CERT-RO

ROMÂNIA
1918-2018 | SĂRBĂTORIM ÎMPREUNĂ

Evolution of the Cyber Threat Landscape 2017

Summary

The present report is the result of the analysis of the information collected and processed by CERT-RO in 2017. Compared to the last year's report, CERT-RO researchers added an analysis on global trends and global threat evolution.

This report was developed using several internal sources: analysis of the notifications received at alerts@cert.ro, alerts collected and processed automatically (feeds), information and reports received from partners, public reports of global cyber security companies. It addresses managers and experts in cyber security from public and private organizations from Romania, but also policy makers, researchers, NGO and citizens.

The report presents a birds' eye view of the threats and vulnerabilities from the national cyberspace and recommendations for the consolidation of prevention and reaction capacities. The information can be used to define public policy initiatives, organizational procedures or to increase the overall protection of individuals.

Ch.1

Context.

The evolution of the threat landscape and policies in the field of cyber security

2017 was very dynamic concerning cyber threat evolution, considering both attacks[1] with a high impact on essential services and attacks resulting in major data breaches[2]. On top of this, a series of accusations were formulated regarded the usage of online environment to influence democratic processes from several national states, focusing on election campaigns.

The threats, vulnerabilities and risks from cyberspace have been more mediatized than ever, as attacks multiplied and became more sophisticated. In the same time, the number of devices connected to the internet is growing exponentially from around 23 billion in 2018 to 75 billion in 2025, while electronics producers are launching daily new IoT products.

Given the context, the cyber security product market is growing exponentially as well, sustained by increased levels of cybercrime and data loss. The market is projected to grow by two-digits YoY for the next years[3].

Therefore, states and international organisations have intensified their efforts to regulate and develop prevention and mitigation capabilities.

The European directive concerning measures for a high common level of security of network and information systems across the Union and the General Data Protection Regulation, which will start producing effects this year, will determine organizations affected by the two to adopt precise measures, technical and governance related, to increase the level of cyber security and to protect user personal data.

The NIS Directive stipulates minimum security measures and major incident notifications for essential service operators from 7 industries: energy, transportation, banking, water, financial market infrastructure, digital infrastructure and health, while **GDPR** applies to all organizations that work with user's private data. Both regulations are expected to radically change company and user culture regarding personal data and cyber security.

The EU Strategy on Cyber Security is in a revision process and a new legislative project is at negotiation stage. The package considers consolidation of ENISA, European Network and Information Security Agency and the introduction of pan-European certification scheme for cyber security products, having the purpose of increasing consumer confidence on one side and the elimination of certification fragmentation across EU countries on the other.

In 2017 CERT-RO processed cyber security alerts covering 2.89 million unique IPs, or 33.71% of the total number of IPs from Romania. However, this is not the whole image, as Romania still misses a legal framework to define the way information is collected regarding national cyber infrastructure. Therefore, the data was marginally collected from information received locally.

Global trends regarding threat diversification and vulnerabilities have been mirrored in the Romanian cyberspace as well, therefore in 2017 CERT-RO introduced new alert types.
Most of the processed alerts (83.63%) involve vulnerable systems (out of date, unsecured or misconfigured), indicating a relatively low level of cyber security culture among Romanian users. 10.32% involve compromised systems or systems infected with various malware types (most often botnet).

Any of the two systems mentioned above can be used as proxy or infrastructure for international attacks, thus representing a potential threat for other systems connected to the internet.

Therefore, the increase in home-use network equipment (routers) and IoT devices (webcams, smart TV, smartphone, printers) connected to the internet becomes problematic while becoming a target for cyber criminals. The vulnerabilities of such devices are usually exploited to compromise the network they are part of or to launch attack on other Internet targets.

Romania is both a country generating cyber security incidents, but also a proxy country for attacker outside national cyberspace, given the use of vulnerable IT systems in Romania.

Ch.2 Global evolution of cyber threats

This section analyses the 5 main types of cyber threats encountered in 2017: malware, ransomware, botnets, DDoS and phishing. These threats can also be found in ENISA's report[5] regarding 2017 threat landscape.

2.1 Malware

Malware remains one of the most important cyber threat and scores a constant upward path regarding technological complexity and diversification.

Facts and trends

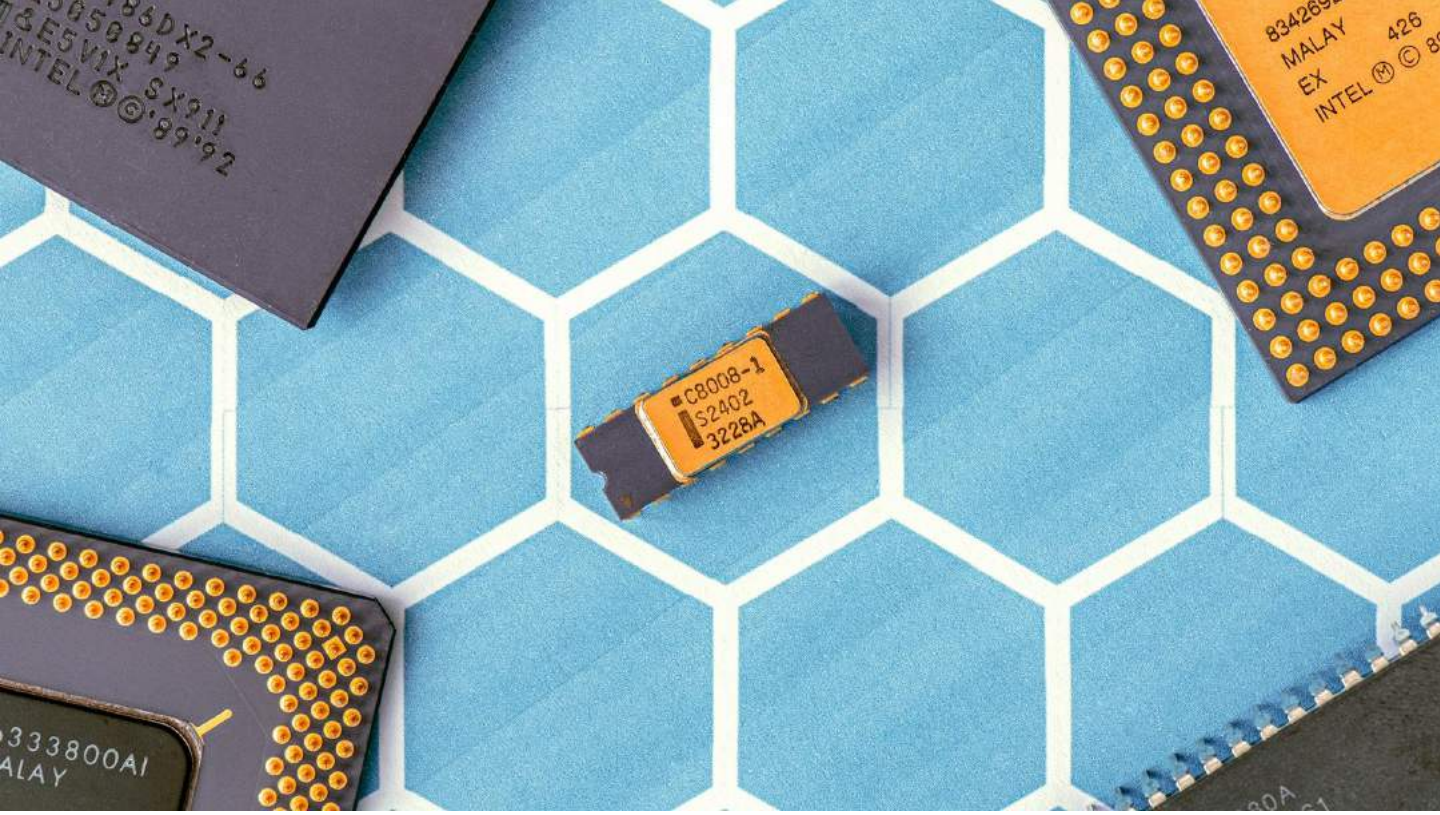
- **RAM-resident malware (fileless)[6]** – attackers are gearing towards malware that doesn't leave traces on memory disks. It is difficult to investigate through classic tools and methodologies. The malware operates just in the RAM memory, its components becoming very volatile.

- **Living off the land[7]** – more and more attacks use malware resulted through combining pre-installed software tools in the target systems: PowerShell, PSExec, WMI, etc. Thus, attacks become harder to detect because those tools are designed to perform legitimate activities on operating systems. NotPetya[8] campaign in 2017 is a relevant example.

- **Clickless** – Due to increased efforts to raise awareness on cyber security threats among individual users, attacker are starting to use infection mechanisms that don't regard any action from the user. The number of cases where infection was possible only through accessing a web page or through automated spread through the network (Worm capabilities) is on the rise. The WannaCry[9] campaign is a relevant example of clickless malware.

- **Malware targeting MAC OS –** Contrary to the general belief that Linux/Unix operating systems are not affected by malware, more and more types of malware specifically designed for MAC OS X have been traced. Moreover, in 2017 the number has doubled[10], highlighting a tendency for attackers to target these systems, sustained by the increased market share of this OS.
- **Exploitation of hardware or firmware vulnerabilities –** the discovery of more and more vulnerabilities led to the spread of malware exploiting[11] them. A recent example is the discovery of Spectre and Metdown[12], known as "side-channel"[13] vulnerabilities.

- **Supply chain attacks –** Attackers observed that sometimes it is more efficient to compromise production, supply or distribution mechanisms for hardware and software, both to target certain systems or to target as many users and companies. One such example is the insertion of malware in a widely used software tool for mass infection. One of the most relevant cases last year was CCleaner[14]. Other campaigns targeted software update tools (like M.E.Doc[15]) or firmware-level[16] malware (BIOS, UEFI).



Prevention and response measure

CERT-RO recommends

- The usage of antimalware products or technologies that can cover all the IT units of the infrastructure: fixed and mobile work stations, mobile devices, servers (files, data bases, email, web, etc)
- Continuously updating of all infrastructure components: OS, applications, network equipment, security solutions
- Ensuring a high level of IT network visibility, using solutions that automatically detect anomalies or suspect activities, such as malware infection activities.
- Development and implementation of efficient procedures and adequate capabilities to respond to cybersecurity incidents, including malware infections.
- Adoption of malware analysis tools and information exchange platforms regarding malware and countermeasures, among which there are open source solutions such as Cuckoo[17] and MISP[18].

2.2 Ransomware

This type of malware has been heavily mediatized throughout 2017, when global campaigns were identified such as WannaCry and NotPetya.

Facts and Trends

- **Targeted attacks –** more and more attacks were directed to profitable[19] organisations from industries such as banking, ransom being set at $500.000 on average.
- **Ransomware-as-a-service** the beginning of 2017 has seen a dramatic increase of ransomware types of malware sold on the black market. Therefore, last year there was a record number of ransomware attacks and generated a record loss of above $1 billion[20].
- **Wipeware –** two of the most popular ransomware campaigns were WannaCry and NotPetya, described by a high destructive potential and fast spread mechanisms. On the other side, it was proven that the two were not designed to decrypt the files after paying ransom, rather to generate a high disruptive impact[21].
- **Medjack –** researchers discovered an increase of ransomware attacks on medical devices. This is due to the tendency to interconnect classic IT systems with special destination ones, OT type (Operational Technology). Moreover, the health industry in general has become one of the favorite targets of ransomware attacks[22].

Prevention and response measures

CERT-RO recommends:

- Implementing anti-malware protection measures
- Accesing CERT-RO's publication "Guide regarding protection against ransomware"[23]
- Increased focus on developing procedures and solutions for important data, this being the most efficient strategy to limit the effects of a potential malware attack

2.3 Botnets

Botnet threats still posts serious problems, as 2017 has been a record considering DDoS attacks bandwidth (over 1Tbps). These attacks unfolded with IoT botnets.

Facts and Trends

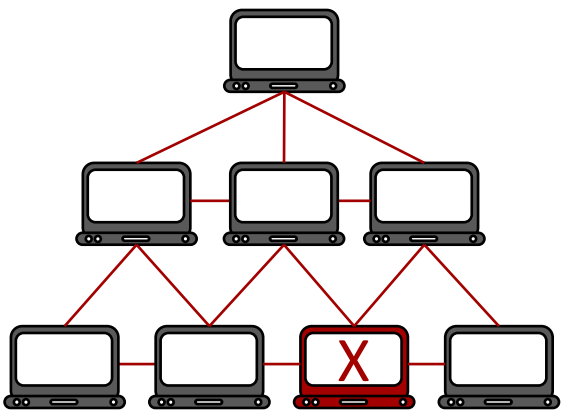
- **Migration to IoT devices** – studies show that botnets have a tendency to migrate towards personal IoT devices . These devices are preferred as they are always connected to the internet, have weak security and the number of devices is increasing globally. Most well-known bots from 2017 are Mirai[24], Reaper[25] and Necurs[26], responsible for some of the largest DDoS attacks in history.

- **Virtual machines become a target[27]** – Along with the increase of cloud-based virtual machines, provided as a service by Google, Microsoft or Amazon, attackers increasingly target the breach of such machines and then include them in botnet networks. Cloud virtual machines are attractive for botnets because these tools are always connected to the internet and most of the times share common vulnerabilities, facilitating mass infection.

Prevention and Response Measures

CERT-RO recommends

- Implementation of anti-malware security measures presented in this report.
- Using Next Generation Firewall
- Using security solutions specific to different services: email (Email Gateway), web (Web Gateway), webserver (WAF – Web Application Firewall) etc.
- Implementing traffic filtering solutions such as IP/URL “blacklisting”



2.4 DoS/DDoS

Denial of Service attacks are used by attackers to target the availability of IT systems or for disruption of a service provided through IT systems. Usually such as attack floods the targeted system with network-level requests in order to overcharge the system, which in turn will net be able to respond to legitimate requests. The main targets are websites.

Distributed Denial of Service attacks are on the rise. Such an attack is different from normal DoS attack because network requests come from a large number of sources, usually part of a botnet network. Due to the large number of sources involved in generating malicious traffic, it is hard and expensive to counteract these types of attacks.

Prevention and response measures

CERT-RO recommends:

- Development and implementation of a security policy that includes detection and response to DoS/DDoS attacks
- Usage of security mechanisms and technologies against DoS/DDoS: traffic/request balancing, Firewall, usage of Access Control Lists (ACL), IPS/IDS, WAF, IDMS (Intelligent DDoS mitigation systems), anti-DDoS cloud-based services

Facts and Trends

- **DDoS attacks increased in numbers** – According to recent studies, DDoS attacks are on the rise, 33% of companies being affected, compared to just 17% in 2016

- **Pulse Wave DDoS attacks[28]** – Some attackers behind DDoS-dedicated botnet networks choose to send the malicious attack in waves, on short periods of time, to more than one target rather than a single one. Compared to the end of 2016, when 1Tbps[29] and 665 Gbps[30] attacks were registered, in 2017 bandwidths were smaller, but wider in distribution.

- **DDoS-as-a-service costs are plummeting** – According to recent studies[31], the costs of a one hour DDoS attack went as low as $4 (four), therefore affordable by a large number of individuals.

- **Cryptocurrency exchanges became a hot target[32]** – Starting from July 2017 an upward trend was started regarding DDoS attacks on online services such as Bitcoin Exchanges and on online stores that accept payment in virtual currencies .

- **Sometimes DDoS attacks conceal other types of attacks** – 53% of the victims of DDoS attacks from the first half of 2017 declared that those attacks actually covered other breaches: malware infections, data exfiltration, intrusions or unauthorised financial transactions[33].

2.5 Phishing

Phishing is an attempt of cyber criminals to obtain confidential information (access credentials to a certain system or service, credit card data, etc.) by using social engineering techniques like replicating credentials of a trusted organization or person.

The most common form of phishing is to create an almost-identical replica of a web page associated with a legitimate service (online banking, social network, webmail service) and to send e-mail to users asking them to log onto fake pages or to update personal data. All data introduced by users are collected by attackers and used for different criminal purposes: financial transactions in the name of the user, abusive takeover of online accounts, even identity theft.

Facts and Trends

- **Targeted attacks (spear phishing) –** A few years ago most phishing attacks were based on sending mass e-mails to as many recipients as possible. Lately, attacks are becoming more targeted[34], as criminals personalize the intrusion attempt depending on target profile, starting with e-mail language and continuing with details that makes the message more trustworthy for the targets: known subjects, disguise in known persons from the circle of the target

- **Phishing delivering malware –** lately phishing e-mails messages have added attachment or links that, once accessed by users, attempt to infect systems with malware[35].

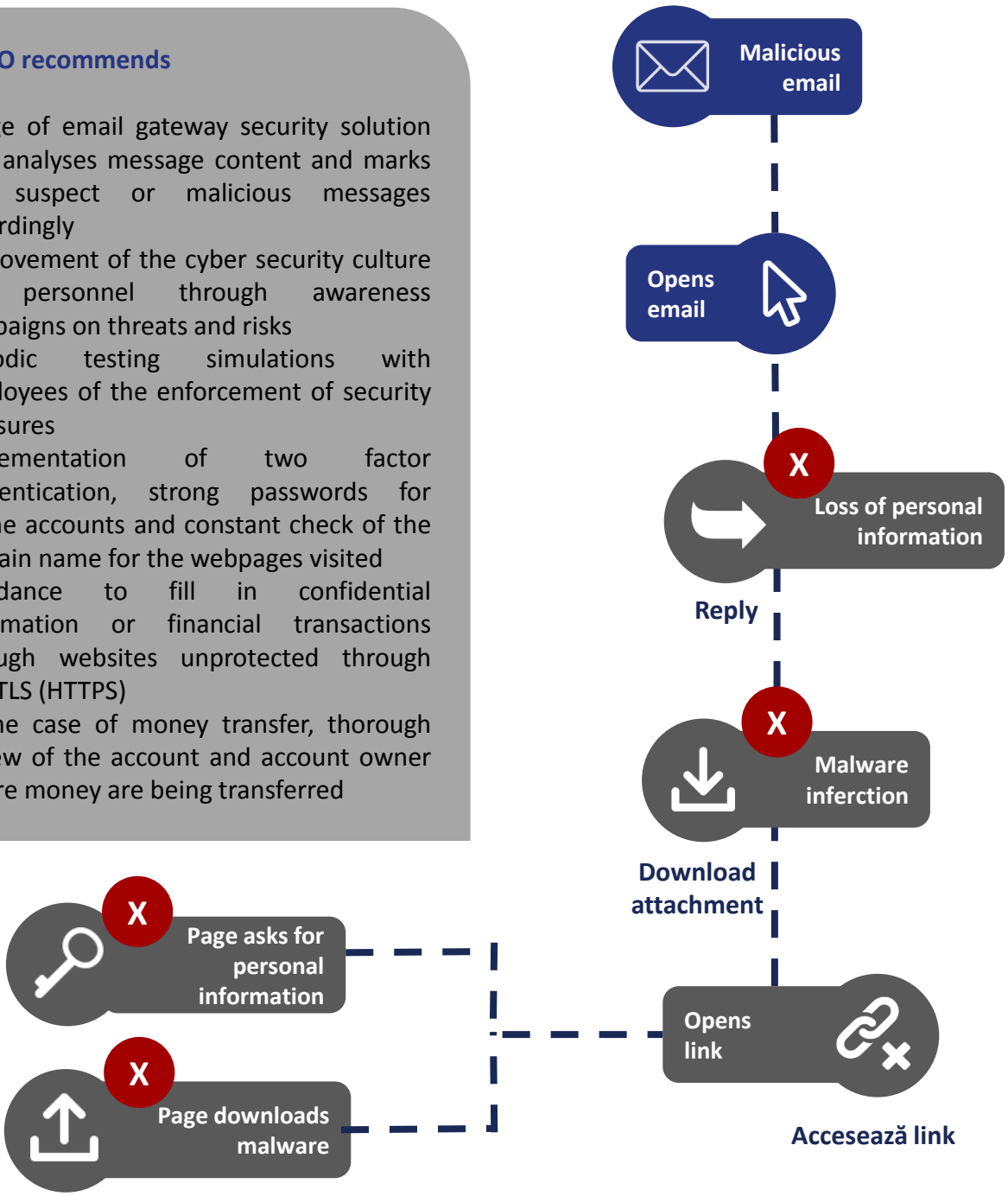
- **Usage of mechanisms that avoid detection** – In recent years efforts to counteract phishing attacks have intensified by including identified phishing pages on different black lists or even through direct warning message in the browser. Attackers therefore started to use more resources for a campaign[36] (more malicious URLs). Another technique used is to first compromise the legitimate websites and then insert phishing pages inside.

Prevention and Response Measures

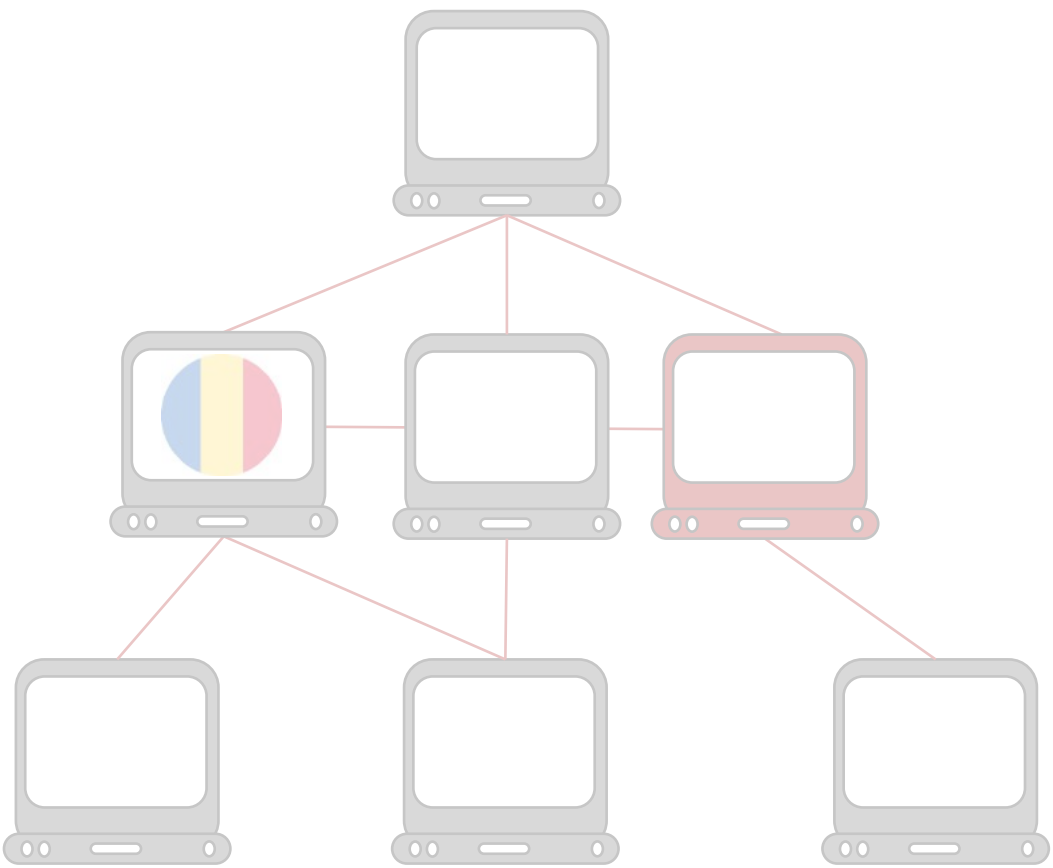
CERT-RO recommends

- Usage of email gateway security solution that analyses message content and marks the suspect or malicious messages accordingly
- Improvement of the cyber security culture for personnel through awareness campaigns on threats and risks
- Periodic testing simulations with employees of the enforcement of security measures
- Implementation of two factor authentication, strong passwords for online accounts and constant check of the domain name for the webpages visited
- Avoidance to fill in confidential information or financial transactions through websites unprotected through SSL/TLS (HTTPS)
- In the case of money transfer, thorough review of the account and account owner where money are being transferred

Typical phishing attack flow from the userțs perspective



Ch.3 Evolution of Cyber Threats in the Romanian Cyberspace



3.1 Statistics

33,71% (2,89 mil.) of the total number of unique IPs from Romania's cyberspace were involved in at least one cyber security alert processed by CERT-RO in 2017, less than in 2016 when 38,72% (2,92 mil.) were involved

83,63% (115,60 mil.) of the processed alerts account for vulnerable IT systems, meaning not updated, not secured or misconfigured, therefore being exposed to attacks that exploit such vulnerabilities

10,32% (14,33 mil.) of alerts are addressing compromised IT systems, infected with different malware types or exploited and used by criminals in different attacks and spam campaigns, most of them being registered in Realtime Blackhole Lists

5,88% (8,17 mil.) of alerts regarding IT systems infected with Botnet – type of malware, allowing criminals to remotely control infected IT systems. Compared to 2016 there is a sharp decrease from 12,81% (14,12 mil.), confirming the global descendent trend of botnet phenomenon.

1709 .ro web domains were reported by CERT-RO as being compromised, 84% less than in 2016 (10639). The number accounts for 0.18% of the total registered .ro domains in Romania as of December 2017 (944.145)37 and around 0.38% of the total number of active .ro domains (438.366)[38].

2017 CERT-RO ANNUAL REPORT HIGHLIGHTS

138M ALERTS

2.89M IPs (34%)

83% VULNERABLE SYSTEMS

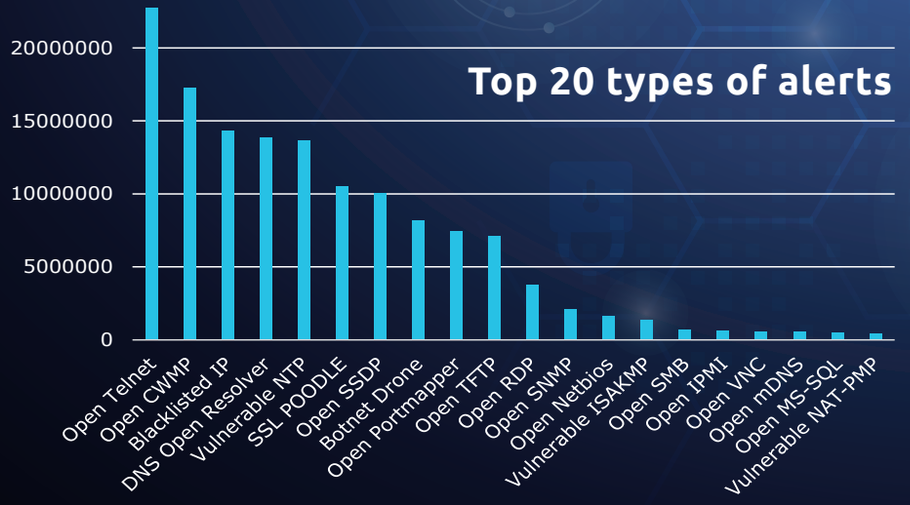
25% INCREASE IN ALERTS

1.7k .RO DOMAINS

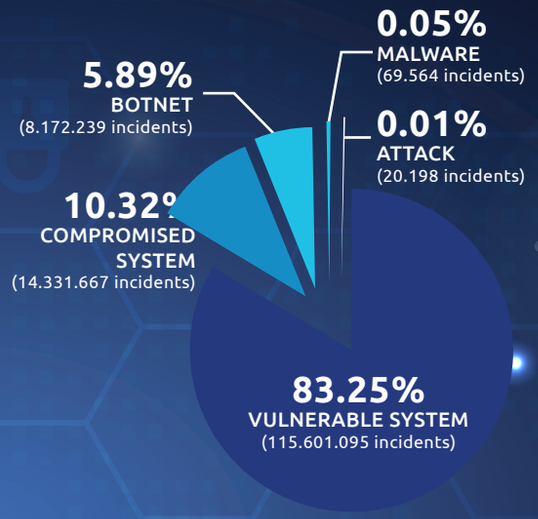
CERT-RO collected and processed 138 .217.026 alerts, an increase of 25% compared to 2016. Total number of unique IPs was 8.590.269, increasing from 7.540.736 unique IPs in 2016, in line with the upward trend of alerts received.

Number of alerts collected by CERT-RO

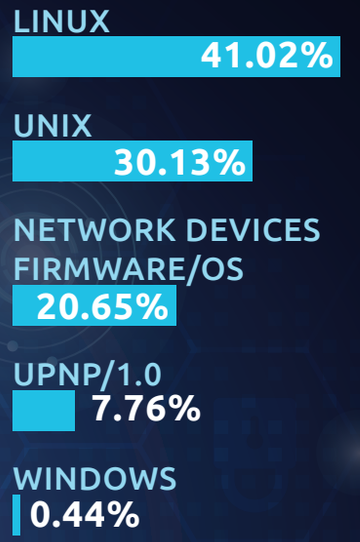
Top 20 types of alerts



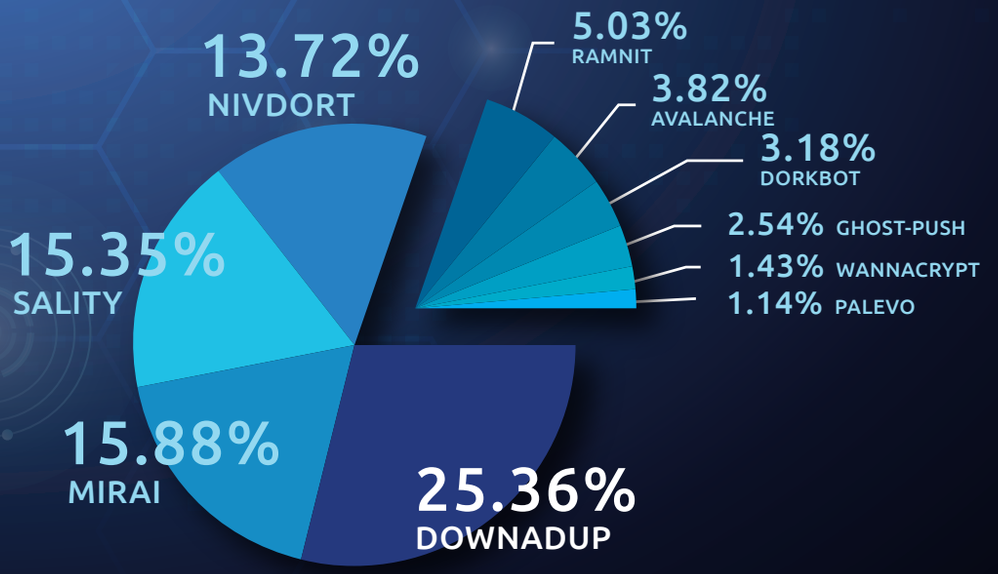
138 217 026 cyber security alerts



Types of operation systems affected



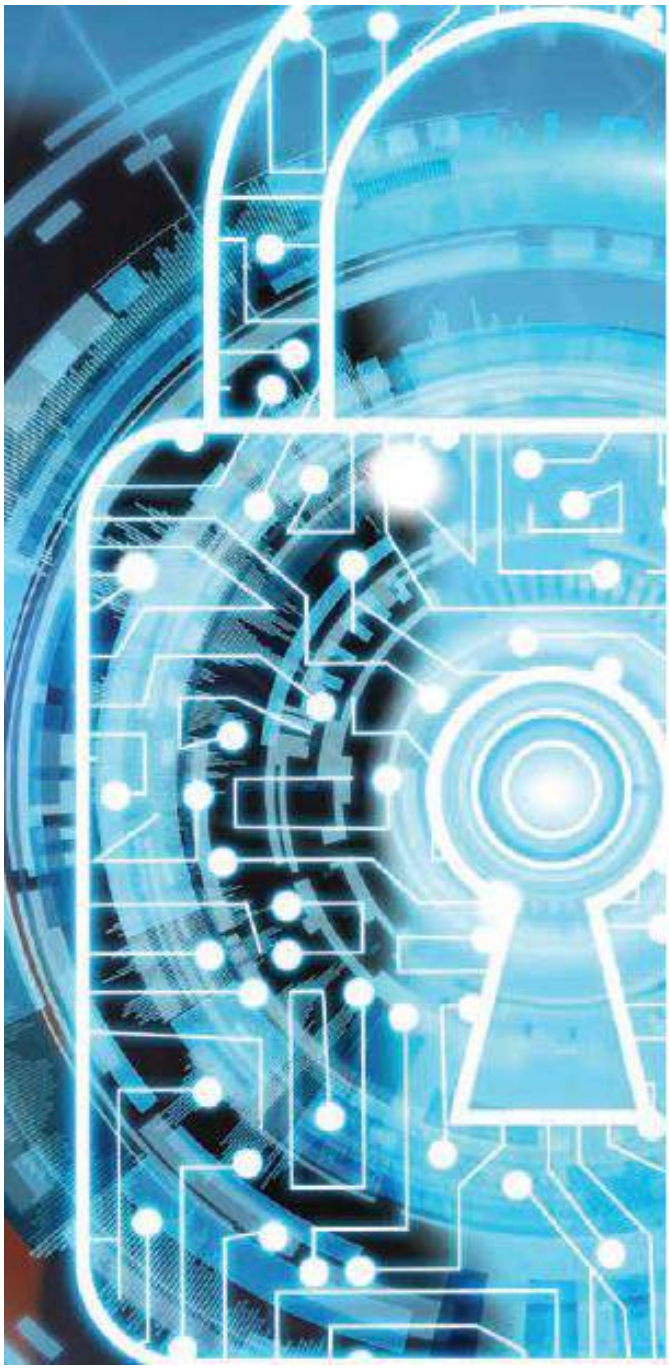
Top 10 types of malware typical to Romanian cyberspace



3.2 Main attacks

Data loss and large scale ransomware attacks have been the highlights of 2017.

Symantec indicated a 100% increase of ransomware infections in 2017, accounting for 60% of the total number of attacks in the first semester of 2017 (Malwarebytes), whine at the beginning of 2018 FBI estimates indicate around 4000 ransomware attacks per day[39].



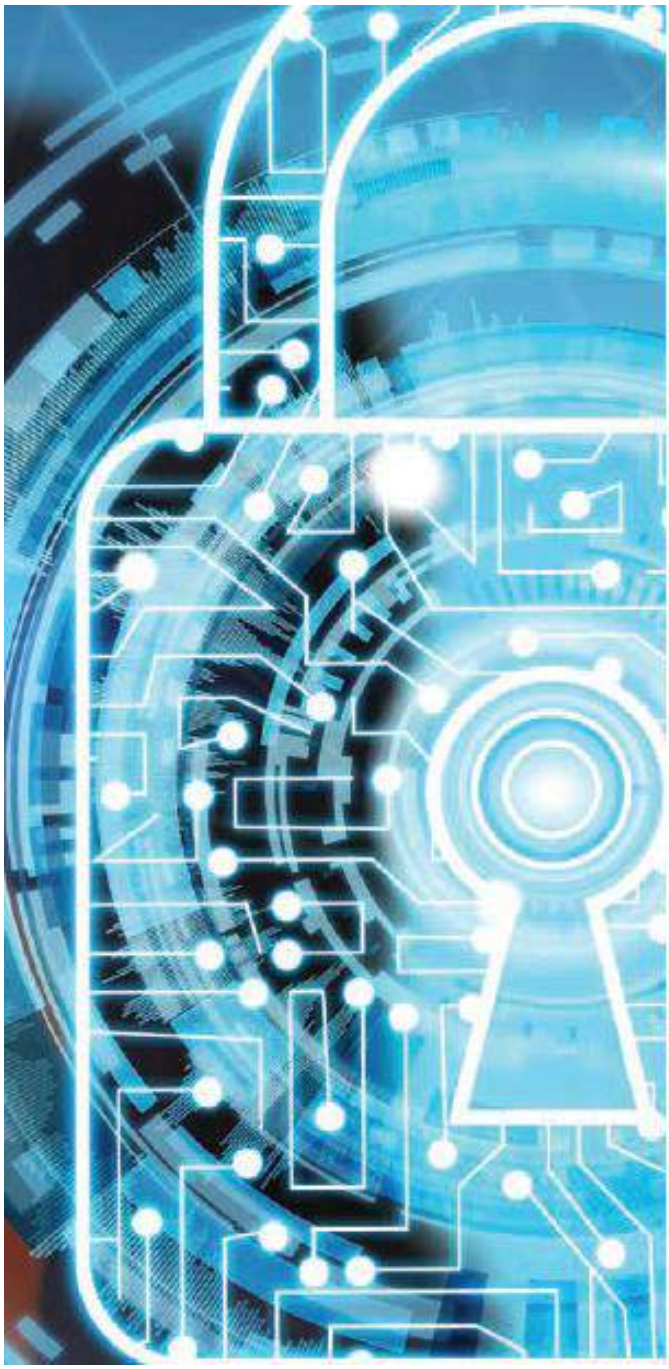
Two major campaigns kept news headlines in 2017, including in Romania: **WannaCry[40] and Petya[41]**. The two campaigns infected hundreds of thousands of systems from areas such as health, transportation, manufacturing and public administration from around 150 countries.

CERT-RO published alerts, updates and recommendations during the two campaigns in order to prevent further spread of the infection among Romanian users or to mitigate infections.

3.2 Main attacks

Data loss and large scale ransomware attacks have been the highlights of 2017.

Symantec indicated a 100% increase of ransomware infections in 2017, accounting for 60% of the total number of attacks in the first semester of 2017 (Malwarebytes), whine at the beginning of 2018 FBI estimates indicate around 4000 ransomware attacks per day[39].



Two major campaigns kept news headlines in 2017, including in Romania: **WannaCry[40] and Petya[41]**. The two campaigns infected hundreds of thousands of systems from areas such as health, transportation, manufacturing and public administration from around 150 countries.

CERT-RO published alerts, updates and recommendations during the two campaigns in order to prevent further spread of the infection among Romanian users or to mitigate infections.

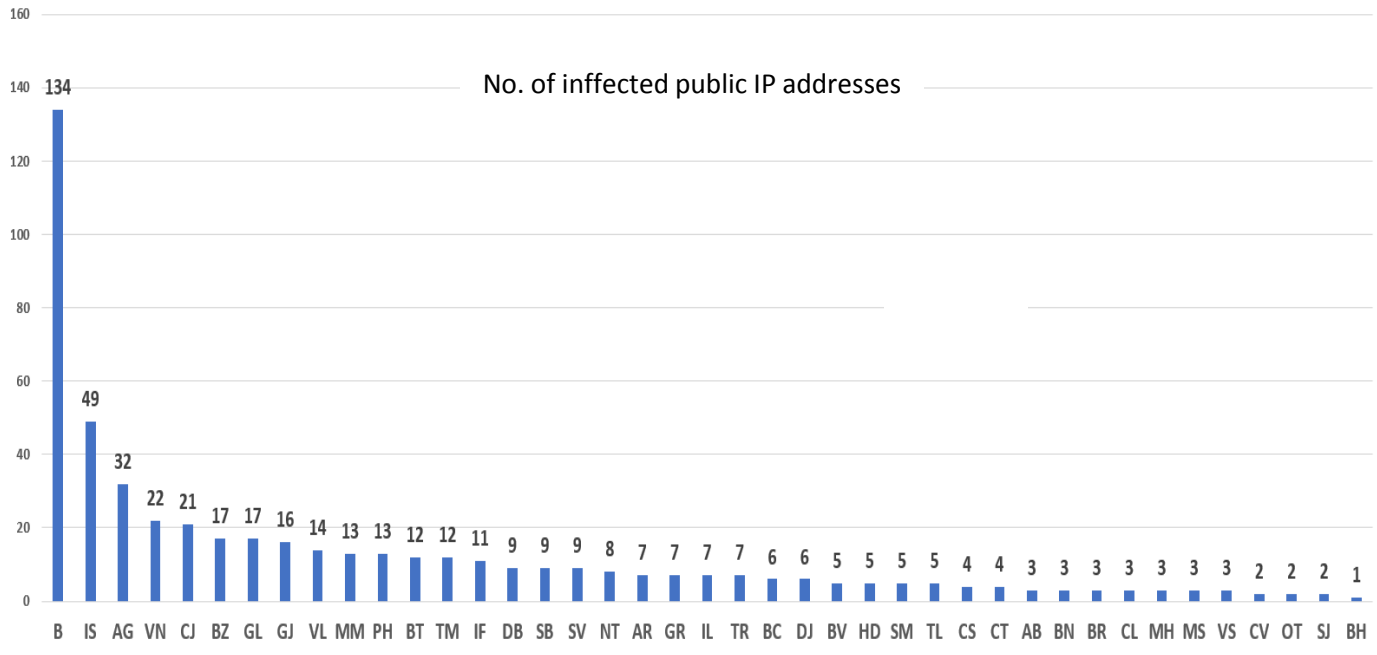
Wannacry

Starting May 12 2017, a large number of organizations worldwide have been hit by a new type of ransomware, WannaCry. Among victims were giant companies such as FedEx, Spain's Telefonica or even the National Health Service from Great Britain.

Wannacry was different that other campaigns because of its ability of lateral movement through an IT network, due to a vulnerability in the SMBv1 protocol. The threat spread through e-mail messages with malicious links or attachments. Attackers used social engineering techniques to determine users to access malicious resources.

Once a workstation was infected, the malware started to spread through the network through SMB protocol, using ports such as UDP/37, UDP/138, TCP/139 și TCP/445. Prevalence was done using the vulnerability CVE-2017-0145 of SMBv1 protocol from Windows.

In March 2017 Microsoft published a security update to solve this vulnerability, known as MS17-010. Some operating systems were passible to be infected if not updated, systems such as Microsift Windows Vista SP2, Microsoft Windows Server 2008 SP2 și R2 SP1, Microsoft Windows 7, Microsoft Windows 8.1, Microsoft Windows RT 8.1, Microsoft Windows Server 2012 și R2, Microsoft Windows 10, Microsoft Windows Server 2016, Microsoft Windows XP, Microsoft Windows Server 2003.



According to CERT-RO's data, the WannaCry campaign was followed by multiple attacks based on the exploitation of the same Windows SMBv1 vulnerability, known as Eternal Blue (CVE-2017-0145), but had different post-exploitation behavior. Worth mentioning EternalRocks (or BlueDoom), UIWIX and Adylkuzz.

Several specialists said that multiple versions of Wannacry exist, having different domains inserted in the script or without the kill switch for malware propagation. The cyber security community reported at least 2 web domains with campaign kill switch.

Wrapping up, over 300.000 computers from 150 countries were infected. Attackers received 100 payments, totaling around $26.000.

In Romania, from CERT-RO's data, 514 IPs were involved, 10 of which belonging to public institutions. In the absence of a legal framework imposing mandatory reporting of such incidents, an exact evaluation of the impact at national level is impossible. During the campaign, CERT-Ro received just 5 official notifications from Romanian organizations.

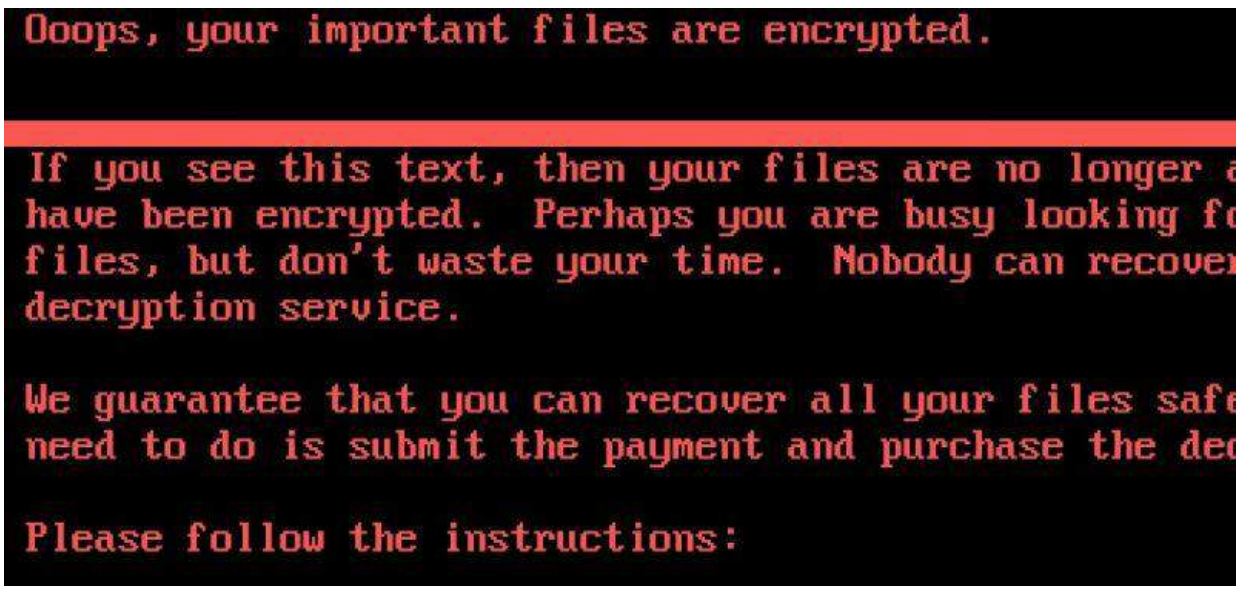
NotPetya

Starting with July 26, 2017, users and companies worldwide, but especially from Ukraine, were infected with a new type of ransomware virus called Petya, known as Petrwrap.

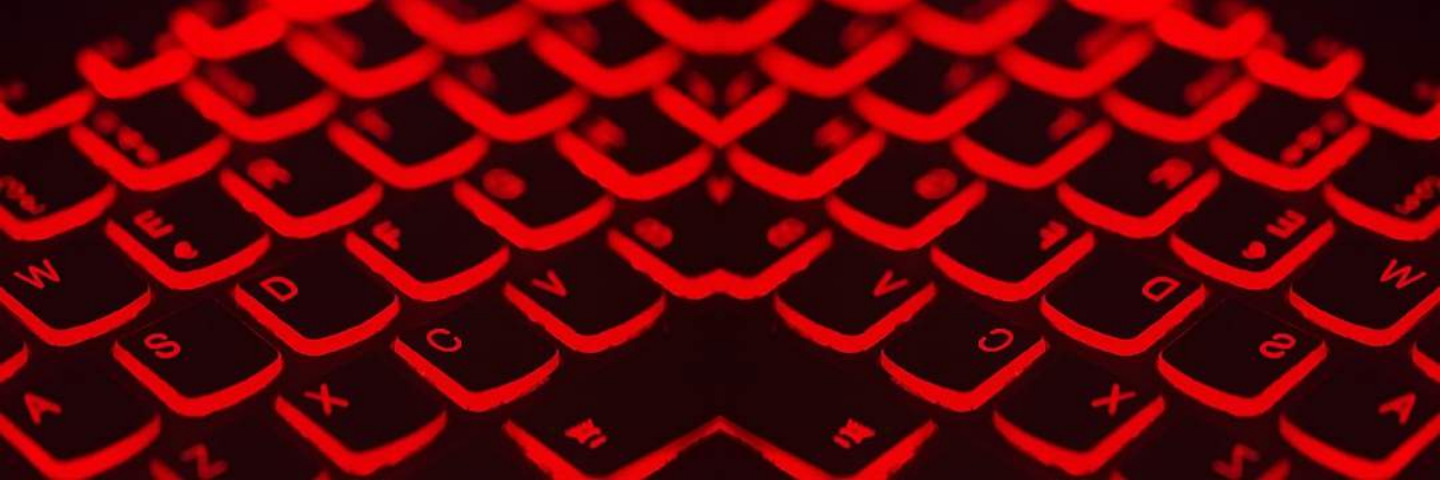
Initial infection of the systems was performed through documents attached to phishing e-mails that users were urged to open. The virus also spread through the update mechanism of MeDoc application (very popular in Ukraine). The information as confirmed through Kaspersky's blog as well.

As was the case with WannaCry, once one workstation was infected, the virus used several techniques for lateral movement inside the network where initial infection took place, using the following identification techniques of target systems:

- Identification of network hardware of the infected system
- Reading the names of other systems from NetBIOS
- Reading information linked to DHCP (lease time)
- All systems identified by the virus in nearby networks are scanned through TCP/445 and TCP/139 (used by SMB protocol) and if the ports were open it attempted to exploied the previously mentioned vulnerabilities.



Ch.4 Review of the Allerts Processed by CERT-RO



In 2017, CERT-Ro acquired and processed 138.217.026 cyber security alerts, 25% more than during 2016 (110.194.890), of which:

- **138.215.593** feeds automatically collected and processed
- **1.433** alerts processed manually, received via e-mail ticketing.

A cyber security alert, in the context of the present report, is a notice containing an IP address or a web domain (URL), regarding a potential incident or security event that might involve IT systems administered by private or corporate entities or individuals from the Romanian cyberspace.

The number of cyber security alerts is 25% higher than compared to 2016, a growth tendency in line with last 3 years.

The alerts targeted **2.896.269 unique IP addresses and 1709 .ro web domains**. The number of unique IPs allocated to Romanian organizations is 8.590.378, an increase from 2016(7.540.736), situated around 2015 levels (8.958.498[42]), but under 2014 (aprox. 10 million) and 2013 (aprox. 13.56 million) levels.

Distribution of alerts on classes and incident type

Alerts processed by CERT-RO were classified based on a taxonomy where classes and incident types were defined. An incident class represents a generic category that can accommodate more specific types of incidents). Taxonomy description is annexed to the present report.

The 5 incident classes, depending on alert frequency, are:

- Vulnerable systems
- Compromised systems
- Botnet
- Malware
- Attack

The table below covers all types of alerts collected by CERT-RO in 2017. Compared to 2016, CERT-RO processed 7 new types of alerts: Blacklisted IP, Trackbaback SPAM, Open SMB, Open VNC, Open MS-SQL, Open Memcached, Open LDAP.

4.1 Alert distribution by class and type

	Incident class	Incident type	No. of alerts	Percentage
1	Vulnerable System	Open Telnet	22.746.467	16,45707%
2	Vulnerable System	Open CWMP	17.245.057	12,47680%
3	Compromised System	Blacklisted IP	14.297.113	10,34396%
4	Vulnerable System	DNS Open Resolver	13.877.359	10,04027%
5	Vulnerable System	Vulnerable NTP	13.679.953	9,89744%
6	Vulnerable System	SSL POODLE	10.515.032	7,60762%
7	Vulnerable System	Open SSDP	10.041.893	7,26531%
8	Botnet	Botnet Drone	8.169.009	5,91028%
9	Vulnerable System	Open Portmapper	7.460.953	5,39800%
10	Vulnerable System	Open TFTP	7.105.127	5,14056%
11	Vulnerable System	Open RDP	3.799.358	2,74884%
12	Vulnerable System	Open SNMP	2.118.977	1,53308%
13	Vulnerable System	Open Netbios	1.637.249	1,18455%
14	Vulnerable System	Vulnerable ISAKMP	1.340.317	0,96972%
15	Vulnerable System	Open SMB	711.579	0,51483%
16	Vulnerable System	Open IPMI	663.362	0,47994%
17	Vulnerable System	Open VNC	606.589	0,43887%
18	Vulnerable System	Open mDNS	548.395	0,39676%
19	Vulnerable System	Open MS-SQL	530.279	0,38366%
20	Vulnerable System	Vulnerable NAT-PMP	414.407	0,29982%
21	Vulnerable System	Open Memcached	272.752	0,19734%
22	Vulnerable System	Open LDAP	119.536	0,08648%
23	Malware	Malicious URL	69.864	0,05055%
24	Vulnerable System	SSL FREAK	39.262	0,02841%
25	Compromised System	Compromised Webserver	34.651	0,02507%
26	Vulnerable System	Open MongoDB	34.304	0,02482%
27	Vulnerable System	Open Chargen	30.482	0,02205%
28	Vulnerable System	Open QOTD	21.296	0,01541%
29	Fast-Flux	Fast-Flux IP	19.327	0,01398%
30	Attack	Bruteforce	13.838	0,01001%
31	Vulnerable System	Open Elasticsearch	12.010	0,00869%
32	Vulnerable System	Unsecured Proxy	11.675	0,00845%
33	Vulnerable System	Vulnerable Netcore/Netis	6.739	0,00488%
34	Attack	Trackback SPAM	6.373	0,00461%
35	Vulnerable System	Open XDMCP	4.882	0,00353%
36	Vulnerable System	Open Redis	4.859	0,00352%
37	Botnet	Botnet C2 Server	3.265	0,00236%
38	Phishing	Phishing URL	1.184	0,00086%
39	Vulnerable System	Open DB2	945	0,00068%
40	Spam	Spam URL	933	0,00068%
41	Malware	Malware Infection	341	0,00025%
42	Attack	Scan	23	0,00002%
43	Attack	DDoS	10	0,00001%
	TOTAL		138.217.026	100%

4.2 Types of incident notifications received by CERT-RO

Beside alerts processed automatically, CERT-RO analysts have received a series of notifications for cyber security incidents reported by individuals or organizations from Romania or abroad. Although considerably less in numbers than automated alerts, information about incidents are more relevant and complete, given the clear details about the incident, the organization involved, attack source and attack method. In most of the cases data is collected by analysts from affected parties at the time the incident is reported.

CERT-RO collected **1433** incident notifications as follows

	Incident Class	Incident Type	No. of notifications	Percentage
1	Phishing	Phishing URL	673	46,96%
2	Malware	Malware Infection	341	23,80%
3	Malware	Malicious URL	239	16,68%
4	Compromised System	Compromised Webserver	97	6,77%
5	Botnet	Botnet Drone	31	2,16%
6	Attack	Scan	23	1,61%
7	Attack	Bruteforce	13	0,91%
8	Attack	DDoS	10	0,70%
9	Botnet	Botnet C2 Server	4	0,28%
10	Spam	Spam URL	2	0,14%

3.3.3. Types of malware characteristic to Romanian cyberspace

A total of 5.77 million alerts (4.16% of the total) from 2017 have information regarding malware type associated with the alert (as botnet alerts or malicious URLs).

	Malware tye	No. of alerts	Percentage
1	Downadup	1.465.355	25,36%
2	Mirai	917.580	15,88%
3	Sality	886.722	15,35%
4	Nivdort	792.761	13,72%
5	Ramnit	290.420	5,03%
6	Avalanche	220.683	3,82%
7	Dorkbot	183.568	3,18%
8	Ghost-Push	146.875	2,54%
9	WannaCrypt	82.584	1,43%

4.3 Types of affected networks

Around 15% of the total number of alerts collected by CERT-RO in 2017 have information regarding the operating system of the targeted IT system.

	OS	Percentage
1	Linux	41,02%
2	Unix	30,13%
3	Network Devices Firmware/OS	20,65%
4	UPnP/1.0	7,76%
5	Windows	0,44%

The taxonomy used by CERT-RO to classify alerts and incidents

Alert class	Alert type	Description
Abusive Content	Spam	Unsolicited electronic communication
Botnet	Botnet C&C Server	IT systems used to control victims (drones, zombies) from a botnet network
	Botnet Drone	Infected IT systems network controlled by other individuals/organizations than the network owner
Cyber Attacks	Bruteforce	Automated password break method, used to find out legitimate user credentials from an IT system. Through automated mechanisms, a high number of password combinations is generated and tested until real credentials are acquired
	Trackback SPAM	A form of Spam based on a automated distribution of a message to a domain when this domain is referenced on a external website/blog (it is usually a comment)
	DDoS	Distributed Denial of Service attacks has the scope of affecting or interrupting Internet services (websites, servers, etc)
Fraud	Phishing	A form of online extorsion by using social engineering techniques to manipulate the identity of individuals/organizations having the scope of obtaining material advantages or confidential information
Compromised System	Blacklisted IP	IP addresses registered in the blocked resource lists (Realtime Blackhole Lists – RBL), often due to having been identified as a source for attacks, malware infections or spam distribution

Alert class	Alert type	Description
Information Gathering	Scanner	Systems that scan whole IP classes from the internet to identify vulnerable systems upon which cyberattacks can be launched. Scanning phase is usually the first step in a cyber attack
Malware	Infected IP	IT systems or services that have the role of infection vector to other IT systems. Basically systems/services host, with or without the will of the administrator, various malware samples that can infect legitimate users.
	Ransomware	Ransomware is a software that blocks access to files stored on an IT system, demanding payment for access
	Malicious URL	Compromised websites, usually without administrator will, that host various types of malware and facilitating infection of legitimate users that visit the URL
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, Open SMB, Open VNC, Open MS-SQL, Open Memcached, Open LDAP*	Protocols or services that run on various misconfigured IT systems or systems or servers with out-of-date software and known security issues, usually servers.

Alert class	Alert type	Description
Vulnerabilities	SSL_POODLE	POODLE attack is defined by the switch to older protocols such as SSL 3.0 when attempting to connect through secure connection ails. An attacker that can trigger a connection error can then force usage of SSL3 protocol and vulnerability exploitation of that protocol.
	FREAK	A new SSL/TLS-FREAK vulnerability, an acronym for Factoring RSA Export Keys. This vulnerability allows attacker to intercept HTTPS connections between vulnerable clients and webservers, forcing them to use “export-grade” cryptography.
	Malicious URL	Compromised websites, usually without administrator will, that host various types of malware, facilitating legitimate user infection while visiting those links.

Note: The tables above contain cyber security alerts that are frequently reported to CERT-RO. Although the number of cyber threats is more varied, not all of them are found in the alerts and notifications processed by CERT-RO.

References

[1] *The Biggest Cybersecurity Disasters of 2017 So Far*. Wired, July 2017 - https://www.wired.com/story/2017-biggest-hacks-so-far/

[2] *Data Breach Investigations Report*. Verizon, July 2017 - https://www.wired.com/story/2017-biggest-hacks-so-far/

[3] *https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/*

[4] *The True Cost of Cybercrime for Businesses.* Forbes, July 2017 - https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/

[5] *ENISA Threat Landscape. Forbes, July 2017 - https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/*

[6] *Fileless Malware: A Hidden Threat.* TrendMicro, 2017 - https://blog.trendmicro.com/fileless-malware-a-hidden-threat/

[7] *Attackers are increasingly living off the land.* Symantec Blog, July 2017 - https://www.symantec.com/connect/blogs/attackers-are-increasingly-living-land

[8] *Alertă Petya/Petwarp ransomware! O nouă amenințare informatică vizează utilizatorii sistemelor de operare Windows.* CERT-RO, July 2017 - https://www.cert.ro/citeste/alerta-petya-ransomware

[9] *WannaCry' - Situația la zi și Wanakiwi - un posibil instrument de decriptare!.* CERT-RO, July 2017 - https://www.cert.ro/citeste/review-campanie-wannacry

[10] *Mac malware more than doubled in 2017.* Computer Weekly, March 2018, http://www.computerweekly.com/news/252436453/Mac-malware-more-than-doubled-in-2017

[11] *Hundreds Of Meltdown, Spectre Malware Smaples Found in the Wild.* Tom's hardware, February 2019 - http://www.tomshardware.com/news/meltdown-spectre-malware-found-fortinet,36439.html

[12] *Reading privileged memory with a side-channel. Project Zero, January 2018 - https://googleprojectzero.blogspot.ro/2018/01/reading-privileged-memory-with-side.html*

[13] *Spectre și Meltdown - Vulnerabilități CPU. CERT-RO, January 2018 - https://www.cert.ro/citeste/spectre-meltdown-vulnerabilitati-cpu*

[14] *Un număr semnificativ de utilizatori ai aplicației CCleaner sunt expuși riscului de a avea PC-urile infectate cu malware.* CERT-RO, September 2017 - https://cert.ro/citeste/versiuni-ccleaner-cu-malware

[15] *The MeDoc Connection.* Talos Intelligence, July 2017 - *http://blog.talosintelligence.com/2017/07/the-medoc-connection.html*

[16] *UEFI malware: how to exploit a false sense of security.* We LiveSecurity, October 2017 - https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-ransomware-actors-focusing-on-targeted-attacks-against-businesses

[17] *https://cuckoosandbox.org/*

[18] *http://www.misp-project.org/*

[19] *Kaspersky Lab identifies ransomware actors focusing on targeted attacks against businesses.* KasperskyLab, April 2017 - https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-ransomware-actors-focusing-on-targeted-attacks-against-businesses

[20] *Ransomware-as-a-Service: Rampant in the Underground Black Market.* Fortinet, February 2017 - https://www.fortinet.com/blog/threat-research/ransomware-as-a-service-rampant-in-the-underground-black-market.html?utm_source=dlvr.it&utm_medium=twitter ;

[21] *Petya.2017 is a wiper not a ransomware.* Comae Technologies Blog, June 2017 - https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b ;
ExPetr/Petya/NotPetya is a Wiper, Not Ransomware. Securelist, June 2017 - https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

[22] https://www.rsaconference.com/events/us17/agenda/sessions/4518-medjack-3-new-research-on-attacks-on-hospital
[23] *GHID privind combaterea amenințărilor informatice de tip „ransomware".* CERT-RO, March 2016 - https://cert.ro/vezi/document/ghid-protectie-ransomware
[24] *Mirai: o amenințare de tip botnet utilizată recent pentru derularea celor mai însemnate atacuri DDoS din istorie.* CERT-RO, November 2016 - https://cert.ro/citeste/mirai-botnet-ddos
[25]*The Reaper IoT Botnet Has Already Infected a Million Networks.* WIRED, October 2017, https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/
[26] *The Many Tentacles of the Necurs Botnet.* CISCO blogs, January 2018, https://blogs.cisco.com/security/talos/the-many-tentacles-of-the-necurs-botnet
[27] *Microsoft Warns that Virtual Machines Could Be Turned into Botnets.* BizTech, January 2017 - https://biztechmagazine.com/article/2017/01/microsoft-warns-virtual-machines-could-be-turned-botnets
[28] *Attackers Use DDoS Pulses to Pin Down Multiple Targets.* Imperva, August 2017 - https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html
[29] *OVH suffers 1.1Tbps DDoS attack.* SC Media, September 2016 - https://www.scmagazineuk.com/ovh-suffers-1tbps-ddos-attack/article/532197/
[30]*Hit With Record DDoS.* KrebsOnSecurity, March 2016 - https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[31]*The cost of launching a DDoS attack.* Securelist, March 2017 - https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/
[32] *Bitcoin Exchanges Under Fire.* Radware, June 2017 - https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/cryptocurrencies-trade-under-fire/
[33] *Kaspersky Lab Research Shows DDoS Devastation on Organizations Continues to Climb.* KasperskyLab, October 2017 - https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizations-continues-to-climb
[34] *2017 Phishing Trends & Intelligence Report.* Phishlab, February 2017 - https://www.phishlabs.com/phishlabs-2017-phishing-trends-intelligence-report-hacking-the-human/
[35] *New Locky Ransomware Phishing Attacks Beat Machine Learning Tools.* DarkReading, September 2017 - https://www.darkreading.com/attacks-breaches/new-locky-ransomware-phishing-attacks-beat-machine-learning-tools/d/d-id/1330010
2017 Threat Landscape Survey: Users on the Front Line. SANS Institute - https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910
New Backdoor targets Russian businesses in apparent spear phishing campaign . SC Media, August 2017 - https://www.scmagazine.com/new-backdoor-targets-russian-businesses-in-apparent-spear-phishing-campaign/article/680268/
[36] *Quarterly Threat Trends Report.* Webroot, September 2017 - https://s3-us-west 1.amazonaws.com/webroot-cms cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf
[37] Conform datelor ICI-ROTLD publicate la http://www.rotld.ro/
[38] http://viewdns.info/data/
[39] *Cyber Incident & Breach Trends Report.* Online Trust Alliance, January 2018 - https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf
[40] *'WannaCry' - Situația la zi și Wanakiwi - un posibil instrument de decriptare!, CERT-RO, mai 2017 –* https://cert.ro/citeste/review-campanie-wannacry
[41] *Alertă Petya/Petwarp ransomware! O nouă amenințare informatică vizează utilizatorii sistemelor de operare Windows. CERT-RO, June 2017 - https://cert.ro/citeste/alerta-petya-ransomware*
[42] *https://www.countryipblocks.net/allocation-of-ip-addresses-by-country.php*

www.cert.ro
+4031-6202187
cooperation@cert.ro
8-10 Mareșal Averescu Blvd., 011455 Bucharest, Romania