State of cyber security in RO

Dan Tofan

Technical Director CERT-RO

29.10.2014

Who is CERT-RO?

- CERT-RO is an independent structure, with expertise in the field of cyber security, that has the capacity to *prevent, analyze, identify and respond* to cyber security incidents threatening RO national cyber-space.
- coordinated by the Ministry for Information Society and is fully financed by the state budget.

What does CERT-RO do?

- Collect alerts from different stakeholders regarding RO IPs and URLs detected as part of different cyber-security incidents (national contact point).
- Maintain a national database regarding cyber-security incidents.
- Operates an EWS on cyber-security incidents, based on the alerts received.
- Other services (pen tests, incident handling, tech support)

Report on alerts received in 2013

- First ever official public report on state of cyber-security in ROMANIA.
- An analysis of the cyber-security incidents reported to CERT-RO.
- Scope: obtaining a general overview of the nature and dynamics of these types of events/incidents, relevant for assessing cyber security risks targeted at the IT&C infrastructures in Romania.

Report on alerts received in 2013

- Total alerts: 43.231.149
- Unique IP's extracted from the alerts: 2.213.426

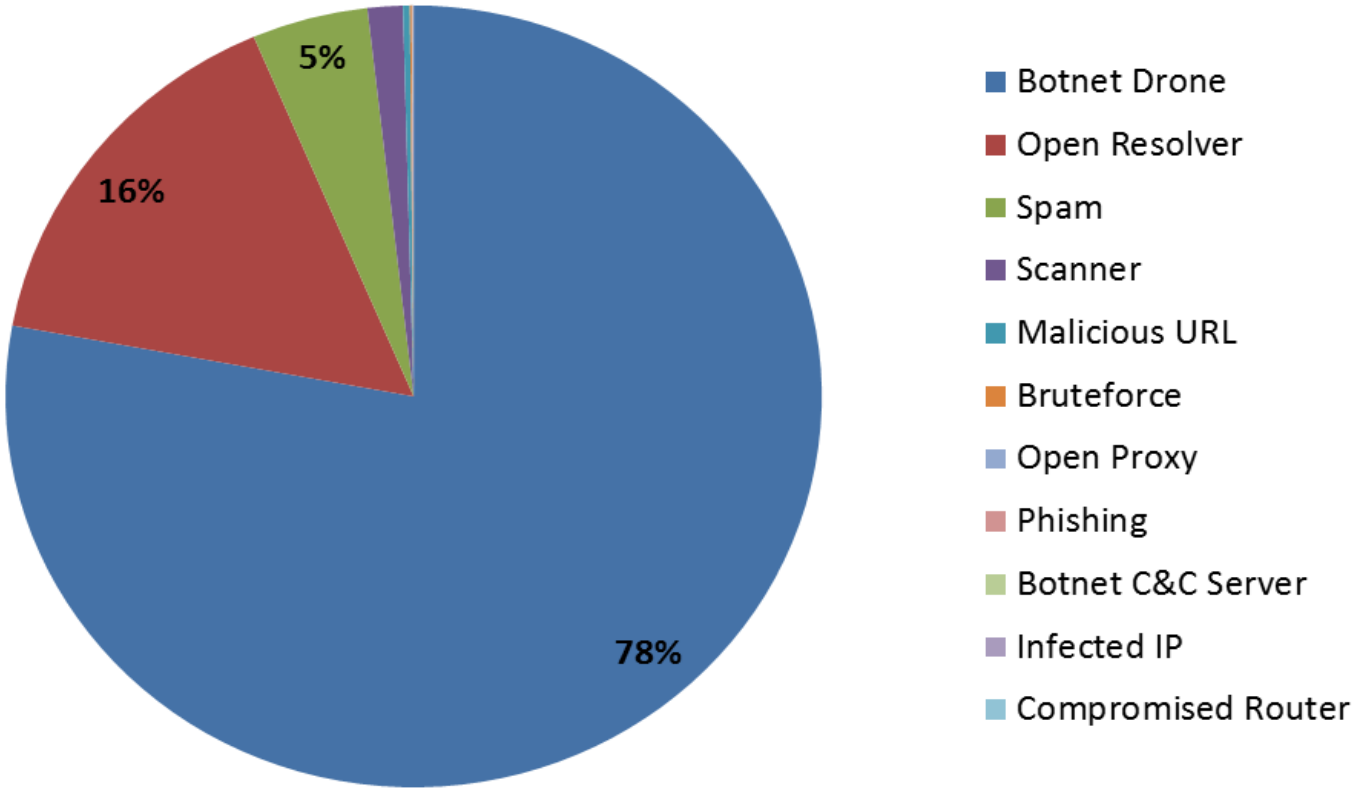
Alert Class	Alert type	Number of alerts
Botnet	**Botnet Drone**	33.677.871
Vulnerabilities	**Open Resolver**	6.782.888
Abusive Content	**Spam**	1.986.605
Information Gathering	**Scanner**	603.524
Malware	**Malicious URL**	116.535
Cyber Attacks	**Bruteforce**	30.150
Vulnerabilities	**Open Proxy**	13.809
Fraud	**Phishing**	13.556
Botnet	**Botnet C&C Server**	4.082

Report on alerts received in 2014 (Q1+Q2)

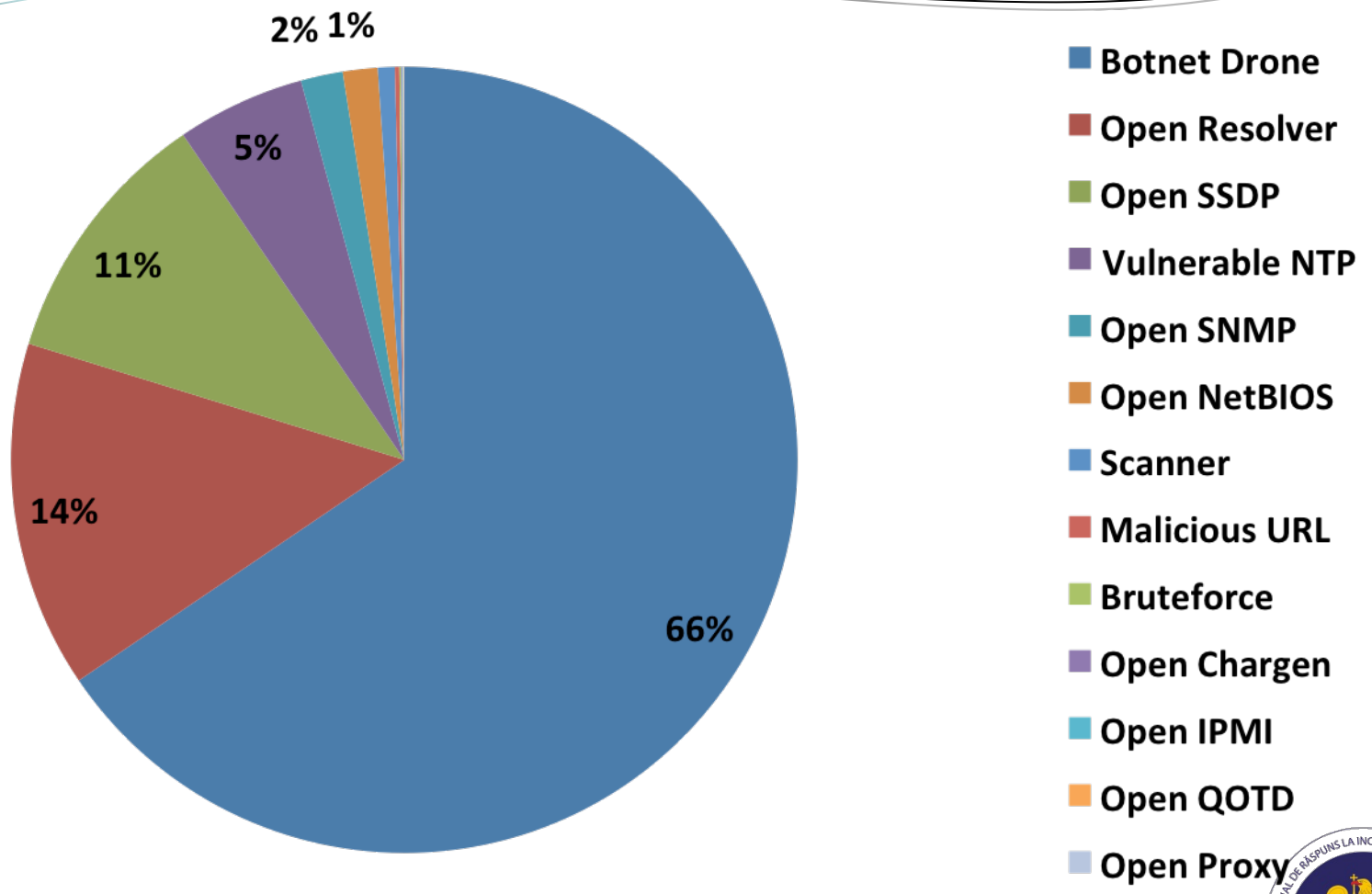
- Total alerts: 54.854.197
- Unique IP's extracted from the alerts: 2.071.962

	Clasă Alerte	Tip Alertă	Nr. Alerte
1	Botnet	Botnet Drone	35938970
2	Vulnerabilities	Open Resolver	7824535
3	Vulnerabilities	Open SSDP	5874180
4	Vulnerabilities	Vulnerable NTP	2893326
5	Vulnerabilities	Open SNMP	946397
6	Vulnerabilities	Open NetBIOS	784430
7	Information Gathering	Scanner	381860
8	Malware	Malicious URL	97835
9	Cyber Attacks	Bruteforce	42080
10	Vulnerabilities	Open Chargen	27847
11	Vulnerabilities	Open IPMI	13047
12	Vulnerabilities	Open QOTD	11685
13	Vulnerabilities	Open Proxy	6465
14	Phising	Phishing	4857
15	Botnet	Botnet C&C Server	4358

Report on alerts received in 2013



Report on alerts received in 2014 (Q1+Q2)



Alerts received in 2014 vs. 2013 (Q1+Q2)

- 26% increase in the number of reported IPs in 2014 vs. first 6 months of 2013.
- 300% rise in number of **processed** alerts 2014 (first 6 months) vs. 2013 (first 6 months).

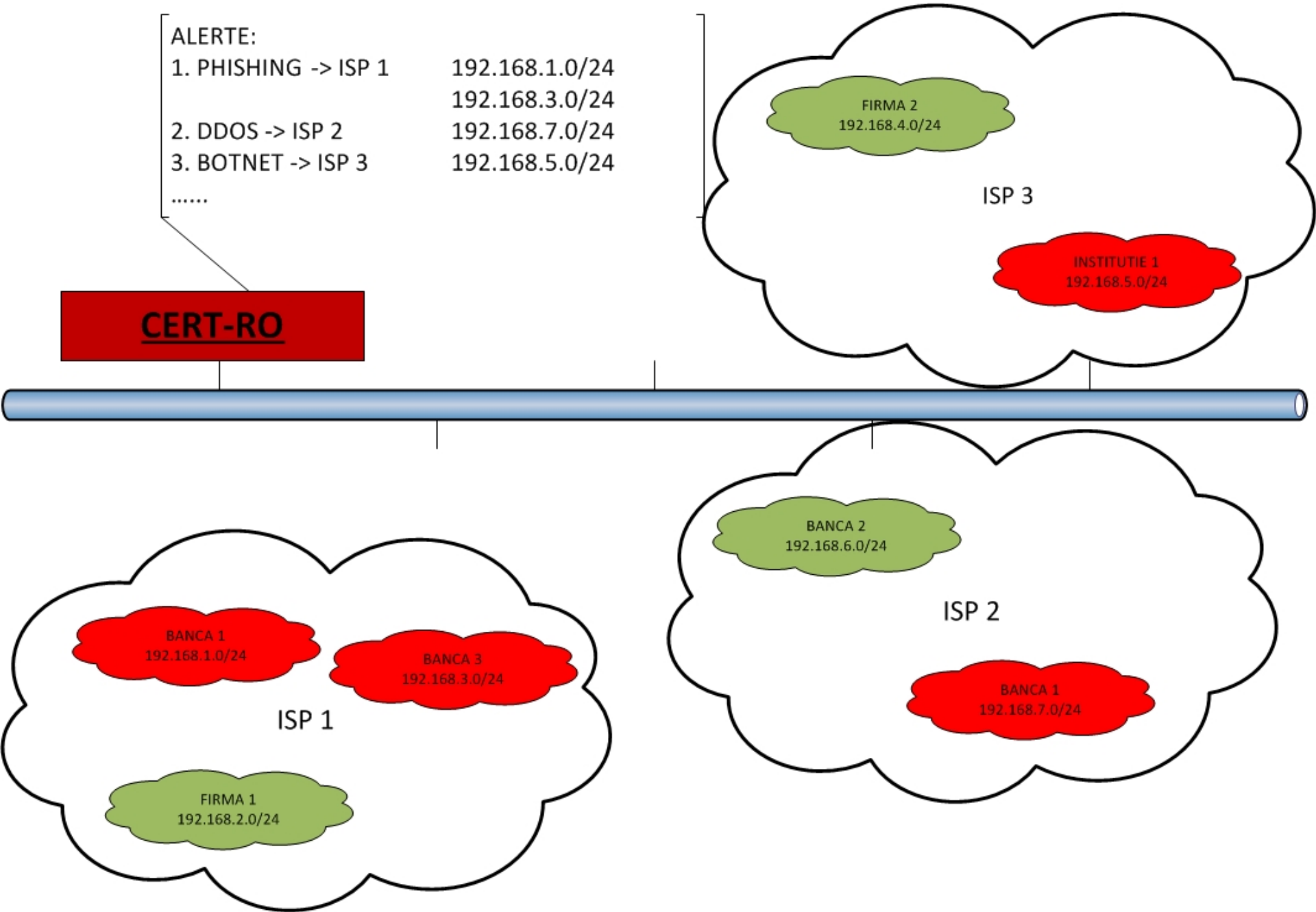
- 2014: 11% of total IPs reffer to compromised systems that are part of a botnet (1,5 mil. IPs) and are used as proxies for further attacks outside RO.

- 2014: 19% of the alerts reffer to misconfigured and compromised systems (type vulnerabilities: DNS, NTP, SNMP, NetBIOS etc.)

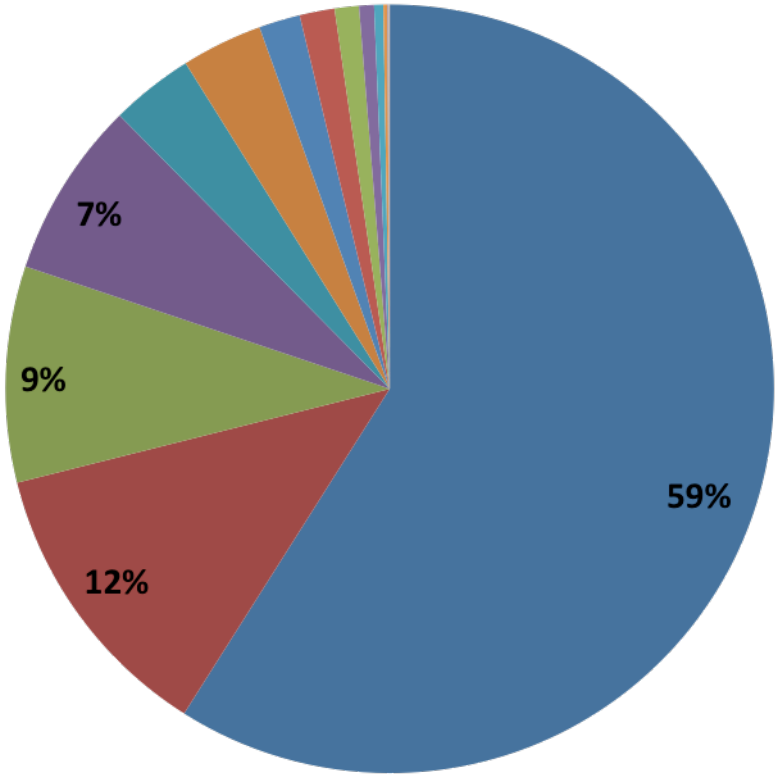
Issues regarding the alerts received!!!

- DHCP - protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters (IP addresses).
- Because of DHCP use among RO ISPs, in present it is impossible to determine the real number of users/clients/computers behind the reported IPs.

- Behind an IP could be one or multiple clients!

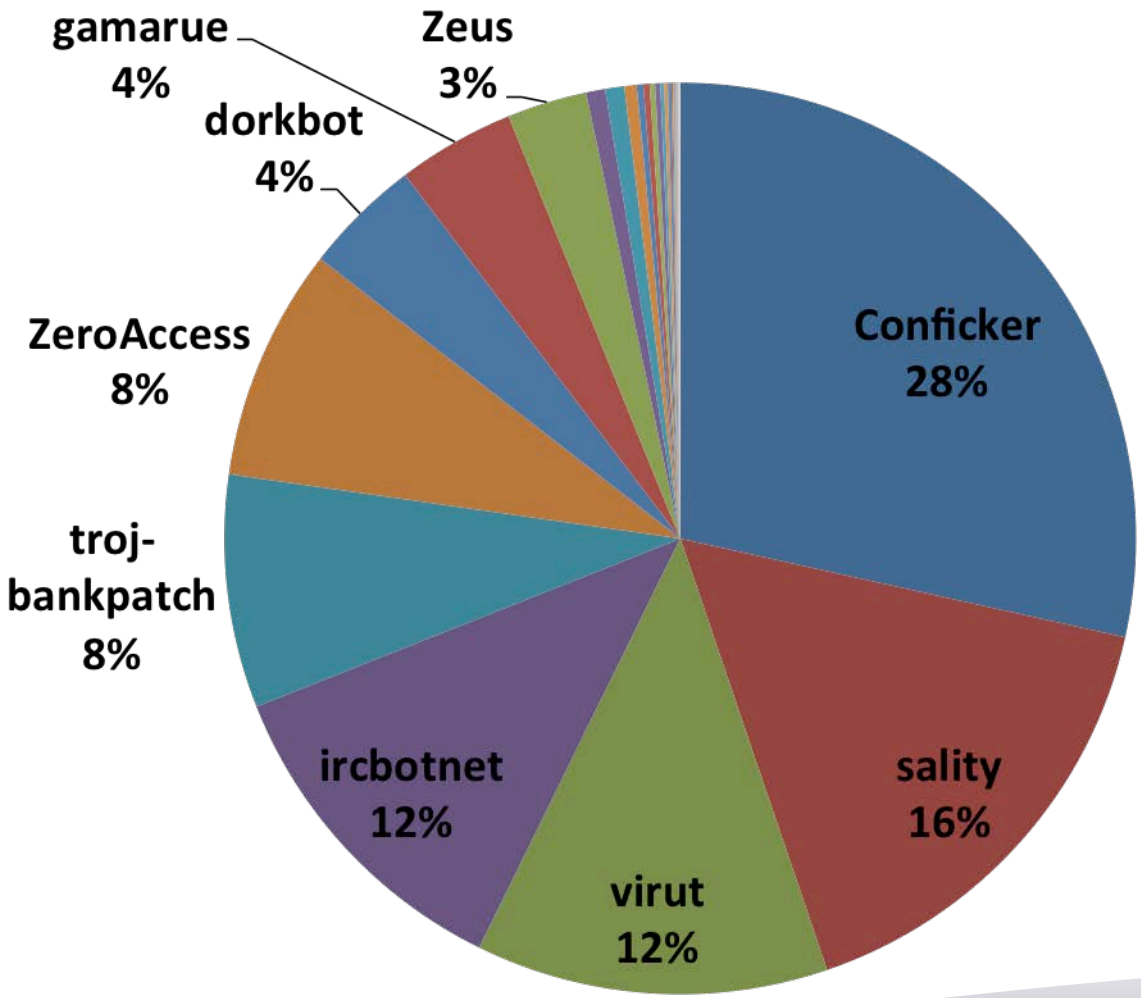

ALERTE:
1. PHISHING -> ISP 1 192.168.1.0/24
192.168.3.0/24
2. DDOS -> ISP 2 192.168.7.0/24
3. BOTNET -> ISP 3 192.168.5.0/24
.....
CERT-RO
FIRMA 2
192.168.4.0/24
ISP 3
INSTITUTIE 1
192.168.5.0/24
BANCA 2
192.168.6.0/24
ISP 2
BANCA 1
192.168.7.0/24
BANCA 1
192.168.1.0/24
BANCA 3
192.168.3.0/24
ISP 1
FIRMA 1
192.168.2.0/24

2013 TOP malware variants in RO



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

2014 (Q1+Q2) TOP malware variants in RO

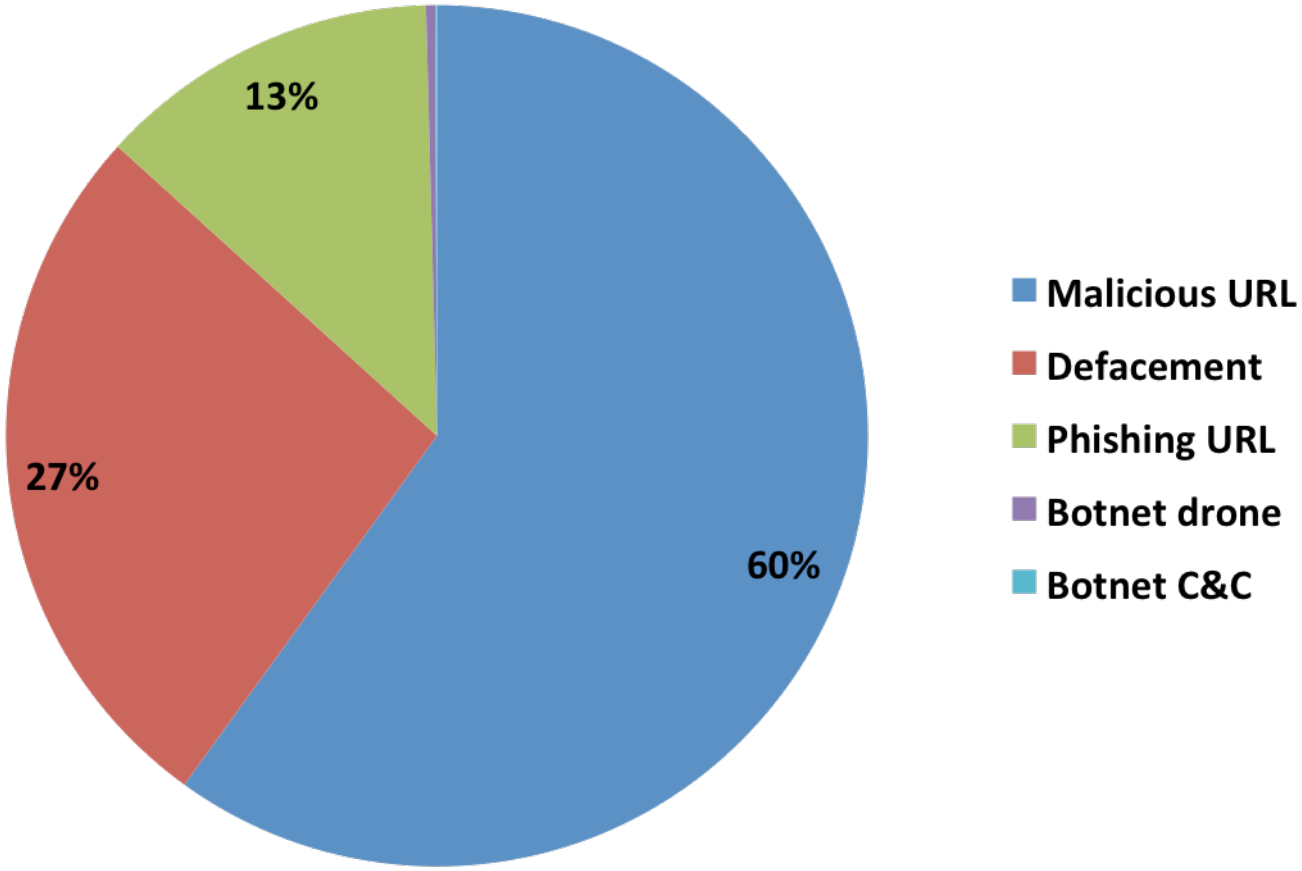


2014 (Q1+Q2) TOP malware variants in RO

- 1.110.563 IPs (8%) affected by Conficker in 2014 (Q1+Q2) vs. 1.693.323 in 2013.

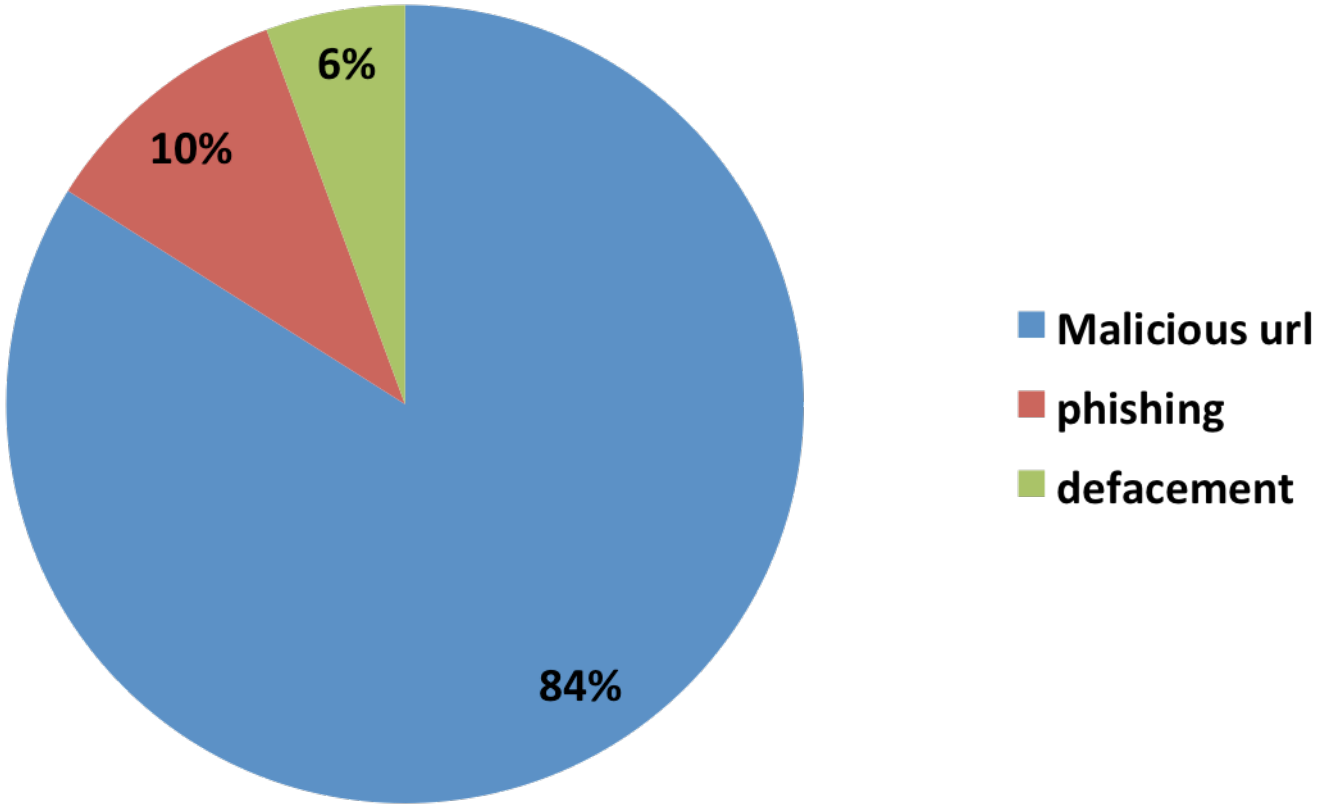
- **Conficker -** is a computer worm targeting the Windows OS that was first detected in November 2008. It uses flaws in Windows OS software and dictionary attacks on admin passwords to propagate while forming a botnet. It infercted millions of computers in over 200 countries, making it the largest known computer worm infection since the 2003 Welchia.
- **Sality** is the classification for a family of malicous software discovered in 2003 that may communicate over a P2P network for sending spam, proxy of comunications, exfiltrating sensitive data, distributed computer tasks.
- **Virut** – primitive virus that takes control of compromised machine and allows a hacker to download and run files from Internet.
- **IRCbotnet** – bots controlled over an IRC channel.

2013 ".ro" compromised domains



10.239 compromised domains (5.678 Q1+Q2)

2014 (Q1+Q2) ”.ro” compromised domains



5.839 compromised domains

Advanced Persistent Threat

- Red October (2013/2014)
- MiniDuke (2013)
- Turla/Snake (2014)
- Energetic Bear (2014)

Conclusions on alerts

- cyber threats targeting the Romanian national cyberspace have diversified, evolutionary trends being observed, both in terms of quantity and of technical degree of complexity;
- 8% of all IPs in RO are infected with the Conficker worm.
- The majority of the compromised systems in Romania, are part of botnets, and being used as proxies for carrying out attacks on targets outside the country;
- most attacks are directed towards outdated, obsolete systems, lacking security features (e.g. systems affected by Conficker) or are not updated with the latest security patches/updates;

Conclusions on alerts

- Romania cannot be considered anymore just a generator of cyber security incidents, because the analysis of the data presented in the current report demonstrates that is ***mostly used as a proxy by other attackers***.

ISP cooperation:

- Why is important:
  - Alerts send to real indivuduals/customers, not ISPs
  - Drastically reduce cyber-incidents and their related issues for ISP (additional traffic, additional costs, blacklisting etc.)
  - Improve overall rating of RO in cyber-security field
- Cooperation protocols with 1 big ISP.
- CERT-ROs *”FREE special offer”* to ISP:
  - Fast alerts related to threats targeting ISPs, before info going public.
  - Support in incident handling/response in case of DDOS.
  - Awareness activities (cyber exercises, workshops etc.).

Projects developed – CYBERCRIME (**SMIS 37595**)

National System for Countering Cyber Crime:

- Aprox. 1,7 mil Euro from EU funds.
- 30 months (27.03.2012 – 27.09.2014).
- Objective: proper framework establishment in order to achieve a higher competitiveness in public policies elaboration and a better response capacity of the public institution in the fight against cyber crime.
- Beneficiary entities: public authorities and institutions that have direct connection to cyber-crime & cyber-security fields of activity.

Projects developed – CYBERCRIME (**SMIS 37595**)

Objectives proposed an achieved:

- Train a 40 person cyber-crime team.
- Develop an attack simulation platform (system) with suitable hardware and technologies (Lab).
- Develop a set of indicators for measuring cyber-crime phenomenon in RO.
- Develop proposals for a suitable legal framework, public policies.

ACDC

- European funded pilot project - 16 mil. €
- Selected under the CIP programme
- Operating from 01/02/2013 ➔ 31/07/2015

Joining forces to fight botnets

The ACDC project partners

- Atos
- BARCELONA DIGITAL
- Bulgarian Posts
- Cassidian Cybersecurity
- Croatian Academic and Research Network - CARNet
- CyberDefcon
- DE-CIX
- DFN-CERT
- eco – Association of the German Internet Industry
- Engineering Ingegneria Informatica
- FCCN - Foundation for National Scientific Computing
- Fraunhofer FKIE
- G Data Software AG
- Institute for Internet Security - if(is)
- Inteco
- ISCOM – Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
- KU Leuven R-B-CCENTRE (Belgian Cybercrime Centre of Excellence for Training, Research and Education)
- LSEC - Leaders in Security
- Microsoft EMEA
- Montimage
- CERT-RO
- SignalSpam
- TECHNIKON Forschungsgesellschaft mbH
- Telecom Italia
- Telefónica I+D
- TU Delft
- University of Luxemburg
- XLAB

28 partners

14 Member States

Austria
Belgium (NSC)
Bulgaria
Croatia (NSC)
Czech Republic
France (NSC)
Germany (NSC)
Italy (NSC)
Portugal (NSC)
Romania (NSC)
Slovenia
Spain (NSC)
The Netherlands
United Kingdom

ACDC Partners

Providing security tools and services used to identify and fight botnets

ACDC

Improve the early detection of botnets
Support their mitigation

- foster an extensive **sharing of information** across Member States
- create a **European source of data sets** stored in an ACDC data clearing house
- provide a complete **set of solutions** accessible online for mitigating on-going attacks
- use the **pool of knowledge** to create best practices that support organisations in raising their cyber-protection level
- create a **European wide network** of cyber defence centres

ACDC – a service approach

Detection

Centralised reports of botnet behaviour

Spam campaign

DDoS traffic detected

Stolen credentials

Drive-by-download

Centralised Data Clearing House

Standardized report findings

Support – notifying affected customer

Mobile network provider

Bank of customer

Security vendor

Hosting provider

Redirect to botfree.eu

Mitigation – helping affected customer

ACDC
the Advanced Cyber Defence Centre

The ACDC Community

Get involved!

The ACDC outreach team

Peter Meyer – peter.meyer@eco.de

Véronique Pevtschin – veronique.pevtschin@eng.it

Kazim Hussain karim.hussain@atosresearch.eu

Thank you!

Questions?

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