Report on Cybersecurity Alerts Processed by CERT-RO in 2015

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

1. Main findings

The objective of this report is to **analyze the cybersecurity alerts collected and processed by CERT-RO in 2015**, so as to obtain an overview on the events relevant for evaluating the cybersecurity risks incurred by the cyber infrastructures on Romanian territory, which are under the CERT-RO constituency.

During the reference period, respectively 01.01.2015 – 31.12.2015, CERT-RO has collected and processed **68,206,856 cybersecurity alerts**, with a drop of 13% compared to 2014 (78,769,993), out of which:

- Alerts collected and processed automatically (feeds): **68,205,633**;
- Alerts collected and processed manually (email ticketing): **1,223**;

Cybersecurity alert means, within the context of this report, any signalling containing an IP address or a web domain (URL), with regards to a possible cybersecurity incident or event, which involves or might involve informatics systems from the national cyber-space held / managed by natural or legal persons from Romania.

The alerts collected by CERT-RO in 2015 regarded a set of 2,321,931 unique IP addresses. The total number of unique IPs assigned to organizations from Romania is of **8,958,498**[1], thus dropping compared to 2014 (approximately 10 million) and 2013 (approximately 13.5 million).

Following the analysis of the cybersecurity alerts collected by CERT-RO in 2015, **the following have been determined:**

- **26% (2.3 mil.) out of the total unique IPS** assigned to the national cyber-space have been involved in at least one cybersecurity alert processed by

[1] According to the data from https://www.maxmind.com/en/allocation-of-ip-addresses-by-country

CERT-RO in 2015, compared to **24% (2.4 mil.) in 2014** and **16% (2.2 mil.) in 2013**;

- **78% (53 mil.) of the collected and processed alerts are related to vulnerable information systems**, namely unsecured or inadequately configured systems. Some of such vulnerable information systems are used by the attackers to launch cyber-attacks on other targets and to mask their identity, most of the times not being necessary to compromise them, but to simply use the available services (such as: DNS servers of Open Resolver type, proxy servers without authentication, NTP servers with inadequate configuration etc.);
- **20,78% (14 mil.) of the collected and processed alerts are related to information systems which are infected with various malicious software versions (malware)**, defined through the fact that they have mechanisms that allow attackers to remotely control the infected information systems;
- **64% (3 mil.) of the total number of incidents resulted from the processing of alerts (section 3.2) consist of information systems which are part of botnet type networks**, there being a chance that they might be used for cyber-attacks on targets from Romania or abroad;
- **17,088 of the „.ro" domains have been reported at CERT-RO as having been compromised in 2015, rising by approximately 58% towards the years 2014 (10.759) and 2013 (10.239)**. Out of the total 855,997[2] domains registered in Romania in February 2015, this number represents approximately **2% of the total „.ro" domains and approximately 6.5% of the total active „.ro" domains.**

2. Types of alerts processed by CERT-RO

CERT-RO processes two types of cyber-security alerts:

- **Alerts collected and sent through automatic systems.** These alerts are sent by specialized organizations which have detection systems for cybersecurity incidents. The majority of such alerts (99%) is automatically processed by CERT-RO and transmitted to the internet services providers, who hold / manage the infrastructures targeted by the alerts (IP, domain/URL, etc.). In case of such alerts, CERT-RO does not have precise data on the IP address user, his/her identification being possible only by the internet services provider (ISP), who should, as a matter of fact, to resend the alert to the client also;
- **The manually processed alerts** are significantly fewer than the automatic ones, but they contain more complete and relevant information about the incident and the affected organization, as well as the attack source and method. In most cases, the data is collected from the affected entities (natural or legal persons from the country or abroad) by the CERT-RO analysts, once the incident is reported.

[2] According to the ICI-ROTLD data

Consequently, in terms of cybersecurity analysis, these alerts are much more valuable, because they reflect better the evolution of a security incident.

3. Statistics based upon the alerts received

The number of alerts collected by CERT-RO in 2015 dropped by 13% (68,205,856) compared to 2014 (78.769.993), as it is also shown in Fig. 1.

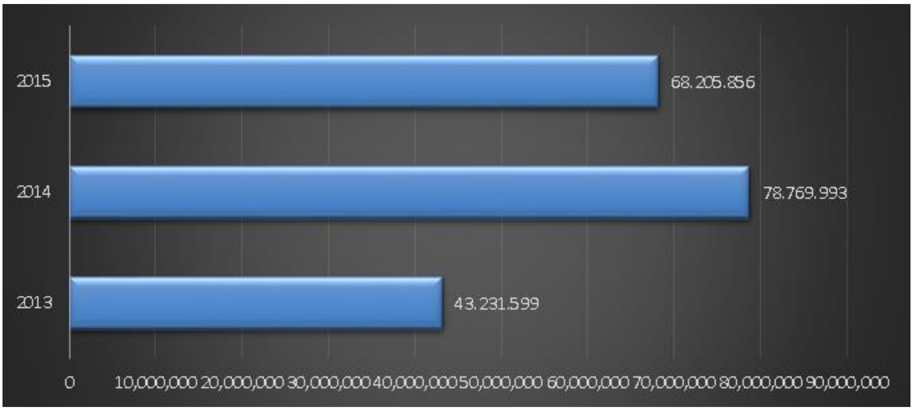

Fig. 1. Evolution in the number of alerts collected in 2013, 2014, and 2015

The drop in the number of alerts collected during 2015 in comparison with 2014 can be explained by the fact that a part of the vulnerable information systems (DNS servers of Open Resolver type, proxy servers without authentication, NTP servers with inadequate configuration, etc.) have been remedied in the previous year.

The significant number of alerts presented in the CERT-RO reports highlights the institution's demand for ensuring high performance systems, which would be able to achieve the automatic processing and dissemination of a large data volume.

3.1. Alert distribution depending on the class (alert category)

The alerts collected and processed by CERT-RO have been classified based upon a taxonomy where several alerts classes and types have been defined (an alerts class is a generic category, which may integrate several specific types of alerts).

The table and graphic below show the distribution of the 5 most frequent categories of alerts, depending on their number.

Tab. 1. Top 5 security alerts, on alert classes (categories)

No.	Alert class	Number of alerts	Percentage
1	Vulnerabilities	53,424,880	78.33%
2	Botnet	14,171,061	20.78%
3	Malware	393,380	0.58%
4	Information Gathering	102,167	0.15%
5	Cyber Attacks	61,751	0.09%

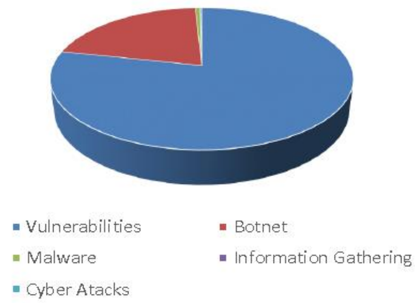

Fig. 2. Alert distribution on classes (categories)

3.2. The alerts' distribution on number of incidents

Given that some of the alerts collected by CERT-RO are repetitive, meaning that more than one refers to the same IP address and the same problem (class / alert type), a reduplication of the alerts through a grouping on incidents has been performed.

The general principle standing at the basis of the alerts' grouping on incidents was to gather all alerts which refer to the same information system and the same type of problem (class / alert type).

Considering that the alerts collected by CERT-RO only refer to public IP addresses, it is impossible to determine the exact number of affected information systems (victims), because of the following 2 reasons:

- The internet services providers (ISP) dynamically assign (DHCP) the public IP addresses to the residential clients. So, throughout a calendar year, public IP addresses can be assigned to several clients;
- Public IP addresses can be an internet connection gateway for an infrastructure composed of several information systems. So, behind a public IP address, there can be several information systems.

Under such circumstances, grouping alerts on incidents has been made depending on the following:

1. The alerts regarding vulnerabilities have a significant weight in the total number of alerts (78.33%). Such vulnerabilities refer to applications and services that run on server-type platforms (web servers, data bases servers, time servers, etc.), whose IP addresses are not dynamically assigned, and that generally do not even change their IP address too often. Consequently, related to vulnerabilities alerts, we have considered that it would be enough for the aggregation to be made on the IP address and the alert class/type;
2. In case of botnet type alerts, whose weight is of 20.78%, we refer to information systems belonging to household users which are infected with various types of botnet malware. In the majority of cases, in such information systems the IP addresses assignment is made dynamically. Consequently, for botnet alerts, their grouping into incidents has been made based upon the IP address, alert class / type, and the time between 2 reports (up to 14 days).

In conclusion, following the grouping of alerts on incidents, according to the algorithm and considerations mentioned above, there resulted a number of 4,900,651 incidents in 2015, distributed according to the table and graphic below.

Tab. 2. Alert distribution on number of alerts

No.	Alert class	Number of incidents	Percentage
1	Botnet	3,161,666	64.52%
2	Vulnerabilities	1,729,042	35.28%
3	Malware	5,847	0.12%
4	Information Gathering	3,730	0.08%
5	Cyber Attacks	366	0.01%

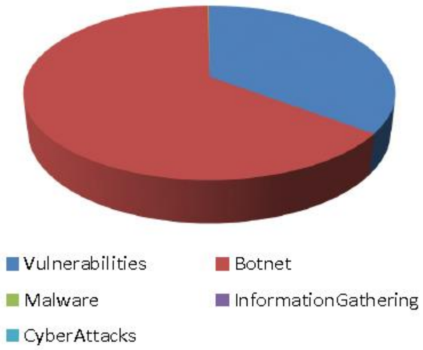

Fig. 3. Alert distribution on incidents

The statistics based upon the aggregation of the collected alerts on incidents show that the main problem of the national cybernetic space consists in information systems which are part of botnet networks (64%), although the statistics based upon the number of alerts show that 78% of these refer to vulnerabilities, and only 20% to botnet networks. This is due to the fact that the alerts that refer to vulnerabilities are more repetitive, many of the targeted systems staying vulnerable for a long period of time, thus being reported several times.

3.3. Malware types typical for the Romanian cybernetic space

A percentage of 20% of the total alerts collected and processed by CERT-RO in 2015 also contain information regarding the type of malware associated to the alert (such as botnet type alerts or the ones referring to malicious URLs).

Tab. 3. Top 10 malware types in Romania 2015

No.	Malwaretype	Percentage (%)
1	Conficker	47.98%
2	Sality	16.98%
3	ZeroAccess	8.19%
4	Ramnit	6.07%
5	Tinba	3.00%
6	Virut	2.82%
7	StealRat	2.74%
8	Pushdo	2.47%

No.	Malwaretype	Percentage (%)
9	NivDort	1.71%
10	Gameover ZeuS	0.99%

3.4. Types of affected information systems

A percentage of 23.87% of the total alerts collected and processed by CERT-RO in 2015 also contain information regarding the operation system of the information systems targeted by the alerts.

Tab. 4. Distribution of the total alerts on affected operation systems

No.	Operating system family	Percentage (%)
1	Network Devices Firmware/OS	32.51%
2	Unix	28.13%
3	Linux	25.83%
4	UPnP OS	9.04%
5	Windows	3.31%

3.5. Peculiarities of the manually processed alerts

Next to automatic alerts, the CERT-RO analysis took over during the reference period a set of cybersecurity alerts reported directly by people or organizations in the country or abroad, classified as **manually processed alerts**.

These are significantly fewer than the automatic ones, but they contain more complete and more relevant information on the incident, the affected organization, as well as on the source of attack and the attack method. In the majority of cases, data is collected from the affected entities (natural or legal persons in the country or abroad) by the CERT-RO analysts, once the incident is reported.

Consequently, during the reference period, CERT-RO collected **1,223 manually processed alerts**, distributed as follows:

Tab. 5. Distribution of individual alerts

No.	Alert class	Alert type	Alert percentage
1	Malware	Infected IP	34%
2	Malware	Malicious URL	25%
3	Fraud	Phishing	16%
4	Information Gathering	Scanner	11%
5	Cyber Attacks	Exploit Attempt	6%

The remainder of 8% of the manually processed alerts can be included in various classes and types of alerts, such as: botnet, spam, defacement, bruteforce, malware, or confidential information dissemination, etc.

In the table below, there is a top 5 most affected types of systems, extracted from the alerts manually processed by CERT-RO.

Tab. 6. Distribution of manually processed alerts on types of affected systems

No.	Type of affected system	Alert percentage
1	Information networks/systems	34%
2	Websites	32%

3	Work stations	22%
4	Banking/payment services	7%
5	Network equipment	5%

3.6. Compromised ”.ro” domains

Throughout the reference period, CERT-RO received alerts regarding **17.088 compromised ”.ro” domain**.

Out of 855,997[3] domains registered in Romania in February 2015, the number represents approximately 2% of the total ”.ro” domains, and approximately 6.5% of the total active ”.ro” domains.

The distribution of the affected domains according to the type of incident can be found in the table below:

Tab. 7. Compromised .ro domains

No.	Category	Number of sites
1	Malicious URL	8,783
2	Phishing	7,846
3	Defacement	459
TOTAL		17.088

3.7. Detailed distribution of alerts on classes and types

The table below contains all types of alerts collected by CERT-RO in 2015. To be noted that, compared with 2014, **CERT-RO processed 8 new types of vulnerabilities**: SSL_POODLE, FREAK, Open NAT PMP, Open MsSql, Netis Vulnerability, Open Mongodb, Open Redis, and Open Elasticsearch.

No.	Alert class	Alert type	No. of alerts	Percentage
1	Vulnerabilities	SSL_POODLE	15,910,893	23.33
2	Botnet	Botnet Drone	14,167,432	20.77
3	Vulnerabilities	Vulnerable NTP	12,743,539	18.68
4	Vulnerabilities	Open Resolver	11,239,636	16.48
5	Vulnerabilities	Open SSDP	5,567,411	8.16
6	Vulnerabilities	Open NetBIOS	2,615,348	3.83
7	Vulnerabilities	Open SNMP	2,221,945	3.26
8	Vulnerabilities	FREAK	943,198	1.38
9	Vulnerabilities	Open IPMI	747,316	1.10
10	Vulnerabilities	Open NAT PMP	655,291	0.96
11	Vulnerabilities	Open MsSql	536,055	0.79
12	Malware	Malicious Url	393,207	0.58
13	Information Gathering	Scanner	102,167	0.15
14	Vulnerabilities	Open Chargen	74,650	0.11
15	Cyber Attacks	Bruteforce	61,198	0.09
16	Vulnerabilities	Netis Vulnerability	52,457	0.08
17	Vulnerabilities	Open Mongodb	49,125	0.07

[3] According to the ICI-ROTLD data

No.	Alert class	Alert type	No. of alerts	Percentage
18	Abusive Content	Spam	40,854	0.06
20	Vulnerabilities	Open QOTD	35,252	0.05
21	Vulnerabilities	Open Redis	19,267	0.03
22	Fraud	Phising	11,538	0.02
23	Vulnerabilities	Open Proxy	7,132	0.01
24	Vulnerabilities	Open Elasticsearch	6,365	0.01
25	Botnet	Botnet C&C Server	3,629	0.01
26	Cyber Attacks	APT	553	0.00
27	Malware	Infected IP	173	0.00
28	Compromised Resources	Compromised Router	2	0.00
TOTAL			**68,205,633**	**100.00%**

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

Alert class	Alert type	Description
Abusive Content	**Spam**	Unrequested electronic communication (email) of commercial nature.
Botnet	**Botnet C&C Server**	Information systems used for the victims' control (drone, zombie) under a botnet-type network.
	Botnet Drone	Network of infected information systems controlled by other people / organizations than their owners.
Compromised Resources	**Compromised Router**	Compromising router-type communication equipment.
Cyber Attacks	**Bruteforce**	Automatic method of breaking passwords, used in order to find out the legitimate credentials of the users of an information system. Basically, a very high number of password combinations is generated and tested through some automatic mechanisms, until the real credentials are found out. The method guarantees the success, but it is a big consumer of time and resources.
	DDoS	An DdoS-type (Distributed Denial of Service) attack is an attack that targets the interference with or even the interruption of internet exposed services (websites, servers, etc.).
	APT	Cyber-attacks with a high level of complexity, launched by groups that have the required capacity and motivation to persistently attack a target, aiming to obtain some benefits (usually access to sensitive information).
Fraud	**Phishing**	A form of online scam that consists in the use of techniques for manipulating the identity of some people/organizations, aiming to obtain material advantages and confidential information.
Information Gathering	**Scanner**	Systems that can whole IP classes on the internet, so as to identify vulnerable systems which could subsequently become targets of a cyber-attack.

Alert class	**Alert type**	**Description**
		The scanning stage is the first stage of most cyber-attacks.
Malware	**Infected IP**	Information systems / services with a role of infection vector for other information systems. The systems / services are basically hosting, with or without the administrator's will, various types of malware that can infect other legitimate users.
	Ransomware	Ransomware is a software that blocks the access to the files stored in an information system, requiring the payment of an amount in exchange for regaining access to such files.
	Malicious URL	Compromised sites, most of the times without the administrator's consent, which host various types of malware, thus facilitating the infection of other legitimate users who visit the respective links.
	Dyre/Dyreza	Dyre is a malware similar to the well-known bank Trojan Zeus. This is installed on the user's computer and becomes active only when the user inputs his/her credentials on a specific site, most of the times in the authentication page of a bank institution. Through a man-in-the browser type of attack, the hackers inject a malicious Javascript code which allows them to steal the authentication credentials or perform unauthorized account operations.
Vulnerabilities	**Open Proxy**	Unsecured proxy servers / services, which can be used by any internet user. Such services are often used by the attackers to launch attacks to various internet targets, thus keeping their identity hidden. Proxy-type services are often used to access the internet through a single IP address, by several users or equipments.
	Vulnerable PLC	This type of alert refers to industrial control devices, of PLC type (Programmable Logic ControlleR), for which various security vulnerabilities have been identified.
	Open Resolver	Unsecured DNS servers which allow the launching of recursive DNS requests for other domains than those served by the DNS server. These are used for DNS Amplification attacks.
	Open SSDP	*Simple Service Discovery Protocol* (SSDP) is part of the *Universal Plug and Play* protocol which has been implemented in order to allow PCs to communicate with the network equipment (routers, media servers, smart TV, WiFi access point, etc.). Through the exploitation of the vulnerabilities of the *broadcast* and *multicast* transmission types of this service, malicious users can launch attacks, such as data theft, DDos, etc.

Alert class	Alert type	Description
	Open SNMP	*Simple Network Management Protocol* has been developed and implemented for the monitoring and management of network devices. The vulnerabilities of this service is especially due to the its implicit settings. Through the exploitation of the typical SNMP vulnerabilities, it becomes possible to launch attack such as DoS and buffer overflow.
	Open NetBIOS	NetBIOS constitutes an API through which the devices connected to a network can share files and printers. *Open NetBIOS* constitutes any host where this service is operational and usable.
	Open Chargen	*CHARGEN* is a testing and debugging service for the suite of protocols on the internet. *Open Chargen* is any host where this service is operational and usable.
	Open IPMI	*Intelligent Platform Management Interface* is a system interface for *out-of-band* management. *Open IPMI* refers to any host where the *IPMU* service is operational and accessible, which responds to IPMI type pings.
	Open QOTD	Any host that presents an operational and usable *Quote Of The Day* service (port).
	SSL_POODLE	The POODLE attack uses the fact that, when a secured connection attempt fails, the servers will negotiate the use of older protocols, such as SSL 3.0. An attacker who can trigger a connection error may then force the use of SSL 3.0 and the exploitation of the vulnerability.
	FREAK	A new SSL/TLS – FREAK vulnerability, acronym of Factoring RSA Export Keys. This vulnerability allows attackers to intercept HTTPS-type connections between vulnerable clients and web servers, forcing them to use the „export-grade"-type cryptography.
	Open NAT PMP	Identifies hosts that have the NAT Port Mapping (NAT-PMP) protocol active and accessible through the internet. Such services have the potential of exposing information on the clients' network.
	Open MsSql	Hosts (IP addresses) that have the MS-SQL Server Resolution service accessible through the internet. This service has the potential to expose information on the network and can even facilitate the propagation of some UDP amplification attacks.
	Netis Vulnerability	NETIS router vulnerability, which allows attackers to obtain control of the device. This may become successful when the external IP address

Alert class	Alert type	Description
		of the equipment is found out and port 53413 UDP is accessed.
	Open Mongodb	Zero-day vulnerability of the MongoDb administration tool. This allows attackers to execute a code without being obliged to authenticate.
	Open Redis	The hosts (IP addresses) that have a storage of a Redis key value type, accessible directly through the internet. The service does not have an authentication process.
	Open Elasticsearch	Any host (IP address) who seems to have Elasticsearch service accessible through the internet. Elasticsearch does not have an authentication process.
	Vulnerable NTP	Any host that presents an operational and accessible *Network Time Protocol* service (port), that answers request of *Mode 6*, respectively *Mode 7 type*.

Note: The table above contains the types of cybersecurity alerts frequently reported by CERT-RO. Although the cyber-threats series is a lot more diverse, not all types can be found in the reports received by our institution. The names of alert classes and types are kept in English language, so that the meaning would not be lost through the translation into Romanian.

4. Conclusions

Based upon the findings above, **the following conclusions can be drawn**:

- The cyberthreats and vulnerabilities targeting the national cyberspace continue to become more diverse, aspect highlighted by the fact that, in 2015, CERT-RO has introduced new types of alerts;
- Most collected alerts refer to vulnerable information systems (inadequately configured or unsecured) and to information systems which are infected with various types of botnet malware;
- Any of the two information systems mentioned above can be used as an interface (proxy) for the running of attacks on targets outside the country, thus representing potential threats to other internet connected systems;
- The household network devices or equipment (e.g. wireless routers) or the ones which are part of the Internet of Things (IoT) category (web cameras, smart TV, smartphone, printers, etc.), once connected to the internet, become a target for the attackers, and their vulnerabilities are exploited by them so as to compromise the network they are connected to or to launch attacks on other targets on the internet;
- Some Romanian entities have been the target of some directed and complex cybernetic attacks of APT type (Advanced Persistent Threat), launched by groups which have the required capacity and motivation to persistently attack

a target in order to obtain some benefits (usually access to confidential information);

- Romania is both a country that generates cybersecurity incidents, and a (transit) proxy for the attackers from outside the national territory, in terms of using vulnerable or compromised information systems which are part of the national cybernetic space.

Despite the technical aspects which make it impossible to identify the exact number of affected devices or people which are behind the over 2.3 mil. IP addresses or 68 mil. alerts reported at CERT-RO, it is important to remember that they cover approximately 26% of the national cybernetic space (in relation to the number of IPs assigned to RO), and, consequently, it is necessary to take measures to solve the situation through the involvement of all actors with technical or legal responsibilities.