SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Romanian Cybersecurity healthcare landscape

Meeting place:Brussels, Belgium

Meeting title:1st Plenary Meeting

Presenter name: Sergiu Marin

Presenter organisation:POLARIS MEDICAL

Date:July 10, 2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

Contents

Medical Network Infrastructure

PIAS
Integrated Health Insurance Platform

SIUI
Integrated
Information
System

SIPE
Information System
for the Electronic
Prescription

CEAS
Health
Insurance
National Card

DES
Electronic Health
Record System

Internet

Current situation

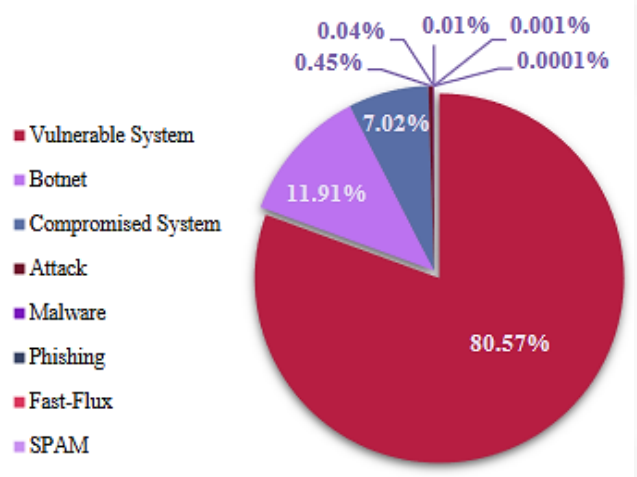
Present and Past together

- ✓ Smart Hospitals & Clinics (public & private) – modern ICT infrastructure, IT-trained personnel, cyber-aware;
- ✓ Classic Hospitals & Clinics (mostly public) – heterogenous ICT infrastructure, missing or outdated security products, not cyber-aware;
- ✓ Individual doctors (family or specialists) – mixed ICT infrastructure, with or without support from trained IT personnel;
- ✓ Pharmacy & Laboratory (chain or independent) – centralized or local management, homogenous or mixed ICT infrastructure, with or without support from trained IT personnel;

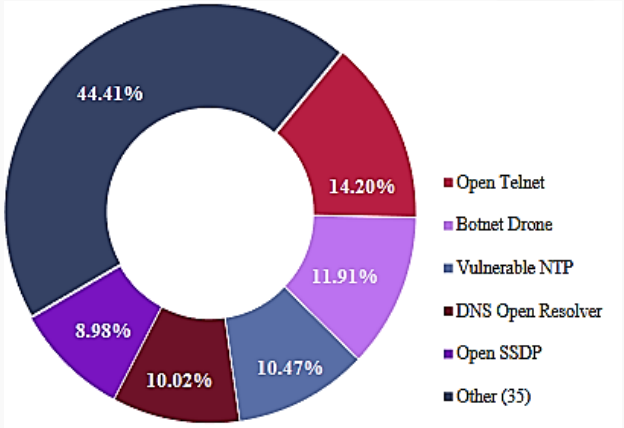
2018 - Cyber Threats

Classification

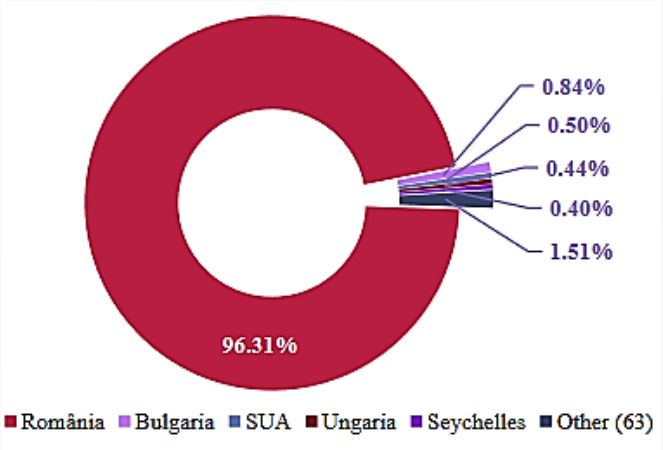
- ✓ class of alert/incident: Vulnerabilities: 80,57%. ; Botnet: 11,91%;



- ✓ type of alert/incident: «Top5 incidents type» 55,59%;
  - OpenTelnet: 44,41%;
  - Botnet Drone: 14,20%;
  - Vulnerable NTP: 11,91%;
  - DNS Open resolver: 10,47%;



- ✓ Country of origin: «Top 5 country» 98,49%. Number of countries: 68. New states:25 (ex: Afghanistan, Armenia, Aruba, Algeria, Estonia, Filipins, Indonesia, Syria etc.).

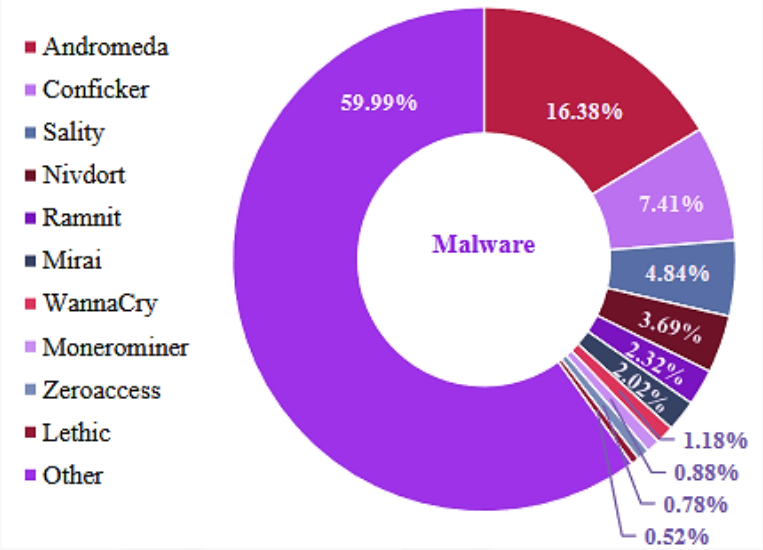


CERT-RO
CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA
ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM

2018 - Cyber Threats

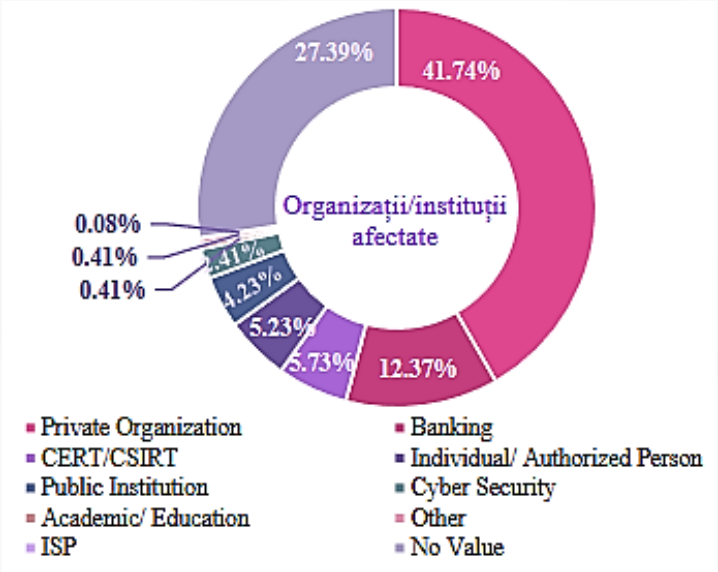
Malware alerts

- ✓ #1 Andromeda-16,38%; #2Downadup(Conficker)-7,41%.
- ✓ New entry: Monerominer, VPNFilter and Eitest;
- ✓ History: Palevo.



Affected organizations

- ✓ Private(41,74%); Banking(12,37%); Public Institution (5,23%)
- ✓ Processed alerts involved 107.430 unique IP's



CERT-RO
CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA
ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM

2018 - Cyber Threats

21.06.2018 – A new wave of ransomware target health institutions

Four hospitals from Bucharest, Husi, Dorohoi, Carbunesti attacked with Maoloa and Phobos.

About Maoloa

Relatively new family of malware, dating from February 2019, Maoloa is inspired from a family of ransomware called GlobeImposter. One of the most popular options is to coordinate **email phishing campaigns** with file attachments or malicious content that once interacted with will lead to the virus infection.

About Phobos

One of the many variants of Crysys family, the Phobos ransomware is distributed via spam email containing infected attachments or by exploiting vulnerabilities in the operating system and installed software. This ransomware was also observed attacking victims by hacking open Remote Desktop Services (RDP) ports. The attackers scan for the systems running RDP (TCP port 3389) and then attempt to brute force the password for the systems.

CERT-RO
CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA
ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Questions?

Presenter Name: Sergiu Marin
Organisation: POLARIS MEDICAL
Email: sergiu.marin@polarismedical.ro

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing