2017 HIGHLIGHTS

CERT-RO

ROMÂNIA
1918-2018 | SĂRBĂTORIM ÎMPREUNĂ

The 2017 report is the result of analyses on information collected and processed by CERT-RO in 2017. It is addressed to managers, cybersecurity experts from public and private institutions, political stakeholders, researchers, NGOs and the general public. The report includes the CERT-RO incidents and alerts taxonomy.

./1 CONTEXT

GDPR

EU Cybersecurity Strategy

NIS Directive

2017 was very dynamic in regard to the evolution of cyber threats, considering both cyber attacks with major societal implications and large scale data breaches. Globally, threats and vulnerabilities are becoming increasingly diverse, in part due to a rise in the number of internet connected devices.

Subsequently, national authorities and private actors are extending their mitigation and prevention efforts. The NIS Directive will be transponsed into national legislation by the end of May, simoultaneously with he General Data Protection Regulation entry into force. This implies that organisations which fall under their legislative regimes must adopt technical and organisational procedures, such as implementing minimum security measures and establishing an adequate reporting mechanism for major incidents.

./2 GLOBAL THREAT LANDSCAPE

Malware

- RAM-resident malware (fileless)
- Living off the land
- Clickless
- Malware targeting MAC OS
- Exploitation of hardware or firmware vulnerabilities
- Supply chain attacks

Ransomware

- Targeted attacks
- Ransomware-as-a-service (Raas)
- Wipeware
- Medjack – an increase of ransomware attacks on medical devices

Botnets

- Migration to IoT devices
- Virtual machines become a target

DoS/DDoS

503

- DDoS attacks increased in numbers
- Pulse Wave DDoS attacks
- DDoS-as-a-service costs are plummeting
- Cryptocurrency exchanges became a hot target
- Sometimes DDoS attacks conceal other types of attacks

Phishing

- Targeted attacks (spear phishing)
- Phishing delivering malware
- Usage of mechanisms that avoid detection

./3 NATIONAL THREAT LANDSCAPE

138M ALERTS

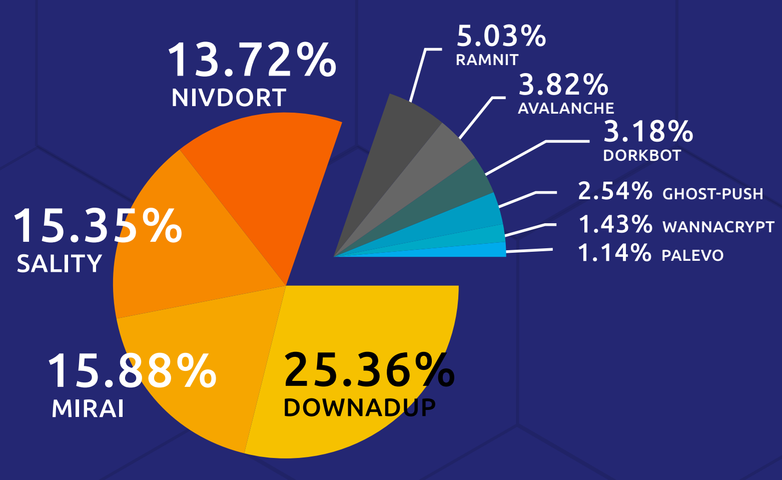
2.89M IPs (34%)

83% VULNERABLE SYSTEMS

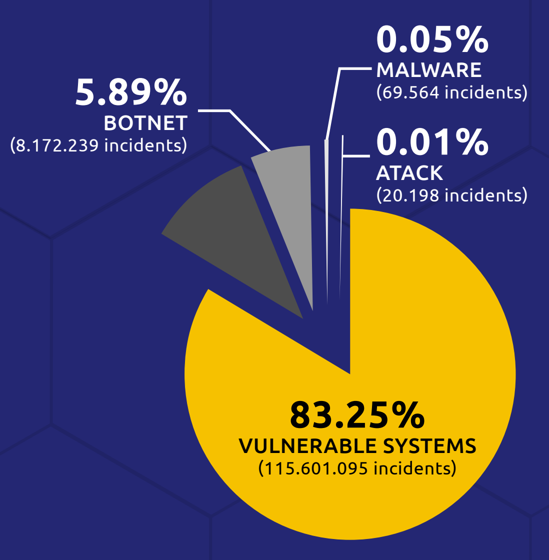
25% INCREASE IN ALERTS

1.7k .RO DOMAINS

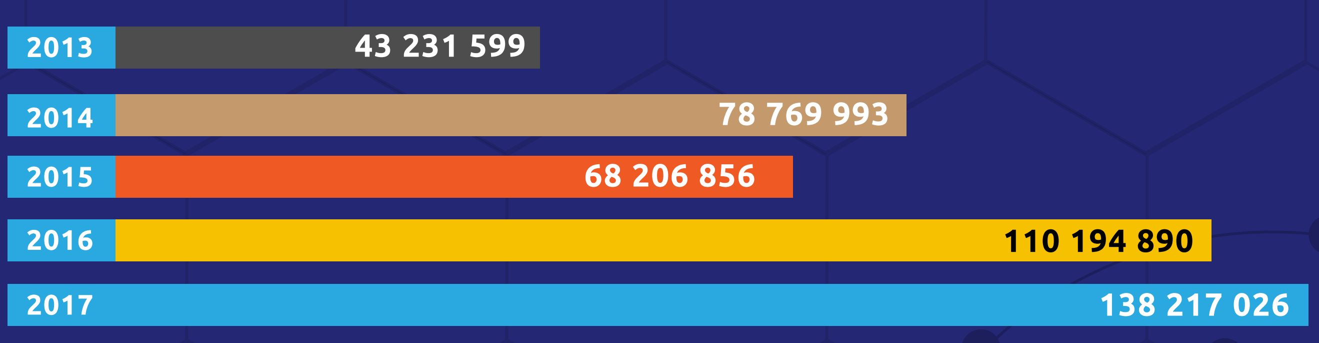
Top 10 types of malware typical to Romanian cyberspace



138,217,026 cyber security alerts



Number of alerts collected by CERT-RO



Read the full report

www.cert.ro

cooperation@cert.ro

+4031-6202187

Mareșal Averescu 8-10
011455 Bucharest, Romania