Report on Cyber Security Alerts Processed by CERT-RO in 2016

Romanian National Computer Security Incident Response Team
office@cert-ro.eu

1. Main findings

The objective of this report is the analysis of cyber security alerts collected and processed by CERT-RO in 2016, in order to obtain an overview of relevant events for an assessment of cyber security risks to cyber infrastructures in Romania within the competence of CERT-RO.

In the reference period, i.e. 01.01.2016 - 31.12.2016, CERT-RO collected and processed **110,194,890 cyber security alerts**, an increase of 61.55% compared to 2015 (68,206,856), of which:

- automatically collected and processed alerts (feeds): **110,193,527**;
- manually collected and processed alerts (email ticketing): 1,363.

In the context of this report, a **cyber security alert** is any report that contains an IP address or a domain (URL) related to a possible incident or cyber security event, which involves or may involve information systems in the national cyberspace, held / managed by individuals or legal entities in Romania.

A total of 2,920,407 unique IP addresses have been targeted by alerts collected by CERT-RO in 2016. The total number of unique IPs allocated to organizations in Romania is **7,540,736**[1], a decrease compared to 2015 (8,958,498), 2014 (approx. 10 mil.) and 2013 (approx. 13.5 mil.).

The analysis of cyber security alerts collected by CERT-RO in 2016 resulted in the following findings:

- 38.72% (2.92 mil.) of total unique IP addresses allocated within the national cyberspace have been involved in at least one cyber security alert processed by CERT-RO in 2016, compared to 26% (2.3 mil.) in 2015;
- **81.39% (89.68 mil.) of the alerts collected and processed are related to vulnerable information systems** (not secured or improperly configured). Some

[1] According to http://www.nirsoft.net/countryip/ro.html

of these vulnerable systems are used by attackers to launch cyber attacks on other targets and to mask their identity; most of the times they do not need to compromise the system, but to merely use the services available;

- **12.81% (14.12 mil.) of alerts collected and processed** are related to systems infected with different variants of malicious software (malware), such as botnets, characterized by the fact that it has mechanisms which allow attackers to remotely control infected systems;
- **58.98% (2.38 mil.) of the total number of incidents resulting from the processing of alerts are related to vulnerable systems**, which can be used in carrying out cyber attacks on targets in the Internet; this allows the possibility for some of the attacks to be achieved without compromising the systems;
- **40.96% (1.65 mil.) of the total number of incidents resulting from the processing of alerts (section 3.2) are related to systems that are part of botnet networks**, which can be used in carrying out cyber attacks on targets in Romania or abroad;
- **10,639 ".ro" domains have been reported to CERT-RO as being compromised in 2016, down about 40% compared to 2015 (17,088)**. Of the 896,726[2] domains registered in Romania by December 2016 (with only 421,973 active[3] ones), the number represents about 1.19% of ".ro" domains and about 2.52% of active ".ro" domains.

Based on these findings, **the following conclusions can be drawn**:

- Most alerts collected are related to vulnerable systems (improperly configured or not secured) and to systems infected with various types of malicious software such as botnets;
- Either of the two types of systems mentioned above can be used as interface (proxy) for carrying out attacks on targets outside the country, thus representing potential threats to other systems connected to the Internet;
- Household network devices or equipment (e.g. wireless routers), or those that are part of the Internet of Things (IoT) (webcams, smart TV, smartphones, printers, etc.), when connected to the Internet they become targets for attackers and their vulnerabilities are exploited to compromise the network to which they belong or to launch attacks on other targets in the Internet;
- Romania is both a country generating cyber security incidents as well as a country with proxy (transit) role for attackers outside the national space, which use vulnerable or compromised computer systems that are part of the national cyberspace;
- Cyber vulnerabilities and threats to the national cyberspace continue to diversify, as evidenced by the fact that in 2016 CERT-RO introduced new types of alerts.

Despite technical issues that make it impossible to identify the exact number of devices or people behind the approximately 2.9 million IP addresses affected or 110 mil. alerts reported to CERT-RO, it is important to remember that they cover about 38.72% of the national cyberspace (by reference to the no. of IPs assigned RO) and therefore

[2] According to ICI-ROTLD data published at http://www.rotld.ro/ 3 http://viewdns.info/data/

[3] http://viewdns.info/data/

remedial measures are necessary, requiring the involvement of all actors with technical or legal responsibilities.

2. Types of alerts processed by CERT-RO

CERT-RO processes two types of cyber security alerts:

- ***Alerts collected and transmitted through automated systems***. These alerts are transmitted by specialized organizations, which own detection systems for cyber security incidents. The large majority of these alerts (99%) are automatically processed by CERT-RO and transmitted to Internet service providers which own/manage the infrastructures concerned by the alerts (IP, domain/URL etc.). In the case of this type of alerts, CERT-RO does not have exact data concerning the IP address user, which means that his identification can only be done by the Internet service provider (ISP), who should also forward the alert to the client;
- ***Manually processed alerts*** are considerably less than the automatically processed ones, but contain information about the incident and the affected organization that are much more complete and relevant, such as the source and the means of the attack. In most cases CERT-RO analysts collect data from the afflicted entities (natural or legal persons, within Romania or abroad), at the time of the notification of the incident. Therefore, these alerts are much more valuable for the analysis on cyber security, as they reflect the evolution of a security incident much better.

3. Statistical data based on alerts received

The number of alerts collected by CERT-RO in 2016 (110,194,890) increased by 61.55% compared to 2015 (68,206,856). The figure below reflects the evolution in the number of alerts per year since 2013.

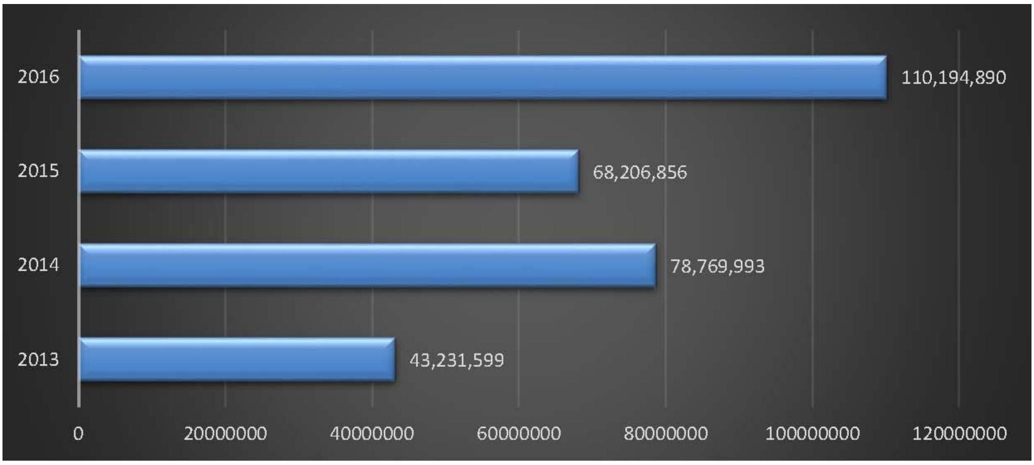

Fig. 1. Evolution in the number of alerts per year collected in 2013, 2014, 2015 and 2016

The significant number of alerts shown in CERT-RO reports highlights the institutional needs to ensure a system able to collect, process and disseminate large volumes of data automatically.

3.1. Alerts distribution according to class (category of alert)

Alerts collected and processed by CERT-RO were classified according to a taxonomy in which classes and types of alerts have been defined (a “class” representing a generic category that can encompass more specific types of alerts).

The description (taxonomy) of the types of alerts processed by CERT-RO can be found in section 3.8 at the end of this report.

The table and chart below show the distribution of the five most common categories of alerts according to their number and the graphical distribution of alerts according to their type.

Table 1. Top 5 security alerts per class (category)

No.	Alert class	Number of alerts	Percentage
1	Vulnerabilities	89,684,933	81.39%
2	Botnet	14,121,119	12.81%
3	Compromised Resources	5,902,174	5.36%
4	Malware	454,807	0.41%
5	Cyber Attacks	26,466	0.02%

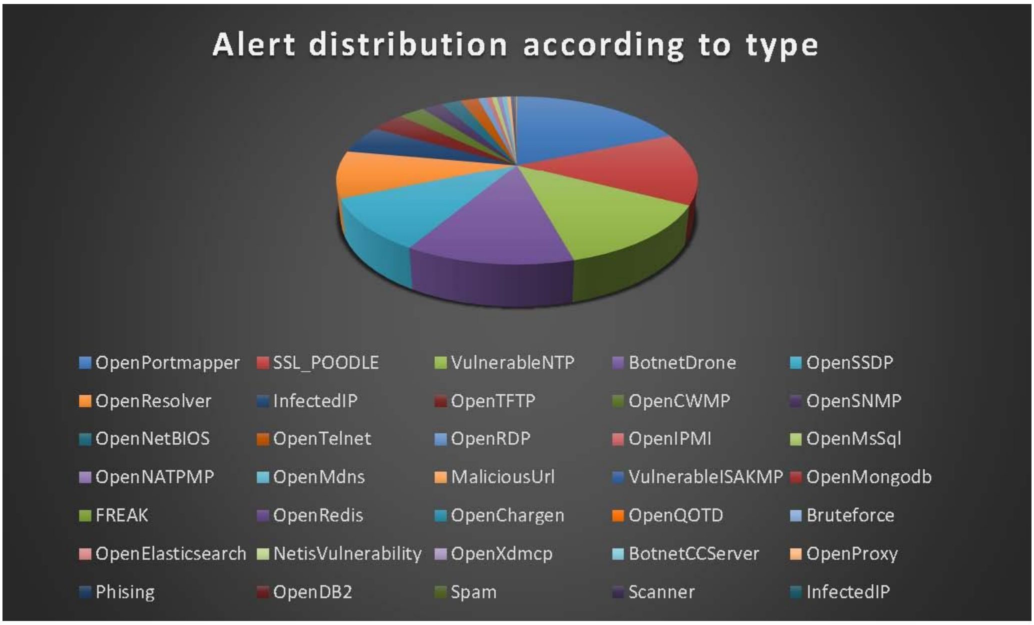

Fig. 2. Alerts distribution depending on their type

3.2. Alerts distribution according to number of incidents

Given that some alerts collected by CERT-RO are repetitive in the sense that more alerts refer to the same IP address and the same problem (class/type of alert) a de-duplication of alerts was made, by grouping them into incidents.

The general principle used for this was to group all the alerts that relate to the same system and the same type of problem (class / type of alert).

Given that alerts collected by CERT-RO refer only to public IP addresses, it is impossible to determine the exact number of systems affected (victims), because of the following two reasons:

- Internet Service Providers (ISPs) assign the public IP addresses to residential customers dynamically (DHCP). As such, within a year, a public IP address can be assigned to several customers;
- A public IP address can be a gateway to Internet connection for an infrastructure formed by multiple computer systems. Thus, behind a public IP address there can be more than one computer system.

In this context, alerts have been grouped on incidents based on the following aspects:

1. Alerts related to vulnerabilities have a significant share in the total number of alerts (81.39%). These vulnerabilities relate to applications and services running on server platforms (web servers, database servers, time servers etc.) whose IP addresses are not dynamically allocated and who generally don’t change their IP address very often. Consequently, for alerts related to vulnerabilities, we felt that it was sufficient for the aggregation to be based on IP address and class/type of alert;
2. In the case of alerts related to botnets, whose share is 12.81%, the aggregation is based on computer systems of home users that are infected with various types of botnet malware. In most cases for these systems the allocation of IP addresses is dynamic. Consequently, for alerts related to botnets the aggregation was based on the IP address, the class / type of alert and the period of time between two notifications (up to 14 days).

In conclusion, by grouping alerts on incidents, according to the algorithm and considerations mentioned above, we obtain a number of 4,035,445 incidents in 2016, distributed as shown in the table and graph below.

Table 2. Distribution of alerts according to the number of incidents

No.	Alert Class	Number of incidents	Percentage
1	Vulnerabilities	2,380,120	58.98%
2	Botnet	1,653,096	40.96%
3	Malware	2,071	0.05%
4	Others	158	0.01%

The statistics based on aggregating alerts collected according to incidents shows that the IT systems that are part of botnet networks (40.96%) are still one of the main problems of the national cyber space, alongside with vulnerable systems (58.98%).

The aggregation of alerts on incidents shows that the botnet threat is much more significant than it was indicated by the statistical data related to the number of alerts. This is happening because the alerts related to vulnerabilities are much more repetitive and many systems remain vulnerable for a longer period of time, being reported repeatedly.

3.3. Types of malware typical to Romanian cyberspace

An alarming 13% of all alerts collected and processed by CERT-RO in the first part of 2016 contain information on the type of malware associated to the alert (such as botnet alerts or malicious URLs).

Table 3. Top 10 malware types in Romania

No.	Malware type	Number of alerts	Percentage
1	Sality	4,953,615	34.16%
2	Downadup	2,570,006	17.72%
3	Nivdort	1,979,510	13.65%
4	Ramnit	1,081,592	7.46%
5	Dorkbot	830,914	5.73%
6	Mirai	522,377	3.60%
7	Zeroaccess	312,785	2.16%
8	Virut	277,460	1.91%
9	Conficker	244,371	1.69%
10	Tinba	187,556	1.29%

3.4. Types of systems affected

20.19% of all alerts collected and processed by CERT-RO in 2016 contain information relating to the operating system of the systems targeted by alerts.

The following table lists the types of alerts according to operating systems.

Table 4. Distribution of alerts according to types of affected operating systems

No.	Operating System Family	Percentage
1	Linux	42.96%
2	Network Devices Firmware/OS	22.91%
3	Unix	24.02%
4	UPnP OS	8.08%
5	Windows	0.57%

3.5. Particularities of alerts processed manually

Along with automatic alerts, CERT-RO analysts have collected a series of cyber security alerts notified directly by individuals or organizations in the country or abroad, classified as manually processed alerts.

They are considerably fewer than automatic ones, but they contain information that is much more complete and relevant about the incident and the organization affected, such as the source and the method of attack. In most cases the data are collected by CERT-RO analysts at the time of the notification of the incident, from affected entities (natural or legal persons in the country or abroad).

In 2016 CERT-RO collected 1,363 manually processed alerts, distributed as follows:

Table 5. Manually processed alerts distribution

No.	Alert class	Alert type	Number of alerts	Percentage
1	Fraud	Phishing	505	37.05%
2	Malware	Malicious Url	363	26.63%
3	Malware	Infected IP	256	18.78%

No.	Alert class	Alert type	Number of alerts	Percentage
4	Botnet	Botnet Drone	84	6.16%
5	Botnet	Botnet CC Server	42	3.08%
6	Cyber Attacks	Bruteforce	37	2.71%
7	Information Gathering	Scanner	23	1.69%
8	Vulnerabilities	Other	23	1.69%
9	AbusiveContent	Spam	17	1.25%
10	Compromised Resources	Infected IP	13	0.95%

3.6. Compromised ”.ro” domains

During the reporting period, CERT-RO received alerts related to 10,639 compromised ".ro" domains.

Of the 896,726[4] domains registered in Romania (by December 2016), this number represents approximately 1.19% of the total ”.ro” domains and approximately 2.52% of all active “.ro” domains.

The distribution of the affected domains by the type of incident is reflected in the table below.

Table 6. “.ro” compromised domains

No.	Alert class	Number of websites
1	Vulnerabilities	8,202
2	Malware	1,363
3	Botnet	677
4	Fraud	361
5	Abusive Content	36
	TOTAL	10,639

3.7. Detailed distribution of alerts by types and classes

The table below shows all the alert types collected by CERT-RO in 2016.

We note that, compared to 2015, CERT-RO has processed 11 new types of vulnerabilities: Open Port Mapper, Open TFTP, Open CWMP, Open NetBIOS, Open Telnet, Open RDP, Vulnerable ISAKMP, Open Redis, Open mDNS, Open XDMCP and Open DB2.

No.	Alert class	Alert type	Alert number	Percentage
1	Vulnerabilities	Open Portmapper	20,539,496	18.63925%
2	Vulnerabilities	SSL_POODLE	15,358,349	13.93744%
3	Vulnerabilities	Vulnerable NTP	14,493,897	13.15297%
4	Botnet	Botnet Drone	14,117,097	12.81103%
5	Vulnerabilities	Open SSDP	11,177,596	10.14348%
6	Vulnerabilities	Open Resolver	10,107,848	9.17270%
7	Compromised Resources	Infected IP	5,902,187	5.35613%
8	Vulnerabilities	Open TFTP	4,027,012	3.65445%
9	Vulnerabilities	Open CWMP	3,026,661	2.74664%
10	Vulnerabilities	Open SNMP	2,430,907	2.20601%

[4] According to ICI-ROTLD data published at http://www.rotld.ro/

No.	Alert class	Alert type	Alert number	Percentage
11	Vulnerabilities	Open NetBIOS	2,306,809	2.09339%
12	Vulnerabilities	Open Telnet	2,116,736	1.92090%
13	Vulnerabilities	Open RDP	981,330	0.89054%
14	Vulnerabilities	Open IPMI	626,050	0.56813%
15	Vulnerabilities	Open MsSql	615,636	0.55868%
16	Vulnerabilities	Open NAT-PMP	604,933	0.54897%
17	Vulnerabilities	Open mDNS	575,435	0.52220%
18	Malware	Malicious Url	455,169	0.41306%
19	Vulnerabilities	Vulnerable ISAKMP	309,947	0.28127%
20	Vulnerabilities	Open Mongodb	143,375	0.13011%
21	Vulnerabilities	FREAK	73,748	0.06693%
22	Vulnerabilities	Open Redis	60,093	0.05453%
23	Vulnerabilities	Open Chargen	48,781	0.04427%
24	Vulnerabilities	Open QOTD	33,792	0.03067%
25	Cyber Attacks	Bruteforce	26,503	0.02405%
26	Vulnerabilities	Open Elasticsearch	12,677	0.01150%
27	Vulnerabilities	Netis Vulnerability	6,003	0.00545%
28	Vulnerabilities	Open Xdmcp	4,162	0.00378%
29	Botnet	Botnet CC Server	4,148	0.00376%
30	Vulnerabilities	Open Proxy	2,685	0.00244%
31	Fraud	Phising	3,062	0.00278%
32	Vulnerabilities	Open DB2	975	0.00088%
33	Abusive Content	Spam	911	0.00083%
34	Information Gathering	Scanner	600	0.00054%
35	Malware	Infected IP	257	0.00023%
36	Vulnerabilities	Other	23	0.00002%
		TOTAL	110,194,890	100.00%

3.8. Description (taxonomy) of alert types processed by CERT-RO

Alert class	Alert type	Description
Abusive Content	**Spam**	Unrequested electronic communication (email) with commercial character.
Botnet	**Botnet C&C Server**	Information systems used for controlling the victims (drone, zombie) within a botnet network.
	Botnet Drone	Network of infected information systems controlled by other persons/organization than the actual owners.
Cyber Attacks	**Bruteforce**	Automated password cracking method, used for revealing the legitimate credentials of the users of an information system. Practically, through automated mechanisms, one can generate and test a large number of password combinations, until retrieving the real credentials.
	DDoS	A DDoS (Distributed Denial of Service) attack aims at affecting or even

Alert class	Alert type	Description
		interrupting some services exposed in the internet (websites, servers, etc.).
Fraud	**Phishing**	A form of online fraud based on employing certain techniques of manipulating the identities of persons/ organizations with the purpose of obtaining material advantages or confidential information.
Information Gathering	**Scanner**	Systems that scan entire IP classes on the internet, with the purpose of identifying vulnerable systems, over which a cyber attack can be subsequently launched. Scanning is the initial phase in most cyber attacks.
Malware	**Infected IP**	Information systems/ services which serve as infection vector for other information systems. The systems/ services are practically hosting, with or without the permission of the administrator, various samples of malware which can infect other legitimate users.
	Ransomware	Ransomware is a software that blocks access to files stored in an information system and requires the payment of a certain amount of money in exchange to restoring access to these.
	Malicious URL	Compromised websites, most of the times without the administrator's permission, which host various types of malware, thus facilitating the infection of other legit users who visit the respective links.
Vulnerabilities	**Open Protocols and Services:** *Portmapper, NTP, SSDP, TFTP, CWMP, SNMP, NetBIOS, Telnet, RDP, IPMI, MsSql, NAT-PMP, mDNS, ISAKMP, Mongodb, Redis, Chargen, QOTD, Elasticsearch, Xdmcp, DB2*	Protocols or services which roll on different information systems, often servers, which are not adequately configured or represent un-updated versions with known security problems. These information systems are vulnerable to different threats which can exploit the respective vulnerabilities.
	Open Resolver	Unsecure DNS servers, which allow launching recurrent DNS requests for other domains, other than those hosted by the DNS server. They are used for DNS Amplification attacks.
	SSL_POODLE	POODLE attacks are based on the fact that when a secured connection fails, the

Alert class	Alert type	Description
		servers negotiate the use of older protocols, such as SSL 3.0. An attacker that can launch a connection error can subsequently force the use of SSL 3.0 and exploit the vulnerability.
	FREAK	A new SSL/TLS – FREAK vulnerability, acronym for Factoring RSA Export Keys. This vulnerability allows attackers to intercept HTTPS connections between vulnerable clients and web servers, forcing them to use „export-grade" cryptography.
	Netis Vulnerability	NETIS router vulnerability, which allows an attacker to gain control over the device. This can be successful when the attacker retrieves the external IP address of the equipment and he accesses the 53413 UDP port.

Note: The table above contains the cyber security alerts frequently notified to CERT-RO. Although the threat landscape is much more diverse, not all are found in the notifications received by CERT-RO.