



MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

DataCentrum
medzi Vami a financiami



CSIRT.SK
WWW.CSIRT.GOV.SK



Computer Security Incident Response Team Slovakia CSIRT.SK

Ján Laštinec, CSIRT.SK

CS Danube, 15th March 2016, Prague



CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.





MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

DataCentrum
medzi Vami a financiami



CSIRT.SK
WWW.CSIRT.GOV.SK



Security incidents in 2015 – Slovakia

Ján Laštinec, CSIRT.SK

CS Danube, 15th March 2016, Prague



CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.





Agenda:

Sources and Classification



Security Incidents in Slovak IP Space

Types of Incidents & Malicious Activity

Statistics & Trends

Comparison with 2014



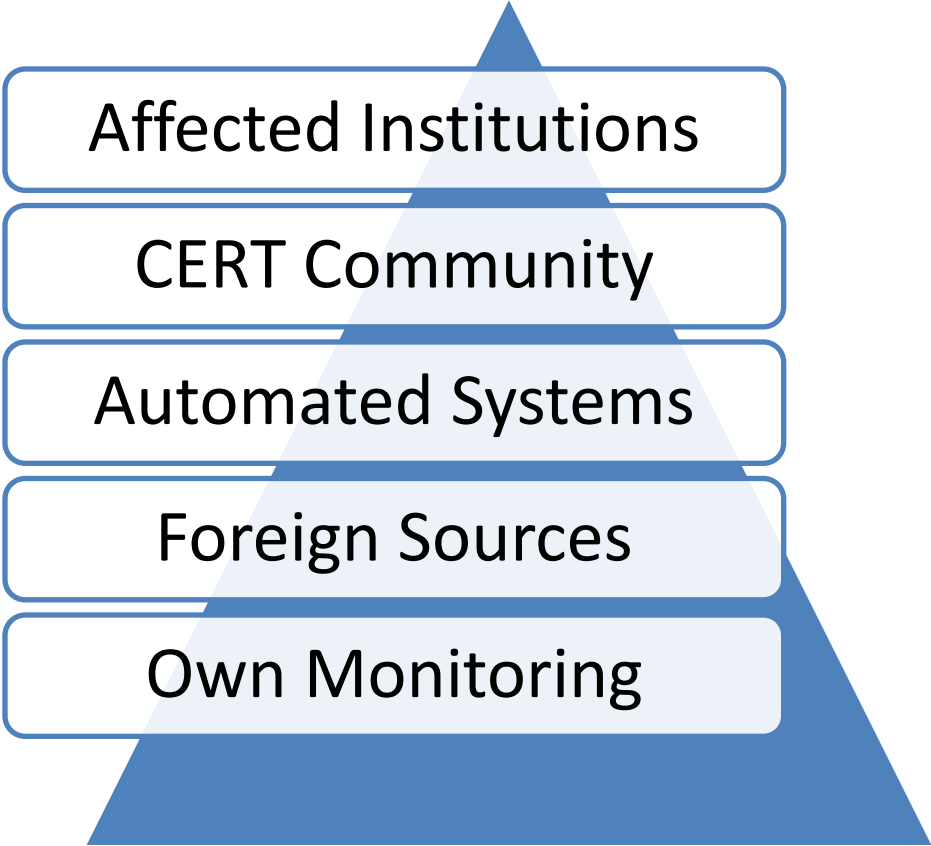
Interesting cases



Conclusions



Data Sources



Affected Institutions

CERT Community

Automated Systems

Foreign Sources

Own Monitoring





MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

DataCentrum
medzi Vami a financiami



CSIRT.SK
WWW.CSIRT.GOV.SK

Data Sources



network security incident exchange



shadowserver



**TEAM CYMRU
COMMUNITY
SERVICES**

KASPERSKY



Google



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



CSIRT.CZ

powered by CZ.NIC



National Cyber Security Centre
Ministry of Security and Justice



Microsoft



CERT
POLSKA



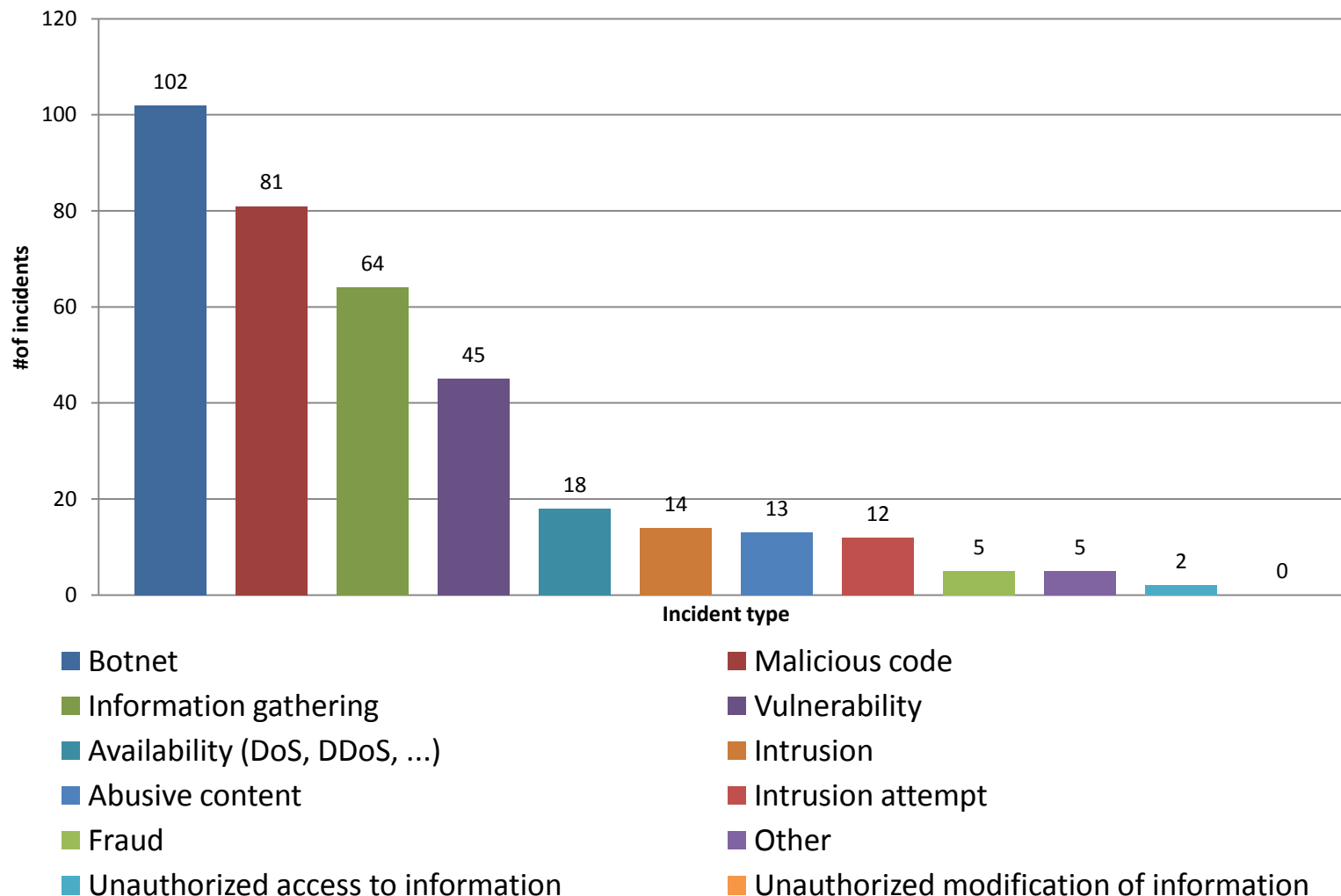


Incident Classification

Botnet	• Zeus...
Availability	• DoS, DDoS...
Unauthorized access/modification	• Disclosure, hijacking...
Abusive content	• Defacement, SPAM...
Fraud	• Copyright...
Intrusion attempt/intrusion	• Bruteforce, SQLi...
Malicious code	• Dridex...
Information gathering	• Phishing...
Vulnerability	• DROWN...

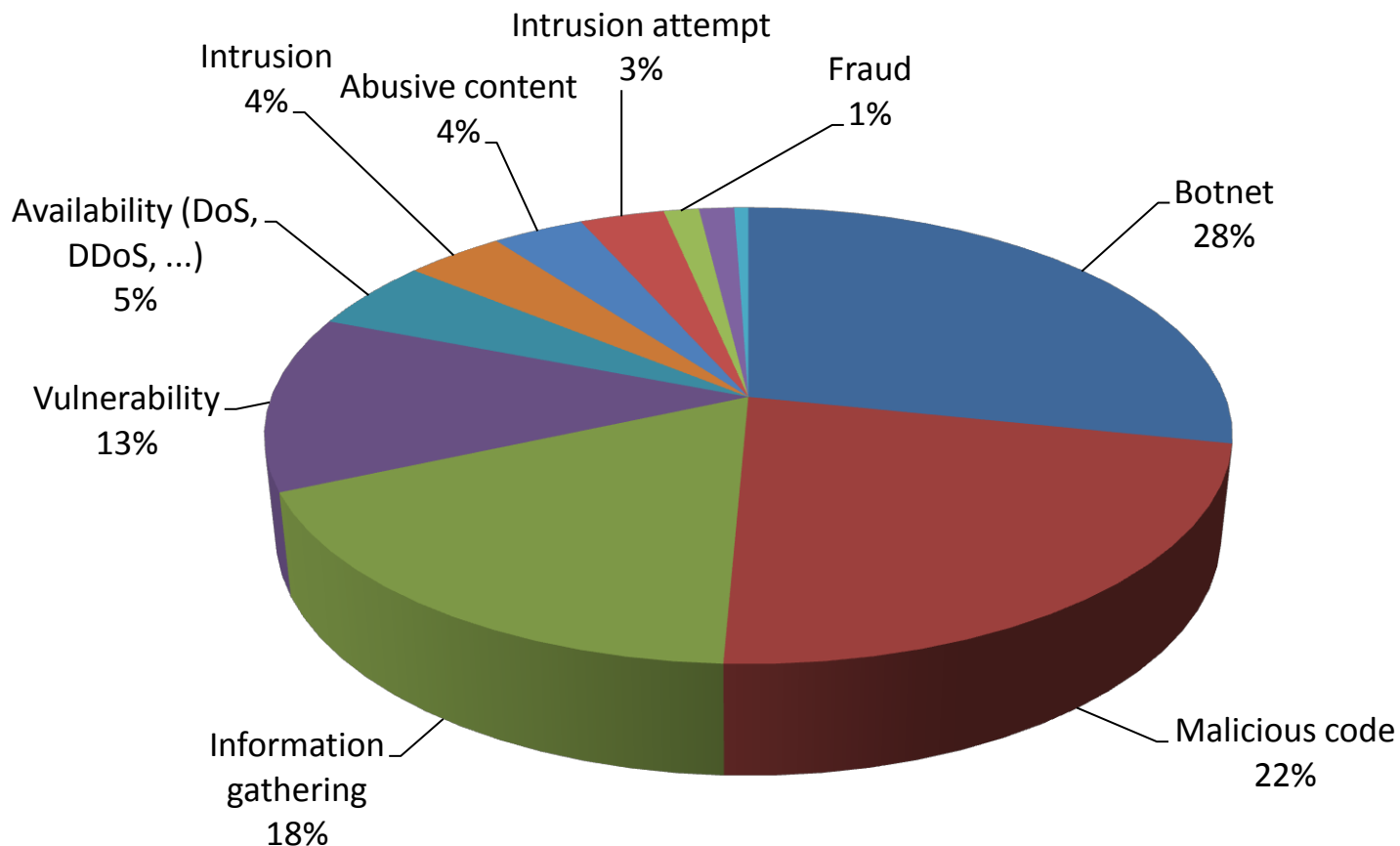


Significant Incidents in 2015



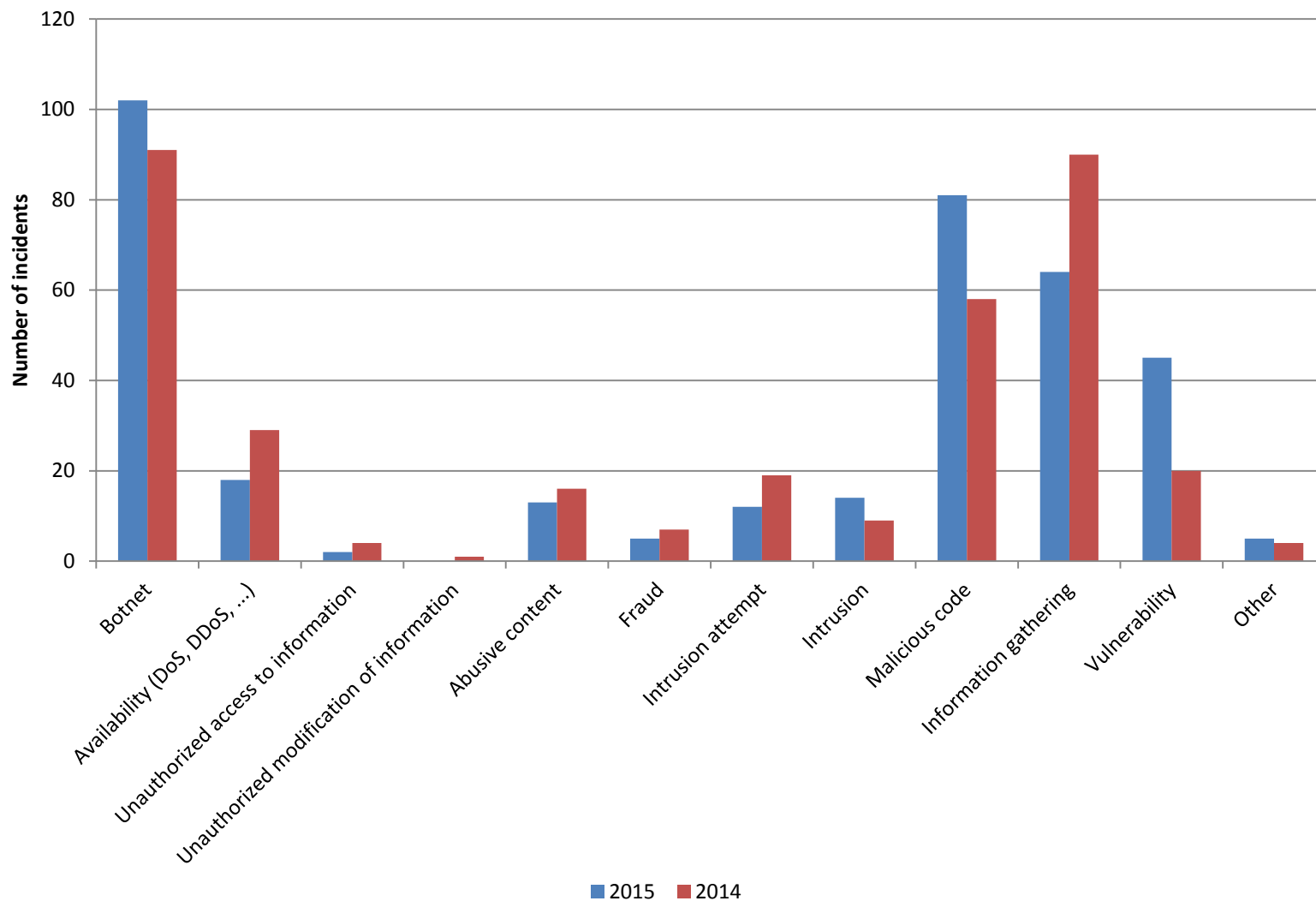


Most Common Incidents





Comparison with 2014



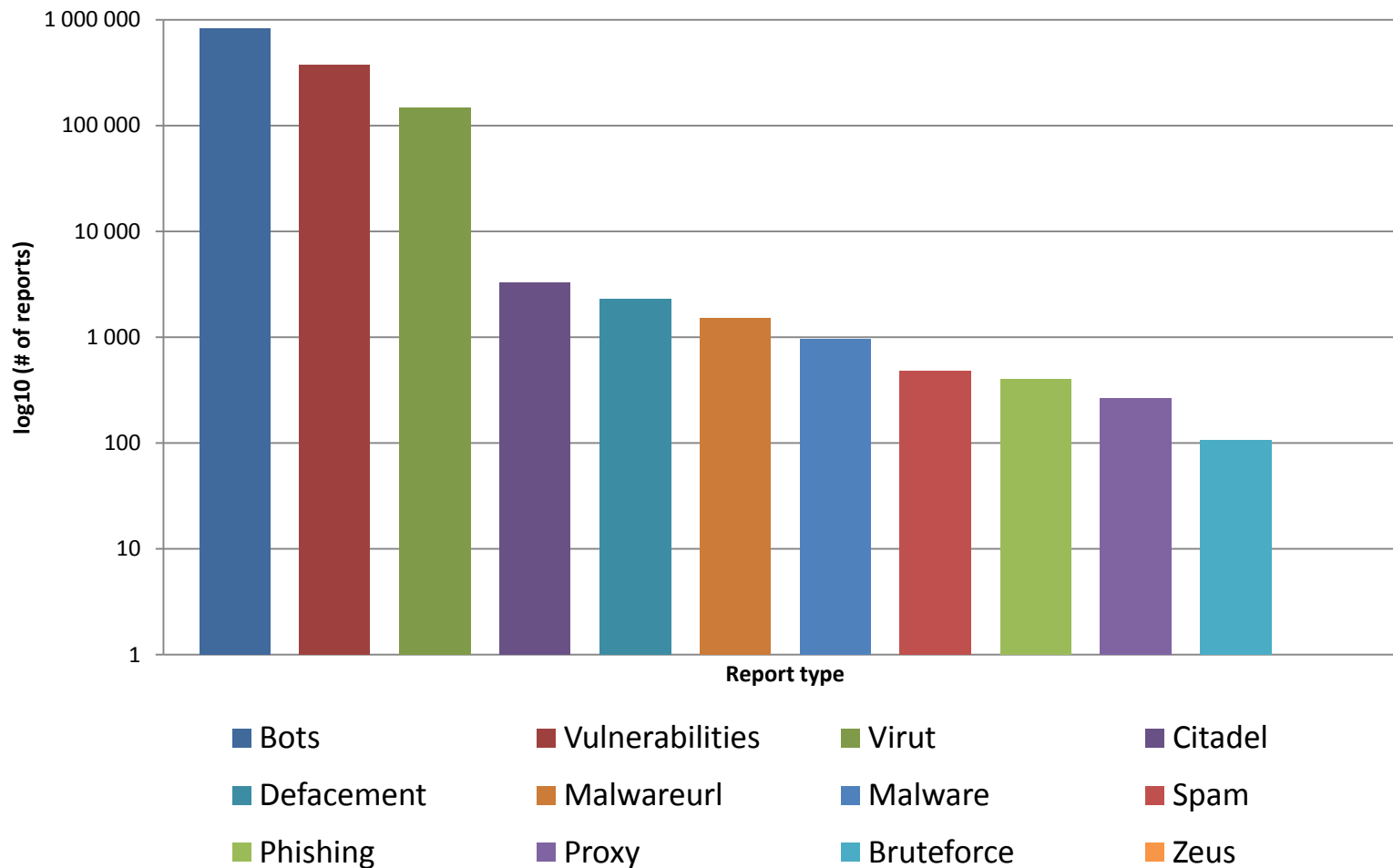


Comparison with 2014

Incident type	2015	2014	Trend
Botnet	102	91	+12,09%
Availability (DoS, DDoS, ...)	18	29	-37,93%
Unauthorized access to information	2	4	-50,00%
Unauthorized modification of information	0	1	-100,00%
Abusive content	13	16	-18,75%
Fraud	5	7	-28,57%
Intrusion attempt	12	19	-36,84%
Intrusion	14	9	+55,56%
Malicious code	81	58	+39,66%
Information gathering	64	90	-28,89%
Vulnerability	45	20	+125,00%
Other	5	4	+25,00%
All	361	348	+3,74%

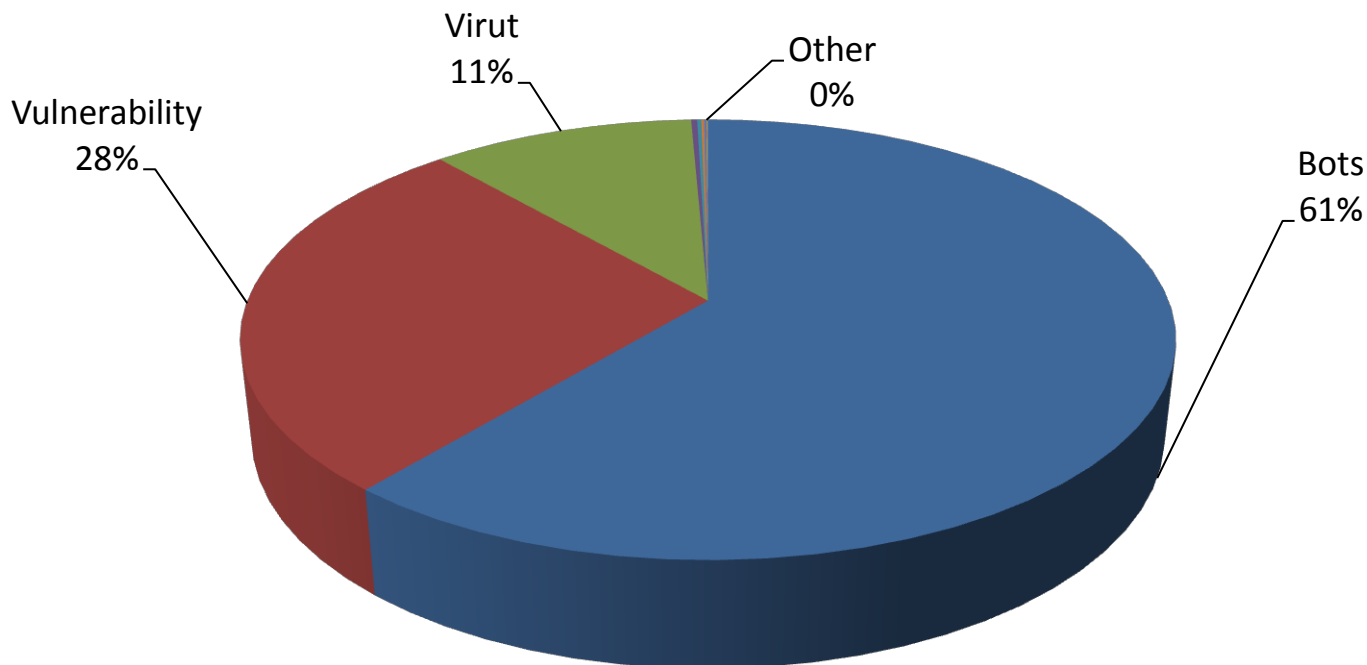


Malicious Activity in Slovak IP Space



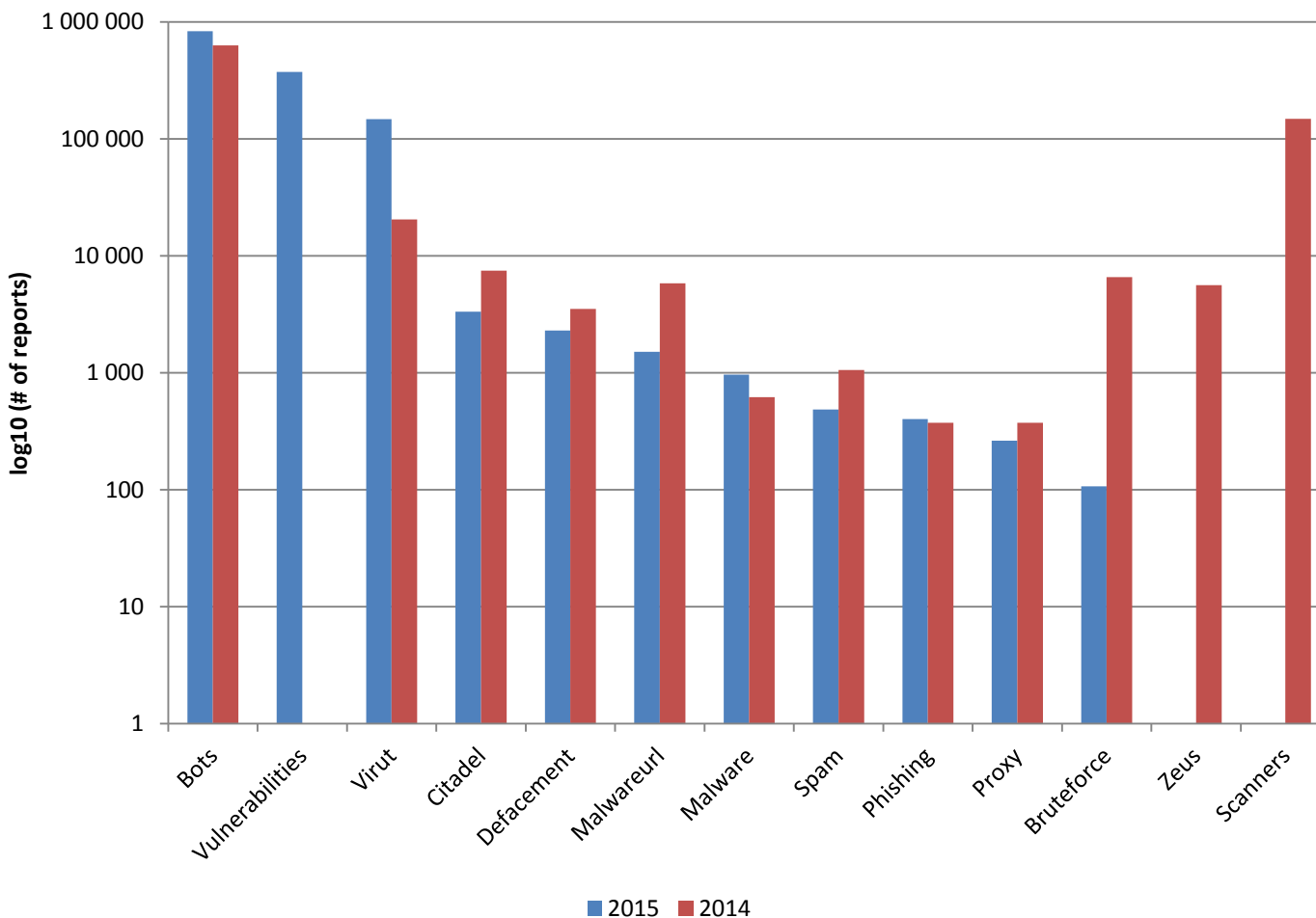


Most Common Reported Activity





Comparison with 2014



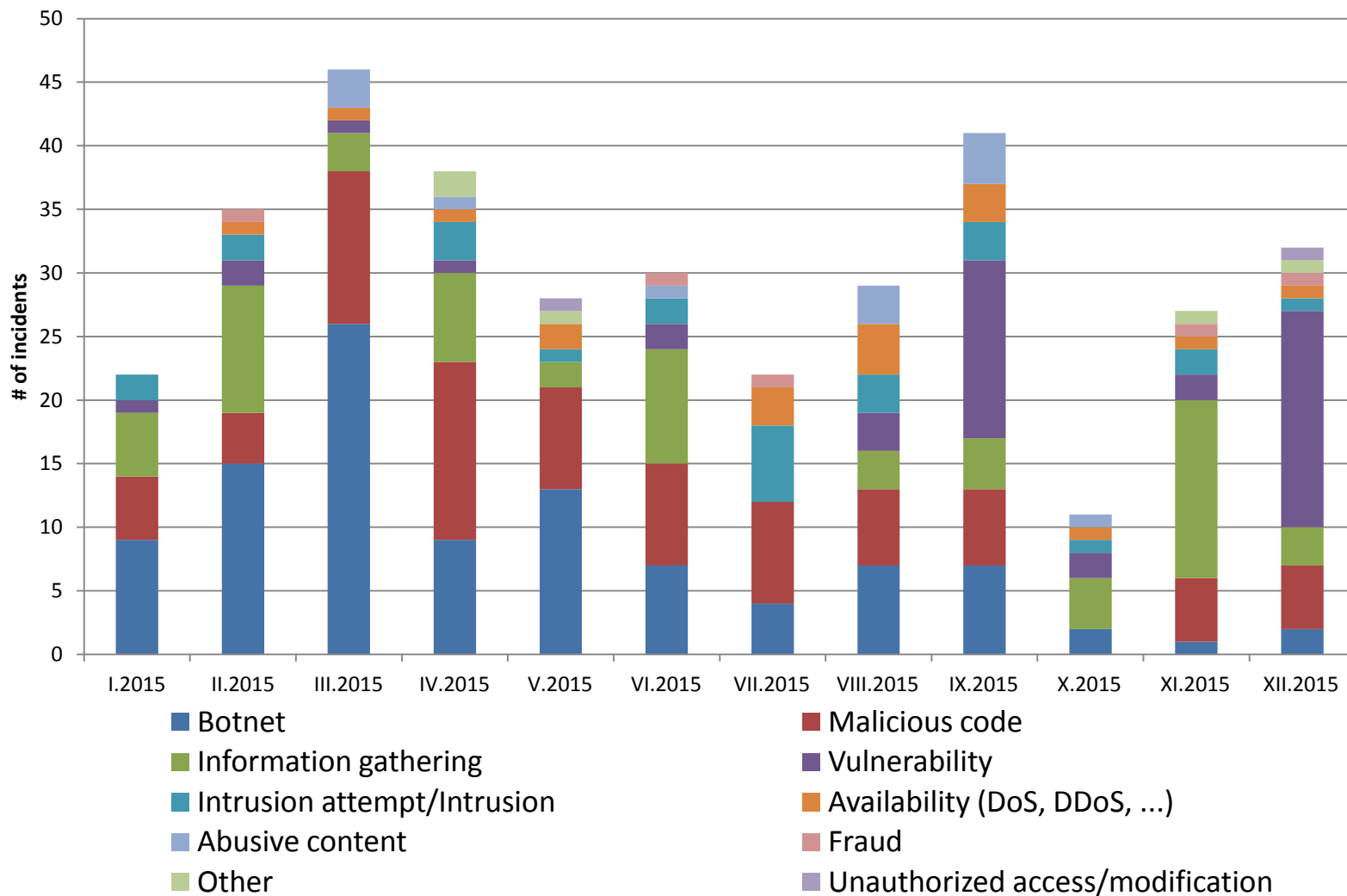


Comparison with 2014

Malicious Activity	2015	2014	Trend
Bots	831 226	629 725	+32,00%
Vulnerabilities	372 978	0	
Virut	146 805	20 393	+619,88%
Citadel	3 314	7 440	-55,46%
Defacement	2 295	3 506	-34,54%
Malwareurl	1 511	5 825	-74,06%
Malware	963	618	+55,83%
Spam	483	1 055	-54,22%
Phishing	402	372	+8,06%
Proxy	263	373	-29,49%
Bruteforce	107	6 571	-98,37%
Zeus	1	5 610	-99,98%
Scanners	0	148 091	
All	1 360 348	829 579	+63,98%

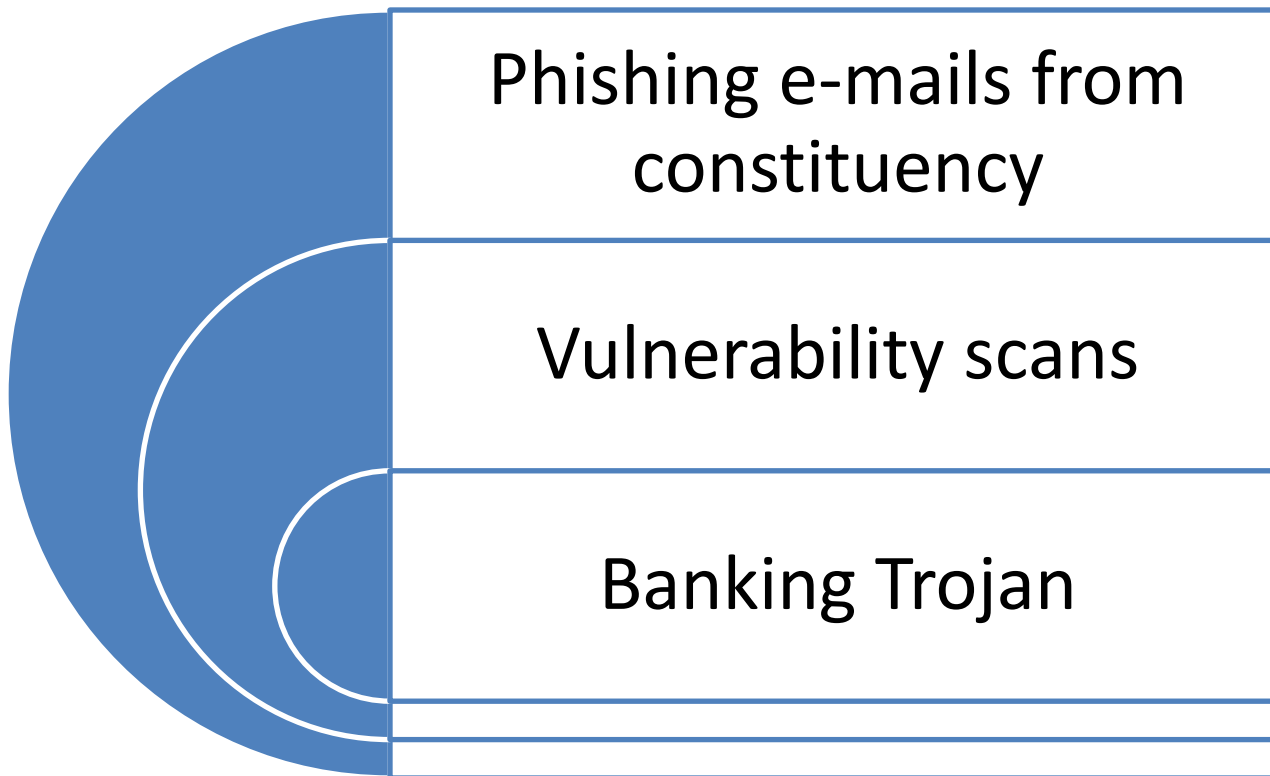


Incident Trends





Interesting Cases





Phishing with Malicious Link

E-mail with criminal proceedings theme
contained link to malicious .pdf.exe



Trojan malware with persistence in
registry



Contacting C&C through HTTP



Injects code to processes such as
browser



Proactive Vulnerability Tests

Rom-0

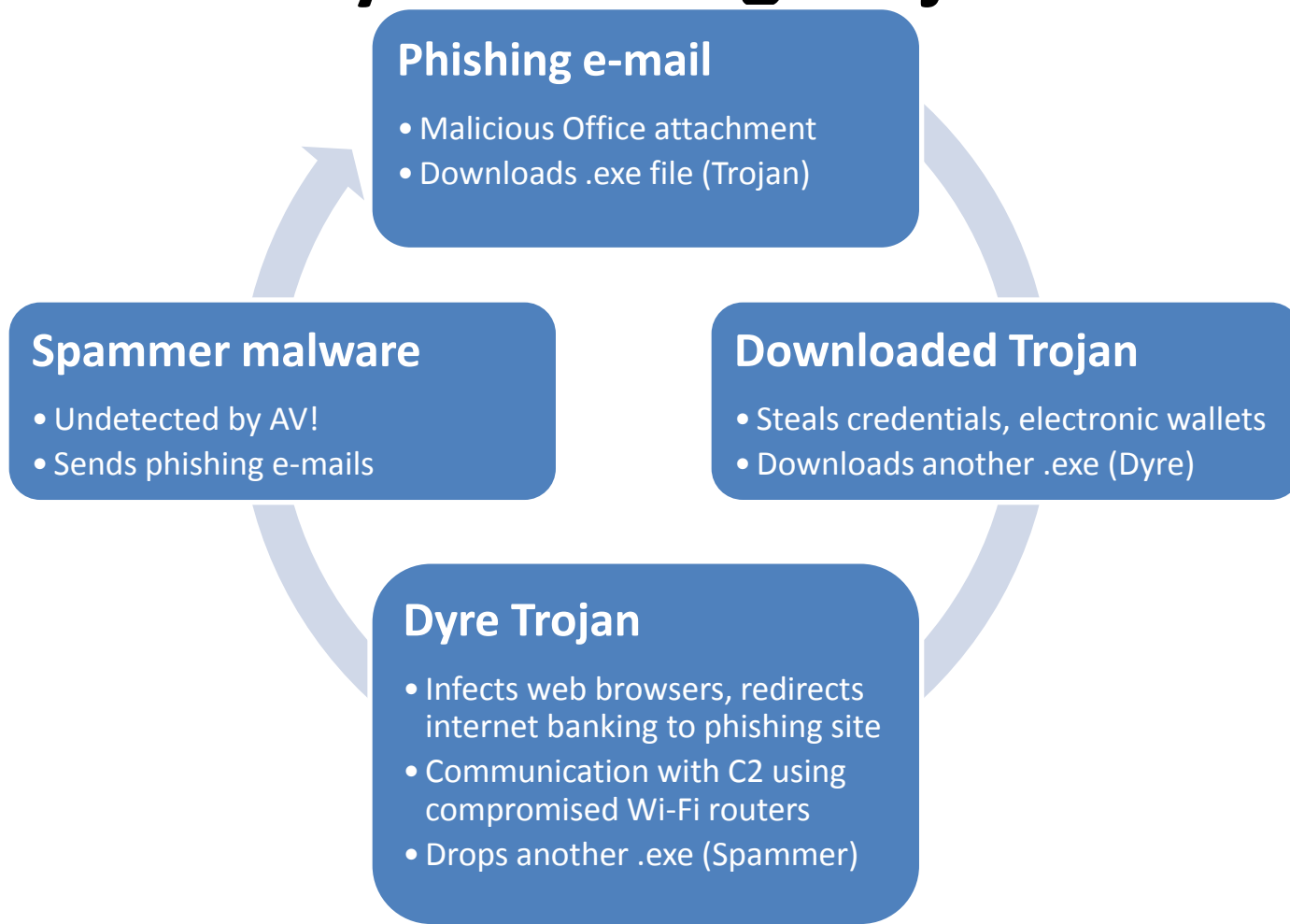
- SOHO router vulnerability
- Publicly accessible configuration
- Possible redirect attacks
- Publicly accessible configuration interfaces

DNS open-resolvers

- Recursive DNS query
- Misuse of server in DDoS amplification attacks



Dyre Banking Trojan





Conclusion

Increase in botnets and malicious code

- Dyre, Ramnit, Dridex...

Several phishing campaigns

- Often connected with malware

Phishing test



MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

DataCentrum
medzi Vami a financiami



CSIRT.SK
WWW.CSIRT.GOV.SK



CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.





MINISTRY OF FINANCE
OF THE SLOVAK REPUBLIC

DataCentrum
medzi Vami a financiami



CSIRT.SK
WWW.CSIRT.GOV.SK



Thank you for your attention!

CSIRT.SK

DataCentrum

Cintorínska 5, 814 88 Bratislava

www.csirt.gov.sk

Telephone: +421 2 59 278 205, +421 2 59 278 454

Contact: info@csirt.gov.sk

Incident report: incident@csirt.gov.sk



CS Danube (Cyber Security in Danube Region) project is part financed by the European Union from the START Danube Region Project Fund.

