Cyber Security Status and Trends in Romania

Catalin Patrascu
Head of Inormation Security and Monitoring Department | CERT-RO
catalin.patrascu@cert-ro.eu

International Conference on Information Security
Seoul, July 2015

1. Current situation – Dynamics and trends

- **Security and confidence in public services represent a national priority for the Romanian Government and a basic requirement for electronic infrastructure data networks and electronic communications services.**

- **Several Romanian agencys have implemented cyber security projects financed by the European Commision, the most important being the following:**

  - National System for Combating Cybercrime
  - Advanced Cyber Defense Center
  - National System for Critical ICT Infrastructure Protection against Cyberthreats
  - Cyber Security Innovation Centre

1.1 National System for Combating Cybercrime

➢Project objective and description:

Creating an appropriate framework to increase capacity for policy drafting and to achieve better regulation and strategic planning by strengthening partnerships at inter-institutional level and between public institutions and representatives of other fields interested in fighting cybercrime.

➢Project results:

- Development and implementation of the IT solution and related equipment;
- Establishment of a set of public policies, drafting of laws and procedures to fight cybercrime;
- Training of the technical team "Cyber Crime" for Romania;
- Awareness campaign on the risks of cybercrime and how to handle it.

1.2 Advanced Cyber Defense Center

➢Project objective and description:

- The project aim is to create a European community for fighting botnets;
- Creation of a HoneyNet (network of honeypot-type sensors), capable of detecting and monitoring various types of cyber attacks;
- The project brings together 28 partners from 14 European countries, including Romania.

➢Project results:

- Creation of a Centralized Data Clearing House at European level to collect data about botnets;
- Developing a set of tools for botnets detection and disinfection;
- Creation of 8 national anti-botnet support centres, one of which in Romania.

1.3. National System for Critical ICT Infrastructure Protection against Cyber Threats

➢ **Project objective and description:**

- Implementation of a system that ensures interoperability between information security components;
- The project ensures streamlining and creation prerequisites for their modernization, including by minimizing the time needed to recover services following an incident or cyber attack;
- The project's proposed central objective is the hierarchical management of information generated by the implementation of systems designed to ensure cyber security, increasing the availability and confidence in public online services.

➢ **Project results:**

Development of web operational portal - platform that ensures:

- interoperability at the organizational level,
- access to working procedures,
- information on Cyber Alert Level,
- the publication of information related to cyber incidents.

1.4. Cyber Security Innovation Centre

This pilot project is part of the grant agreement signed June 2014 by CERT-RO and USTDA, aiming to define the strategy and conceptual model for the establishment of a Cybersecurity Innovation Center in Romania.

CERT-RO covers the related infrastructure necessary for the pilot, the overall organizational framework and the necessary human resources.

The CIC project is unique in the region and will provide the cooperation framework between the Romanian Government, governments of neighboring countries and multinational cybersecurity companies.

2. Critical infrastructure protection

In accordance with Romanian National Cyber Security Strategy, the responsibility for the protection of national cyber infrastructures is given to Cyber Security Operational Council composed by:

- Ministry of National Defense
- Ministry of Internal Affaires
- Ministry of Foreign Affaires
- Ministry for Information Society
- Romanian Intelligence Service
- Special Telecommunication Service
- Foreign Intelligence Service
- Protection and Guard Service
- National Registry Office for Classified Information
- Secretary of Supreme Council of Country's Defense

3. Threats and vulnerabilities

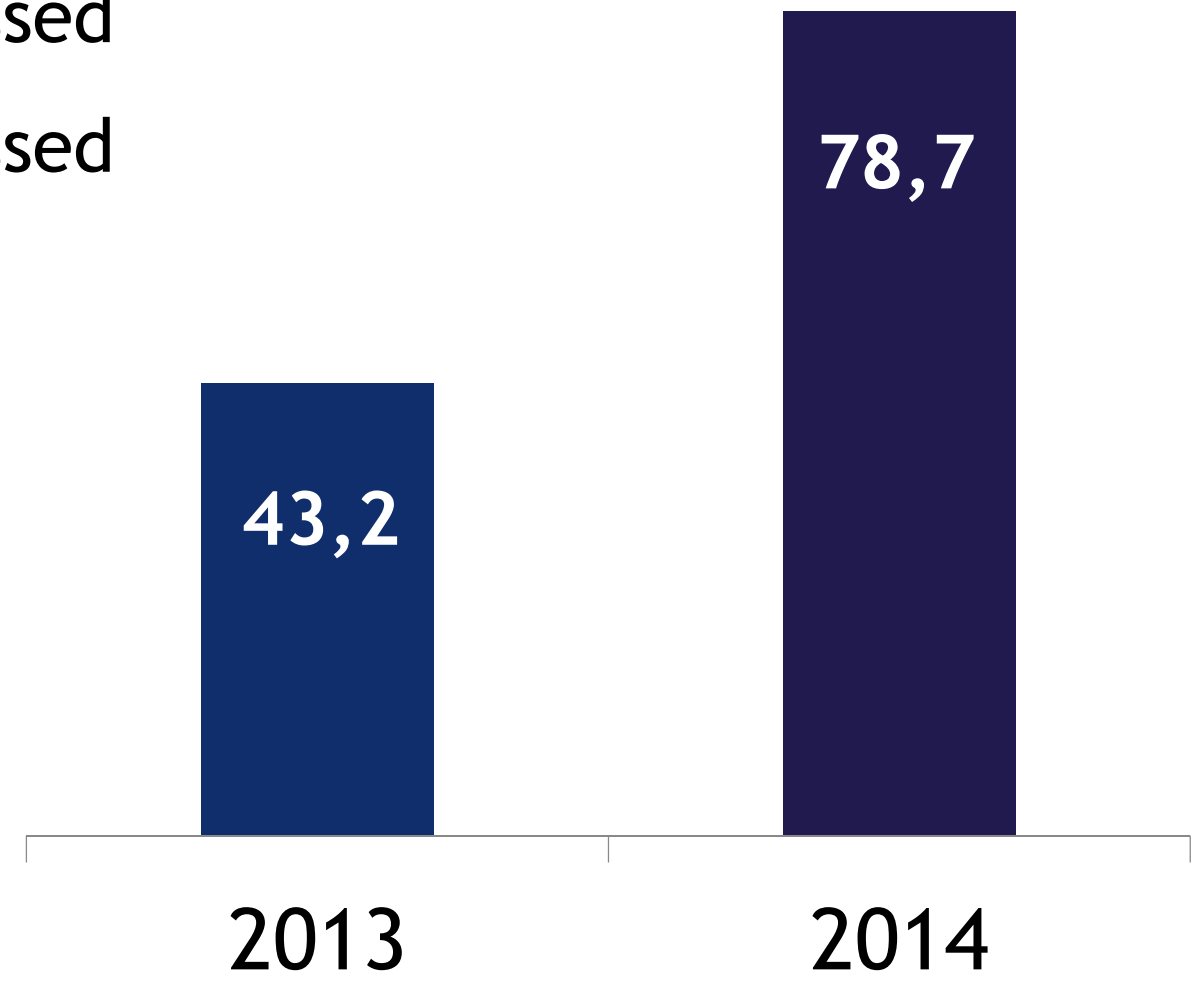
➢ **Cyber threats targeting the Romanian national cyberspace have diversified, evolutionary trends being observed, both in terms of quantity and technical degree of complexity.**

➢ **Conclusions of the analysis of cyber security alerts processed by CERT-RO in 2014:**

- threats on national cyberspace continues to diversify;
- most of the alerts received are related to infected systems with different variations of malware, which are part of different networks botnet, as well as misconfigured systems or unsecured;
- either one of the systems mentioned above can be used with the role of "proxy" for carrying out other attacks on targets outside the country;
- SOHO and Internet of Things (IoT) devices once connected to the Internet are becoming the targets of attackers and their vulnerabilities are exploited to access network and eventually used to launch attacks on other targets on the Internet;
- lately entities in Romania have been the target of APT's (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).

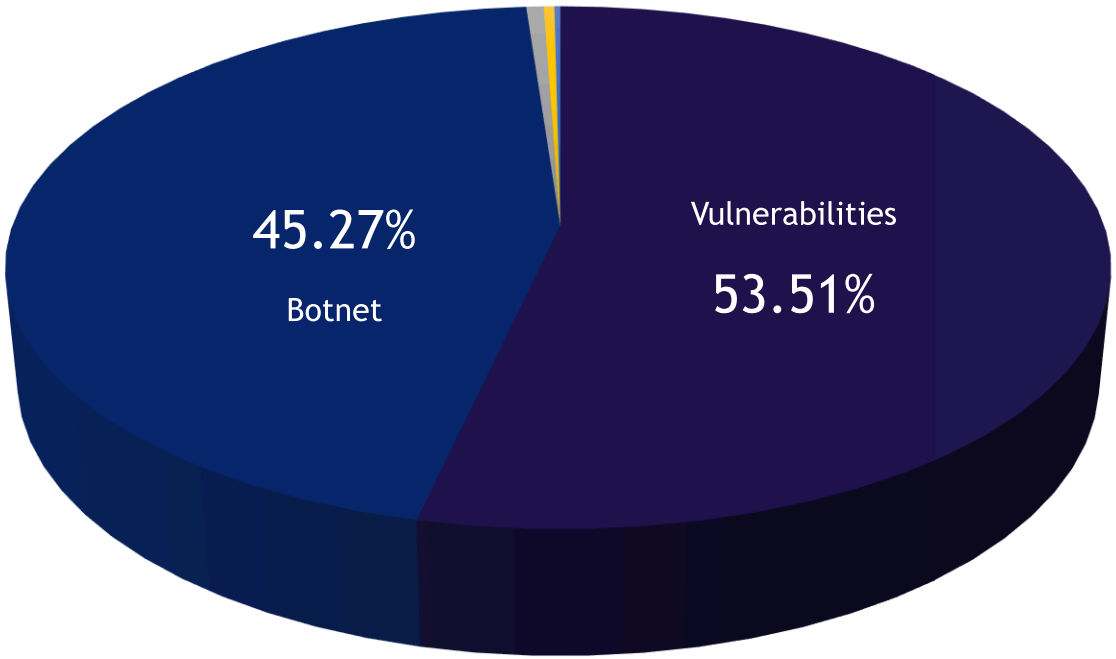
3.1. Alerts received in 2014 and 2013

- 2013 – 43.2 million alerts processed
- 2014 – 78.7 million alerts processed
- Approximated 82% growth



3.2. Type of alerts received in 2014 and 2013

- Vulnerabilities 42.146.259
- Botnet 35.657.806
- Information gathering 465.288
- Malware 284.158
- Other attacks 160.304



3.3. Statistics on Malicious Activities

2.4 millions IP's affected by cyber security incidents in 2014 (24% of total number of IP's allocated to Romanian organizations)

10.759 .rodomainswere compromise in 2014 (5% increase comparing with 2013)

Dozens of complex incidents and APT campaigns:

- **Snake/Turla/Uroburos**
- **Red October/ROCRA**
- Energetic Bear
- Botnet: Zeus, Citadel
- **Shylock Malware**
- **Ransomware: Cryptolocker, Cryptowall, CBT-Locker etc.**

4. Legal framework

➢**National Legislative Acts concerning the cyber security area are:**

- **Emergency Ordinance no.98/2010** regarding the identification, designation and protection of critical infrastructures
- **Government Decision no.718/2011** for the approval of Romanian National Strategy for Critical Infrastructure Protection
- **Government Decision no.494/2011** for the establishment of CERT-RO - computer security incident response team, a specialized organization responsible for preventing, analyzing, identifying and reacting to cyber incidents.
- **Government Decision no.271/2013** for the approval of Romania National Cyber Security Strategy and National Action Plan for the implementation of National Cyber Security System
- **Government Decision**, from April 7th 2015, for the approval of National Strategy regarding Digital Agenda for Romania 2020

➢**At European level there are ongoing negotiations for the approval of Network and Information Security Directive (NIS), but for the moment there is no mandatory European legislation regarding cyber security.**

5. Human resources

➢**Employment in Romanian IT&C sector:**

✓2011 - 128.000 employees

✓Romania's target for 2020 – 250.000 employees in IT&C sector

➢**Romanian Government strategies for improvement of employment rate in IT&C sector:**

✓Promotion of continuous training,

✓Introduction in schools of compulsory training on cyberspace security,

✓Creation of specializations for undergraduate and postgraduate education in the field of cybersecurity.

6. Cooperation and information exchange

- **National Cyber Security System** (SNSC) is the framework for cooperation which brings together public authorities and institutions with responsibilities and capabilities in the cyber security field.
- Cyber security incident response activities have been constantly a coordinated effort between institutions with responsibilities in this field:
  - Romanian Intelligence Service - National Center CYBERINT
  - Special Telecommunications Service – CORIS
  - Ministry of Defense – CERTMIL
  - Ministry for Internal Affaires CERT-INT
- Recognition of Romanian structures professionalism in the cyber security field has determined the nomination, within NATO, of some responsibilities for providing support to Ukraine in the field of cyber security.

- **CERT-RO**

- Signed, up to now, 30 national protocols with entities holding important networks or major information systems.
- signed cooperation protocols with national CERT's of China, South Korea, Japan, Moldova, Kazakhstan, Hungary and Uzbekistan.
- is a full member in two specialized international organizations:

✓ Trusted Introducer / TERENA, the European forum CERT centers with over 150 members

✓ FIRST, an international forum of CERT structures with over 250 members, deployed on all continents.

THANK YOU!

Catalin Patrascu
Head of Inormation Security and Monitoring Department | CERT-RO
catalin.patrascu@cert-ro.eu