Statistics, threats and cyber security trends on Romanian national cyberspace

Cătălin Pătrașcu
Chief of Incident Handling Team @ CERT-RO
catalin.patrascu@cert.ro

/ho is CERT-RO?

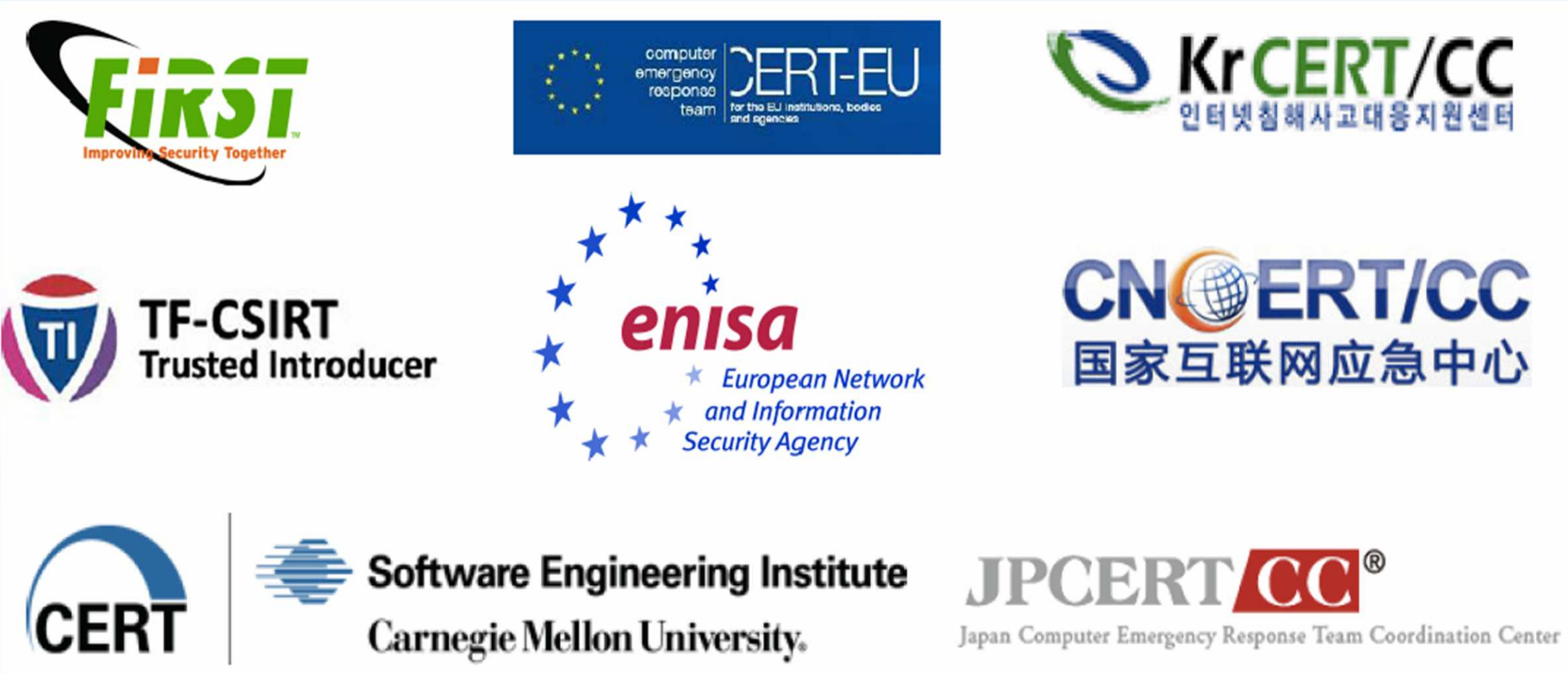
Romanian National Computer Security Incident Response Team – www.cert.ro

- an independent structure, with expertise in the field of cyber security, that has the capacity to **prevent**, **analyze**, **identify** and **respond to cyber security incidents** threatening Romanian national cyber-space
- coordinated by the **Ministry of Communications and Information Society** and fully financed by the state budget
- founded by **G.D. 494/2011**

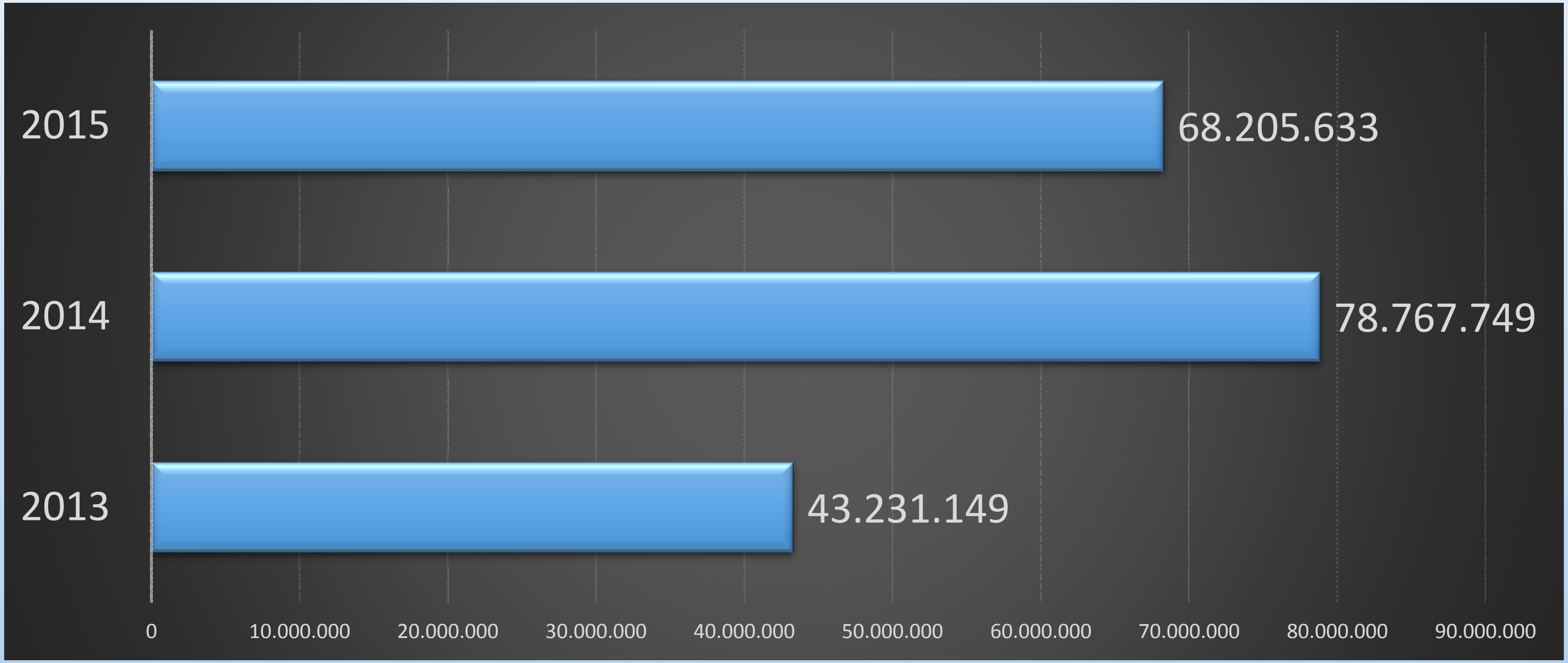
/hat does CERT-RO do?

- Acts as a **National Point of Contact**, collecting cyber security alerts from different stakeholders regarding vulnerabilities and incidents (IP’s, domains, URLs, IoC’s)
- **Incident response** activities (first response, investigations, mitigation, technical support, data dissemination and coordination)
- Operates an **Early Warning System** (EWS) on cyber-security incidents, based on the alerts received and data gathered from own detection sensors
- **Technical Audits**, **Pentests**, **Foreniscs**, **Technical Workshops**
- **Cooperation** at national and international level

ERT-RO International Partners


FIRST
Improving Security Together
computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies
KrCERT/CC
인터넷침해사고대응지원센터
TF-CSIRT
Trusted Introducer
enisa
European Network and Information Security Agency
CNCERT/CC
国家互联网应急中心
CERT
Software Engineering Institute
Carnegie Mellon University
JPCERT CC®
Japan Computer Emergency Response Team Coordination Center

yber security alerts processed by CERT-RO rends)



015 statistics based on processed alerts

Full report at **cert.ro/raport2015/**

- **26% (2.3 mil.)** of unique IPs in RO were involved in at least one cyber security alert
- **78% (53 mil.)** of processed alerts are about vulnerable systems
- **20,78% (14 mil.)** of processed alerts refers to botnets
- **17.088 „.ro” domains** were reported to CERT-RO as being compromised in 2015 (on the rise with almost 60% compared to 2014)

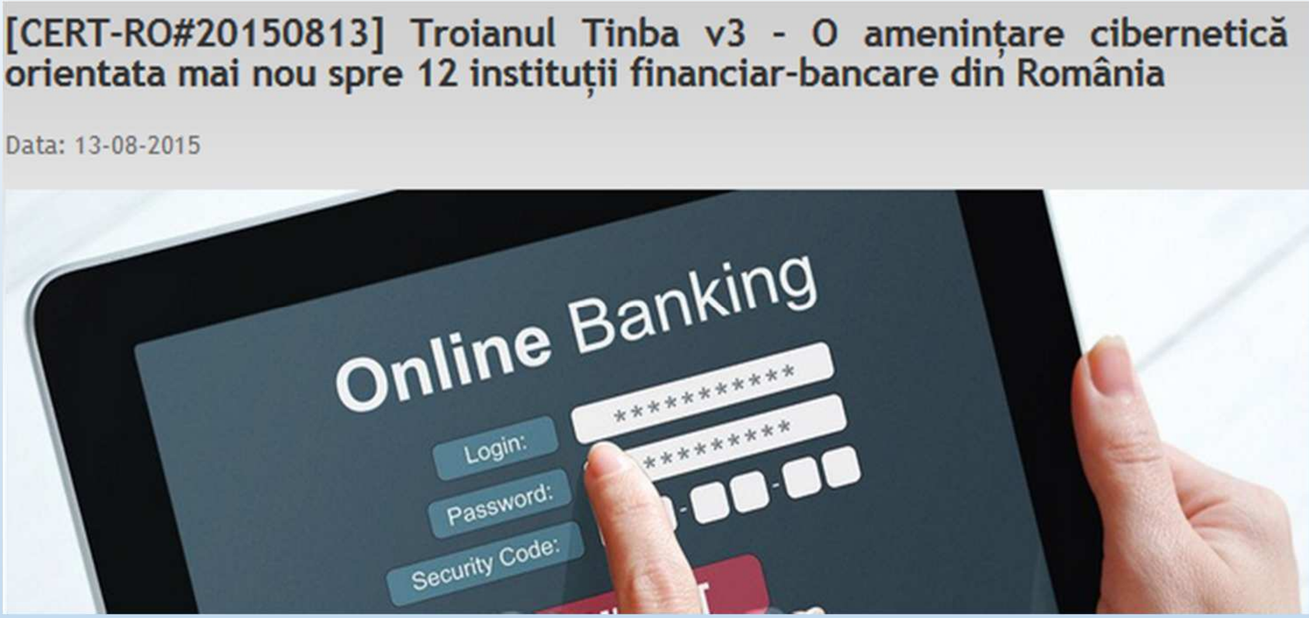
cidents classification

r.	Alert Type	Count	Pct.
	Vulnerabilities	53.424.880	78,33 %
	Botnet	14.171.061	20,78 %
	Malware	393.380	0,58 %
	Scans	102.167	0,15 %
	Cyber Attacks	61.751	0,09 %

Nr.	Incident Type	Count	Pct.
1	**Botnet**	3.161.666	64,52 %
2	Vulnerabilities	1.729.042	35,28 %
3	Malware	5.847	0,12 %
4	Scans	3.730	0,08 %
5	Cyber Attacks	366	0,01 %

inancial malware România (2015)

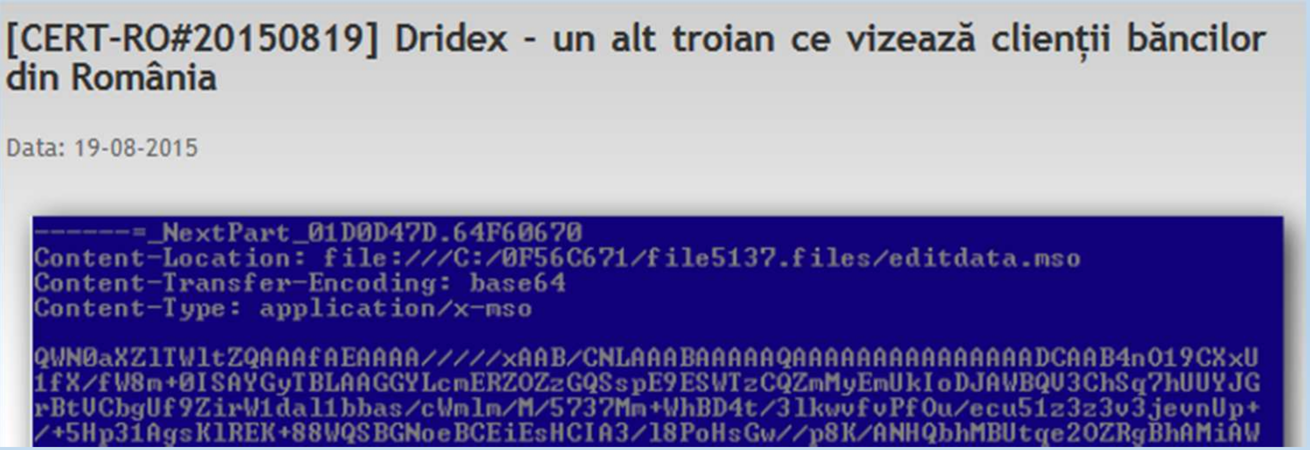
NBA



[CERT-RO#20150813] Troianul Tinba v3 - O amenințare cibernetică orientata mai nou spre 12 instituții financiar-bancare din România

Data: 13-08-2015

RIDEX



[CERT-RO#20150819] Dridex - un alt troian ce vizează clienții băncilor din România

Data: 19-08-2015

```
------=_NextPart_01D0D47D.64F60670
Content-Location: file:///C:/0F56C671/file5137.files/editdata.mso
Content-Transfer-Encoding: base64
Content-Type: application/x-mso

QWN0aXZlTWltZQAAAfAEAAAA/////xAAB/CNLAAABAAAAAQAAAAAAAAAAAAAAAADCAAB4nO19CXxU
1fX/fW8m+0ISAYGyTBLAAGGYLcmERZOZzGQSspE9ESWTzCQZmMyEmUkIoDJAWBQV3ChSq7hUUYJG
rBtVCbgUf9Zirl1dal1bbas/cWmlm/M/5737Mm+WhBD4t/3lkwvfPf0u/ecu51z3z3v3jevnUp+
/+5Hp31AgsKlREK+88WQSBGNoeBCEiEsHCIA3/18PoHsGw//p8K/ANHQbhMBUtqe2OZRgBhAMiAW
```

ansomware threat

Fast growing

Rapidly evolving and changing in terms of complexity

Hard to mitigate and stop

All industry sectors affected (including public institutions)

CERT-RO dedicated guide: www.cert.ro/ransomware/

/hat is to be done?

➢Coordinated and continuous effort

- Users
- Technology and service providers
- Authorities
- Specialized bodies

➢ Cooperation and information sharing

➢ Proper/updated legislation

➢ CERT/CSIRT bodies

- national, governmental, sectorial, private

THANK YOU!

tălin Pătrașcu

talin.patrascu@cert.ro

RT-RO

QUESTIONS ?