549
DIALTELECOMRO Dial Telecom S.R.L.	6910	519.221	21.812
NG-AS SC NextGen Communications SRL	48161	475.030	17.754
ASN-ORANGE-ROMANIA Orange Romania SA	8953	203.936	8.441
SNR-RO S.N. Radiocomunicații S.A.	15471	46.380	5.640
VODAFONE_RO Vodafone Romania S.A.	12302	261.749	2.776
COSMOROM COSMOTE ROMANIAN MOBILE TELECOMMUNICATION SA	35725	65.258	2.048
MEDIASUD-AS SC MEDIA SUD SRL	50604	38.047	1.921
RO-TVSAT-AS TV SAT 2002 SRL	41496	70.985	1.597
ENIASAN-AS ENIASAN SRL	44563	44.222	1.551
NETVISION-AS Net Vision Telecom SRL	39737	39.381	1.483
DIGINET-AS DIGINET SA	34711	56.724	1.474
STARNETRANS-AS STARNETRANS SRL	47148	40.972	1.273
NEWCOM-ASN SC NextGen Communications SRL	35002	45.209	1.155
ELECTROSIM-AS Electrosim SRL	41273	42.373	1.119
ROEDUNET	2614	66.344	1.081
TTI-NET Euroweb Romania SA	6663	46.649	1.063

Tabel 2 – Top 20 ASN ce găzduiesc IP-uri malițioase

[2] Autonomous System Number, http://en.wikipedia.org/wiki/Autonomous_System_Number

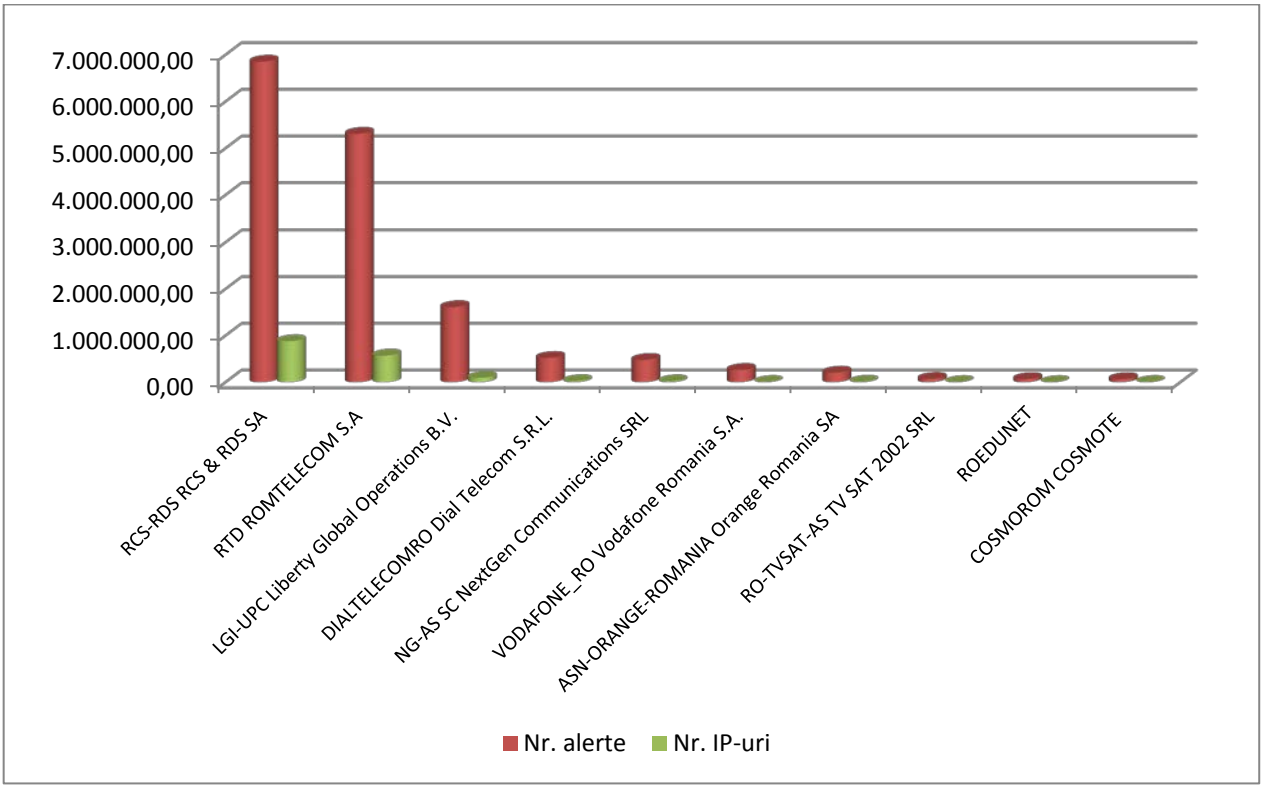

Fig. 2 – Top 20 ASN ce găzduiesc IP-uri malițioase

Notă: Prezența unui IP compromis/infectat în rețeaua unui ISP nu înseamnă că furnizorul de servicii internet (ISP) se face vinovat de respectivul incident. De cele mai multe ori, IP-ul infectat, care a generat alerta, reprezintă un client al respectivului furnizor de servicii internet, iar responsabilitatea asupra traficului generat, asupra dezinfectării precum și asupra securizării corespunzătoare a sistemului informatic revine în totalitate clientului.

5.1.3. Repartiția geografică a IP-urilor raportate

Pentru aproximativ 1.454.935 dintre IP-urile raportate am reușit identificarea locației geografice a acestora pe baza serviciului de geo-localizare oferit de MaxMind[3]. Astfel, în tabelul de mai jos regăsiți repartiția IP-urilor semnalate, pe regiuni sau orașe din România.

Nr. Crt.	Oraș/Regiune	Nr. IP-uri	Nr. Crt.	Oraș/Regiune	Nr. IP-uri	Nr. Crt.	Oraș/Regiune	Nr. IP-uri	Nr. Crt.	Oraș/Regiune	Nr. IP-uri
1	Bucuresti	288.366	51	Brebu	2.932	101	Ianca	709	151	Filipestii De Padure	107
2	Neidentificat	189.720	52	Pascani	2.704	102	Tecuci	704	152	Joseni	105
3	Iasi	62.274	53	Husi	2.665	103	Carei	676	153	Jilava	100
4	Constanta	59.227	54	Pantelimon	2.567	104	Dragasani	675	154	Lipanesti	92
5	Oradea	55.454	55	Turnu Magurele	2.472	105	Chiajna	665	155	Rosiorii De Vede	88
6	Timisoara	53.410	56	Otopeni	2.452	106	Moldova Noua	631	156	Barcanesti	86
7	Craiova	50.298	57	Gherla	2.428	107	Uricani	587	157	Buzias	79
8	Galati	46.912	58	Motru	2.293	108	Busteni	571	158	Moldovita	79
9	Brasov	46.135	59	Cernavoda	2.202	109	Orsova	542	159	Miercurea	69
10	Cluj-napoca	42.481	60	Fagaras	2.170	110	Buftea	540	160	Berceni	63
11	Sibiu	36.559	61	Aiud	2.038	111	Corabia	534	161	Piatra	60
12	Arad	33.605	62	Gheorghe Doja	2.032	112	Bals	505	162	Plopeni	60
13	Ploiesti	25.397	63	Panduri	2.032	113	Mizil	488	163	Utvin	59
14	Pitesti	25.136	64	Voluntari	2.021	114	Reghin	487	164	Odorheiul Secuiesc	55

[3] http://www.maxmind.com/en/home

15	Baia Mare	23.081	65	Giurgiu	1.961	115	Jimbolia	465	165	Brazi	53
16	Targu-mures	22.430	66	Panciu	1.949	116	Negresti-oas	462	166	Costesti	52
17	Bacau	21.504	67	Alba Iulia	1.907	117	Covasna	439	167	Ulmeni	52
18	Buzau	20.320	68	Matasari	1.881	118	Urlati	434	168	Mogosoaia	49
19	Satu Mare	16.442	69	Baicoi	1.766	119	Adjud	426	169	Cosbuc	48
20	Braila	13.557	70	Sighet	1.744	120	Tinca	405	170	Copalnic	42
21	Suceava	13.047	71	Mioveni	1.731	121	Victoria	386	171	Rahova	38
22	Focsani	12.823	72	Fetesti	1.661	122	Urziceni	371	172	Balan	34
23	Slatina	11.621	73	Avrig	1.657	123	Sacele	360	173	Ghencea	34
24	Turnu	11.316	74	Rosiori De Vede	1.617	124	Titu	356	174	Magura	33
25	Valcea	11.220	75	Cosoveni	1.603	125	Fieni	343	175	Scoala	33
26	Botosani	10.346	76	Capleni	1.594	126	Filiasi	327	176	Timis	30
27	Roman	9.156	77	Topoloveni	1.487	127	Alba	257	177	Siret	29
28	Resita	9.123	78	Vladimirescu	1.308	128	Odorheiu Secuiesc	257	178	Magurele	22
29	Deva	9.066	79	Traian	1.214	129	Nasaud	255	179	Stefanesti	21
30	Targoviste	8.910	80	Codlea	1.159	130	Dobroesti	253	180	Ferdinand	16
31	Cluj	8.623	81	Deta	1.151	131	Otelu Rosu	253	181	Popescu	16
32	Hunedoara	8.601	82	Mangalia	1.150	132	Peris	250	182	Ungheni	14
33	Vaslui	7.583	83	Tarnaveni	1.134	133	Rovinari	250	183	Bors	10
34	Balotesti	7.261	84	Simeria	1.104	134	Ludus	245	184	Dealul	9
35	Zalau	6.989	85	Bragadiru	1.093	135	Macin	242	185	Predeal	9
36	Onesti	6.890	86	Caransebes	1.057	136	Simleu Silvaniei	213	186	Florea	7
37	Bistrita	6.492	87	Sebes	1.050	137	Mihai Bravu	205	187	Rogoz	7
38	Caracal	6.402	88	Sovata	1.047	138	Blaj	200	188	Sabareni	7
39	Lugoj	6.255	89	Zimnicea	1.011	139	Snagov	198	189	Vitan	7
40	Miercurea-ciuc	6.246	90	Sighetu Marmatiei	967	140	Oancea	189	190	Harghita	5
41	Tulcea	5.966	91	Cavnic	946	141	Gheorgheni	182	191	Horezu	4
42	Alexandria	5.688	92	Moreni	928	142	Jibou	156	192	Iorga	3
43	Radauti	5.243	93	Biharia	909	143	Borca	149	193	Bratianu	2
44	Medias	5.196	94	Slobozia	895	144	Borsa	130	194	Banca	1
45	Calarasi	4.979	95	Bocsa	850	145	Bucurestii Noi	130	195	Dimitrie Cantemir	1
46	Piatra Neamt	4.757	96	Toplita	810	146	Baiut	129	196	Domnesti	1
47	Oltenita	4.386	97	Corbeanca	806	147	Oravita	124	197	Lazar	1
48	Turda	4.125	98	Curtea De Arges	782	148	Iernut	122	198	Ripiceni	1
49	Afumati	3.324	99	Moinesti	741	149	Baciu	118	199	Rosia	1
50	Falticeni	3.072	100	Strejnicu	741	150	Cristuru Secuiesc	113	200		

Table 3 – Repartiție geografică IP-uri cu trafic suspect

5.1.4. Statistică domenii ”.ro” compromise

Alertele primite deseori se referă la domenii ”.ro” afectate de diverse tipuri de incidente.
Astfel, pentru perioada de referință, CERT-RO deține date referitoare la 5.678 domenii compromise.
Din 691.419[4] domenii înregistrate în România, în luna august 2013, numărul reprezintă mai puțin de 1% din totalul domeniilor ”.ro”.
Repartiția domeniilor afectate, după tipul de incident, se regăsește în tabelul de mai jos.

[4] Conform datelor ICI-ROTLD

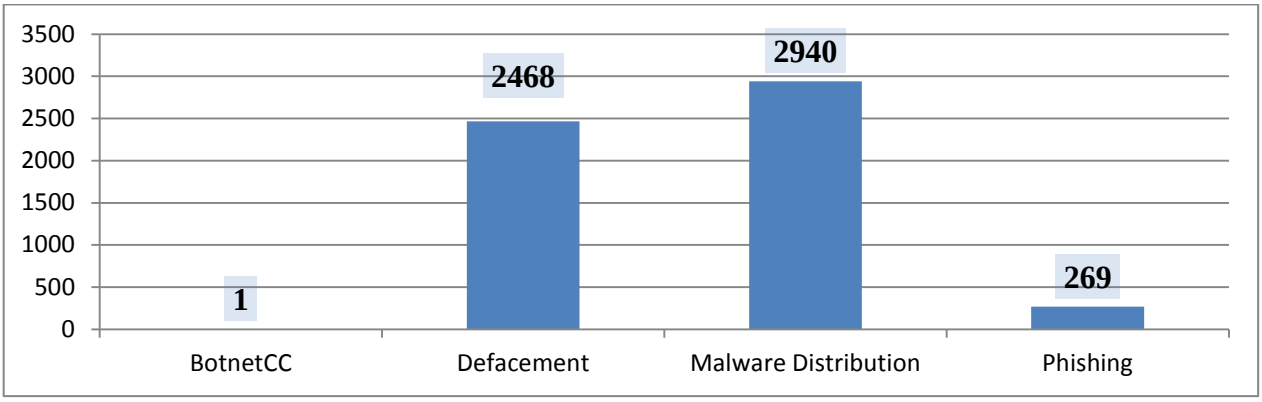

Fig. 3 – Domenii .ro compromise

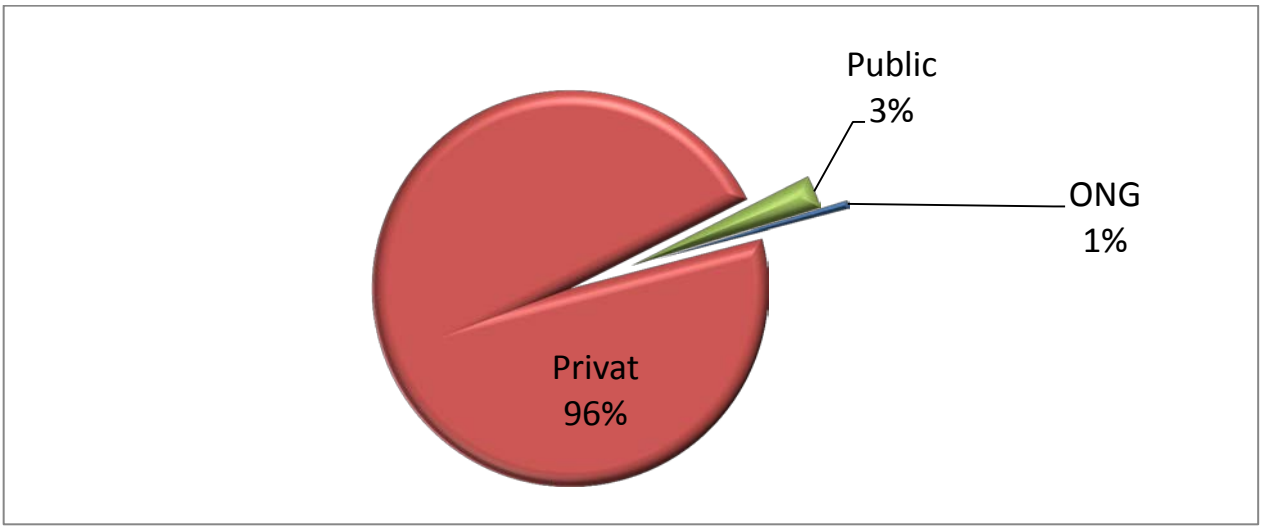

Fig. 4 – Domenii .ro – distribuție după tipul entității afectate

5.2. Alerte individuale

În perioada de referință, analiștii CERT-RO au preluat o serie de incidente de securitate cibernetică, raportate direct de către persoane sau organizații din țară sau străinătate, astfel:

Clasa alerte	Tip Alertă	Număr incidente
Phishing	Phishing URL	87
Malware infected resource	Infected machine	13
Malware infected resource	Malicious URL	9
Scanners	Scanners	7
Botnet	Botnet drone	6
Other unlawful activities	Other incidents	5
Other unlawful activities	Scam	5
Spam	Spam	3
Denial of Service	Distributed Denial of service	2
Other unlawful activities	Vulnerable systems (data leakage)	2
APT	MiniDuke	1
TOTAL		**140**

Tabel 4 – Statistică alerte individuale

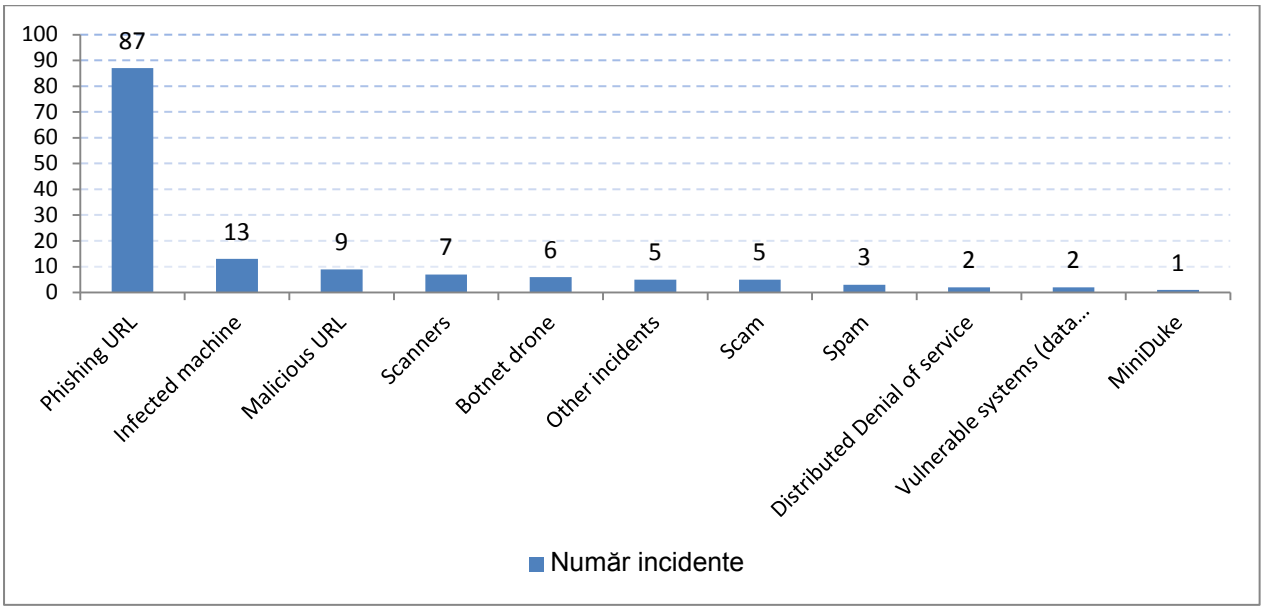

Fig. 5 – Statistică alerte individuale

În funcție de tipul entității afectate repartiția incidentelor este cea din graficul de mai jos. De menționat este faptul că entitățile afectate nu reprezintă neapărat persoane fizice sau juridice din România.

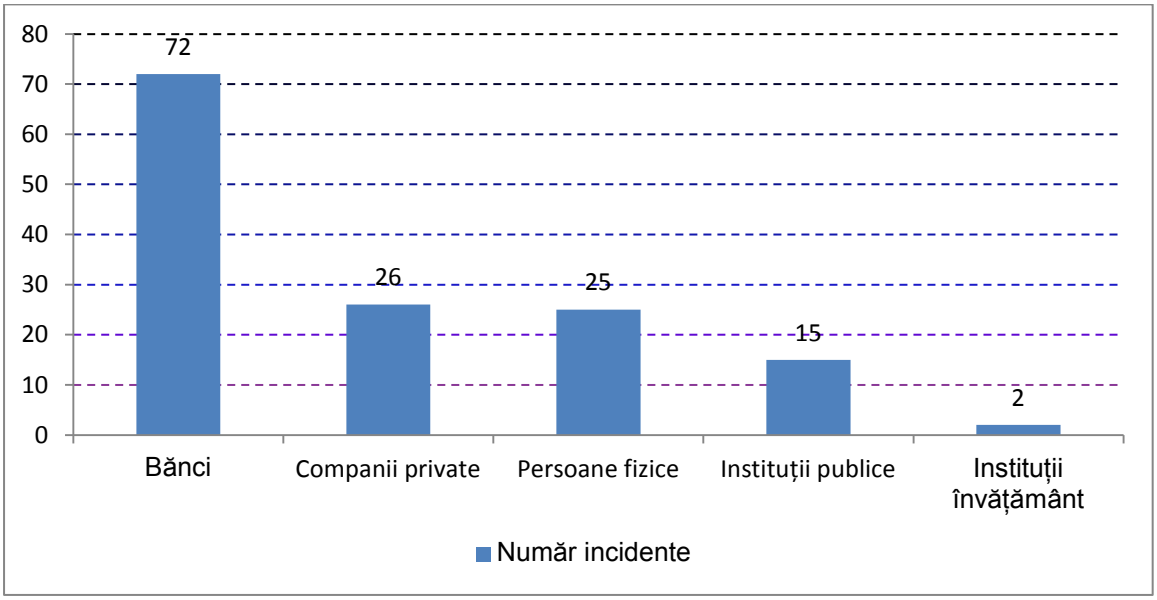

Fig. 6 – Repartiție incidente pe entități afectate

De asemenea, în funcție de tipul sistemului afectat, repartiția incidentelor de securitate este următoarea:

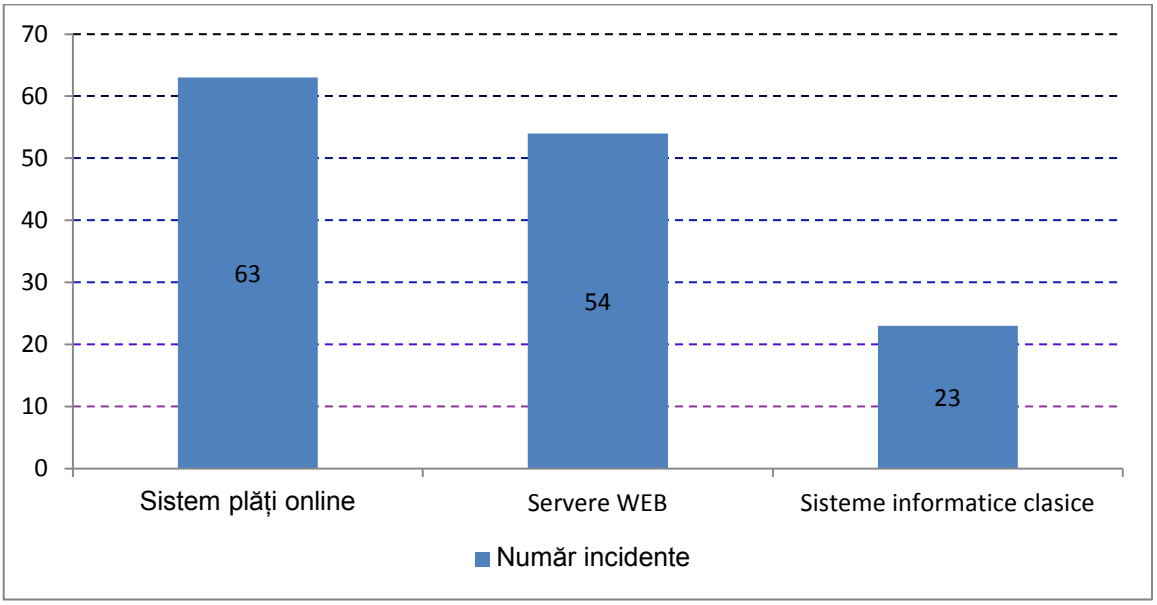

Fig. 7 – Repartiție incidente pe tipuri de sisteme afectate

5.3. Amenințări de tip Advanced Persistent Threath (APT)[5]

În data de 25.02.2013 CERT-RO a primit o notificare asupra unei noi amenințări cibernetice denumită ”MiniDuke”, ce face parte din categoria APT-urilor cu grad ridicat de risc, specializat în extragerea de informații în format electronic de pe sistemele informatice ţintă, fiind vizate entităţi din cadrul ”structurilor guvernamentale și instituțiilor de cercetare”[6]. Virusul asociat amenințării exploata o vulnerabilitate a aplicației Adobe Reader, se propaga prin email, cu ajutorul unor tehnici speciale de inginerie socială, copiind fișiere pe care ulterior le transmitea către atacator. În România au fost detectate 6 victime infectate, iar pentru remedierea situației s-a colaborat cu alte autorități cu competențe legale din România.
Atacuri de tip APT au fost identificate și in cursul anului trecut (ROCRA) și au vizat de asemenea structuri guvernamentale sau ambasade din România.

[5] Advanced Persistent Threat
[6] http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_MiniDuke_a_New_Malicious_Program_Designed_for_Spying_on_Multiple_Government_Entities_and_Institutions_Across_the_World

6. Concluzii și comentarii

Din analiza datelor deţinute la nivelul CERT-RO, rezultă faptul că ameninţările, de natură informatică, asupra spațiului cibernetic național s-au diversificat, fiind relevate tendinţe evolutive, atât din perspectivă cantitativă, cât şi din punct de vedere al complexităţii tehnice evidenţiate.

Majoritatea incidentelor analizate de CERT-RO, fie că provin din segmentul alertelor automate sau a celor individuale, se referă la entități din România, victime ale unor atacatori care, de regulă prin exploatarea unor vulnerabilităţi tehnice, au vizat infectarea unor sisteme informatice cu diverse tipuri de aplicaţii malware, în scopul constituirii unor reţele rețele de tip botnet (zombie). Rețelele de tip botnet sunt folosite pentru lansarea de atacuri asupra altor sisteme informatice, ascunzând identitatea reală a atacatorului. În acest fel, conform statisticilor prezentate în raport, cele 1.546.472 IP-uri naționale folosite de către diverși atacatori în scopuri malițioase, cele câteva mii de URL-uri infectate sau serverele slab securizate ce pot oricând să fie folosite de persoane neautorizate, nu fac decât să susţină afirmațiile potrivit cărora România este exportatoare de malware sau trafic maliţios la nivelul rețelei mondiale Internet, fapt semnalat de nenumărate studii publicate de diverse companii de securitate.

Analizând numărul total de IP-uri unice semnalate (1.716.278), în raport cu numărul total de IP-uri alocat României (aprox. 13,5 mil), rezultă că un procent de peste 12,5% din numărul de IP-uri alocate României sunt infectate cu diverse variante de malware, majoritatea sistemelor informatice fiind deținute de utilizatori persoane fizice (home user). Conform ultimului raport asupra României al Business Software Alliance[7], rata pirateriei informatice în România, la nivelul anului 2011, a fost de aprox. 63%. Software-ul piratat, deseori descărcat de pe site-uri tip torrent sau hub-uri de DC, conține de cele mai multe ori cod maliţios ascuns (rootkits, backdoors etc.) ce poate transforma computerul într-un ”zombie” controlat de către atacator. Practic utilizatorul se bucură de folosirea unui software, care pe lângă funcționalitățile legitime, are și o serie de funcționalități adiționale folosite strict de către atacator în scopuri de el știute.

Astfel, prin victimele din România, folosite ca proxy, sunt desfăşurate atacuri asupra unor ţinte din afara ţării, identitatea reală a atacatorului rămânând ascunsă.
În acest context, România nu mai poate fi considerată doar o ţară generatoare de incidente de securitate cibernetică, analiza datelor prezentate demonstrând caracterul intermediar/de tranzit al unor resurse informatice semnificative conectate la reţeaua Internet în România.

Printre dificultățile întâmpinate în activitatea de răspuns la incidente de securitate cibernetică, putem menționa lipsa prevederilor legale exprese referitoare la responsabilitățile legate de notificarea, răspunsul, combaterea și eliminarea efectelor incidentelor de securitate de către autoritățile statului sau entitățile din domeniul privat, ceea ce duce la îngreunarea activităților de răspuns în timp real la astfel de incidente. În acest context, considerăm necesară completarea cadrului normativ național cu prevederile conținute de unele documentele existente la nivel European.

[7] Business Software Alliance, 2011 Global Software Piracy Study, 2012,disponibil la: http://globalstudy.bsa.org/2011/downloads/opinionsurvey/survey_romania_ro.pdf.

Anexa 1 – Termeni și definiții

Clasa alerte	Tip Alertă	Definire
APT	MiniDuke	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). MiniDuke este un tip de amenințare APT.
Botnet	Botnet C&C	Sisteme informatice utilizate pentru controlul victimelor (drone, zombie) din cadrul unei rețele de tip botnet.
Botnet	Botnet drone	Rețea de sisteme informatice infectate controlate de alte persoane/organizații decât deținătorii acestora.
Denial of Service	Distributed Denial of service	Afectarea disponibilității unor sisteme/servicii informatice sau de comunicații 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.
Intrusion attempts	Brute force	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.
Malware infected resource	Infected machine	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.
Malware infected resource	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.
Open resources	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 resources	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.
Other unlawful activities	Other incidents	Alte activități ilegale derulate în mediul online (pornografie infantilă, comerț electronic ilegal etc.).
Other unlawful activities	Scam	Diverse scheme de afaceri frauduleute în mediul online.
Other unlawful activities	Vulnerable systems (data leakage)	Diverse incidente de securitate ce au ca efect afectarea confidențialității unor date sensibile sau

		accesarea acestora de persoane neautorizate.
Phishing	Phishing URL	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.
Scanners	Scanners	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.
Spam	Spam	Comunicări electronice (mail) nesolicitate cu caracter comercial.
Website hacking	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.

Notă: Tabelul de mai sus conține majoritatea alertelor 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 noi. Am preferat menținerea denumirilor în limba engleză a claselor și tipurilor de alerte pentru a nu pierde sensul anumitor categorii prin traducere în limba română.