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

RAPORT
cu privire la alertele de securitate cibernetică primite de CERT-RO în cursul anului 2013

Pagină albă

CUPRINS

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 01.01 – 31.12.2013, 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: **43.231.149**
    - număr total de IP unice compromise, extrase din totalul alertelor: **2.213.426**
2. Alertele colectate manual prin notificări individuale precum și cele constituite pe baza informațiilor colectate de CERT-RO: **450**.

Obiectivul prezentului raport este analiza incidentelor de securitate cibernetică colectate/gestionate la nivelul CERT-RO în anul 2013 în vederea obţinerii 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 României, aflate în aria de competență a CERT-RO.

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

- peste 16% din totalul numărului de IP-uri alocat României (aprox. 13,5 mil), a fost implicat în cel puțin o alertă de securitate cibernetică raportată la CERT-RO în anul 2013;
- aproximativ 78% din alerte vizează sisteme informatice din România, victime ale unor atacatori care, de regulă prin exploatarea unor vulnerabilităţi tehnice, au vizat infectarea sistemelor cu diverse tipuri de aplicaţii malware, în scopul constituirii unor reţele de tip botnet (zombie); Numărul total de IP-uri unice identificate, în baza acestor alerte, este de 1.945.597, respectiv 14% din plaja totală de IP-uri alocate României.
- peste 16% din alerte vizează sisteme informatice din România, victime ale unor atacatori care, de regulă prin exploatarea unor configurări defectuoase sau vulnerabilități ale serverelor DNS, au vizat folosirea sistemelor informatice vulnerabile pentru lansarea unor atacuri asupra altor ținte din Internet (DNS amplification attacks, DNS cache poisoning etc.);
- peste 5% din alerte vizează entități din România ce trimit mesaje email nesolicitate de tip spam, către diverse ținte din rețeaua Internet;
- 40% din totalul alertelor vizează sisteme informatice din România infectate cu viermele Conficker, pentru care există deja patch-uri de securitate sau mecanisme de dezinfecție; conform datelor deținute aprox. 12,5% din IP-urile unice din RO, au fost raportate în 2013 ca fiind infectate cu Conficker. Troianul, identificat în anul 2008, vizează sisteme informatice ce rulează sisteme de operare din familia Microsoft Windows, ce nu au instalate ultimele patch-uri de securitate;
- peste 50% din totalul IP-urilor unice raportate rulează sisteme de operare din familia Microsoft Windows, versiunile 98, 2000, XP sau 2003;
- peste 39% din totalul alertelor individuale (5.2) vizează entități din România ce găzduiesc pagini web de tip phishing, ce afectează activitatea unor instituții financiare din România sau străinătate;

- 10.239 domenii .ro au fost compromise în 2013, reprezentând aprox. 1,4% din totalul domeniilor .ro; 60% dintre acestea sunt domenii infectate cu diverse variante de malware, ce pot infecta alți vizitatori;
- 61 de IP-uri au fost semnalate ca fiind infectate cu diverse variante de malware de tip APT.

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

- 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 sistemelor informatice compromise din România, fac parte din rețele de tip ”botnet”, fiind folosite cu rol de „proxy” pentru desfășurarea altor atacuri asupra unor ținte din afara țării, reprezentând astfel potentiale amenințări la adresa altor sisteme conectate la Internet;
- pe baza analizei tipurilor de malware specifice spațiului cibernetic național precum și a tipurilor de sisteme compromise, reiese faptul că, din punct de vedere cantitativ, majoritatea atacurilor sunt îndreptate către sisteme învechite, depășite moral, fără posibilități native de securizare (ex: sisteme afectate de Conficker) sau care nu sunt actualizate cu ultimele patch-uri/update-uri de securitate;
- entități din România devin din ce în ce mai frecvent ținta amenințărilor de tip APT, respectiv 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); având în vedere functiile complexe ale unor astfel de aplicații malware, prezente într-un număr mai redus în perioada analizata (capabilități de interceptare a comunicatiilor electronice, accesarea neautorizata a datelor aferente tranzactiilor financiare si mijloacelor de plata electronice, spionaj cibernetic etc. Ex: Red October, Miniduke), precum și faptul ca aceste tipuri de amenințări prezintă un caracter evolutiv moderat, se poate estima o crestere a numărului și severității unor astfel de atacuri la nivel national pe parcursul anului 2014;
- 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.

Recomandări:

- O serie de recomandări, atât pentru administratorii de sistem din cadrul organizațiilor cât și pentru utilizatorii casnici, se regăsesc în anexele 1 și 2.

2. Despre CERT-RO?

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*** 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 național, 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 Ministerul Societății Informaționale (MSINF) sau Consiliului Suprem de Apărare a Ţării, 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 nou-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 minimum posibil a efectelor incidentului;
2. stabilirea preliminară a impactului incidentului/evenimentului;

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

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;
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.

Conform atribuţiilor legale, CERT-RO asigură cadrul organizatoric şi suportul tehnic necesar schimbului de informaţii dintre diverse entități (autorități, persoane fizice sau juridice, echipe de tip CERT, furnizori de soluții de securitate, furnizori de servicii etc.) implicate în incidente de securitate cibernetică, asigurând buna cooperare a acestora.
De asemenea, CERT-RO nu are atribuții în soluționarea tuturor tipurilor de incidente de securitate cibernetică. De exemplu, soluționarea incidentelor de securitate cibernetică care au rezultat în urma săvârşirii unor infracţiuni circumscrise criminalităţii informatice, revin în sarcina organelor 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. În cazul în care CERT-RO primește astfel de notificări, acestea sunt transmise instituțiilor competente.

3. Obiectivul prezentului raport

Obiectivul raportului este de a analiza incidentele de securitate cibernetică raportate la CERT-RO în perioada 01.01 – 31.12.2013 în vederea obţinerii 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 anul 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 poate fi considerat 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 în activitatea CERT-RO. 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 ale 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 sau poate implica entități de pe teritoriul României.

4. 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, precum site-uri de profil sau companii de securitate, 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 exacte 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. Sistemul de Alertă Timpurie (SAT) al CERT-RO

În cadrul CERT-RO funcționează un proiect pilot al Sistemul de Alertă Timpurie și Informare în Timp Real (SAT) privind incidentele cibernetice, respectiv un ansamblu proceduri și sisteme informatice ce procesează toate alertele primite, în vederea avertizării în timp real a părților afectate (ISP, persoane fizice sau juridice direct afectate etc.), a emiterii de rapoarte cu privire la distribuţia şi natura incidentelor precum și a colaborării cu autorităţile naţionale responsabile în asigurarea securităţii cibernetice, în vederea prevenirii şi înlăturării efectelor incidentelor. Prezentul raport a fost redactat pe baza alertelor procesate pe parcursul anului 2013 de SAT al CERT-RO.
În contextul analizei modului de implementare al Strategiei Naționale de Securitate Cibernetică, așa cum s-a prezentat și în ultimul bilanț al Consiliului Operativ de Securitate Cibernetică, un pas important în operaționalizarea Sistemului Național de Securitate Cibernetică l-a constituit dezvoltarea de către CERT-RO a sistemului pilot al Sistemului de Alertă Timpurie (SAT). În perioada următoare, CERT-RO cu sprijinul celorlalte instituţii cu responsabilităţi în domeniul securităţii cibernetice, va dezvolta proiectul pilot de SAT, astfel încât, odată cu identificarea surselor financiare necesare, **acesta să fie extins în cât mai multe entităţi, în special în mediul privat**.

6. Statistică pe baza alertelor primite

6.1. Alerte colectate și transmise prin intermediul unor sisteme automate

În perioada de referință, respectiv 01.01 – 31.12.2013, la CERT-RO au fost primite sesizări (alerte), astfel:

1. **număr total de alerte automate primite: 43.231.149**
2. **număr total de IP unice extrase din totalul alertelor: 2.213.426**

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

6.1.1. Distribuția alertelor pe tipuri și clase de incidente

Tabelul și graficul de mai jos redau distribuția 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[2]	Număr alerte
Botnet	**Botnet Drone**	33.677.871
Vulnerabilities	**Open Resolver**	6.782.888
Abusive Content	**Spam**	1.986.605
Information Gathering	**Scanner**	603.524
Malware	**Malicious URL**	116.535
Cyber Attacks	**Bruteforce**	30.150
Vulnerabilities	**Open Proxy**	13.809
Fraud	**Phishing**	13.556
Botnet	**Botnet C&C Server**	4.082
Malware	**Infected IP**	1840
APT	**RedOctober**	287
Compromised Resources	**Compromised Router**	2
	TOTAL	**43.231.149**

Tabel 1 – Distribuția alertelor pe tipuri

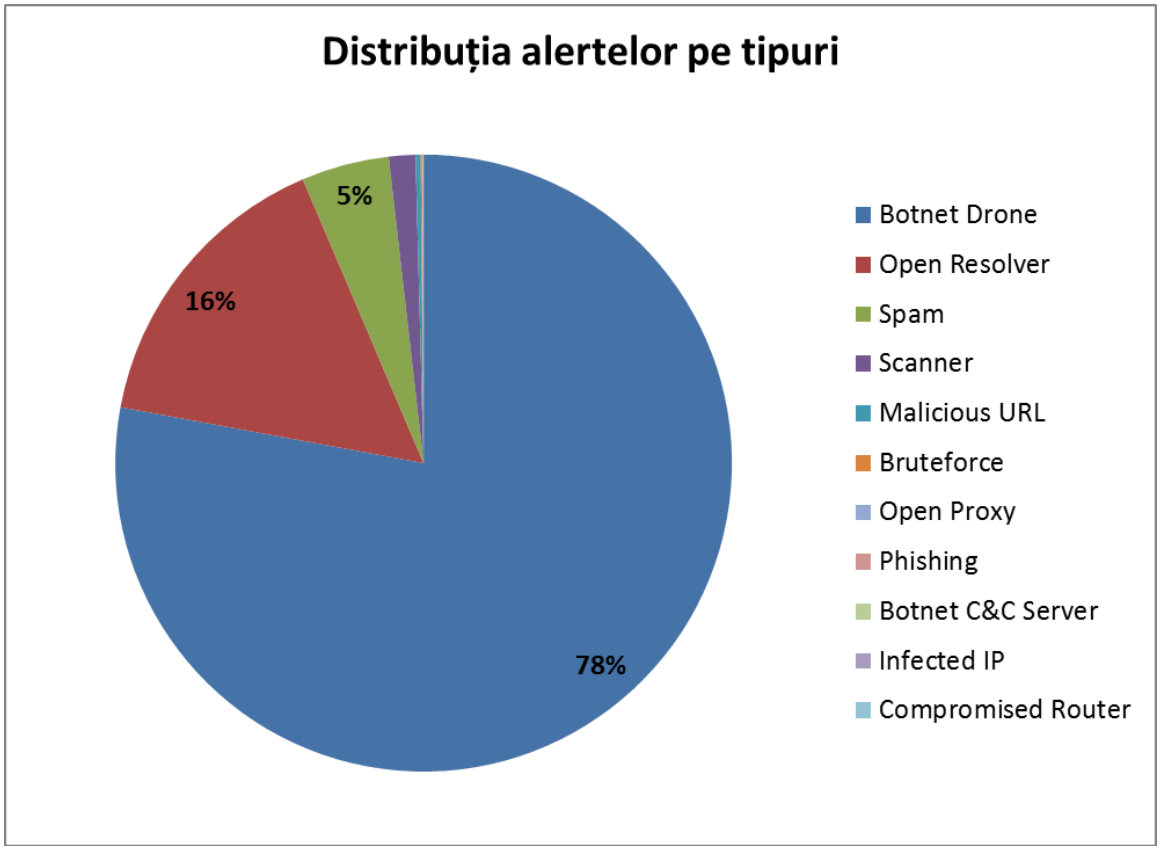

Fig. 1 – Distribuția alertelor pe tipuri

Alertele din categoria ”Botnet Drone”, respectiv computere infectate cu diverse tipuri de malware, ce fac parte din diverse rețele de tip botnet, predomină, în proporție de **78%, în totalul alertelor automate primite în anul 2013**. Numărul total de IP-uri unice identificate în baza acestor alerte este de 1.945.597, respectiv **14% din plaja totală de IP-uri alocate României**.

[2] Explicația claselor și a tipurilor de alerte se regăsește în anexa nr. 3.

6.1.2. Distribuția alertelor pe luni calendaristice

Graficul de mai jos reprezintă distribuția alertelor, în funcție de luna calendaristică în care acestea au fost primite de CERT-RO.

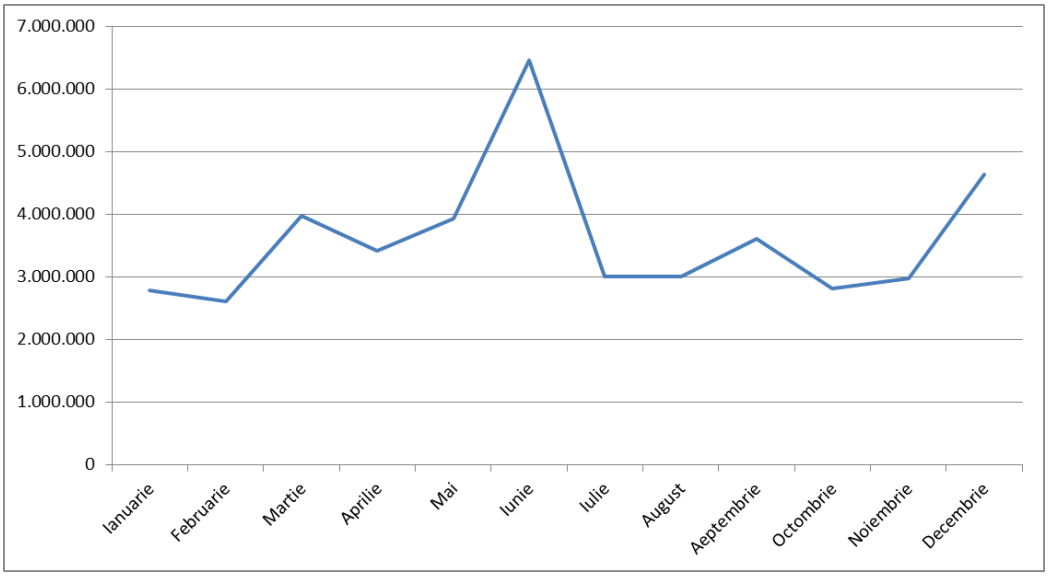

Fig. 2 – Distribuția alertelor pe luni calendaristice

6.1.3. Distribuția alertelor pe Autonomous System Number (ASN)

În baza alertelor primite, acestea au fost repartizate pe ASN[3]-uri, după IP-ul conținut de fiecare alertă. Astfel, alertele primite vizează 1148 ASN-uri din România, acest număr acoperind toate ASN-urile din România (http://bgp.he.net/country/RO). În tabelul și graficul următor sunt prezentați primii 30 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). În general, un ISP are alocat unul sau mai multe ASN-uri.

Nr.	AS NUMBER	AS NAME	Procent (%)
1	8708	RCS & RDS SA	35,96
2	9050	ROMTELECOM	32,27
3	6830	UPC	7,88
4	6910	DIAL TELECOM S.R.L	3,46
5	48161	SC NextGen Communications SRL	2,68
6	12632	RCS & RDS SA	2,27
7	12302	Vodafone Romania S.A.	1,36
8	8953	Orange Romania SA	1,17

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

9	2614	RoEduNet	0,45
10	35725	COSMOTE ROMANIAN MOBILE TELECOMMUNICATION SA	0,33
11	34711	DIGINET SA	0,31
12	41496	TV SAT 2002 SRL	0,29
13	39743	Voxility S.R.L.	0,25
14	6663	Euroweb Romania SA	0,24
15	39737	Net Vision Telecom SRL	0,24
16	44563	ENIASAN SRL	0,24
17	15471	S.N. Radiocomunicatii S.A.	0,22
18	50604	SC MEDIA SUD SRL	0,22
19	41273	Electrosim SRL	0,22
20	47148	STARNETRANS SRL	0,22
21	41571	Transilvania Digital Network SA	0,21
22	35002	SC NextGen Communications SRL	0,20
23	51102	IMPATT SRL	0,20
24	39543	TENNET TELECOM SRL	0,18
25	31605	Canal S SRL	0,18
26	40997	TITA & Company SRL	0,17
27	35664	CCC Blue Telecom SA	0,17
28	31102	TV Adler-Trading SRL	0,17
29	39464	Star Design I&E SRL	0,15
30	44605	TeleCablu&Net Srl	0,15
		Altii	7,96

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

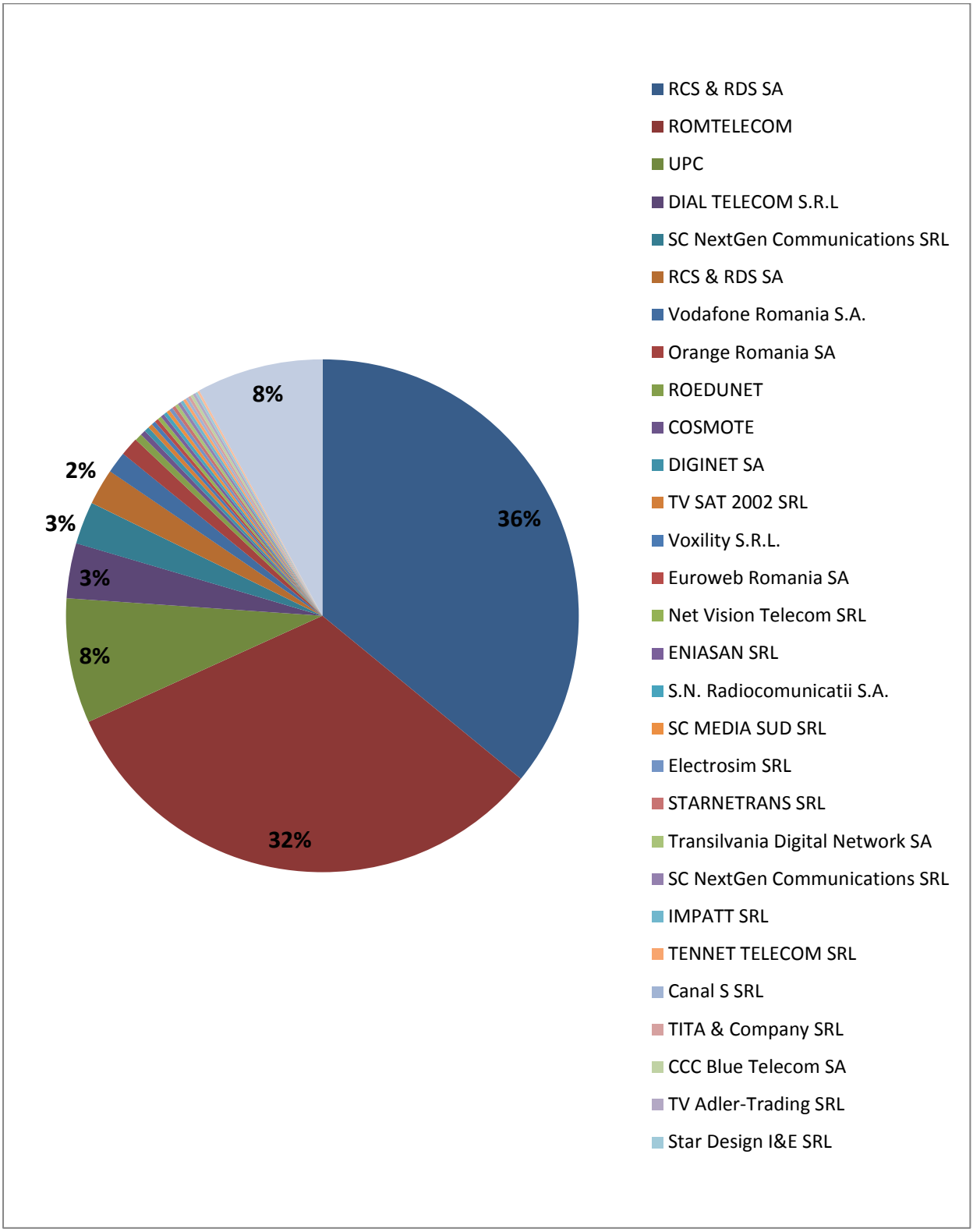

Fig. 3 – Top 30 ASN ce găzduiesc IP-uri malițioase

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, (conform art. 13 din Legea 365/2002 precum și a altor acte normative din domeniu). asupra dezinfectării precum și asupra securizării corespunzătoare a sistemului informatic revine clientului.

6.1.4. Tipuri de malware caracteristice spațiului cibernetic românesc

În aproximativ 75% din alertele primite, a fost posibilă identificarea tipului de malware ce a afectat sistemul compromis. În acest sens, a fost întocmit un ”Top 25” al celor mai întâlnite tipuri de malware din spațiul cibernetic românesc.

Nr. Crt.	Tip Malware	Procent (%)
1	Conficker	53,4543
2	Sality	10,9534
3	Citadel	8,2338
4	Pushdo	6,7392
5	Zeroaccess	3,1662
6	Slenfbot.5050	3,0855
7	Virut	1,5755
8	Kelihos	1,3314
9	IRCBot	0,9238
10	Zeus	0,5706
11	Trafficconverter	0,3484
12	Grum	0,1508
13	Torpig	0,0252
14	Ransomware	0,0199
15	Blackenergy	0,0127
16	Tdss	0,0075
17	Trojan.Iframe.BMY	0,0045
18	Neurevt	0,0038
19	Trojan.Script.CEV	0,0031
20	Hermes	0,0025
21	Dorkbot	0,0024
22	DDoS_Khan	0,0023
23	DDoS_DirtJumper	0,0022
24	Gamarue	0,0017
25	Trojan.Iframe.BZW	0,0016

Tabel 3 – Top 25 tipuri de malware România 2013[4]

Potrivit Wikipedia.org, „Conficker” (cunoscut şi sub numele de Downadup) este un vierme apărut în 2008, ce exploatează vulnerabilități ale sistemelor de operare Microsoft. Viermele ataca numai sisteme de calcul cu sistem de operare Windows şi se folosea de anumite vulnerabilităţi ale acestuia precum şi de atacuri de tip „dicţionar” pentru aflarea parolelor de administrator. Scopul este obţinerea controlului asupra calculatorului infectat, acesta putând fi ulterior controlat de la distanţă. Conform datelor deținute 1.693.323 IP-uri unice (76% din totalul IP-urilor raportate sau 12,5% din totalul IP-urilor unice din RO) din RO sunt infectate cu acest vierme.

[4] Explicații referitoare la cele 25 de tipuri de malware se regăsesc în anexa nr. 4

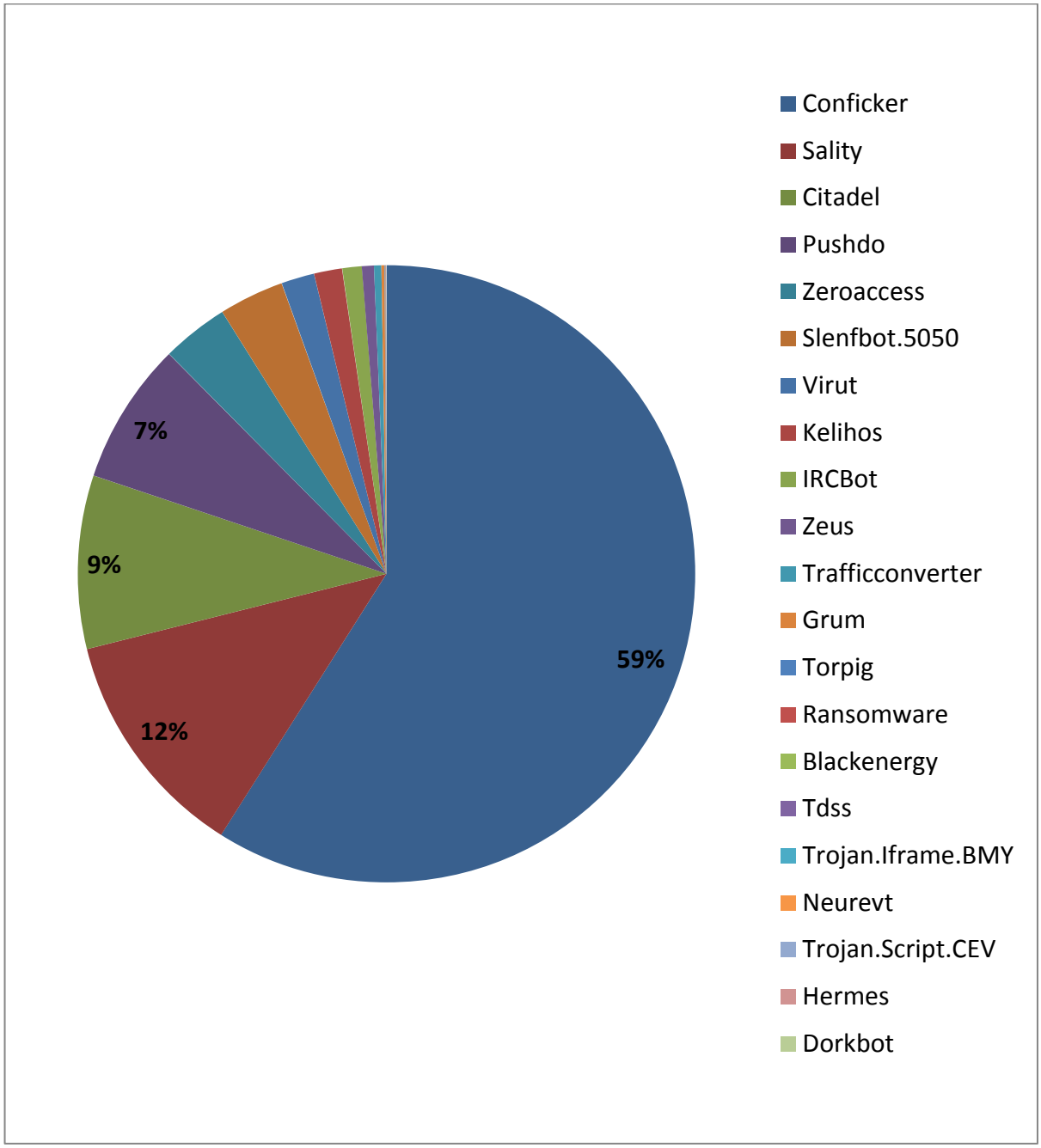

Fig 4 – Top 25 tipuri de malware România 2013

6.1.5. Tipuri de sisteme afectate de alerte

În aproximativ 11% din alertele primite a fost posibilă identificarea cu exactitate a tipului de sistem de operare al clientului afectat. În acest sens, tabelul de mai jos, redă un clasament al celor mai afectate tipuri de sisteme de operare din RO.

Nr. Crt.	Familie sistem operare	Nr. total alerte
1	Windows	**4.344.677**
2	Solaris	**55.524**
3	Linux	**8.532**
4	ChacheFlow	**698**
5	FreeBSD	**95**
6	OpenBSD	**69**
7	NetBSD	**61**
8	Novell	**25**
9	Cisco	**23**
10	Checkpoint	**9**
TOTAL		**4.409.713**

Tabel 4 – Repartiție nr. de alerte totale per tipuri de sisteme de operare afectate

Conform datelor raportate la CERT-RO, majoritatea sistemelor de tip Windows infectate rulează versiunile 98/XP/2000/2003. O parte dintre aceste versiuni nu mai beneficiază de suport din partea producătorului, fiind declarate ca ”end of life”, iar alte versiuni urmează a nu mai beneficia de suport în viitorul apropiat. Aceste versiuni de sisteme de operare Windows rulează pe aprox. 50% din totalul IP-urilor unice raportate la CERT-RO.

6.2. Alerte individuale

Alături de alertele automate, 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 alerte
Fraud	**Phishing**	173
Malware	**Infected IP**	95
Information Gathering	**Scanner**	43
Cyber Attacks	**DDoS**	42
Malware	**Malicious URL**	31
Abusive Content	**Spam**	11
Botnet	**Botnet Drone**	11
Compromised Resources	**Compromised Website**	7
Cyber Attacks	**Exploit Attempt**	7
Compromised Resources	**Defacement**	6
Compromised Resources	**Compromised Network/System**	4

Abusive Content	**Disclosure of Confidential Data**	3
Fraud	**Unlawful eCommerce/Services**	3
Other	**Alte tipuri**	3
Abusive Content	**Disclosure of Personal Data**	2
Botnet	**Botnet C&C Server**	2
Compromised Resources	**Comprimised Application/Service**	2
Cyber Attacks	**APT**	2
Abusive Content	**Child Pornography**	1
Cyber Attacks	**Bruteforce**	1
Information Gathering	**Social Engineering**	1
	TOTAL	**450**

Tabel 5 – Distribuție alerte individuale per tipuri

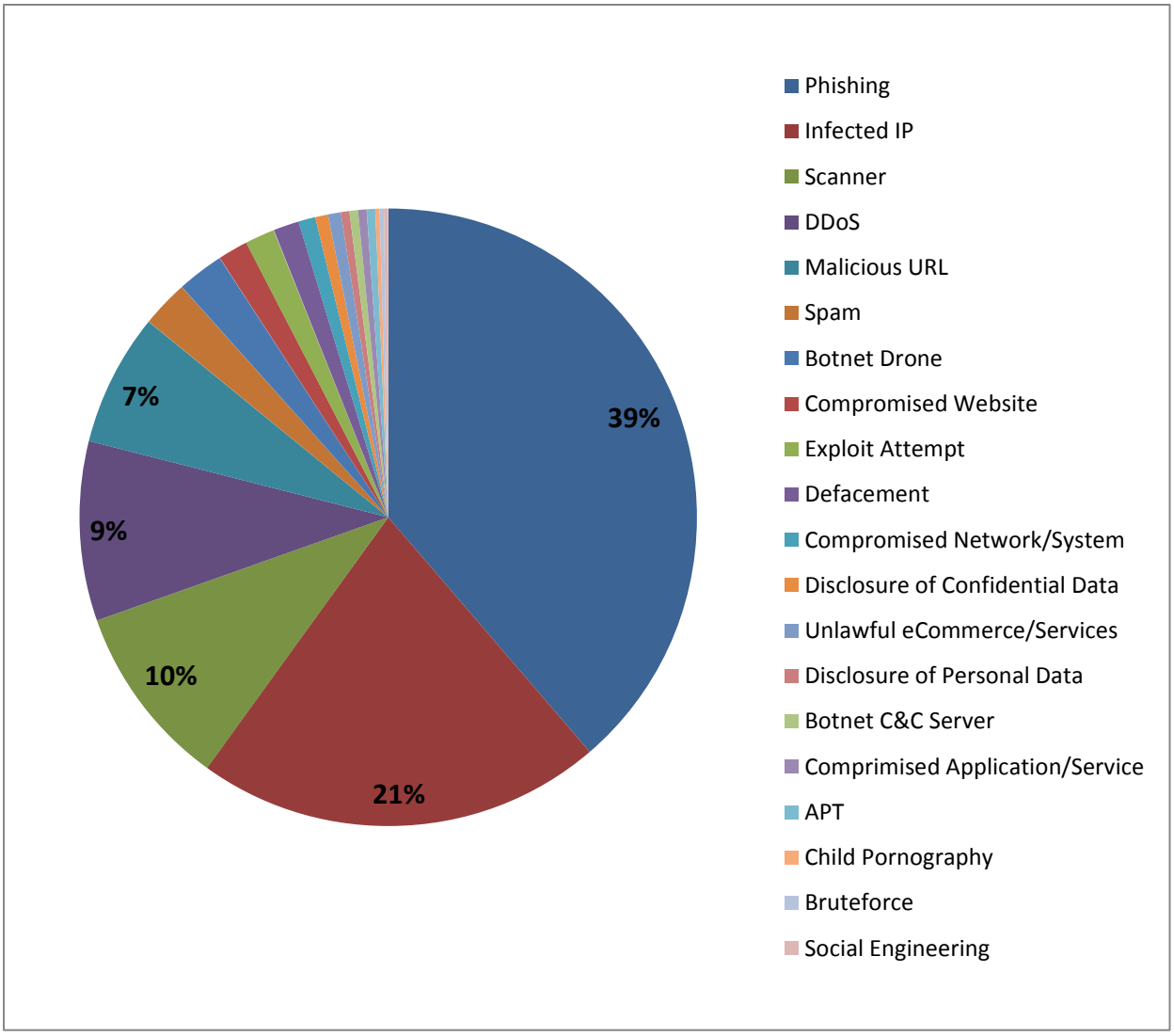

Fig. 5 – Distribuție alerte individuale per tipuri

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

Nr. Crt.	Tipul entităţii afectate	Nr. alerte
1	Instituţii bancare	142
2	Organizaţii private	80
3	Instituţii de învăţământ	29
4	Instituţii publice	18
5	Persoane fizice	17
6	ISP	5
7	Agenții de tip ”law enforcement”	1
8	Neprecizat	158
TOTAL		**450**

Fig. 6 – Repartiție incidente pe entități afectate

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

Nr. Crt.	Tipul sistemelor afectate	Nr. alerte
1	Reţele	180
2	Servicii de tip banking/payment	132
3	Siteuri web	85
4	Email	18
5	Staţii de lucru	15
6	Reţele de socializare	3
7	Baze de date	2
8	Neprecizat	15
TOTAL		450

Fig. 7 – Repartiție incidente pe tipuri de sisteme afectate

6.3. 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 **10.239** domenii compromise.
Din 710.000[5] domenii înregistrate în România, în luna decembrie 2013, numărul reprezintă aproximativ 1,4% din totalul domeniilor ”.ro”.
Distribuția domeniilor afectate, după tipul de incident, se regăsește în tabelul de mai jos.

[5] Conform datelor ICI-ROTLD

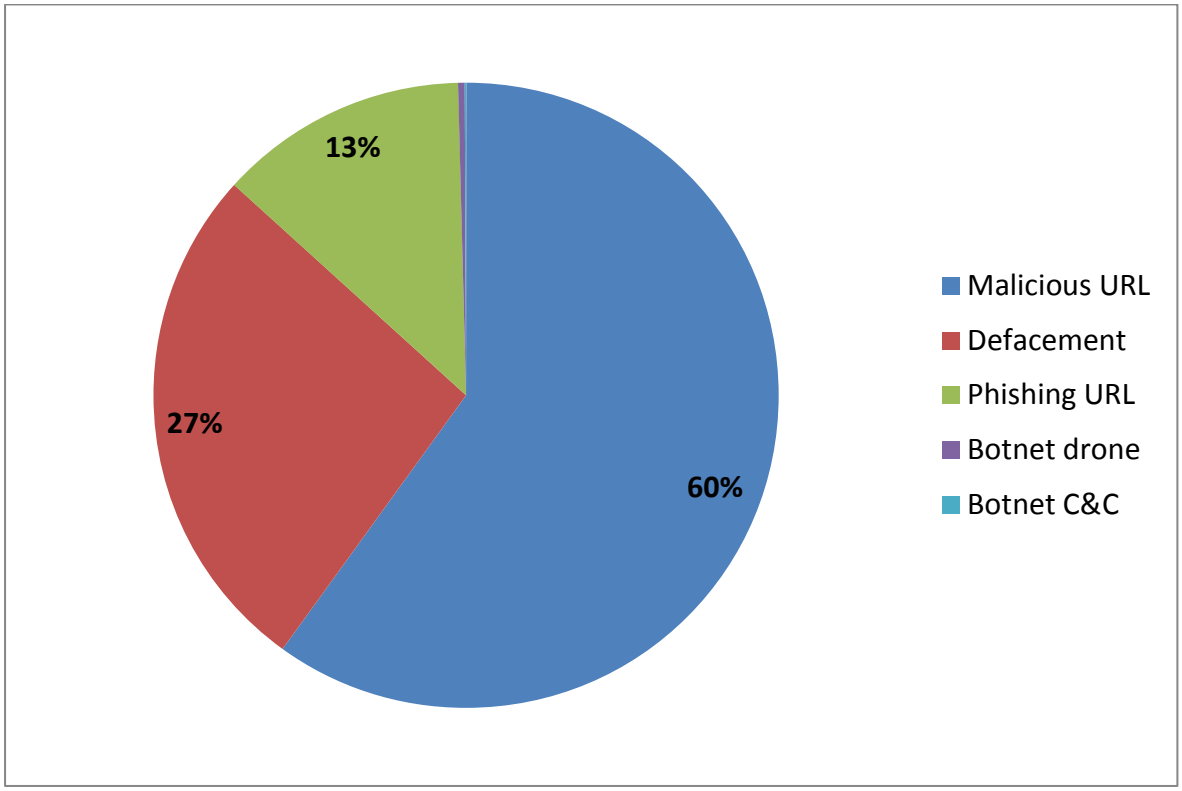

Fig. 6 – Domenii .ro compromise

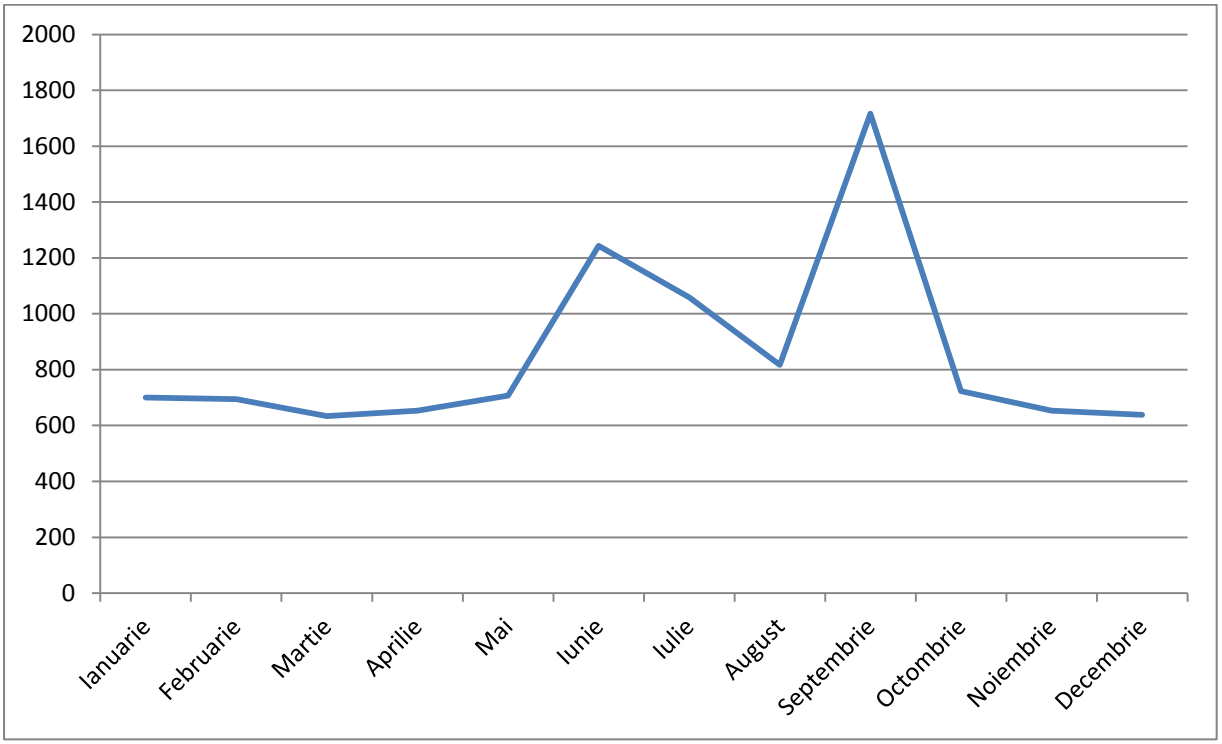

Fig. 7 – Domenii .ro compromise – distribuție alerte per luni

6.4. Amenințări de tip Advanced Persistent Threath (APT)[6]

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”[7]. 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.
De asemenea, pe parcursul anului 2013 au fost primite 287 alerte referitoare la amenințarea cibernetică de tip APT intitulată ”Red October”. Aceste alerte au vizat 55 de IP-uri unice din România, către acestea fiind transmise alerte de atenționare. Atacuri de acest gen au fost identificate și in cursul anului trecut și au vizat structuri guvernamentale sau ambasade din România.

7. Concluzii și comentarii

Din analiza datelor deţinute la nivelul CERT-RO, rezultă faptul că amenințările 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 de tip botnet (zombie).
Aceste sisteme compromise (victime), ce reprezintă potențiale amenințări la adresa altor entități conectate la Internet, sunt apoi folosite cu rol de ”proxy” pentru desfășurarea altor atacuri asupra unor ținte din afara țării. Avantajele pentru atacator sunt semnificative, respectiv posibilitatea ascunderii identității sale reale precum și posibilitatea utilizării unui număr mare de computere (in funcție de numărul sistemelor de calcul infectate) pentru a lansa atacuri.
De asemenea, pe baza analizei tipurilor de malware specifice spațiului cibernetic național precum și al tipurilor de sisteme compromise, reiese faptul că, din punct de vedere cantitativ, majoritatea atacurilor sunt îndreptate către sisteme învechite, depășite moral, fără posibilități native de securizare (ex: sistemele afectate de Conficker) sau care nu sunt actualizate cu ultimele patch-uri / update-uri de securitate.
Este de remarcat faptul că entități din România devin din ce în ce mai frecvent ținta amenințărilor de tip APT, respectiv 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). De asemenea, având în vedere funcțiile complexe ale unor astfel de aplicații malware, prezente într-un număr mai redus în perioada analizata (capabilități de interceptare a comunicațiilor electronice, accesarea neautorizata a datelor aferente tranzacțiilor financiare si mijloacelor de plata electronice, spionaj cibernetic etc. Ex: Red October, Miniduke), precum și faptul ca aceste tipuri de amenințări prezintă

[6] Advanced Persistent Threat
[7] 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

un caracter evolutiv moderat, se poate estima o creștere a numărului și severității unor astfel de atacuri la nivel național pe parcursul anului 2014;

În acest context, se menține concluzia din raportul publicat de CERT-RO pentru primele 6 luni ale anului, respectiv faptul că 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 resurse informatice semnificative conectate la rețeaua 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.

Anexa 1 – Recomandări pentru utilizatorii casnici

Având în vedere constatările precum și concluziile prezentului raport, considerăm absolut necesară cunoașterea, de către utilizatorii casnici, cel puțin a recomandărilor de securitate expuse mai jos:

1. **Folosiți numai software cu licență.** Sistemele de operare, aplicațiile de securitate, filmele, muzica precum și alte pachete software pirat, descărcate de pe site-uri de tip ”torrent” sau hub-uri de DC, pot conține cod malițios ascuns (rootkits, backdoors etc.) ce poate transforma computerul într-un ”zombie”, parte dintr-o rețea de tip botnet, controlat de către atacator.
2. **Folosiți, în măsura posibilităților, pachete software (sisteme operare și aplicații) ce beneficiază de suport din partea producătorului**, pentru care update-uri de securitate sunt publicate periodic. Pachetele software ce nu mai beneficiază de suport tehnic (actualizări) nu vă pot oferi protecție împotriva ultimelor tipuri de atacuri sau variante de malware.
   Dacă, din diverse motive, este necesară folosirea de pachete software ce nu mai beneficiază de suport din partea producătorului (declarate ”end of life”) asigurați-vă de securizarea suplimentară a acestora prin instalarea de aplicații dezvoltate de terți (antimalware, firewall, aplicații de control parental etc.), care să acopere breșele de securitate neacoperite de producător.
3. **Folosiți întotdeauna**, indiferent de sistemul de operare sau tipul de echipament folosit, **software de securitate de tip antimalware**, care să dispună de multiple module de protecție (ex: antivirus, antispam, antirootkit, antiphishing, firewall, control parental etc.). În prezent, există variante de malware pentru fiecare tip de sistem de operare, instalat fie pe sisteme convenționale (desktop, laptop), fie pe dispozitive mobile (tablete, smartphone). Indiferent de soluția folosită, aceasta trebuie actualizată permanent.
4. **Securizați-vă rețeaua locală wireless**. În cazul în care dispuneți de mai multe dispozitive ce necesită acces la Internet și folosiți o rețea locală wireless, router-ul folosit pentru conectarea dispozitivelor și partajarea conexiunii la Internet trebuie securizat corespunzător. Detalii suplimentare despre securizarea rețelelor wireless puteți găsi în ghidul ”Cum să te ferești de viruși, viermi și troieni”, disponibil la http://www.cert-ro.eu/articol.php?idarticol=762.
5. **Protejați corespunzător calculatorul sau dispozitivul folosit în comun de mai mulți membri ai familiei**. Crearea de conturi de utilizator individuale sau folosirea de software de control parental sunt doar câteva din măsurile pe care le puteți implementa. Detalii suplimentare despre securizarea rețelelor wireless puteți găsi în ghidul ”Cum să te ferești de viruși, viermi și troieni”, disponibil la http://www.cert-ro.eu/articol.php?idarticol=762.
6. **Folosiți parole puternice și nu dezvăluiți nimănui credențialele de acces** la diferite aplicații, servicii sau sisteme.
7. **Navigați prudent pe Internet** și acordați o atenție sporită informațiilor disponibile pe rețelele sociale (link-uri, aplicații etc.), acestea fiind folosite mai nou ca vector pentru distribuirea de malware.
8. **Evitați folosirea calculatoarelor/dispozitivelor** publice pentru accesarea diverselor servicii online (rețele socializare, aplicații de mesagerie instant etc.). De asemenea nu realizați tranzacții financiare sau cumpărături online de pe calculatoarelor/dispozitivelor publice.

O serie de măsuri suplimentare pot fi găsite în ghidul ”Cum să te ferești de viruși, viermi și troieni”, disponibil la http://www.cert-ro.eu/articol.php?idarticol=762, sau în ghidul ”Securitatea utilizatorului final”, disponibil la http://www.cert-ro.eu/articol.php?idarticol=770.
Pentru documentare suplimentară referitoare la tipuri de malware sau amenințări generice de securitate cibernetică vă rugăm consultați http://www.cert-ro.eu/articol.php?idarticol=763.

Anexa 2 – Recomandări pentru administratorii de sistem din cadrul organizațiilor

Sistemele informatice din cadrul organizațiilor necesită măsuri suplimentare de securitate față de utilizatorii casnici, în general datorită numărului mai mare de utilizatori precum și diversității de tehnologii folosite.
În acest sens, considerăm absolut necesară cunoașterea, de către administratorii de sistem, cel puțin a recomandărilor de securitate expuse în anexa 1 și suplimentar, a celor de mai jos:

1. **Țineți evidența dispozitivelor precum și a pachetelor software** folosite în cadrul sistemului informatic al organizației.
2. **Evaluați periodic nivelul de securitate al sistemului informatic** prin teste de penetrare, audituri de securitate sau simple scanări pentru identificarea vulnerabilităților.
3. **Faceți back-up permanent al datelor.**
4. **Aplicați măsuri de securitate pentru limitarea accesului neautorizat la sistemul informatic:** protecție fizică, blocare porturi, separare logică prin rețele virtuale (VLAN), acces pe bază de smartcard-uri, conturi de utilizatori individuale protejate prin parolă etc.
5. **Controlați permanent modul de folosire al conturilor de acces privilegiate** (conturi de administrator). Acestea trebuie folosite doar în caz de necesitate și nu permanent de către persoanele responsabile cu administrarea sistemului informatic.
6. **Verificați periodic fișierele de tip "log"** ale componentelor sistemului informatic, pentru identificarea eventualelor intruziuni.
7. **Folosiți tehnologii avansate de protecție a sistemului informatic**: IDS/IPS, soluții antimalware de tip enterprise, criptare fișiere și conexiuni, acces la distanță prin VPN etc.
8. **Folosiți proceduri de răspuns la incidente de securitate cibernetică** și stabiliți responsabili pentru astfel de activități.
9. **Instruiți periodic personalul** cu privire la folosirea sistemului informatic și raportarea incidentelor de securitate.
10. **Documentați arhitectura sistemului informatic al organizației și țineți evidența tuturor modificărilor.**

O serie de măsuri suplimentare pot fi găsite în ghidul"Cum să te ferești de viruși, viermi și troieni", disponibil la http://www.cert-ro.eu/articol.php?idarticol=762.

Anexa 3 – Clasificarea tipurilor de alerte tratate 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 reţea permițând decodificarea ulterioară a acestora. Această metodă se foloseşte 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.
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.

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 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.

Anexa 4 – Descriere TOP 25 tipuri de malware caracteristice spațiului cibernetic național

Nr. Crt.	Nume Malware	Tip malware	Descriere	Afecteaza Confidentialitatea	Afecteaza Disponibilitatea	Afecteaza Integritatea
1	**Conficker**	Vierme	de asemenea cunoscut sub denumirile *Downup*, *Downadup* sau *Kido*, este un vierme informatic care a infectat milioane de calculatoare începând de la finele anului 2008. Scopul principal al lui Conficker este acela de a compromite un număr cât mai mare de sisteme, acest lucru fiind posibil prin exploatarea vulnerabilităților sistemelor de operare *Microsoft Windows*. Odată ce sistemul a fost compromis, viermele blochează opțiunile de actualizare automate ale acestuia și restricționează accesul utilizatorului la site-urile producătorilor de soluții de securitate. Mai mult decât atât, variantele ulterioare ale lui Conficker includ și mecanisme de exploatare a funcției *Autorun*, posibilitatea de a accesa resursele partajate din rețea, precum și deschiderea și menținerea unei linii de comunicare între mașinile infectate și centrul de comandă și control (structură de tip *botnet*).	DA	DA	NU
2	**Sality**	Virus	este un virus polimorfic cu capabilităţi de backdoor şi keylogging care infectează fişierele executabile (.EXE) şi încearcă ştergerea fişierelor asociate programelor anti-virus, anti-spyware şi în unele cazuri firewall. După acest pas, Sality rulează un modul keylogger care colectează informaţii despre sistemul infectat, înregistrează parolele şi conturile de login folosite după care le trimite la o adresă de e-mail predefinită. De asemenea, virusul creează un backdoor prin care atacatorul poate prelua controlul calculatorului. Ca metode de propagare virusul se răspandeşte în reţea şi pe alte medii de stocare copiindu-se cu denumiri aleatoare şi creând o cale în fişierul "autorun.inf" pentru a fi sigur că va fi rulat.	DA	DA	DA
3	**Citadel**	Troian	este un program malițios ce face parte din familia troienilor bancari (*Zeus*, *SpyEye* etc.) ce au ca scop manipularea tranzacțiilor online. În plus, acesta permite susținerea unui atac informatic de tip *DDoS* prin intermediul sistemelor infectate sau executarea de la distanță a unor programe malițioase de tip *ransomware*, respectiv *scareware* pe acestea (structură de tip *botnet*).	DA	DA	DA
4	**Pushdo**	Troian	este un troian care permite accesul şi controlul neautorizat a unui calculator infectat. Atacatorul poate efectua un număr ridicat de acţiuni remote printre care menţionăm: descărcarea şi executarea de fişiere; upload-ul unor fişiere rezidente pe staţia infectată; infectarea altor sisteme prin diverse metode de propagare; capabilităţi de keylogging; modificarea setărilor sistemului de operare; ştergerea de fişiere; executarea sau închiderea unor aplicaţii.	DA	NU	DA
5	**Zeroaccess**	Troian	cunoscut și sub denumirile *max++* și *Sirefef*, este un malware de tip troian care afectează sistemele de operare *Microsoft Windows*. Scopul acestuia este de a descărca alte programe malițioase pe mașinile compromise din cadrul unei rețele de boți (*botnet*) de cele mai multe ori implicată în operațiuni de fraudare a click-urilor sau a monedelor virtuale (*Bitcoin*).	DA	DA	DA
6	**Slenfbot.5050**	Vierme	este un vierme care odată ce infectează sistemul îl transformă într-un bot. Acesta se răspândește via programe de mesagerie instantă printre care MSM Messenger, Yahoo Messenger şi Skype. De asemenea se poate răspândi via	DA	NU	DA

			dispozitive de stocare sau exploatând vulnerabilitatea MS06-040. În urma infectării acesta se conectează la un canal IRC, iar sistemul victimă poate fi comandat de către un server de comandă şi control.			
7	**Virut**	Virus	este un program malițios de tip *botnet* care este utlizat pentru distribuirea de malware, inițierea unor atacuri informatice de tip *DDoS*, *spam*, *furt de date* etc. prin intermediul sistemelor compromise. O caracteristică specifică a acestuia este răspândirea prin infectarea fișierelor executabile.	DA	DA	DA
8	**kelihos**	Troian	este un troian care distribuie mesaje de spam via email. Mesajele de spam pot conţine hyperlinkuri pentru a instala malware-ul Kelihos. Malware-ul poate comunica cu servere remote pentru a oferi informaţii despre victimă şi pentru a executa diverse sarcini precum: trimiterea de spam; capturarea unor informaţii sensibile; download-ul şi executarea unor fişiere.	DA	NU	DA
9	**IRCBot**	Troian	reprezintă o familie de troieni cu capabilităţi de backdoor care vizează sistemele de operare Microsoft Windows. Troianul are posibilitatea de a descărca o gamă de aplicaţii maliţioase pe sistemul infectat şi realizează o conexiune către servere de IRC. Troianul poate menţine multiple conexiuni pentru a primi comenzi de la atacatori.	DA	NU	DA
10	**Zeus**	Troian	aceasta familie de troieni sunt folosiţi pentru a fura informaţii cu caracter personal şi oferă atacatorilor control asupra staţiei respective. Acţiunile de furt de informaţii vizează în special instituţiile financiare. Acesta poate încetini conexiunea la internet, opri firewall-ul, descărca şi executa fişiere. Principalele modalităţi de propagare sunt via email-uri spam, site-uri web compromise sau aplicaţii freeware care execută şi alte operaţii decât cele din descriere.	DA	DA	DA
11	**Trafficconverter**	Troian (Conficker)	provine de la denumirea domeniului *trafficconverter.biz*, domeniu de unde mașinile infectate cu viermele *Conficker* își descărcau versiunile actualizate. O altă utilitate a acestui domeniu a fost de înșelare a utilizatorilor sistemelor compromise să descarce soluții false de scanare/devirusarea a lui *Conficker* în schimbul unei sume de bani.	NU	NU	DA
12	**Grum**	Troian	este un troian care în urma infecţiei permite atacatorilor să folosească staţia infectată ca şi server proxy pentru a accesa Internetul. Acest virus este distribuit via email-uri spam sau driveby download.	DA	DA	NU
13	**Torpig**	Troian	cunoscut și sub denumirile de *Sinowal* sau *Anserin*, este un malware de tip de *botnet* distribuit de o varietate de *troieni* care afectează mașini care au instalate sisteme de operare *Microsoft Windows*. Acesta scanează mașinile infectate pentru a obține credențiale, informații despre conturi sau parole, permițând astfel accesul deplin al atacatorului la acestea. Torpig este recunoscut pentru fraudele din domeniul bancar online.	DA	NU	NU
14	**Ransomware**	Troian/ Vierme	reprezintă o clasă de malware care restricţionează accesul la staţia infectată şi obligă utilizatorul să plătească pentru a primi acces din nou. Unele variante criptează doar fişiere sau porţiuni din dispozitivul de stocare, iar altele restricţionează accesul la sistemul de operare şi afişează un mesaj cu cerinţele atacatorului.	NU	DA	NU
15	**Blackenergy**	Troian	este un malware *HTTP-based* de tip *botnet* utilizat în principal pentru inițierea atacurilor de tip *DDoS*. O caracteristică a acestuia este că spre deosebire de un botnet comun, Blackenergy nu comunică cu serverul de comandă și control prin canale de tip *IRC.*	NU	DA	NU
16	**Tdss**	Troian	cunoscut și sub denumirea de *Alureon*, este un malware de tip *troian* dezvoltat cu scopul de a sustrage date de pe mașinile compromise prin interceptarea traficului din rețea și căutarea de nume de utilizatori, parole sau date referitoare la conturile bancare.	DA	DA	NU
17	**Trojan.Iframe.BMY**	Troian	este un troian care identifică pagini web hostate pe staţia respectivă şi le infectează inserând un iframe ascuns la finalul codului de html. Iframe-ul ascuns poate conţine un link către o pagină web.	NU	NU	DA
18	**Neurevt**	Troian	cunoscut și sub numele de *Beta Bot*, este un malware *HTTP-based* de tip *botnet* care în urma infecției schimbă anumite setări ale sistemului compromis și sustrage date sensibile. De asemenea, acesta poate permite unui	DA	DA	DA

			atacator să controleze de la distanță mașina compromisă.			
19	**Trojan.Script.CEV**	Troian	Nu exista descriere disponibila.			
20	**Hermes**	Vierme	este un vierme pentru mass-mailing. Un vierme de mass mailing reprezintă un cod maliţios care se propagă prin trimiterea acestuia via email. Acesta foloseşte propriul motor de SMTP astfel copii ale viermelui trimise via email nu apar pe staţia utilizatorului sau in folder-ul send a aplicaţiei de email.	NU	DA	NU
21	**Dorkbot**	Vierme	este denumirea unei familii de viermi informatici care comunică prin canale de tip *IRC* și se răspândesc prin dispozitive USB, programe de mesagerie instantă și rețele sociale. Variante de Dorkbot pot captura numele utilizatorilor și parolele acestora prin spionarea traficului din rețea și pot bloca site-uri utilizate pentru actualizări de mașinile compromise.	DA	NU	DA
22	**DDoS_Khan**	Troian	este un troian care în urma infecţiei transformă staţia într-un bot în cadrul unui botnet. Principalul obiectiv a acestui troian este de a executa atacuri DoS prin realizarea de trafic HTTP.	NU	DA	NU
23	**DDoS_DirtJumper**	Troian	este un troian care în urma infecţiei transformă staţia într-un bot în cadrul unui botnet. Principalul obiectiv a acestui troian este de a executa atacuri DoS prin realizarea de trafic HTTP.	NU	DA	NU
24	**Gamarue**	Virus	reprezintă o familie de viruşi care pot descărca şi fura informaţii despre staţia infectată. Acestea sunt distribuite via kituri de exploit şi spammed email. Anumite variante ale malware-ului sunt viermi şi se pot răspândi prin infectarea unor dispozitive de stocare mobile.	DA	NU	NU
25	**Trojan.Iframe.BZW**	Troian	este un troian care identifică pagini web hostate pe staţia respectivă şi le infectează inserând un iframe ascuns la finalul codului de html. Iframe-ul ascuns poate conţine fie un link către o pagină web.	NU	NU	DA