Security through open innovation and data sharing

November 11th, 2016

DefCamp#7

Bucuresti

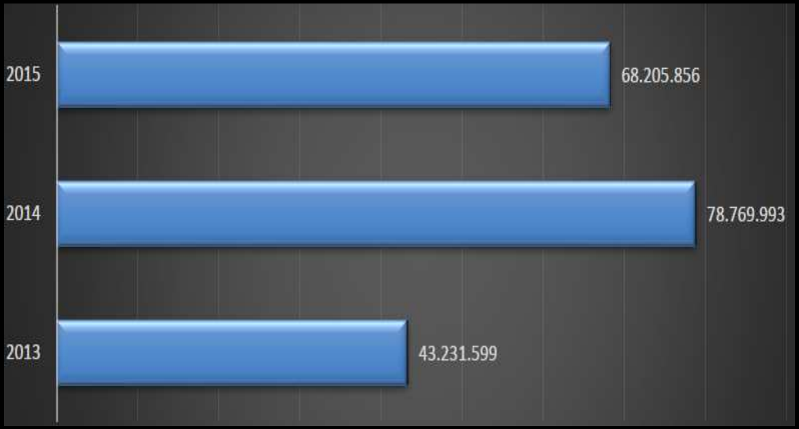
Cristian Patachia

Development & Innovation Manager

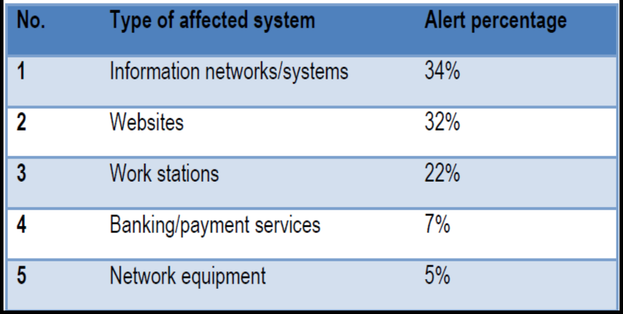
DefCamp#7
Where Hacking & Security Collide
app2own
bug bounty
DefCamp#6
Where Hacking & Security Collide

CERT-RO reports on cybersecurity
we are not safe online

the YoY evolution of total number of security alerts

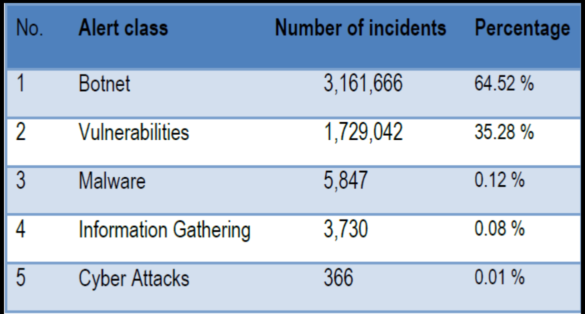


2015 top 5 affected systems



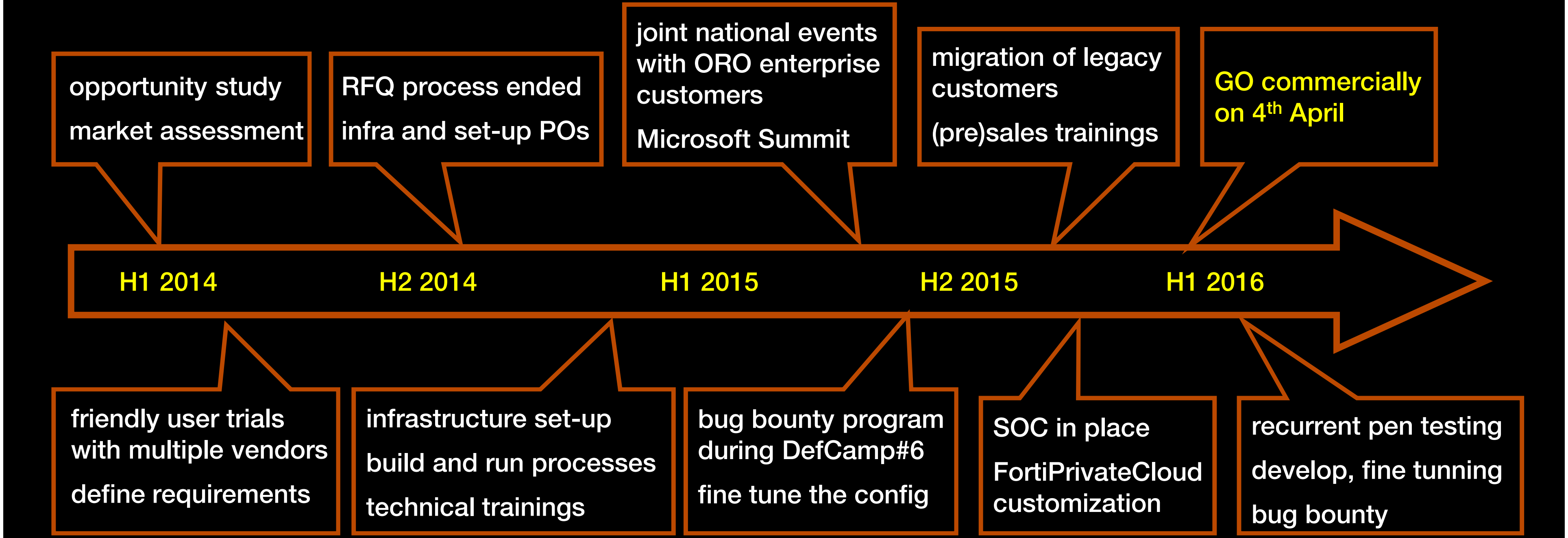
No.	Type of affected system	Alert percentage
1	Information networks/systems	34%
2	Websites	32%
3	Work stations	22%
4	Banking/payment services	7%
5	Network equipment	5%

2015 top 5 security alerts by incidents



No.	Alert class	Number of incidents	Percentage
1	Botnet	3,161,666	64.52 %
2	Vulnerabilities	1,729,042	35.28 %
3	Malware	5,847	0.12 %
4	Information Gathering	3,730	0.08 %
5	Cyber Attacks	366	0.01 %

design process – Business Internet Security
think, build, test, run, test



opportunity study

market assessment

RFQ process ended

infra and set-up POs

joint national events with ORO enterprise customers

Microsoft Summit

migration of legacy customers

(pre)sales trainings

GO commercially on 4th April

H1 2014

H2 2014

H1 2015

H2 2015

H1 2016

friendly user trials with multiple vendors

define requirements

infrastructure set-up

build and run processes

technical trainings

bug bounty program during DefCamp#6

fine tune the config

SOC in place

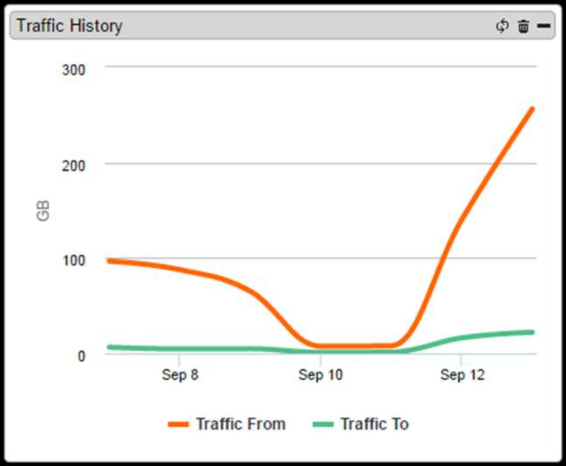
FortiPrivateCloud customization

recurrent pen testing

develop, fine tunning

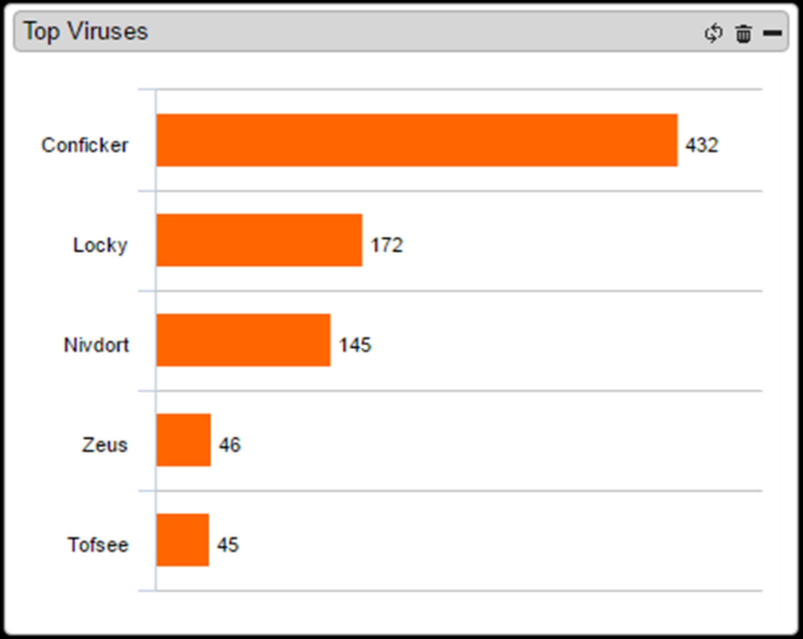
bug bounty

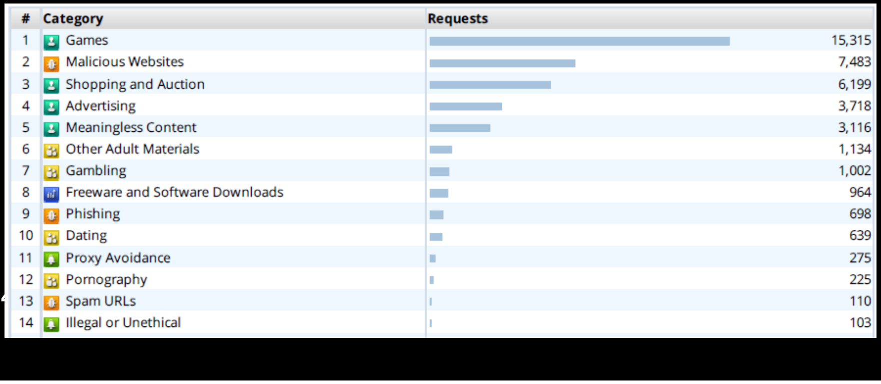
cyber security risk awareness
and customer reaction



back to school

education, September - October



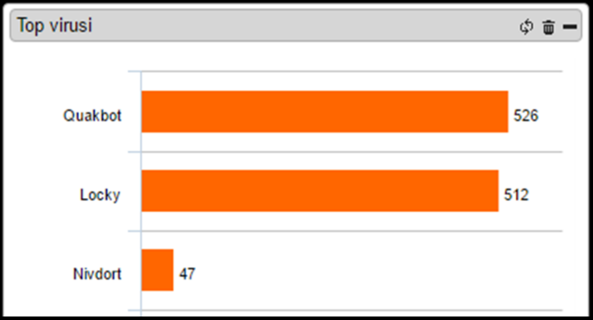


#	Category	Requests
1	Games	15,315
2	Malicious Websites	7,483
3	Shopping and Auction	6,199
4	Advertising	3,718
5	Meaningless Content	3,116
6	Other Adult Materials	1,134
7	Gambling	1,002
8	Freeware and Software Downloads	964
9	Phishing	698
10	Dating	639
11	Proxy Avoidance	275
12	Pornography	225
13	Spam URLs	110
14	Illegal or Unethical	103

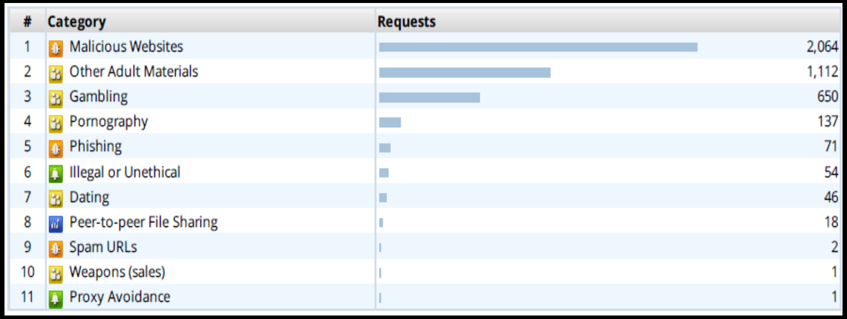
most blocked categories

cyber security risk awareness
and customer reaction

public services sector, 7 days stats

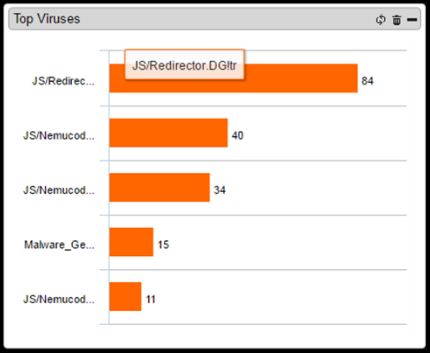


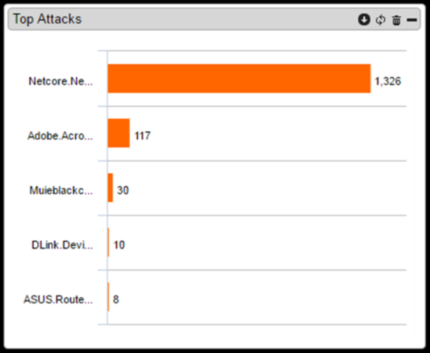
most blocked categories



#	Category	Requests
1	Malicious Websites	2,064
2	Other Adult Materials	1,112
3	Gambling	650
4	Pornography	137
5	Phishing	71
6	Illegal or Unethical	54
7	Dating	46
8	Peer-to-peer File Sharing	18
9	Spam URLs	2
10	Weapons (sales)	1
11	Proxy Avoidance	1

health care, October stats





Netcore. Netis. Devices. Hardcoded. Password. Security. Bypass

Adobe. Acrobat. PostScript. Font. Memory. Corruption

DLink. Devices. Unauthenticated. Remote. Command. Execution

ASUS. Router. infosvr. UDP. Broadcast. Command. Execution

recurring pen test
for security assurance

- a successful cyber attack involves different steps: reconnaissance, footprinting, gaining access, maintaining access and erasing the logs
- present conventional tools of the industry only have a reactive nature, they only respond when the attack has already been conducted
- Orange approach aims to respond before the attack turns into a real threat
- all successful attacks are conducted by real human hackers – why let only a machine fight against a real human's mind?

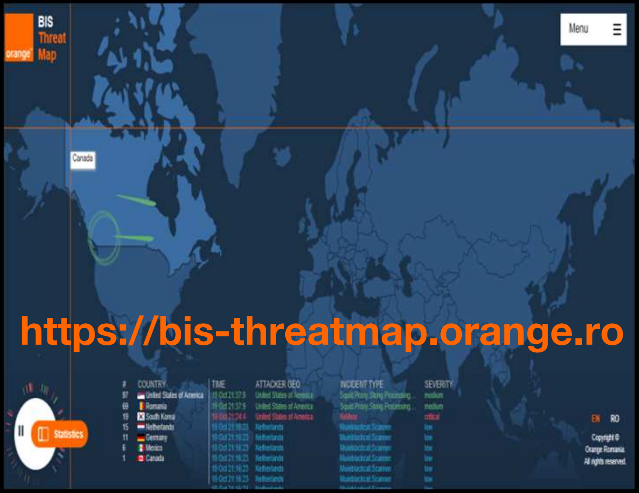
ethical hacking and cyber intelligence
for a safer online experience

Europe Cyber Security Challenge

ROMANIA CYBER SECURITY CHALLENGE
EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!

http://www.cybersecuritychallenge.ro

real time threat map



https://bis-threatmap.orange.ro

#	COUNTRY
97	United States of America
69	Romania
19	South Korea
15	Netherlands
11	Germany
6	Mexico
1	Canada

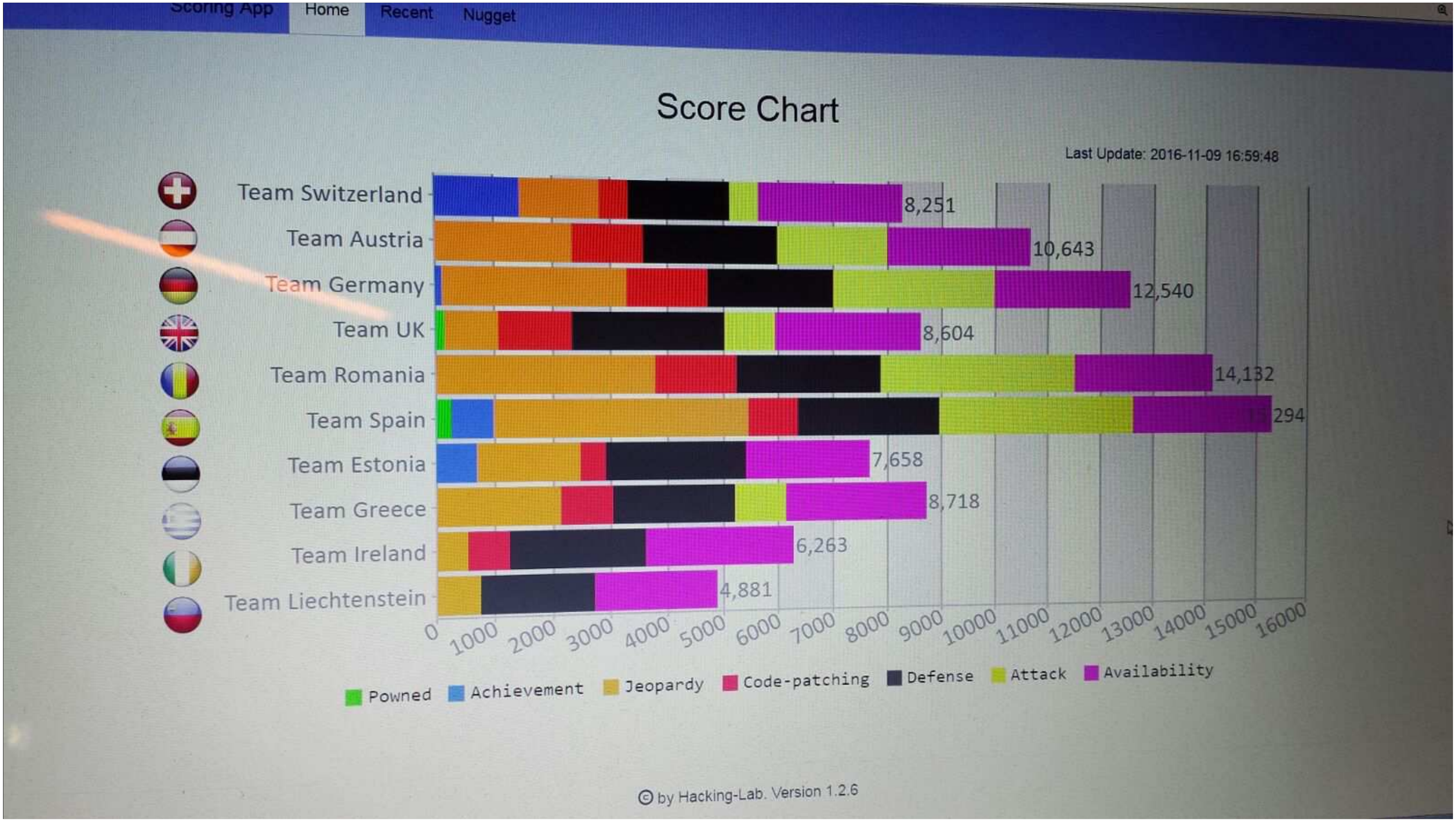
TIME	ATTACKER GEO	INCIDENT TYPE	SEVERITY
19 Oct 21:37:9	United States of America	Squid Proxy String Processing ...	medium
19 Oct 21:37:9	United States of America	Squid Proxy String Processing ...	medium
19 Oct 21:24:4	United States of America	Kelihos	critical
19 Oct 21:18:23	Netherlands	Muieblackcat Scanner	low
19 Oct 21:18:23	Netherlands	Muieblackcat Scanner	low
19 Oct 21:18:23	Netherlands	Muieblackcat Scanner	low
19 Oct 21:18:23	Netherlands	Muieblackcat Scanner	low
19 Oct 21:18:23	Netherlands	Muieblackcat Scanner	low
19 Oct 21:18:23	Netherlands	Muieblackcat Scanner	low

Copyright © Orange Romania. All rights reserved.

Orange bug bounty program

DefCamp #7
Where Hacking & Security Collide
App2Own
DefCamp
DefCamp 6
Where Hacking & Security Collide

Business Services
TRAIN YOUR
STAFF
Global Education
Program
Online Security
Training
On-Site Security
Training



Score Chart

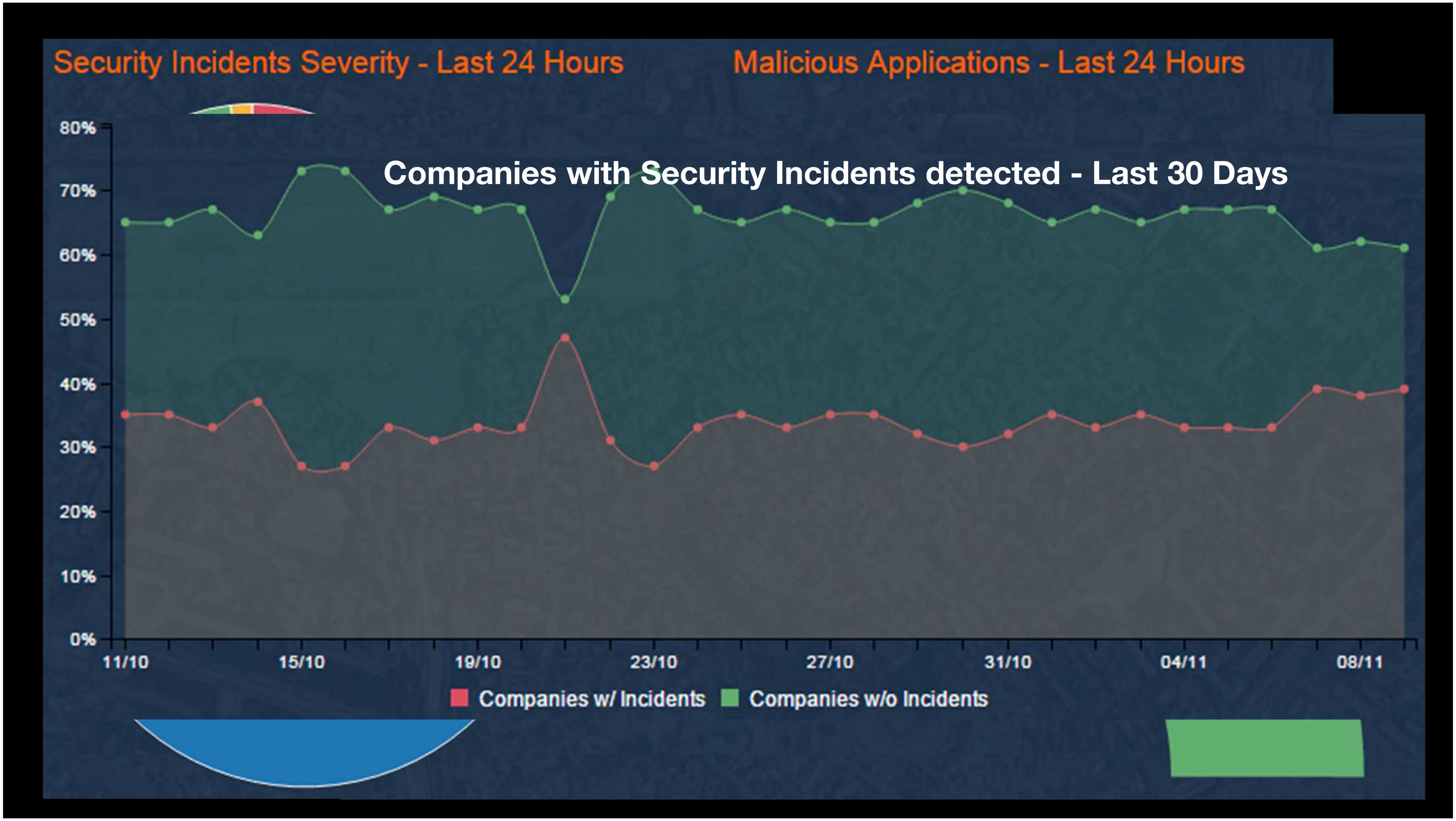
Last Update: 2016-11-09 16:59:48

© by Hacking-Lab. Version 1.2.6

EURO
CYBER SECURITY
CHALLENGE
Evil prevails when good humans do nothing!

https://bis-threatmap.orange.ro

developed in partnership with BIT SENTINEL


Security Incidents Severity - Last 24 Hours
Malicious Applications - Last 24 Hours
Companies with Security Incidents detected - Last 30 Days
80%
70%
60%
50%
40%
30%
20%
10%
0%
11/10
15/10
19/10
23/10
27/10
31/10
04/11
08/11
🟥 Companies w/ Incidents
🟩 Companies w/o Incidents

Orange App2Own Bug Bounty program
for a safer online environment

Orange promotes Bug Bounty initiatives in order to test and improve the accuracy of the cybersecurity solutions developed to protect the Internet access for organizations.

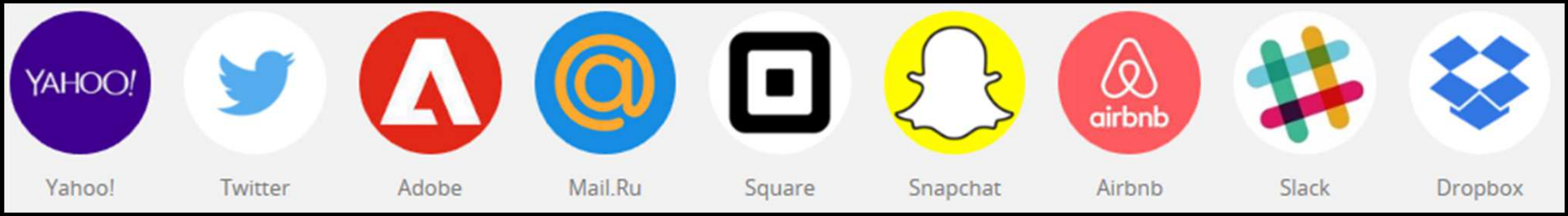
Orange is the only telecommunication operator from Romania that supports vulnerabilities identification and responsible disclosure.

Orange Bug Bounty challenge will continue
http://def.camp

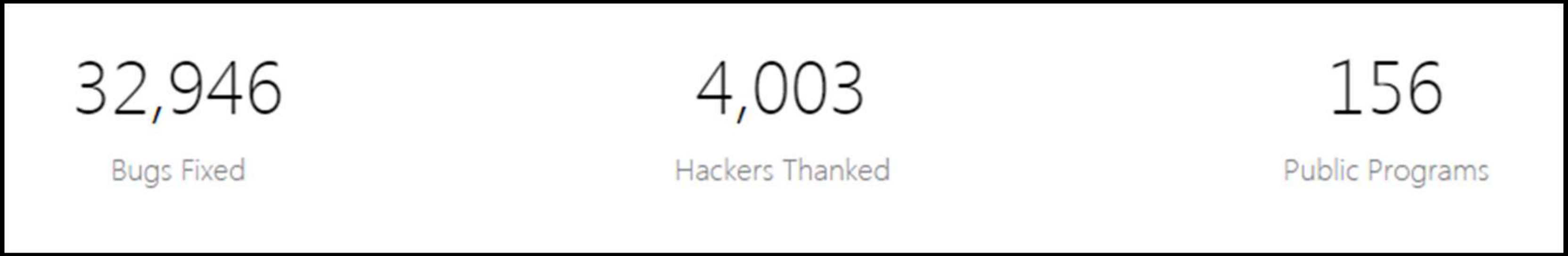
bug bounty in the world

modern security is hacker-powered

Top Companies work with Hackers



Yahoo! · Twitter · Adobe · Mail.Ru · Square · Snapchat · Airbnb · Slack · Dropbox



32,946	4,003	156
Bugs Fixed	Hackers Thanked	Public Programs

https://hackerone.com

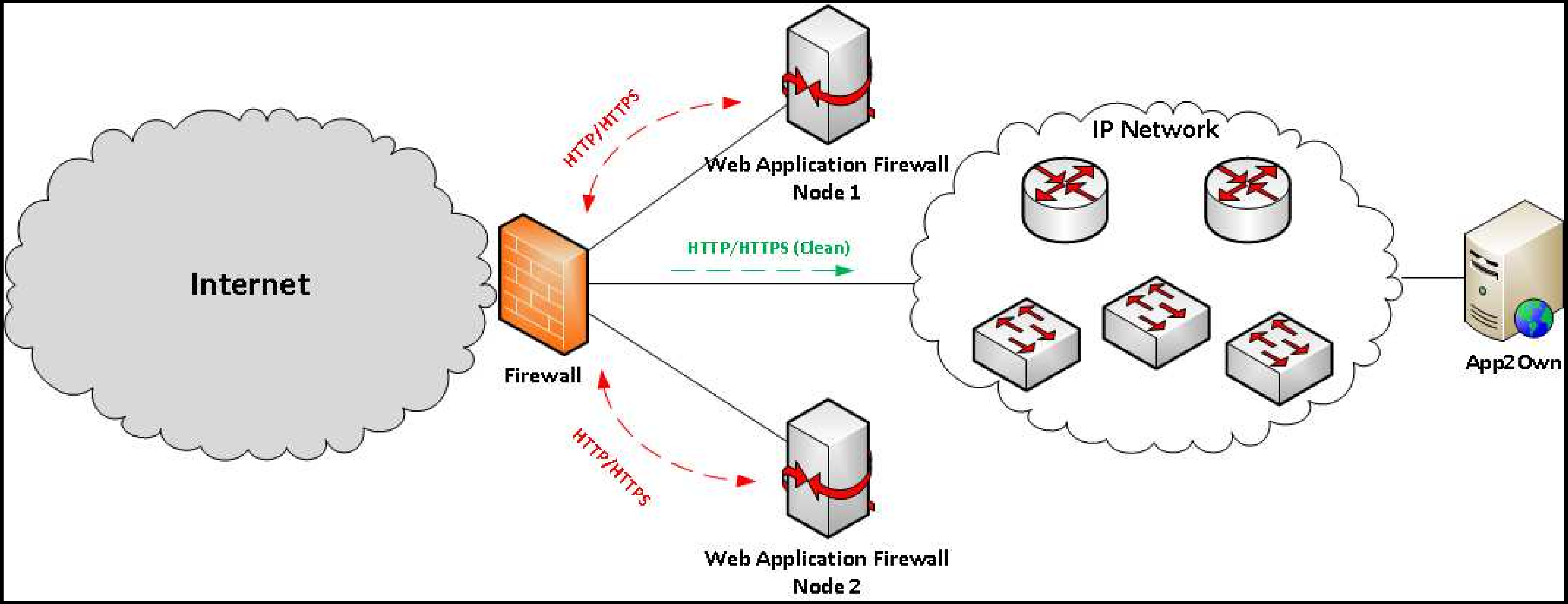
guidelines to follow
for a winning competition

- start : October 31st
- register
- info about the target
- bypass the security to reach the target
- send asap the exploit report
- if validated the rank will be updated
- stop : November 11th

rules of game
for a responsible disclosure

- points based on the vulnerability risk you managed to exploit
- play only as an individual, the rule of first to report the same bypass
- dashboard page with assets you have permission to attack
- cheating or destroying challenges is not allowed
- (D)DOS is not accepted
- trying to ignore the rules above will get you banned
- innovative methods will get you extra points

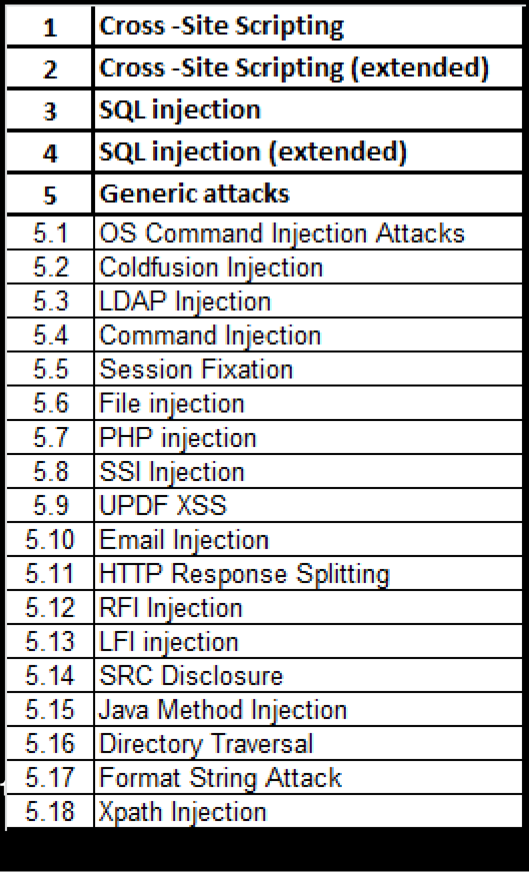
infrastructure set-up
ready for commercial switch on



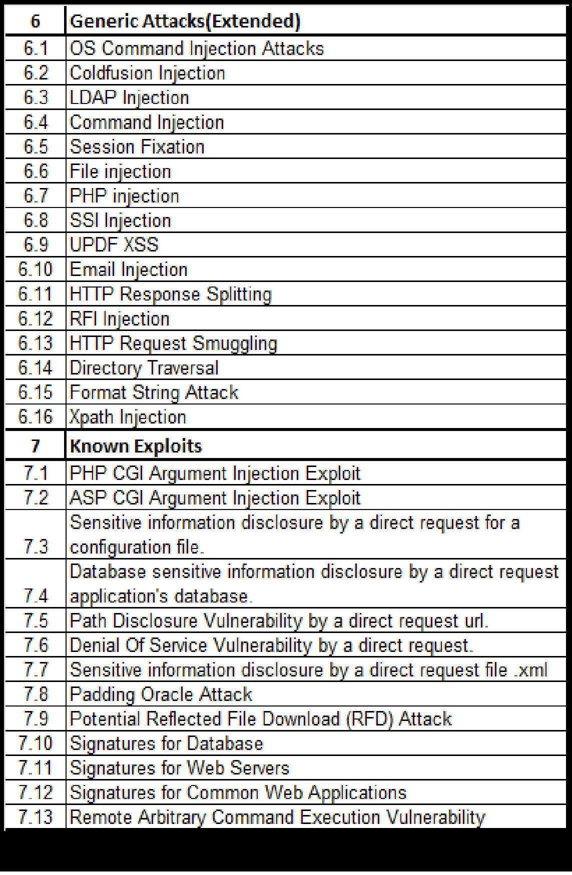
various difficulty levels
to challenge and be challenged

- Oct 31st – Nov 6th: online contest, with some security features deactivated (low sec profile)
- Nov 7th – Nov 9th: online contest, with most security features activated (high sec profile)
- Nov 10th, from 9:00 – to Nov 10th, 19:00: on site contest, with some security features deactivated (low sec profile)
- Nov 11th, from 9:00 – to Nov 11th, 16:00: on site contest, with most security features activated (high sec profile)

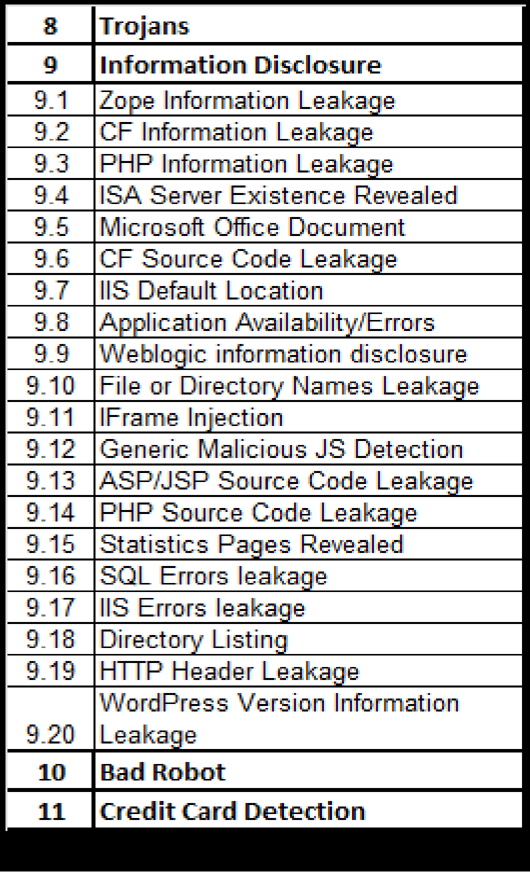
low sec profile
to emulate real life situation



1	**Cross -Site Scripting**
2	**Cross -Site Scripting (extended)**
3	**SQL injection**
4	**SQL injection (extended)**
5	**Generic attacks**
5.1	OS Command Injection Attacks
5.2	Coldfusion Injection
5.3	LDAP Injection
5.4	Command Injection
5.5	Session Fixation
5.6	File injection
5.7	PHP injection
5.8	SSI Injection
5.9	UPDF XSS
5.10	Email Injection
5.11	HTTP Response Splitting
5.12	RFI Injection
5.13	LFI injection
5.14	SRC Disclosure
5.15	Java Method Injection
5.16	Directory Traversal
5.17	Format String Attack
5.18	Xpath Injection

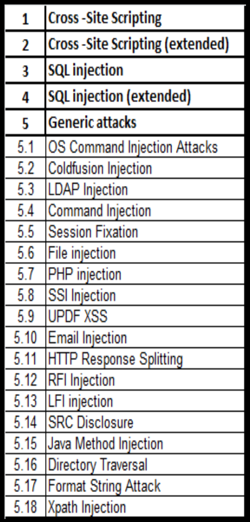


6	**Generic Attacks(Extended)**
6.1	OS Command Injection Attacks
6.2	Coldfusion Injection
6.3	LDAP Injection
6.4	Command Injection
6.5	Session Fixation
6.6	File injection
6.7	PHP injection
6.8	SSI Injection
6.9	UPDF XSS
6.10	Email Injection
6.11	HTTP Response Splitting
6.12	RFI Injection
6.13	HTTP Request Smuggling
6.14	Directory Traversal
6.15	Format String Attack
6.16	Xpath Injection
7	**Known Exploits**
7.1	PHP CGI Argument Injection Exploit
7.2	ASP CGI Argument Injection Exploit
7.3	Sensitive information disclosure by a direct request for a configuration file.
7.4	Database sensitive information disclosure by a direct request application's database.
7.5	Path Disclosure Vulnerability by a direct request url.
7.6	Denial Of Service Vulnerability by a direct request.
7.7	Sensitive information disclosure by a direct request file .xml
7.8	Padding Oracle Attack
7.9	Potential Reflected File Download (RFD) Attack
7.10	Signatures for Database
7.11	Signatures for Web Servers
7.12	Signatures for Common Web Applications
7.13	Remote Arbitrary Command Execution Vulnerability

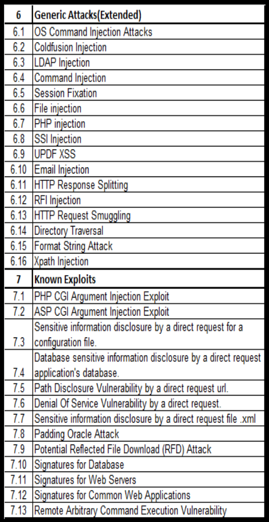


8	**Trojans**
9	**Information Disclosure**
9.1	Zope Information Leakage
9.2	CF Information Leakage
9.3	PHP Information Leakage
9.4	ISA Server Existence Revealed
9.5	Microsoft Office Document
9.6	CF Source Code Leakage
9.7	IIS Default Location
9.8	Application Availability/Errors
9.9	Weblogic information disclosure
9.10	File or Directory Names Leakage
9.11	IFrame Injection
9.12	Generic Malicious JS Detection
9.13	ASP/JSP Source Code Leakage
9.14	PHP Source Code Leakage
9.15	Statistics Pages Revealed
9.16	SQL Errors leakage
9.17	IIS Errors leakage
9.18	Directory Listing
9.19	HTTP Header Leakage
9.20	WordPress Version Information Leakage
10	**Bad Robot**
11	**Credit Card Detection**

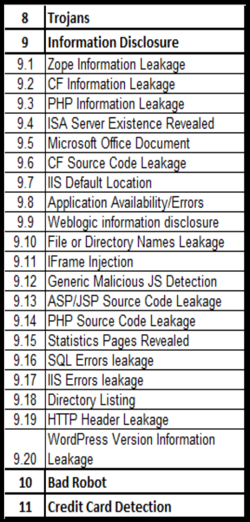
high sec profile
to emulate real life situation



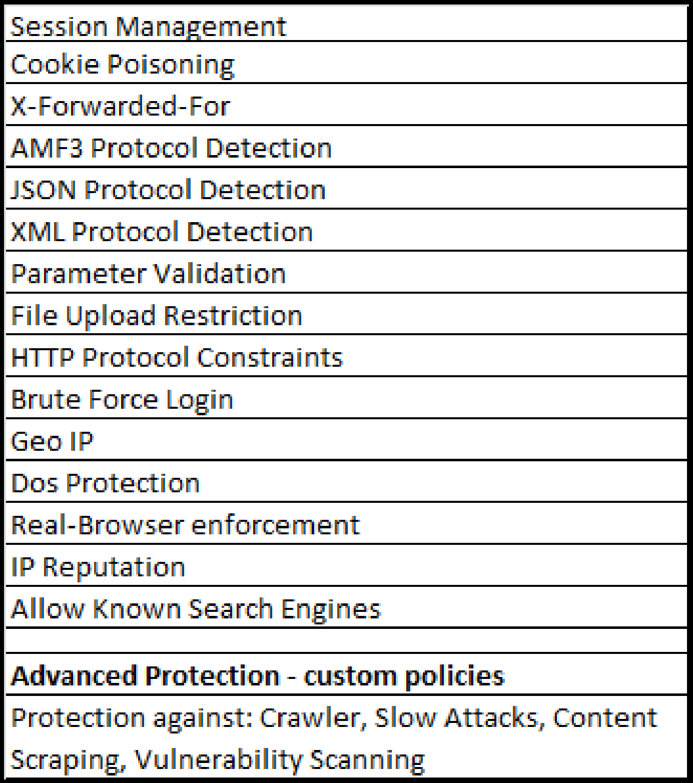
1	**Cross -Site Scripting**
2	**Cross -Site Scripting (extended)**
3	**SQL injection**
4	**SQL injection (extended)**
5	**Generic attacks**
5.1	OS Command Injection Attacks
5.2	Coldfusion Injection
5.3	LDAP Injection
5.4	Command Injection
5.5	Session Fixation
5.6	File injection
5.7	PHP injection
5.8	SSI Injection
5.9	UPDF XSS
5.10	Email Injection
5.11	HTTP Response Splitting
5.12	RFI Injection
5.13	LFI injection
5.14	SRC Disclosure
5.15	Java Method Injection
5.16	Directory Traversal
5.17	Format String Attack
5.18	Xpath Injection



6	**Generic Attacks(Extended)**
6.1	OS Command Injection Attacks
6.2	Coldfusion Injection
6.3	LDAP Injection
6.4	Command Injection
6.5	Session Fixation
6.6	File injection
6.7	PHP injection
6.8	SSI Injection
6.9	UPDF XSS
6.10	Email Injection
6.11	HTTP Response Splitting
6.12	RFI Injection
6.13	HTTP Request Smuggling
6.14	Directory Traversal
6.15	Format String Attack
6.16	Xpath Injection
7	**Known Exploits**
7.1	PHP CGI Argument Injection Exploit
7.2	ASP CGI Argument Injection Exploit
7.3	Sensitive information disclosure by a direct request for a configuration file.
7.4	Database sensitive information disclosure by a direct request application's database.
7.5	Path Disclosure Vulnerability by a direct request url.
7.6	Denial Of Service Vulnerability by a direct request.
7.7	Sensitive information disclosure by a direct request file .xml
7.8	Padding Oracle Attack
7.9	Potential Reflected File Download (RFD) Attack
7.10	Signatures for Database
7.11	Signatures for Web Servers
7.12	Signatures for Common Web Applications
7.13	Remote Arbitrary Command Execution Vulnerability



8	**Trojans**
9	**Information Disclosure**
9.1	Zope Information Leakage
9.2	CF Information Leakage
9.3	PHP Information Leakage
9.4	ISA Server Existence Revealed
9.5	Microsoft Office Document
9.6	CF Source Code Leakage
9.7	IIS Default Location
9.8	Application Availability/Errors
9.9	Weblogic information disclosure
9.10	File or Directory Names Leakage
9.11	IFrame Injection
9.12	Generic Malicious JS Detection
9.13	ASP/JSP Source Code Leakage
9.14	PHP Source Code Leakage
9.15	Statistics Pages Revealed
9.16	SQL Errors leakage
9.17	IIS Errors leakage
9.18	Directory Listing
9.19	HTTP Header Leakage
9.20	WordPress Version Information Leakage
10	**Bad Robot**
11	**Credit Card Detection**

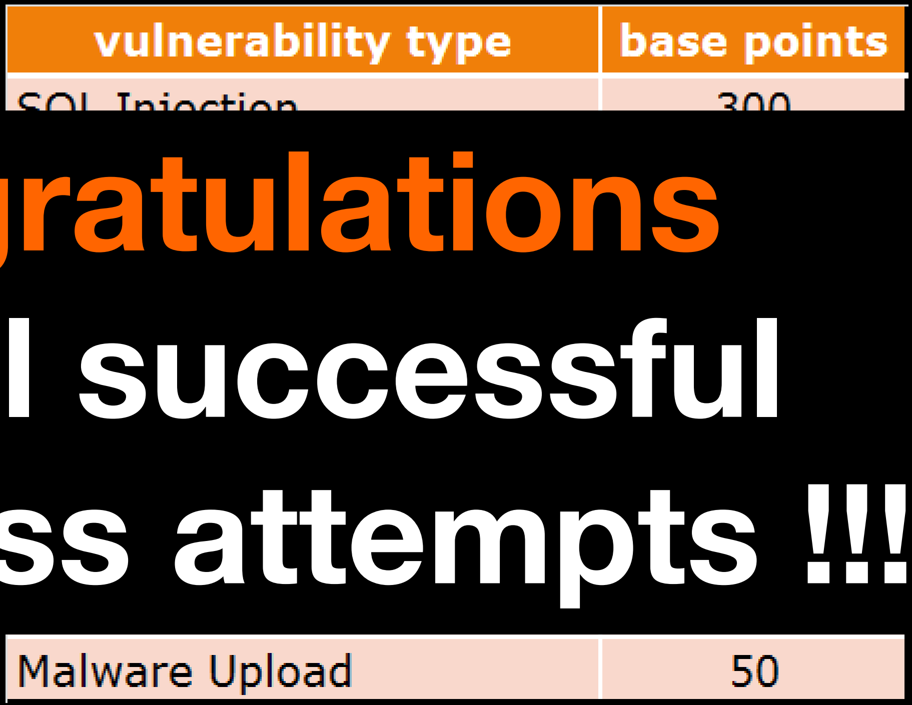


Session Management
Cookie Poisoning
X-Forwarded-For
AMF3 Protocol Detection
JSON Protocol Detection
XML Protocol Detection
Parameter Validation
File Upload Restriction
HTTP Protocol Constraints
Brute Force Login
Geo IP
Dos Protection
Real-Browser enforcement
IP Reputation
Allow Known Search Engines
Advanced Protection - custom policies
Protection against: Crawler, Slow Attacks, Content Scraping, Vulnerability Scanning

contest draft statistics
until 10th Nov, 18:00

- 58 registered p
- 8 participants
- 68 received re
- 48 validated re
- 3,143 granted points

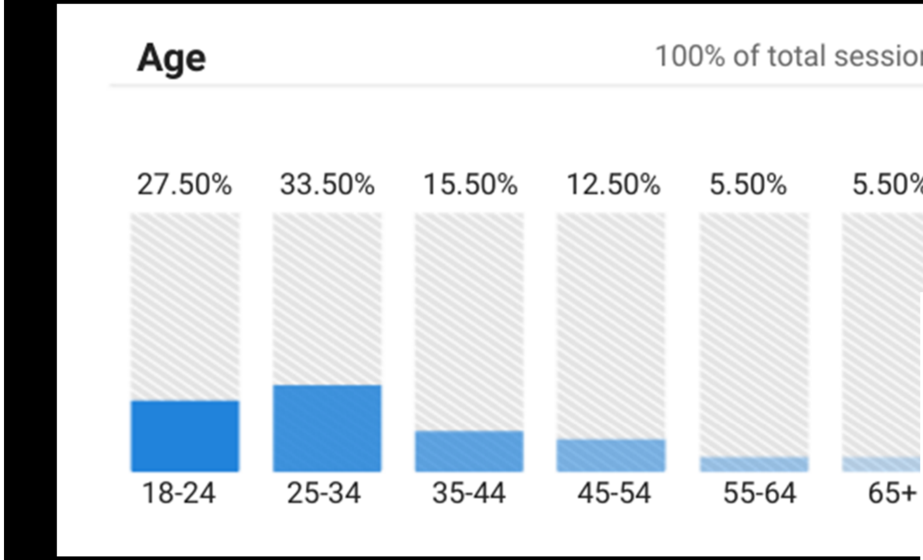
Congratulations for all successful bypass attempts !!!



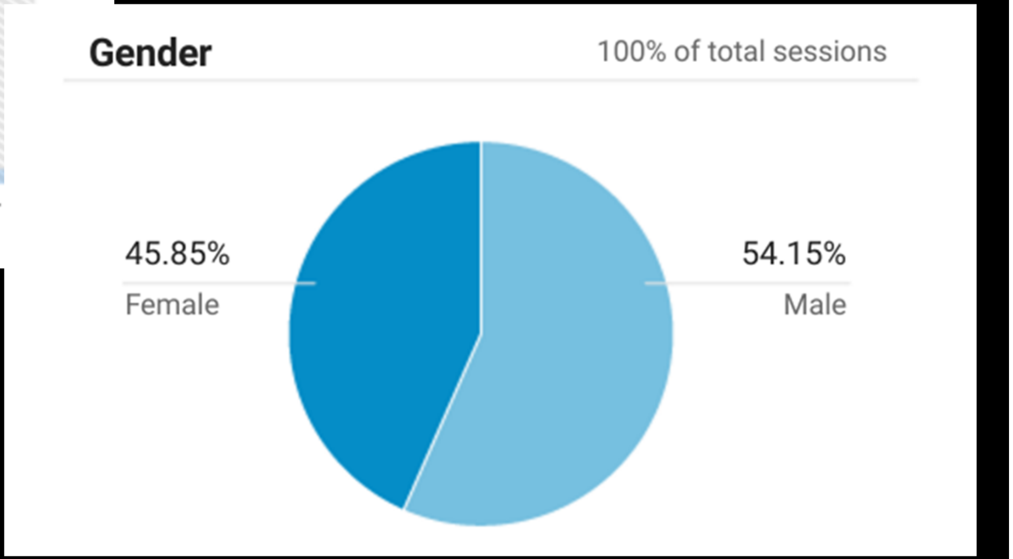
vulnerability type	base points
SQL Injection	300
Malware Upload	50

low sec profile : 40% scoring
high sec profile : 100% scoring

more funny stats

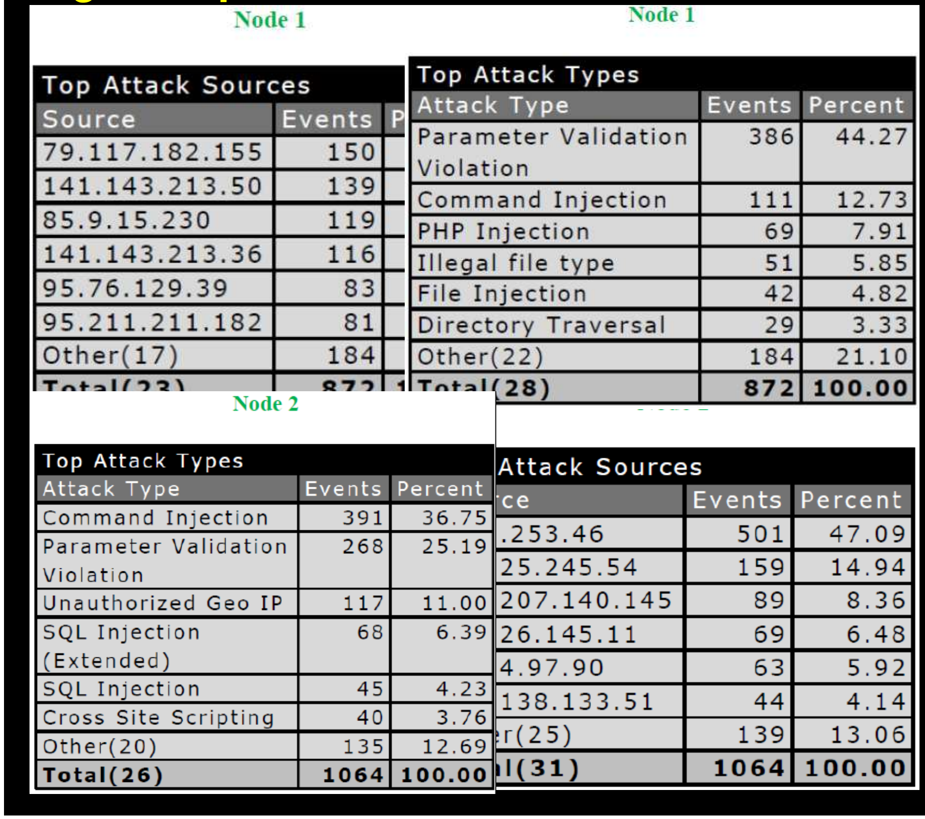


10 countries



detected attacks
FortiWeb [10th Nov, 18:00]

high sec profile



Node 1

Top Attack Sources

Source	Events	P
79.117.182.155	150	
141.143.213.50	139	
85.9.15.230	119	
141.143.213.36	116	
95.76.129.39	83	
95.211.211.182	81	
Other(17)	184	
Total(23)	872	1

Node 1

Top Attack Types

Attack Type	Events	Percent
Parameter Validation Violation	386	44.27
Command Injection	111	12.73
PHP Injection	69	7.91
Illegal file type	51	5.85
File Injection	42	4.82
Directory Traversal	29	3.33
Other(22)	184	21.10
Total(28)	872	100.00

Node 2

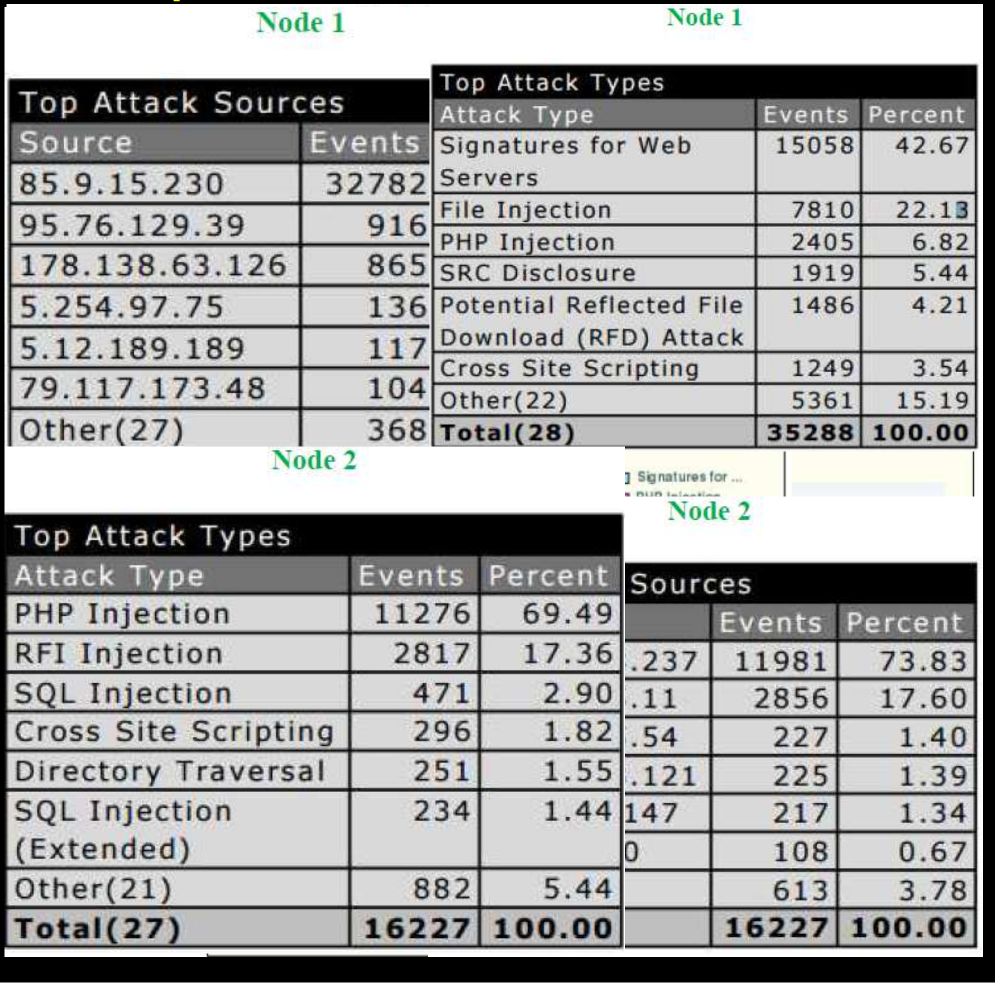
Top Attack Types

Attack Type	Events	Percent
Command Injection	391	36.75
Parameter Validation Violation	268	25.19
Unauthorized Geo IP	117	11.00
SQL Injection (Extended)	68	6.39
SQL Injection	45	4.23
Cross Site Scripting	40	3.76
Other(20)	135	12.69
Total(26)	1064	100.00

Attack Sources

ce	Events	Percent
.253.46	501	47.09
25.245.54	159	14.94
207.140.145	89	8.36
26.145.11	69	6.48
4.97.90	63	5.92
138.133.51	44	4.14
r(25)	139	13.06
l(31)	1064	100.00

low sec profile



Node 1

Top Attack Sources

Source	Events
85.9.15.230	32782
95.76.129.39	916
178.138.63.126	865
5.254.97.75	136
5.12.189.189	117
79.117.173.48	104
Other(27)	368

Node 1

Top Attack Types

Attack Type	Events	Percent
Signatures for Web Servers	15058	42.67
File Injection	7810	22.13
PHP Injection	2405	6.82
SRC Disclosure	1919	5.44
Potential Reflected File Download (RFD) Attack	1486	4.21
Cross Site Scripting	1249	3.54
Other(22)	5361	15.19
Total(28)	35288	100.00

Node 2

Top Attack Types

Attack Type	Events	Percent
PHP Injection	11276	69.49
RFI Injection	2817	17.36
SQL Injection	471	2.90
Cross Site Scripting	296	1.82
Directory Traversal	251	1.55
SQL Injection (Extended)	234	1.44
Other(21)	882	5.44
Total(27)	16227	100.00

Signatures for ...

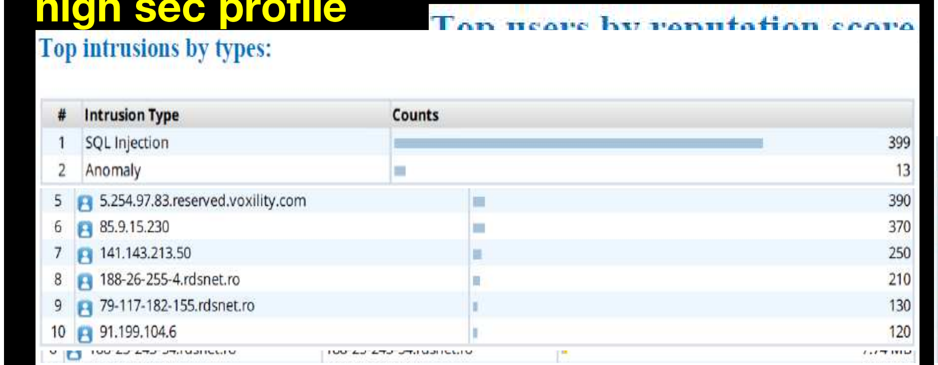
Node 2

Sources

	Events	Percent
.237	11981	73.83
.11	2856	17.60
.54	227	1.40
.121	225	1.39
147	217	1.34
0	108	0.67
	613	3.78
	16227	100.00

detected attacks
FortiGate [10th Nov, 18:00]

high sec profile

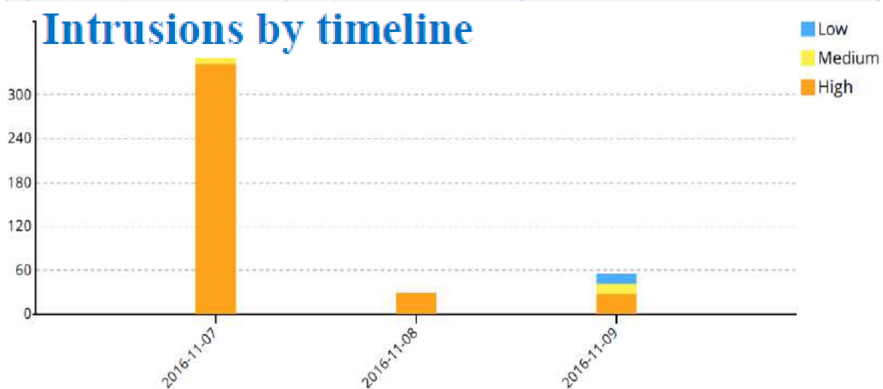


Top users by reputation score

Top intrusions by types:

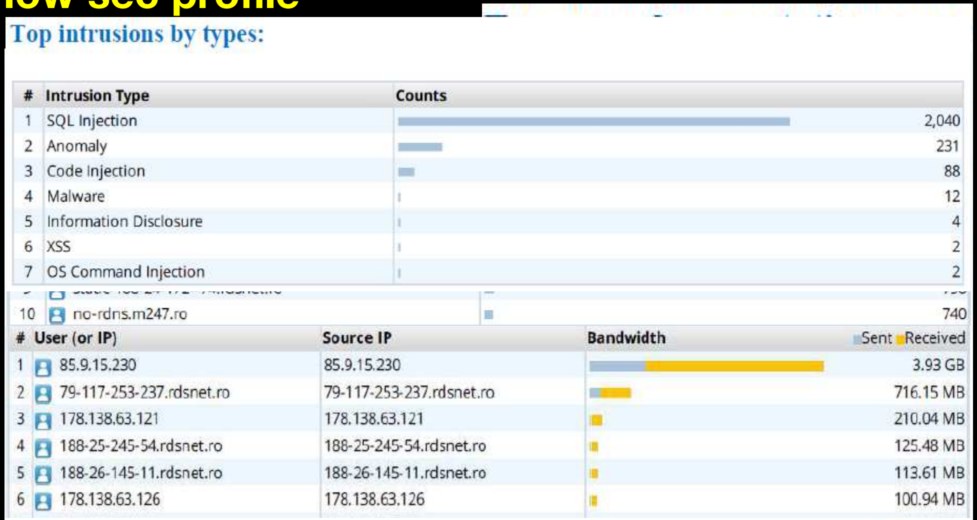
#	Intrusion Type	Counts
1	SQL Injection	399
2	Anomaly	13

5	5.254.97.83.reserved.voxility.com	390
6	85.9.15.230	370
7	141.143.213.50	250
8	188-26-255-4.rdsnet.ro	210
9	79-117-182-155.rdsnet.ro	130
10	91.199.104.6	120



Intrusions by timeline

low sec profile

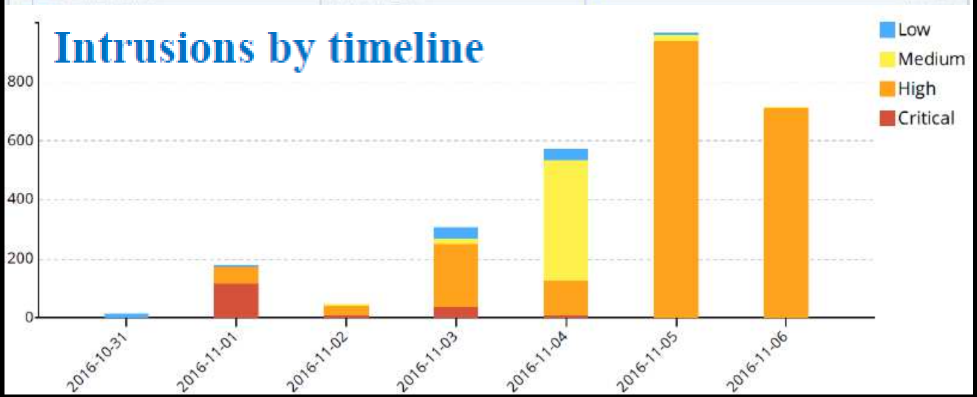


Top intrusions by types:

#	Intrusion Type	Counts
1	SQL Injection	2,040
2	Anomaly	231
3	Code Injection	88
4	Malware	12
5	Information Disclosure	4
6	XSS	2
7	OS Command Injection	2

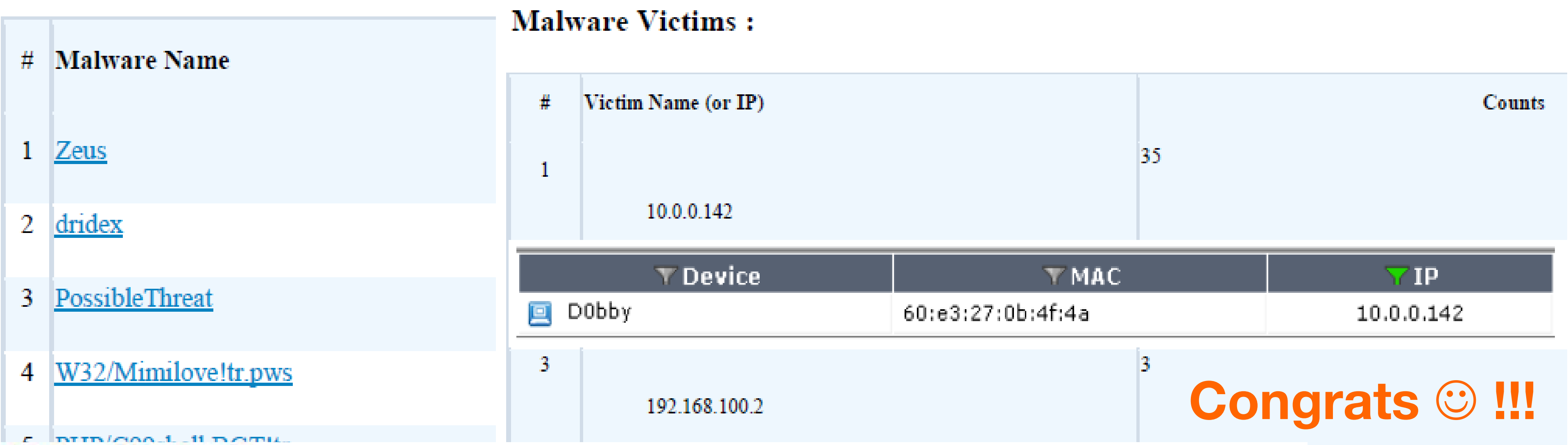
10	no-rdns.m247.ro	740

#	User (or IP)	Source IP	Bandwidth ▨Sent ▨Received
1	85.9.15.230	85.9.15.230	3.93 GB
2	79-117-253-237.rdsnet.ro	79-117-253-237.rdsnet.ro	716.15 MB
3	178.138.63.121	178.138.63.121	210.04 MB
4	188-25-245-54.rdsnet.ro	188-25-245-54.rdsnet.ro	125.48 MB
5	188-26-145-11.rdsnet.ro	188-26-145-11.rdsnet.ro	113.61 MB
6	178.138.63.126	178.138.63.126	100.94 MB



Intrusions by timeline

Malware Detected:



#	Malware Name
1	Zeus
2	dridex
3	PossibleThreat
4	W32/Mimilove!tr.pws
5	PHP/C99shell.BGT!tr

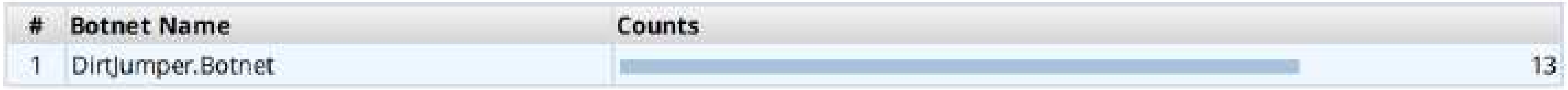
Malware Victims :

#	Victim Name (or IP)	Counts
1	10.0.0.142	35
3	192.168.100.2	3

Device	MAC	IP
D0bby	60:e3:27:0b:4f:4a	10.0.0.142

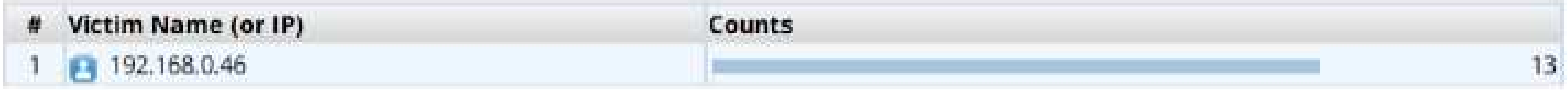
Congrats ☺ !!!

Botnets Detected:



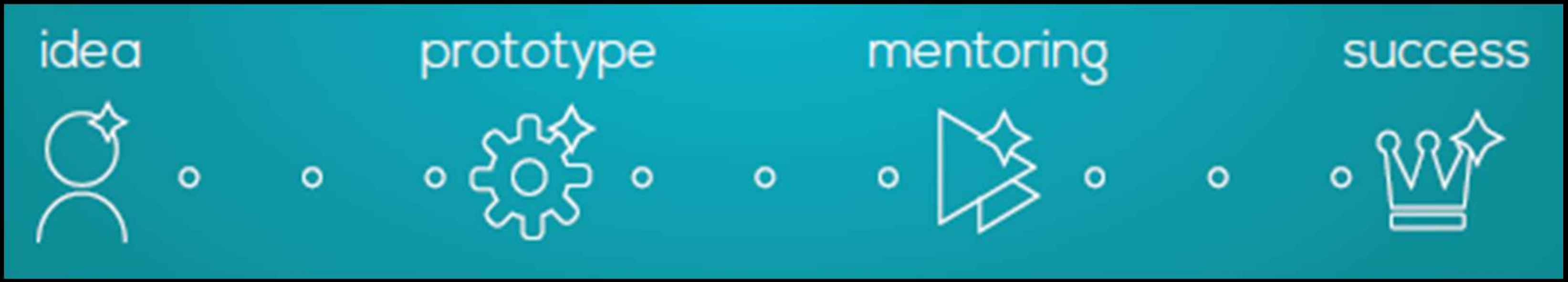
#	Botnet Name	Counts
1	DirtJumper.Botnet	13

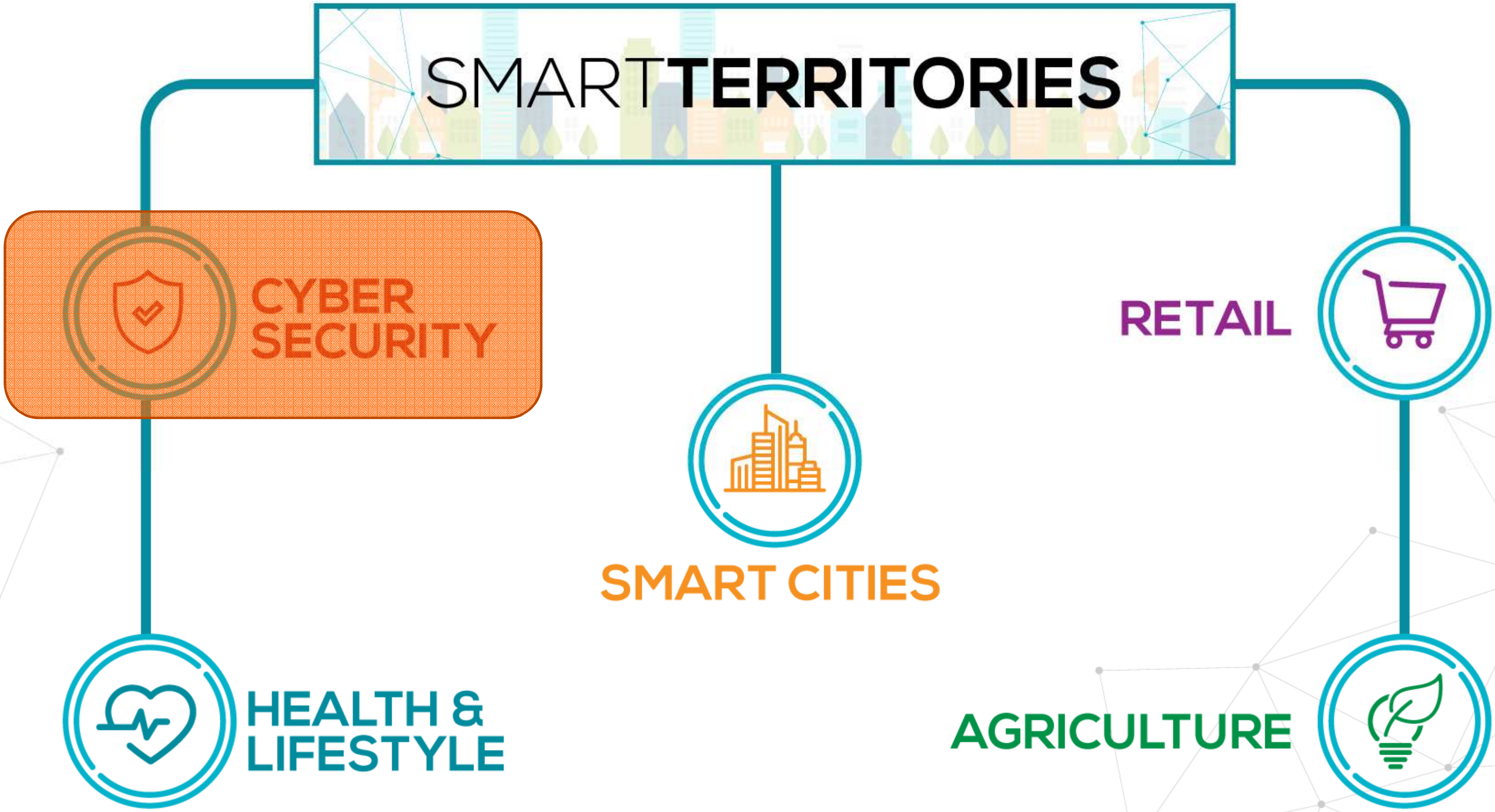
Botnets Victims:



#	Victim Name (or IP)	Counts
1	192.168.0.46	13

INNOVATION LABS 2017





SMART**TERRITORIES**

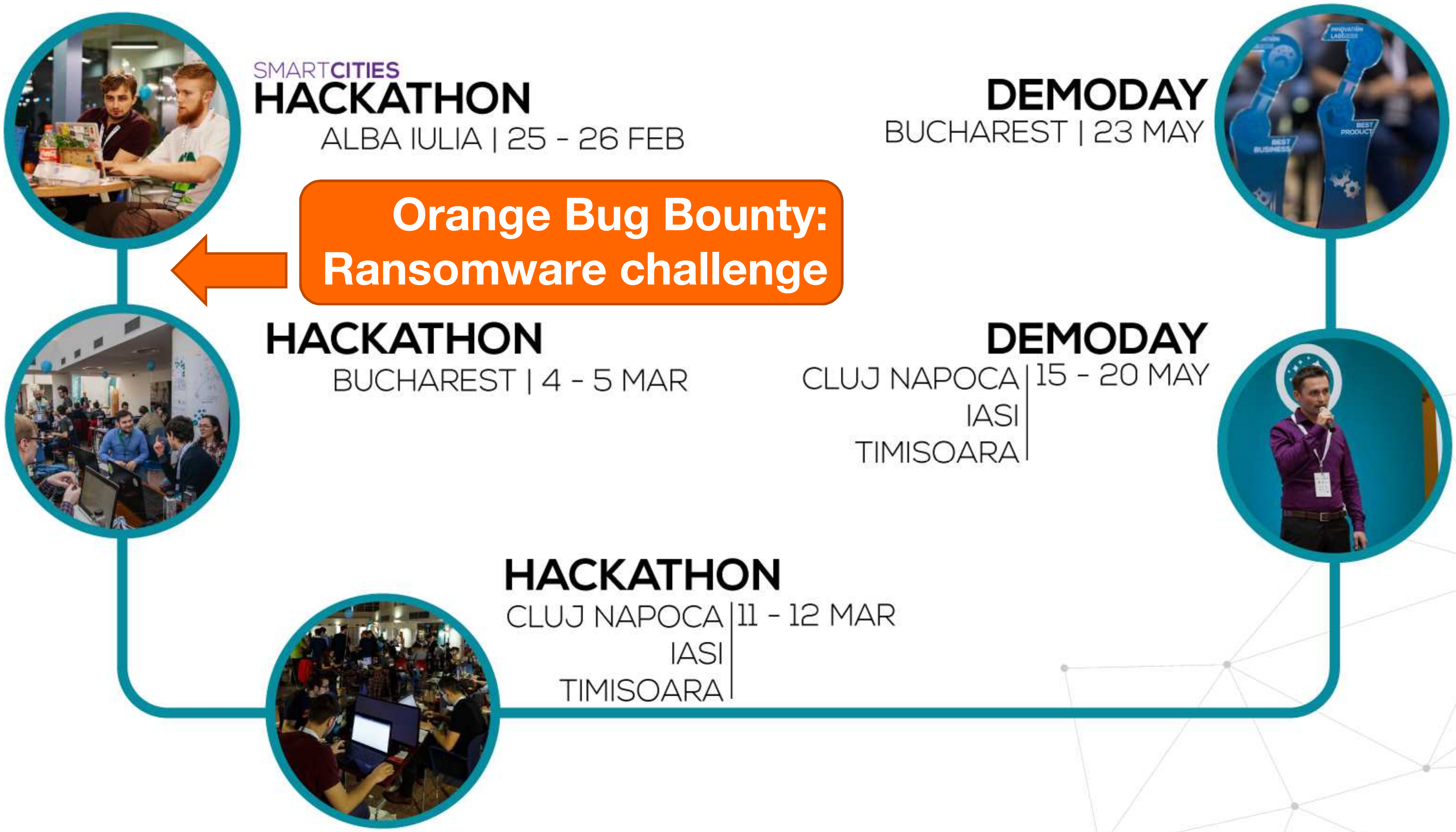
CYBER SECURITY

SMART CITIES

RETAIL

HEALTH & LIFESTYLE

AGRICULTURE



SMARTCITIES
HACKATHON
ALBA IULIA | 25 - 26 FEB

Orange Bug Bounty: Ransomware challenge

HACKATHON
BUCHAREST | 4 - 5 MAR

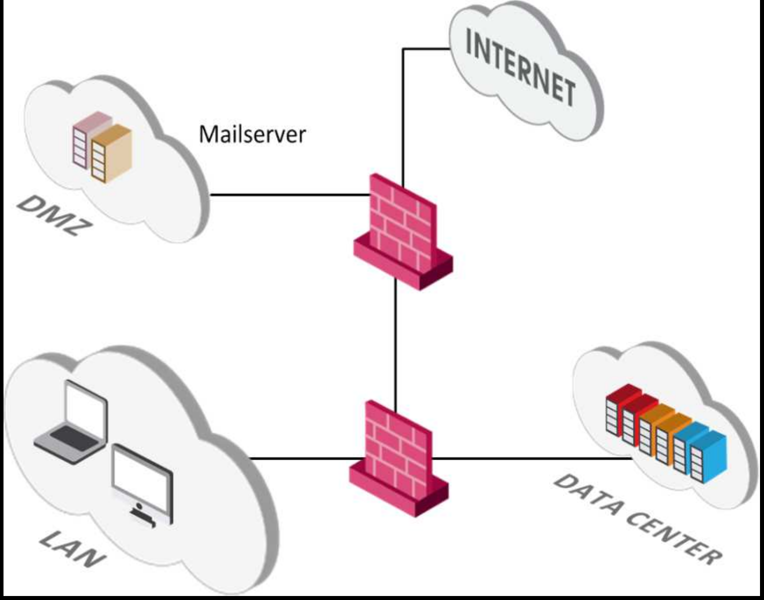
HACKATHON
CLUJ NAPOCA | 11 - 12 MAR
IASI |
TIMISOARA |

DEMODAY
CLUJ NAPOCA | 15 - 20 MAY
IASI |
TIMISOARA |

DEMODAY
BUCHAREST | 23 MAY

Ransomware challenge
to continue the bug bounty

- target: one large corporation’s HR department
- HR department receives CVs or other docs, but they will click on any attachment [pdf, doc, xls, …]
- the challenge is to encrypt “important_file.xls” and ask for ransom
- extra points if you can encrypt the file with preventive measures implemented from at least one solution
- even more extra points for data exfiltration



Ransomware challenge
to continue the bug bounty

- according to security level there will be more than one mailbox, each with increasing levels of protection/difficulty
- each participant can chose which mailbox to target, or can target all of them
- once the file is encrypted you receive points based on the time elapsed
- if you manage to bypass one or more of the protections you receive extra points (min 2 sandboxing solutions will be used)
- if you manage to communicate the contents of the file you receive even more extra points

Ransomware challenge
to continue the bug bounty

- 2 weeks for online challenge [13th – 25th Feb 2017], 1 day for award ceremony during Innovation Labs hackathon in Bucharest [4th – 5th March 2017]

- follow DefCamp and Innovation Labs sites for more details

takeaways
that might be useful

- security audits and penetration tests as a business as usual processes
- Orange is looking for start-ups, local innovators and public data sets providers to help extend the smart cities ecosystem
- security through open innovation and data sharing
- Orange is looking for real time RO security logs to update the threat map and rise the awareness on cyber security risks

always look for the quality of the TEAM behind

Orange Bug Bounty challenges will continue with Ransomware challenge

http://def.camp

https://bis-threatmap.orange.ro

join us in Innovation Labs 2017

http://www.innovationlabs.ro

Thanks.
We are here for you.
We’re listening.

orange™