Incidente de securitate in spatiul cibernetic national

Liviu NICOLESCU
Director General CERT-RO

CERT-RO?

- ***Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO*** este punct național de contact cu privire la incidente de securitate cibernetică.
- structură independentă care dispune de capacitatea necesară pentru prevenirea, analiza, identificarea şi reacţia la incidentele de securitate cibernetică ale sistemelor informatice.

CERT-RO?

- ***H.G. 494/2011***.
- CERT-RO se află în coordonarea Ministerului pentru Societatea Informațională și este finanțat integral de la bugetul de stat.
- Comitet de Coordonare:
  - MSI, MApN, MAI – DIPI, SRI, SIE, STS, SPP, ORNISS, ANCOM

Raport analiză alerte 2013

- Scopul raportului este de a prezenta o analiză a incidentelor de securitate cibernetică raportate la CERT-RO în perioada 01.01 – 31.12.2013 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, aflate în aria de competență a CERT-RO.

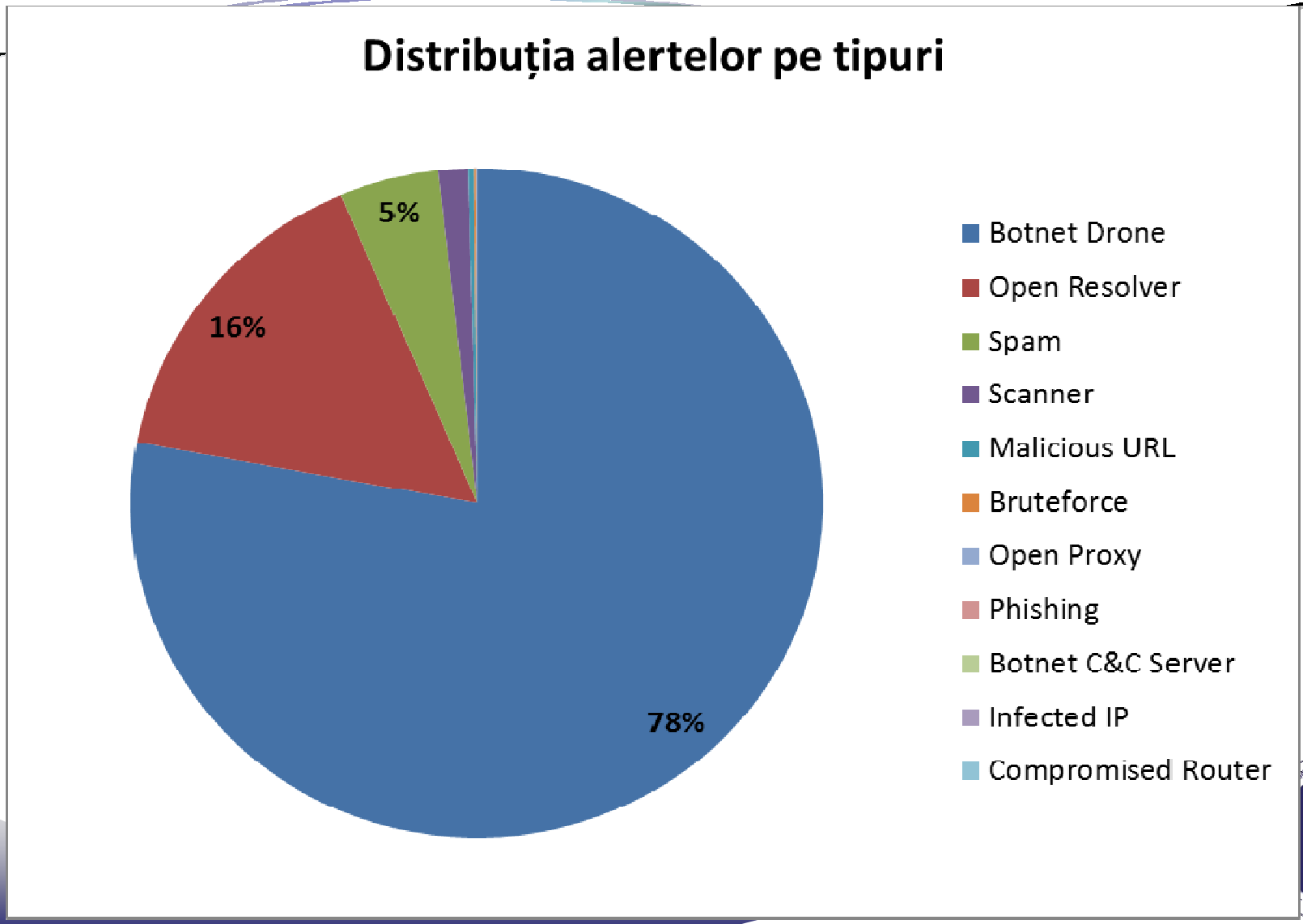
- Raportul este disponibil la: http://www.cert-ro.eu sectiunea Documente

Raport analiză alerte 2013

- Total alerte: **43.231.149**
- Nr. total de IP-uri unice afectate: **2.213.426**

Clasa alerte	Tip alertă	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**

Raport analiză alerte 2013



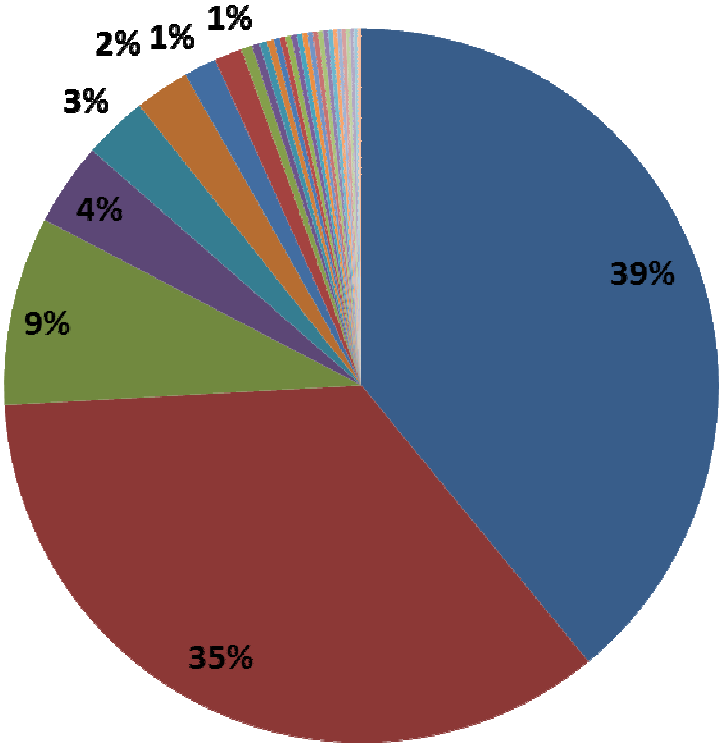
Raport analiză alerte 2013

- Botnet drone - Rețea de sisteme informatice compromise, controlate, de la distanță, de alte persoane/organizații decât deținătorii acestora.

- Microsoft Safety & Security Center: ”Atacatorii folosesc rețelele de tip botnet pentru a trimite spam, a răspândi viruși informatici, pentru a ataca alte computere și servere sau pentru a comite alte tipuri de fraude sau infracțiuni. Dacă computerul tău devine parte dintr-un botnet ai putea în mod involuntar să-i devii complice atacatorului.

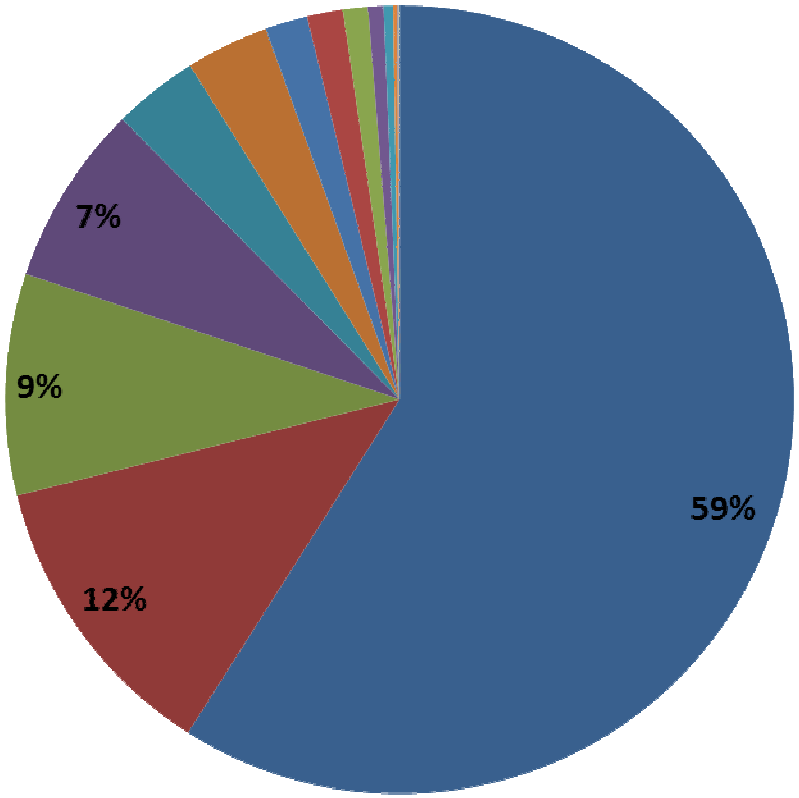
http://www.microsoft.com/security/resources/botnet-whatis.aspx

Raport analiză alerte 2013 – TOP ISP



- RCS & RDS SA
- ROMTELECOM
- UPC
- DIAL TELECOM S.R.L
- SC NextGen Communications SRL
- RCS & RDS SA
- Vodafone Romania S.A.
- Orange Romania SA
- ROEDUNET
- COSMOTE

Raport analiză alerte 2013 – TOP malware

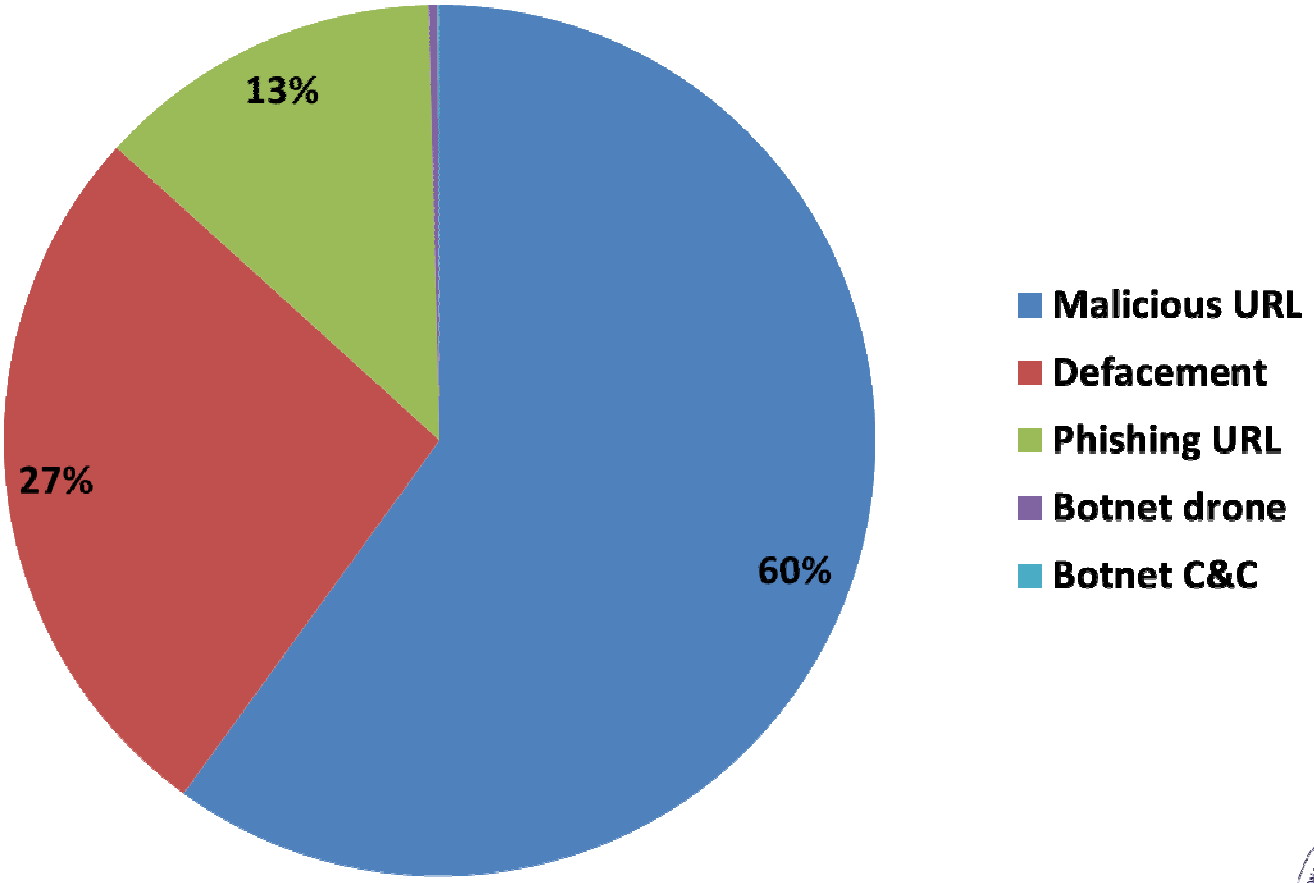


- Conficker
- Sality
- Citadel
- Pushdo
- Zeroaccess
- Slenfbot.5050
- Virut
- Kelihos
- IRCBot
- Zeus
- Trafficconverter
- Grum
- Torpig
- Ransomware
- Blackenergy
- Tdss
- Trojan.Iframe.BMY
- Neurevt

Raport analiză alerte 2013 – TOP SO

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

Raport analiză alerte 2013 – alerte individuale



10.239 domenii compromise, 1,4% din totalul .ro

Advanced Persistent Threat

- 2013 – ROCRA
  - APT specializat pe spionaj cibernetic asupra unor structuri de tip guvernamental, ambasade, institute de cercetare și structuri militare.
  - Campanie începută în 2007.
  - Mod de atac: spear phishing email, exploatare vulnerabilități MS Word și Excel.
  - 287 alerte, 55 IP unice.
- Martie 2013 – MiniDuke
  - Specializat pe furt de date și spionaj cibernetic din structuri guvernamentale.
  - Metodă de atac: spear phishing, exploatare vulnerabilități Adobe Reader.

Concluzie raport

- 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;
- peste 16% din plaja de IP-uri alocată României este infectată cu diverse variante de malware (botnet), ce ulterior sunt folosite în diverse atacuri asupra unor ținte din afara țării, identitatea reală a atacatorului rămânând ascunsă.
- Peste 50% din numărul total al IP-urilor unice raportate, rulează sisteme de operare din familia XP/2000.
- RO nu mai poate fi considerată generatoare de incidente de securitate cibernetică, raportul demonstrând caracterul intermediar/de tranzit al sistemelor din RO.

Vă mulțumesc!

Întrebări?

http://www.cert-ro.eu/