CERT-RO
Cooperation and handling incidents

Sabin Popescu
Cooperation Counselor

About CERT-RO

Proactive

- Alerts on new threats, risks and vulnerabilities that may affect cyber space
- It monitors the vulnerabilities of different technologies
- Conducts, on request, cyber security audit for public institutions

Reactive

- Alerts and warns about new cyber security incidents that have an impact on entities in Romania
- Responds to incidents and coordinates impact minimization efforts
- Investigates malware and cyber incidents

Support

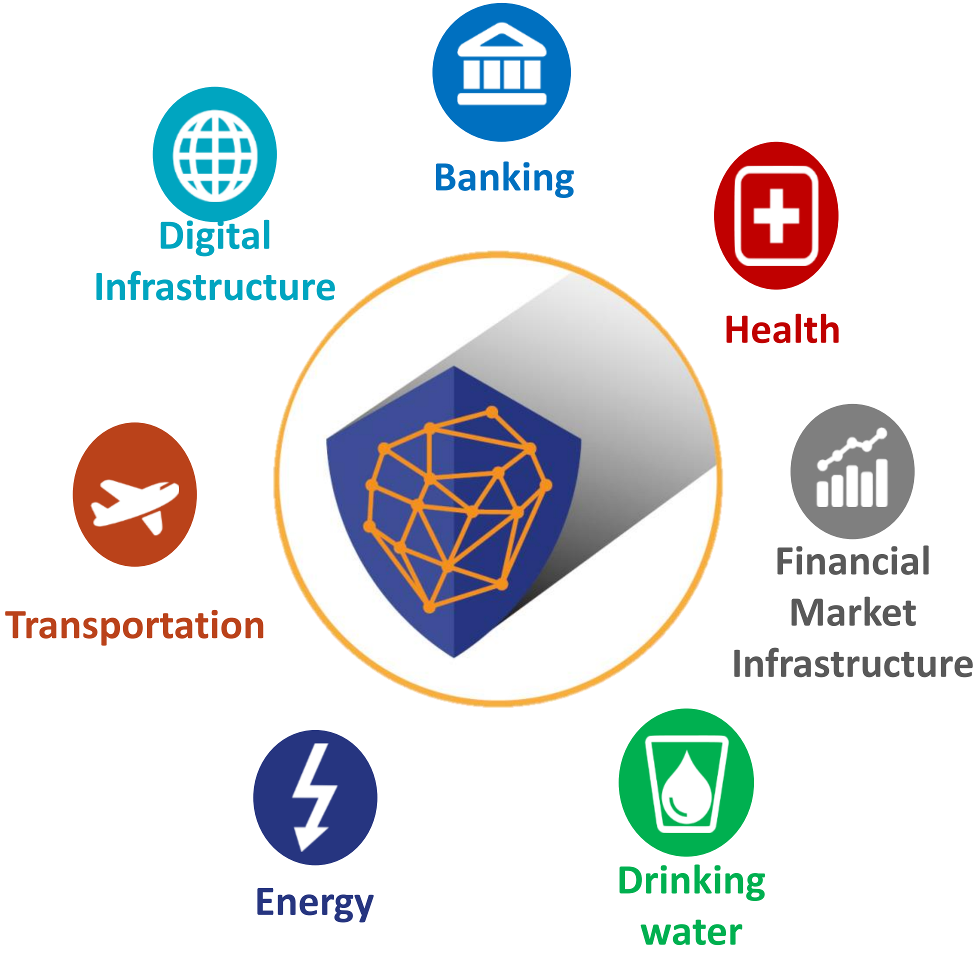
- Coordinates awareness campaigns
- Provides support to other organizations for setting up CERT structures
- Provides consulting for securing critical infrastructure
- Provides expertise for development policies, regulation and strategy development

CERT-RO is a competent authority at national level, single point of contact and CSIRT team, for the prevention, analysis, identification and response to cyber security incidents in computer networks and systems in Romania.

Follows the implementation NIS Directive

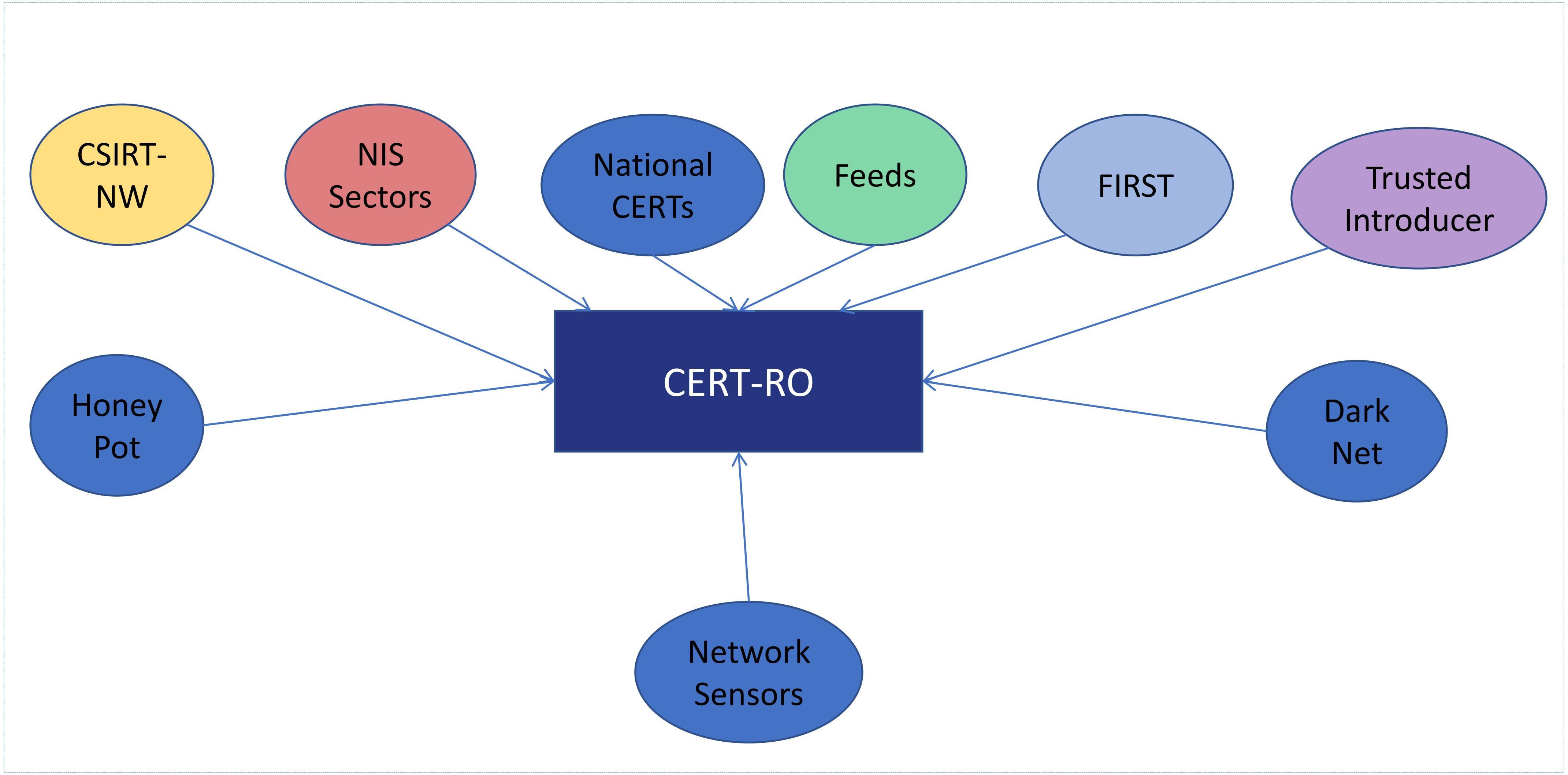
CERT-RO

- Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of security of information networks and systems in the EU
- The Directive takes into account the risks associated with cyber security incidents, having the effect of disrupting economic activities, financial losses of companies, citizens and institutions, as well as intentional or unintentional disruptions of the IT systems that support the essential services
- The aim is to improve national capabilities, strengthen cooperation at European level, promote risk mitigation and a culture of incident disclosure between key operators providing essential services.



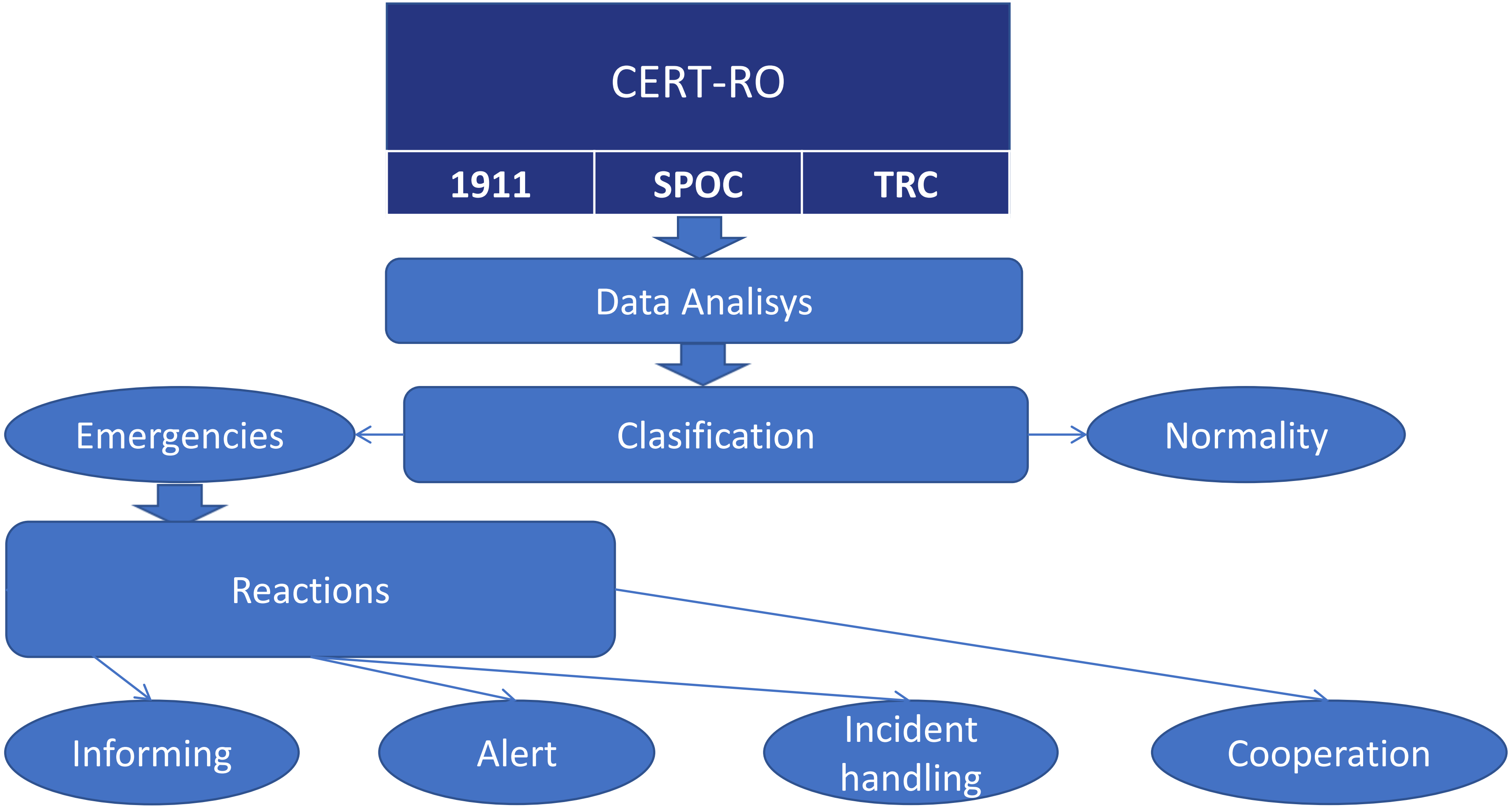
CERT-RO flow
Level I

CERT-RO

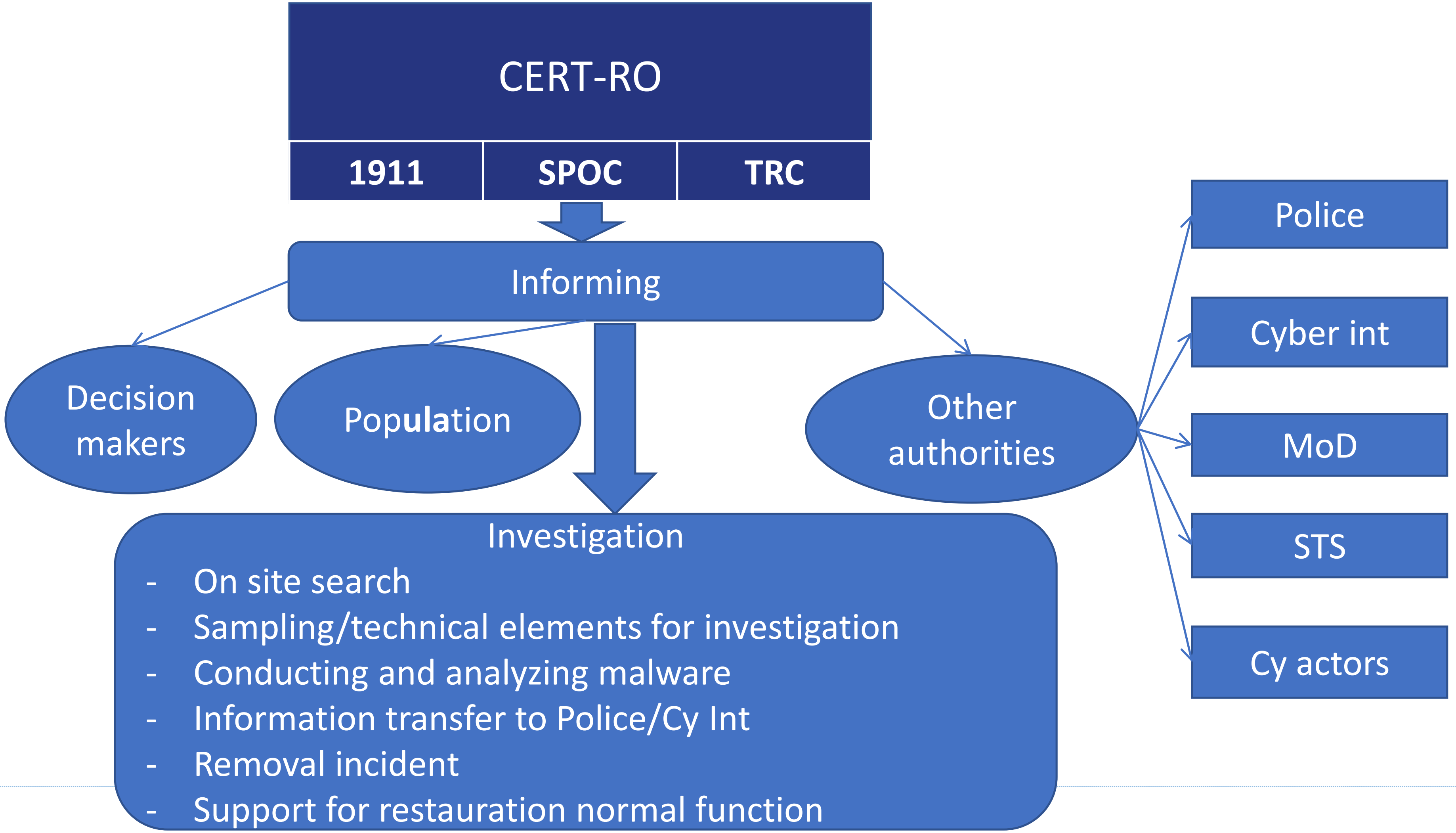


CERT-RO flow
Level II

CERT-RO



CERT-RO Incident handling



CERT-RO

1911

SPOC

TRC

Informing

Decision makers

Population

Other authorities

Police

Cyber int

MoD

STS

Cy actors

Investigation

- On site search
- Sampling/technical elements for investigation
- Conducting and analyzing malware
- Information transfer to Police/Cy Int
- Removal incident
- Support for restauration normal function

Cybercrime – law enforcement cooperation

CERT-RO

- Between the two institutions (Police – CERT-RO) there is an agreement in order to facilitate the exchange of   information related to cyber security events or incidents;
- This protocol was drafted in accordance with Romanian national law regarding:

  - Law for the foundation of CERT-RO;

  - Romania’s national Security Law

  - Law for the ratification of the Budapest Convention

  - Law for the protection and processing of personal data

PRINCIPLES

- Lawfulness
- Confidentiality
- Prevention of cyber security events or incidents
- Complementary
- Coordination in “response activities”
- Need to know processing of personal data

Riding the pony - example

- Back in January we received an incident report a bit different than the usual
- At 10 AM somebody reported us that their business partners complained that they receive unsolicited emails
- That “somebody” was a state owned company in the field of nuclear energy
- So we suspected the worse could have happened
- Performing the needed tests we came to the conclusion that their mail server was an open relay
- And probably this was how the unsolicited emails were sent
- At 11 AM a Romanian bank contacted us and told them they received suspicious emails originating from the first caller’s mail server and provided us with a sample

Riding the pony - example

- And a .doc file as attachment called data analysis.doc
- Extracting the hash and searching on VT revealed nothing
- So we decided to keep the file for later analysis and focus on what information we might get from the SMTP headers
- We noticed a few interesting things
- The email appears to be sent from a Nigerian IP address through a compromised Greek mail server (webmail.ogb.gr) Web mail application (Horde).

Riding the pony - example

- Analyzing the .doc file attached to the mail sample we received we came to the conclusion it was in fact packing two exploits for CVE 2017-11882 and CVE 2018-0802.
- CVE-2017-11882 affects Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016
- CVE-2018-0802 affects Equation Editor in Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013, and Microsoft Office 2016
- And both of them give remote code execution abusing OLE objects

Riding the pony - example

- Analyzing the payload of both exploits we identified the C2 server which was also used to deliver the second stage malware
- Further analyzing the second stage sample we identified heavy anti analysis capabilities, network ability to connect to the same C2 server, keylogging & screenshot capabilities, credential harvesting capabilities, etc.
- But most important, **we were able to identify code constructions commonly used by Pony malware**
- At this point we contacted the Romanian Police for support and they facilitated access to the C2 infrastructure
- We identified 7557 victims on this single Pony C2 server
- The malware was collecting credentials from HTTP, HTTPS, FTP, TELNET, RDP and SMTP
- The second stage malware was monitoring for credentials sent on a list of 18269 websites from Romania, Russia, Spain, France, Portugal, Italy and Turkey
- But the victims came from a larger number of countries..
- CERT-RO alerted the CERT teams responsible for all the identified IP addresses

Elements of healthcare system attacks

Targets

- 5 Romanian hospitals and a private medical center

Time of attack

- April 2019 (1 attack); June 2019 (4 attacks);September (1 attack)

Type of attack

- Ransomware

April attack

- Spotted an hospital in the NE of the country
- Part of a widespread attack, not targeted;
- Malware SCARAB;

Elements of healthcare system attacks

June attack

- 4 hospitals in Bucharest;
- 4 attacks in 24 hour;
- the attacks were reported at 1911, the national unique call center number;
- 3 of 4 attacks were part of an widespread malware campaign, with PHOBOS malware;
- the forth attack was a targeted one, using the malware Maoloa;
- The attackers with Maoloa tried to direct the investigations on a false direction, using the name Rabbitt4444

How the alert chain worked

CERT-RO

- the alert was received through 1911 green line;
- The operator activated the chain of decision, informing the CERT-RO decision makers, and introducing in parallel the information in the CERT-RO database;
- It was issued an cyber attack alert, and it was informed the Ministry of Health, to make aware the health chain institution and to take measures in this regard for avoiding the spreading of attacks;
- From the attack reporting until the MH was informed didn’t pass more than 30 minutes;
- CERT-RO issued a public alert, making aware the public, private institutions, and the population, regarding the attack, with the suggestion of avoiding actions that could spread the infection;
- there were used the media channels that CERT-RO has, as well as the partnership with national press-news agency, Agerpress;
- 2 hours since the first reporting of the attack, the alert became a news in Romania, being posted on all public and private mass media;
- The very next day, CERT-RO convoke a press conference, explaining the first conclusions and offering the pieces of news that the public and other stakeholder needed;
- In parallel, it was a strong cooperation with Cyberint (internal intelligence structure) and police, in order to asses possible influences of attack on national security. No such kind of influences were revealed;
- All the available date were sent to CSIRT network, for analysis and possible measures taken.

Thank you!

CERT-RO

Sabin Popescu