Report on Cyber Security Alerts Processed by CERT-RO in 2014

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

The objective of this report is to analyze cyber security alerts collected and processed by CERT-RO in 2014, in order to obtain an overview of the relevant events to risk assessment on cyber security IT infrastructure and electronic communications in Romania, located within the competence of CERT-RO.

During the reporting period, i.e. 01.01 - 31.12.2014, CERT-RO received notifications (alerts) as follows:

- Total number of alerts processed: 78.769.993 (automatic: 78.767.749, manually collected alerts: 2.244)
- Total number of unique IPs extracted from all alerts: 2.481.648

Total number of unique IPs allocated to organizations in Romania is 10.021.888, decreasing from 2013 when there were 13.5 million. By cyber security alert, in the context of this document, we mean any signal containing an IP address or a URL (website), concerning a possible cyber security incident or event, that involves or may involve systems that belong to legal or non-legal persons part of the national cyberspace.

Based on data collected, we identified the following:

- 24% of all unique IP addresses allocated to Romanian cyberspace (2.4 million) were involved in at least one cyber security alert processed by CERT-RO. In 2013, 16% (2.2 million) of unique IPs assigned to the national cyberspace have been involved in at least one cyber security alert.
- 54% of the received alerts targeting systems configured improperly (misconfigured), insecure or vulnerable, providing various insecure services over the Internet, were used by attackers to conceal their identity and launch cyber-attacks on other targets. In most cases, these systems are not compromised, their simple use is enough (ie DNS open resolver, open SNMP, NTP open, etc.); this trend is observed by the increasing number of alerts that have targeted business type network equipment (routers, firewalls, etc.) or home user (wireless routers, webcams, smart TV, smartphone, etc.) as against to other operating systems, increase highlighted in subsection 3.1.4.
- 46% of alerts target systems in Romania, victims of attackers who managed to takeover resources in botnet networks (zombie) by exploiting technical vulnerabilities and infect systems with various types of malware. Botnet networks represent the most important problem existing in national cyberspace

because these compromised computers can be used in the development of cyber attacks on other targets in Romania or from the outside of our country.

- 10.759 .ro domains have been reported to CERT-RO as being compromised during the year 2014, a 5% increase as opposed to 2013, during which 10.239 domains were reported. From 710.000 domains registered in Romania in December 2013, the number represents about 1.5% of all .ro domains.

Types of alerts processed by CERT-RO

CERT-RO collects data regarding cyber security incidents, events or alerts from several sources, as follows:

- Alerts collected and transmitted via automated systems (eg: honeypots). Those types of alerts are sent only by specialized organizations, such as CERT's or other security companies, which have in their possession cyber security incident detection systems. The number of these kinds of alerts is significantly higher than other types and can reach values around 500,000 daily alerts.
- Individual alerts, reported by various entities – individuals or legal persons from Romania and abroad. The number of this kind of alerts reaches 5-10 daily;
- Information collected by CERT- RO, from various sources. These sources includes various information collected from public or restricted sources, such as specialized websites or security companies, about specific vulnerabilities, cyber security threats or incidents.

The nature of the reported alerts, as well as the quantity of available data for each of the categories requires a different approach for each case.

Alerts sent by automated systems require automatic processing. In this case, the received data it resumes to lists of IPs detected as doing malicious or suspicious activities over the Internet, and some extra details about the suspicious activity (timestamp, incident type, used ports, the attack etc.).

Most of these alerts are automatically processed by CERT-RO and are sent to the ISPs who own the networks that contain the system which triggered the alert. Most of the time, in this type of alerts, CERT-RO has no exact information about the real user behind the IP address, so the identification process is passed to the internet service provider (ISP). Also, the ISP has the responsibility to forward the alert to the real client.

Although this type of alerts does not provide details about the target, they provide an overview of the types of cyber threats that are affecting Romanian cyber infrastructures. Individual alerts as well as the alerts collected by CERT- RO, are considerably reduced in number, but the reported information about the incident is much more accurate and relevant (the affected organization, the source of the attack and the vector of attack).

In most of the cases, the data is collected by CERT-ROs analysts from the affected entities, along with incident reporting. Statistically speaking, these types of alerts are valuable, because they reflect better the state of national cyber security.

Statistics based on incoming alerts

The number of alerts received by CERT-RO in 2014 has increased by 82% (78.767.749) as opposed to 2013 (43.231.149), the increase being displayed in the table below.

Fig. 1. Evolution of the number of alerts received 2013/2014

Distribution of alerts based on type

The table and graph below render the distribution of the top 5 types of alerts received.

Table 1. Distribution of alerts based on type

No.	Alert type	Number of alerts	Percentage
1	Vulnerabilities	42.146.259	53.51%
2	Botnet	35.657.806	45.27%
3	Information Gathering	465.288	0.59%
4	Malware	284.158	0.36%
5	CyberAttacks	160.304	0.20%

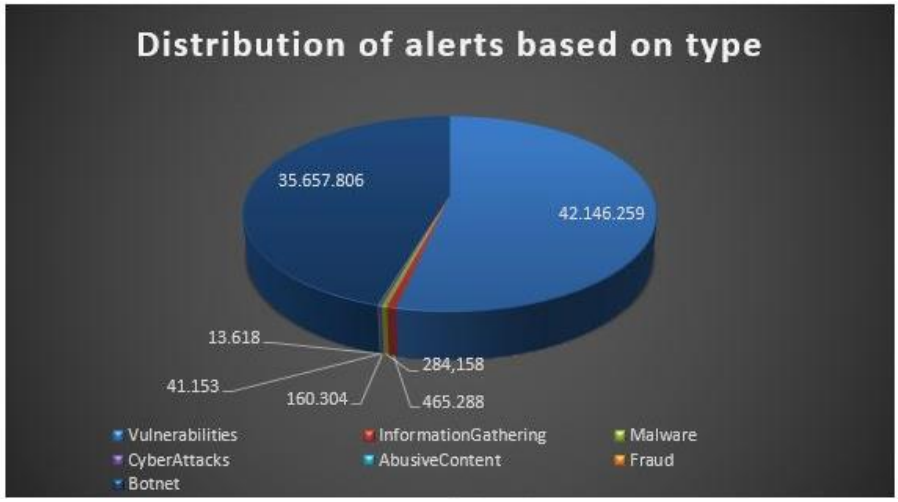

Fig. 2. Distribution of alerts based on type

Types of malware present in the Romanian cyberspace

Identification of the type of malware was possible in 37.5% of the received alerts.

Table 2. Top 10 malware types present in Romania - 2014

No.	Malware type	Percentage
1	Downadup	10.79%
2	Zeus	8.73%
3	Sality	4.55%
4	Virut	3.30%
5	Zeroaccess	2.94%
6	Irc-bot	2.13%
7	Troj-bankpath	1.98%
8	Gameoverzeus	1.14%
9	Gamarue	0.94%
10	Dorkbot	0.89%

Types of systems affected by alerts

Identification of the operating system was possible in about 24.6% of all alerts.

Table 3. Partitioning total alerts per types of affected operating systems

No.	Malware type	Percentage
1	Linux	8.68%
2	Cisco	5.69%
3	OS 1.0 UPnP (household devices with SSDP) (eg: routers, web camera, printers, smart TV etc.)	3.87%
4	Unix	3.53%
5	Windows	2.23%

Particularities of manually processed alerts

Along with automatic alerts, during the given period, CERT-RO analysts have taken a series of cyber security alerts directly reported by individuals or organizations from Romania or from abroad, classified as manually processed alerts.

They are considerably fewer than those received automatically, but contain more complete and relevant information about the incident, about the organization affected, like the source of the attack and the method of attack. In most cases, the data is collected from affected entities (legal or non-legal persons from Romania or abroad) by CERT-RO analysts, once the incident is reported.

Thus, during the referenced period, CERT-RO collected 2244 manually processed alerts, distributed as follows:

Table 4. Distribution of the alert types

No.	Alert class	Alert type	Percentage
1	Malware	Infected IP	40%

No.	Alert class	Alert type	Percentage
2	Malware	Malicious URL	22%
3	Fraud	Phishing	12%
4	Information Gathering	Scanner	11%
5	Cyber Attacks	Exploit Attempt	6%

The remaining 9% of manually processed alerts fall into different classes and types of alerts such as botnets, spam, defacement, brute force, malware samples or dissemination of confidential data (disclosure of confidential data).

The table below retrieves top 5 most affected types of systems, extracted from the manually processed alerts by CERT-RO.

Table 5. Partitioning manually processed alerts based on types of affected systems

No.	Type of affected systems	Percentage
1	Networking / Information Systems	34%
2	Websites	28%
3	Workstations	26%
4	Services of banking / payment type	5%
5	Network equipment	3%

.ro compromised domains

For the given period, CERT-RO received alerts about 10.759 .ro compromised domains. From 710.000 domains registered in Romania in December 2013, the number represents about 1.5% of all .ro domains.

Distribution of areas affected by the type of incident can be found in the table below:

Table 6. .ro compromised domains

No.	Category	Number of websites
1	Phishing	2,164
2	Malicious URL	8,037
3	Defacement	558
	TOTAL	10,759

Conclusions

Following the above findings, the next conclusions can be drawn:

- cyber security threats on national cyberspace continues to diversify;
- most of the received alerts are related to infected systems with various malware forms that are part of different botnet networks and computer systems configured improperly (misconfigured) or unsecured;

- either of the two types of the above mentioned systems can be used with the role of "proxy" for carrying out other attacks on targets outside the country, thus representing potential threats to other systems connected to the Internet;
- network devices and household equipment (wireless routers) or devices that are part of the Internet of Things (IoT) (webcams, smart TV, smartphones, printers, etc.), when connected to the Internet, are the targets of attackers and their vulnerabilities are exploited by attackers to access the network in which they are used or to launch attacks on other targets in the Internet;
- entities in Romania have been the target of complex targeted attacks called APT (Advanced Persistent Threat) launched by groups that have the ability and motivation to persistently attack a target in order to obtain certain benefits (usually access to sensitive information);
- Romania can no longer be considered just a generating cyber security incidents country, analysis of present data showing the intermediate / transit nature of connected systems that are part of the national cyberspace.

Despite the technical aspects that make it impossible to identify the exact number of devices or people affected that are behind the over 2.4 million IP addresses or 78 million alerts reported to CERT-RO, it is important to remember that these cover about 24% of the national cyberspace (reported on the number of IPs assigned to RO) and, therefore, there are remedial measures necessary, involving all entities with technical or legal responsibilities.