EUROPEAN CYBER SECURITY CHALLENGE
LONDON, UNITED KINGDOM 2016

HELLENIC CYBER SECURITY TEAM

enisa
European Network and Information Security Agency

The new Landscape of Cyber Threats and the European Cyber Security Challenge

Systems Security Laboratory (http://ssl.ds.unipi.gr/)

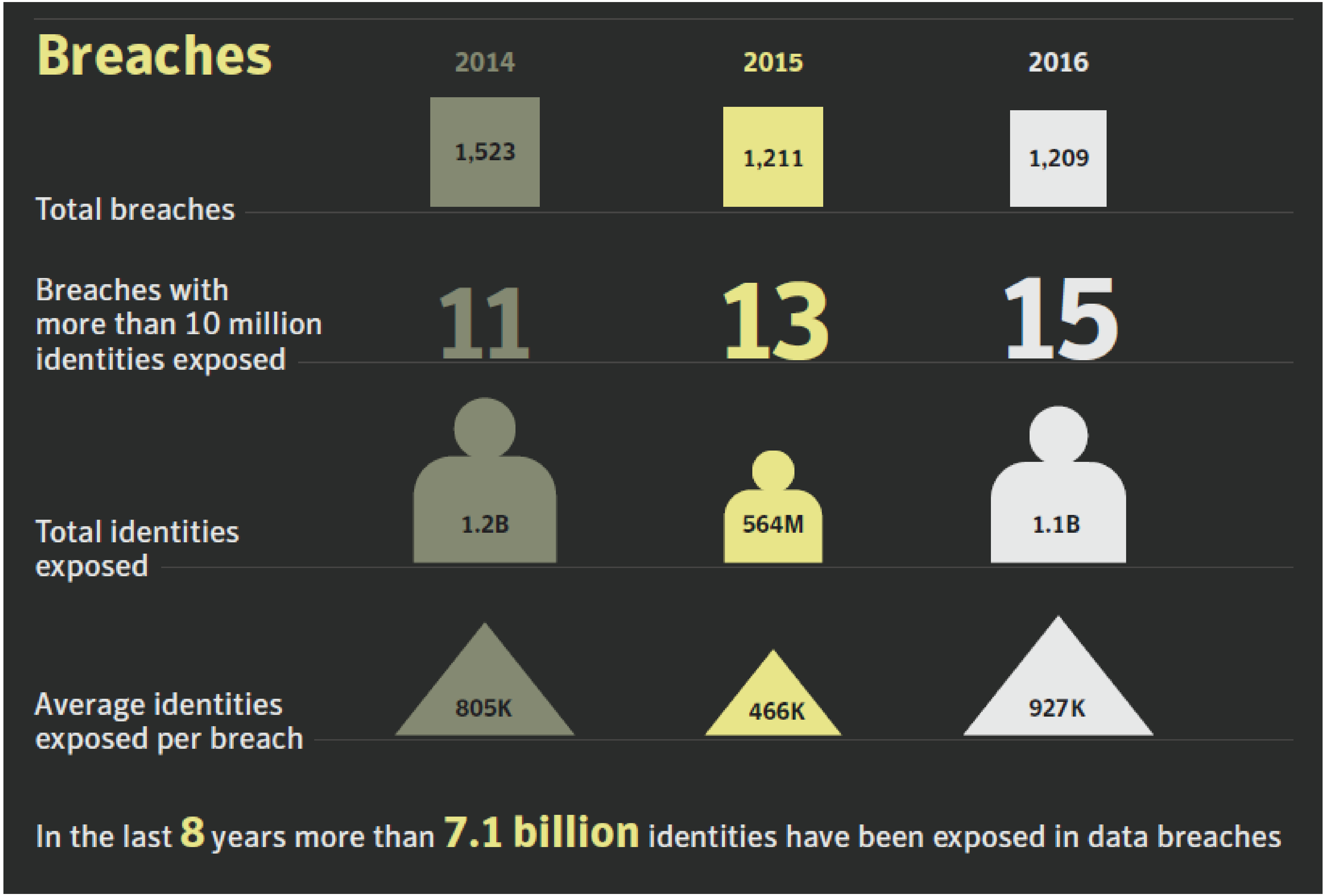
Member of the European Cyber Security Challenge Steering Committee

Department of Digital Systems, University of Piraeus

Associate Professor Christos Xenakis

UNIVERSITY OF PIRAEUS

UNIVERSITY OF PIRAEUS RESEARCH CENTER

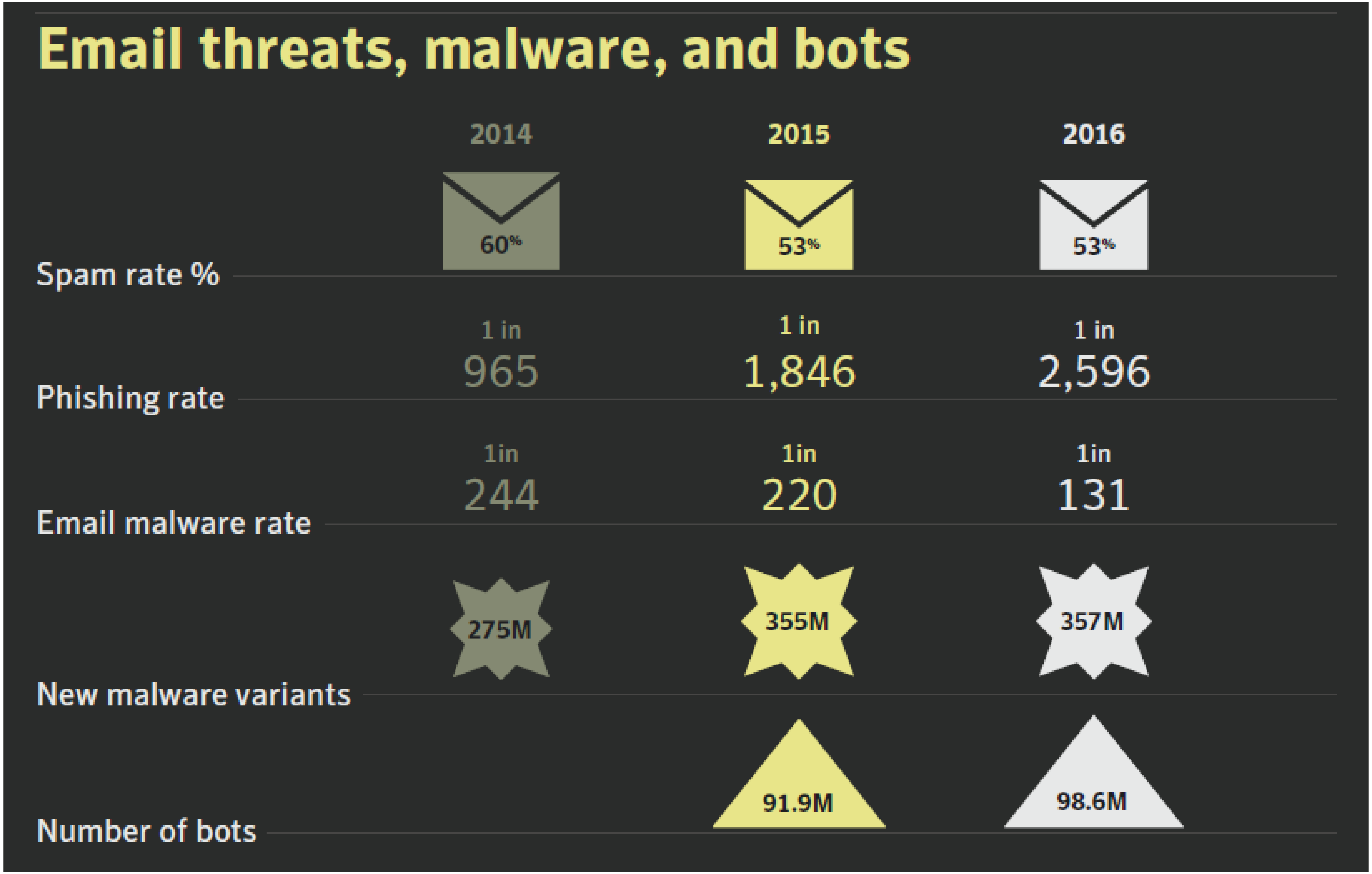


Breaches

	2014	2015	2016
Total breaches	1,523	1,211	1,209
Breaches with more than 10 million identities exposed	11	13	15
Total identities exposed	1.2B	564M	1.1B
Average identities exposed per breach	805K	466K	927K

In the last **8** years more than **7.1 billion** identities have been exposed in data breaches

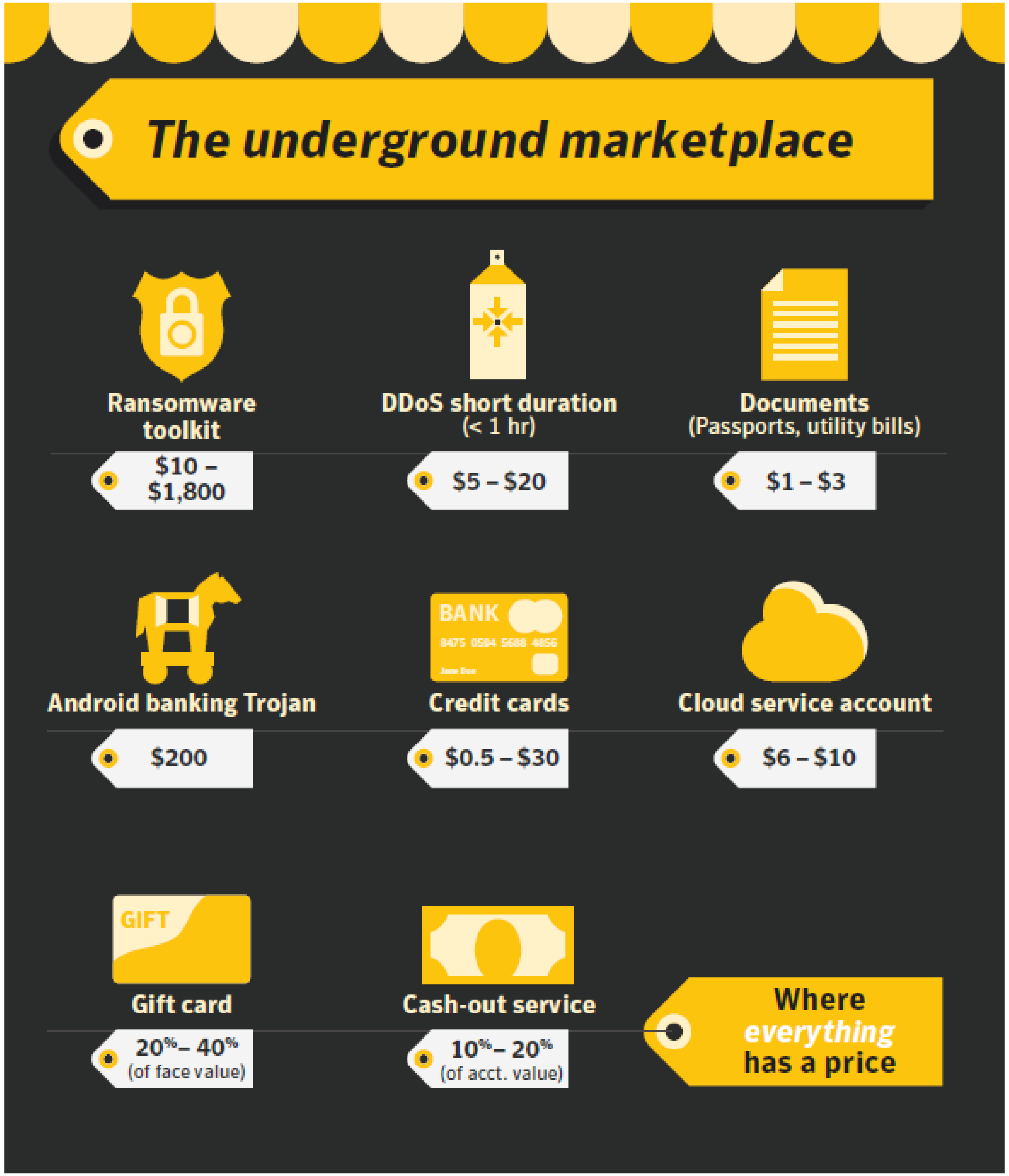
https://www.symantec.com/security-center/threat-report



Email threats, malware, and bots

	2014	2015	2016
Spam rate %	60%	53%	53%
Phishing rate	1 in 965	1 in 1,846	1 in 2,596
Email malware rate	1in 244	1in 220	1in 131
New malware variants	275M	355M	357M
Number of bots		91.9M	98.6M

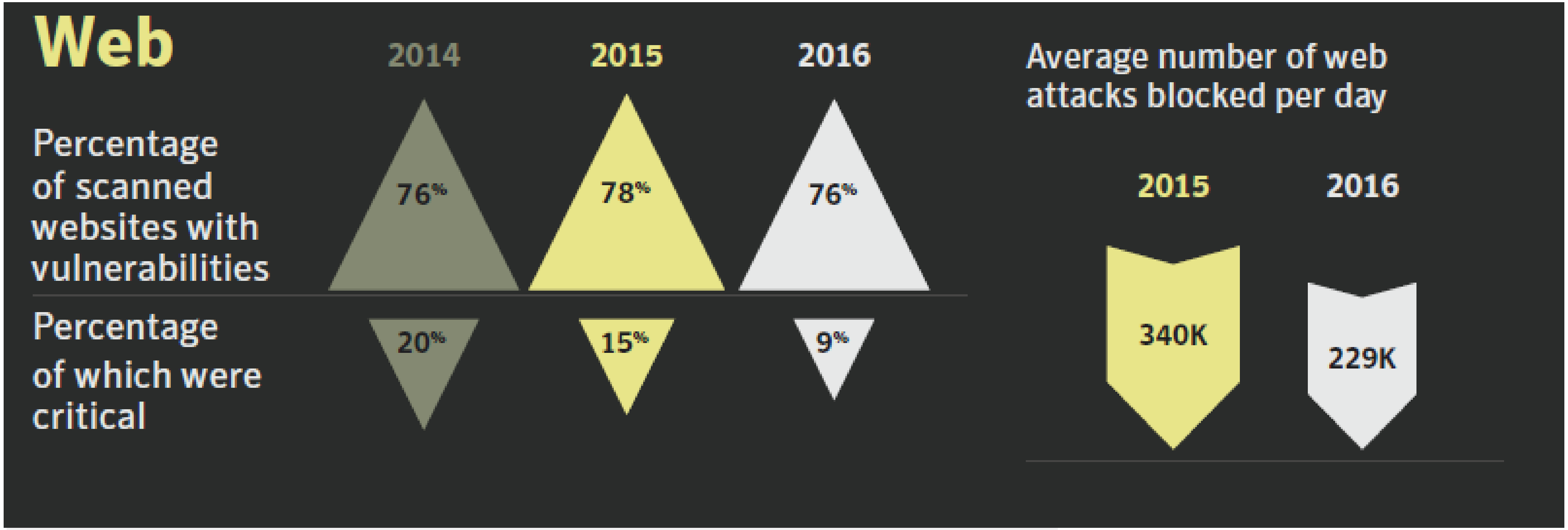
https://www.symantec.com/security-center/threat-report

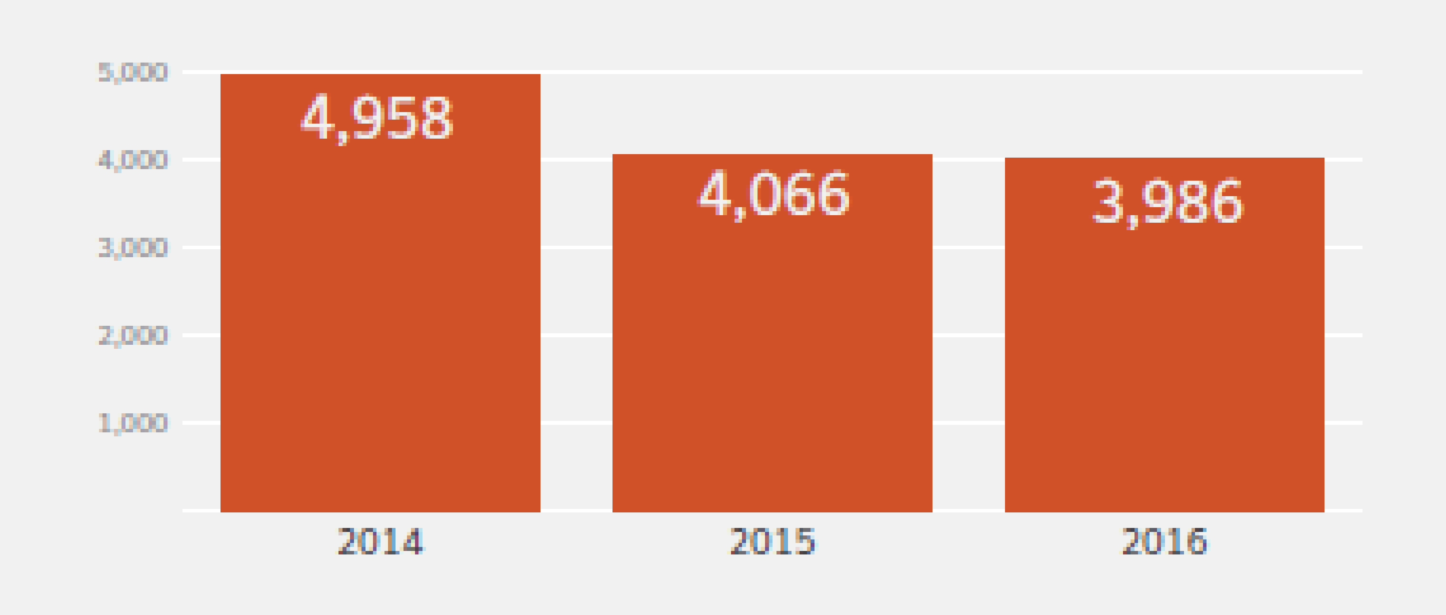


The underground marketplace

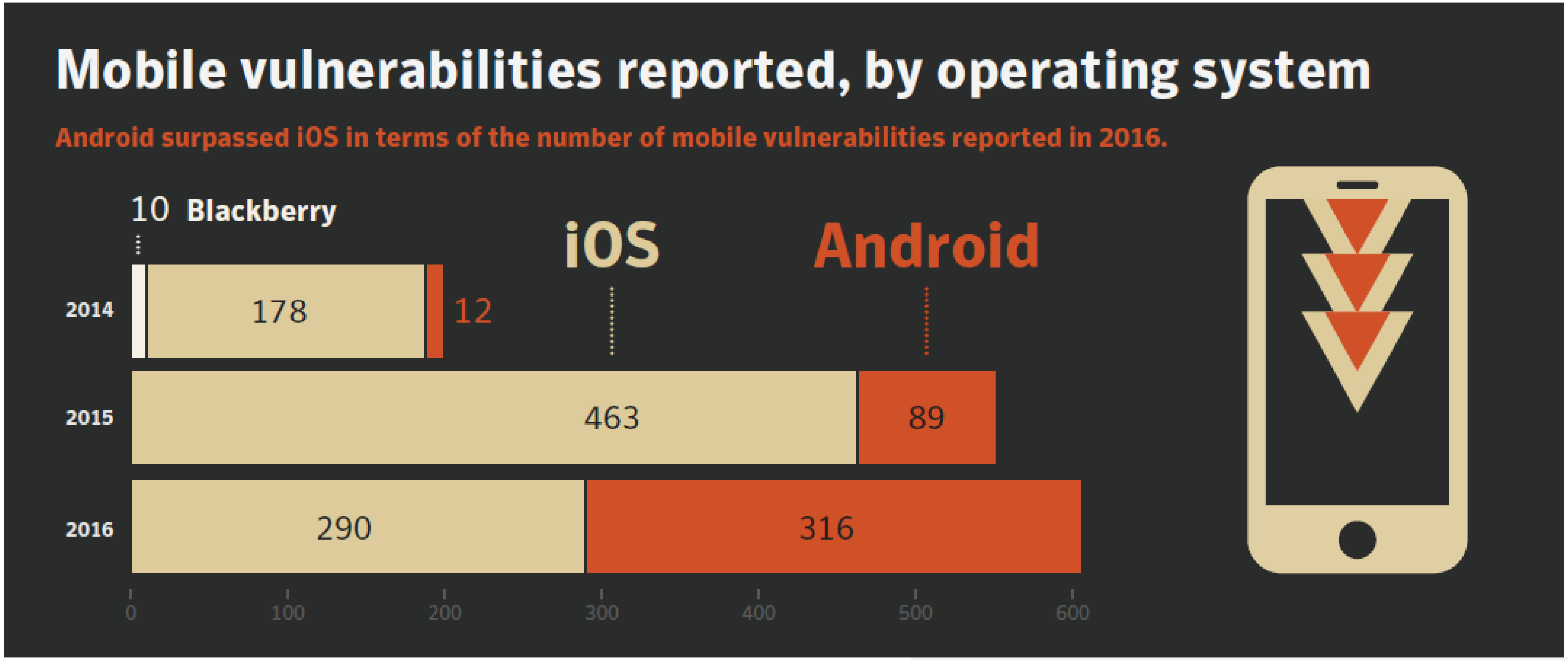
Ransomware toolkit	$10 – $1,800
DDoS short duration (< 1 hr)	$5 – $20
Documents (Passports, utility bills)	$1 – $3
Android banking Trojan	$200
Credit cards	$0.5 – $30
Cloud service account	$6 – $10
Gift card	20% – 40% (of face value)
Cash-out service	10% – 20% (of acct. value)

Where *everything* has a price





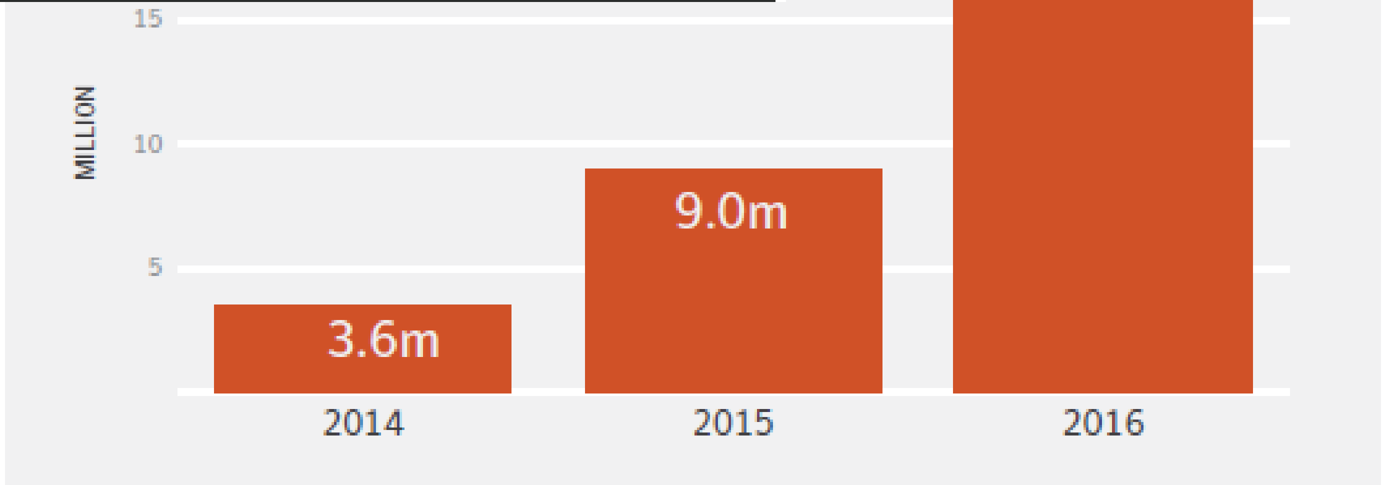
← **Zero-day vulnerabilities**



Mobile vulnerabilities reported, by operating system

Android surpassed iOS in terms of the number of mobile vulnerabilities reported in 2016.

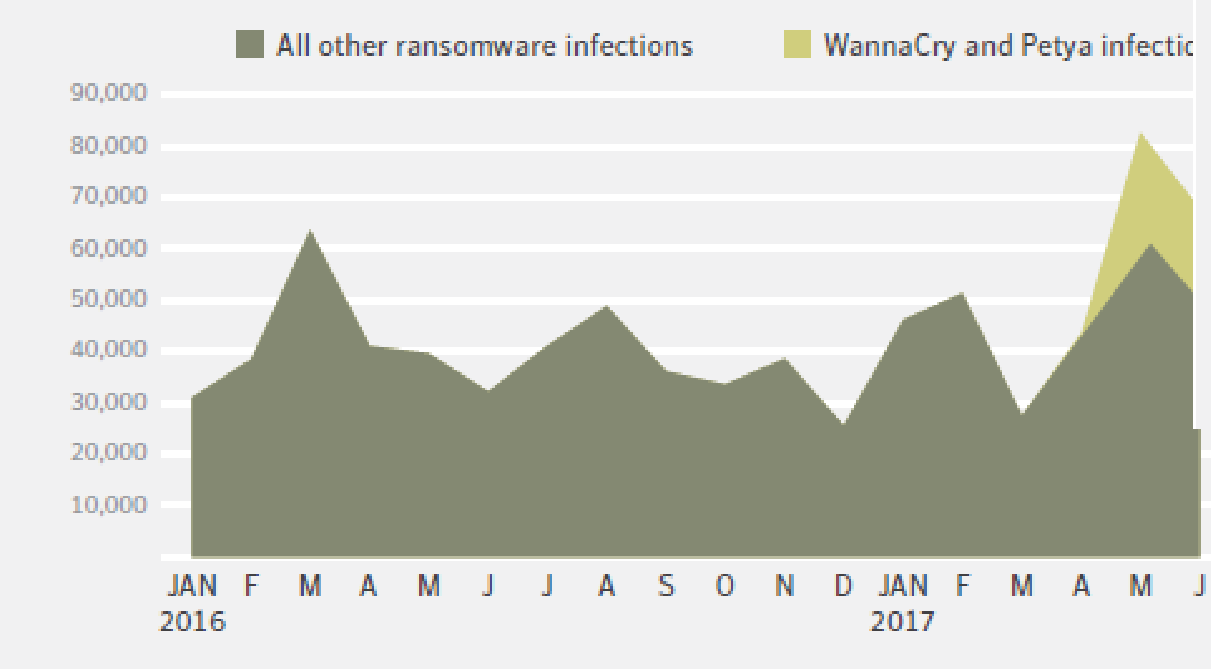
Number of mobile malware detection ➔

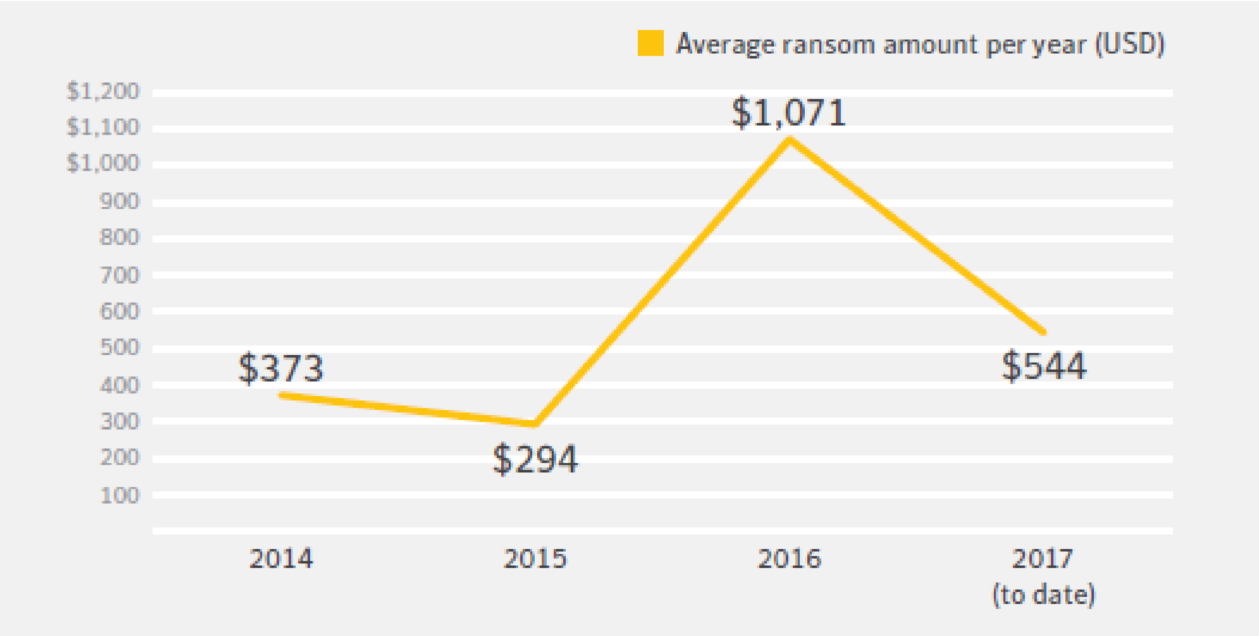


https://www.symantec.com/security-center/threat-report

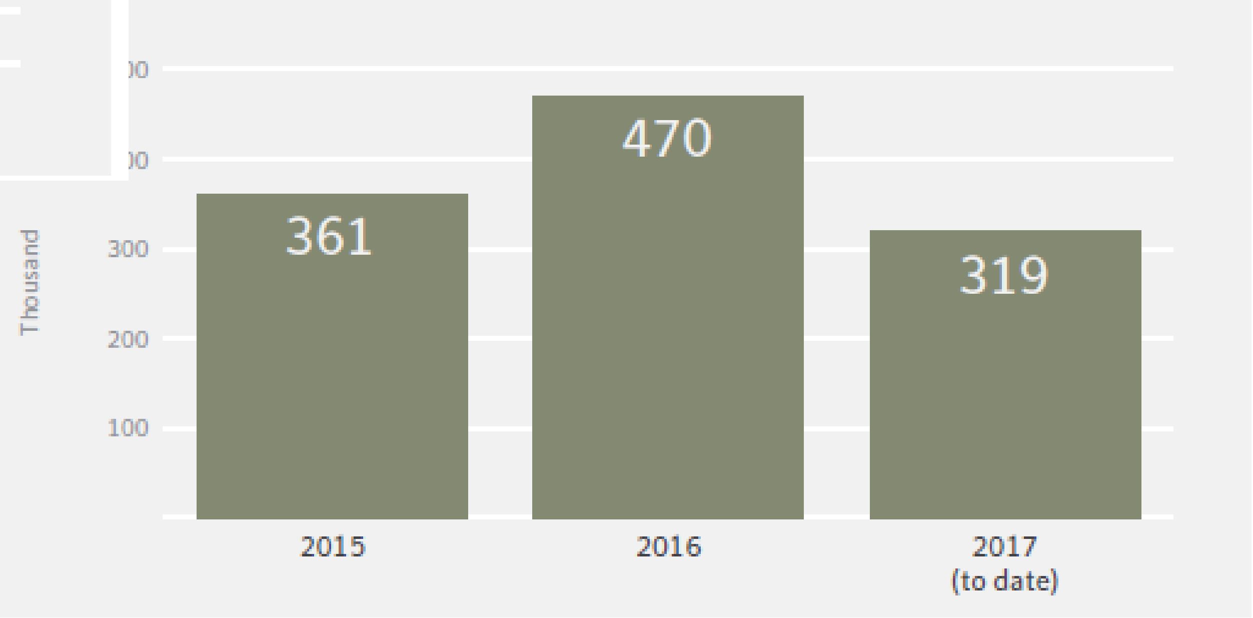
Ransomwares

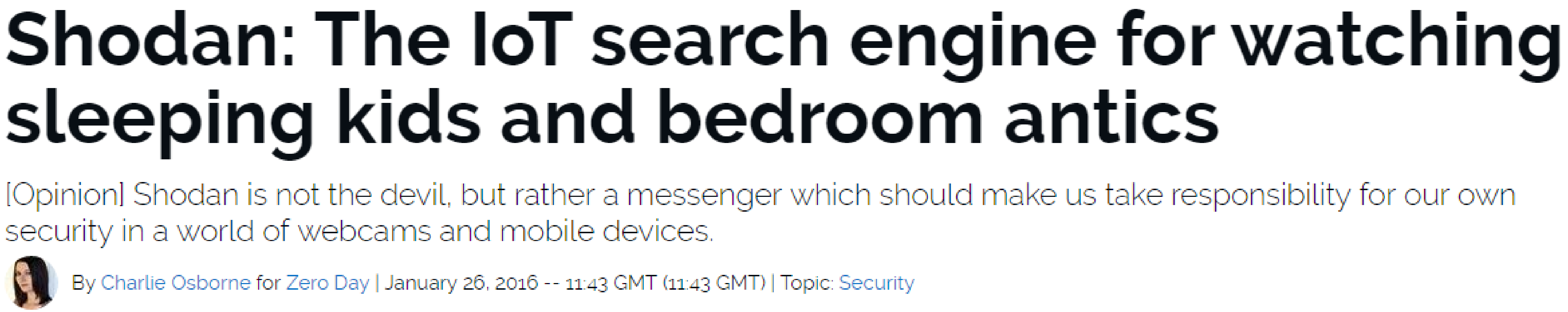
# of infection per month





Total number of infection per year ➔

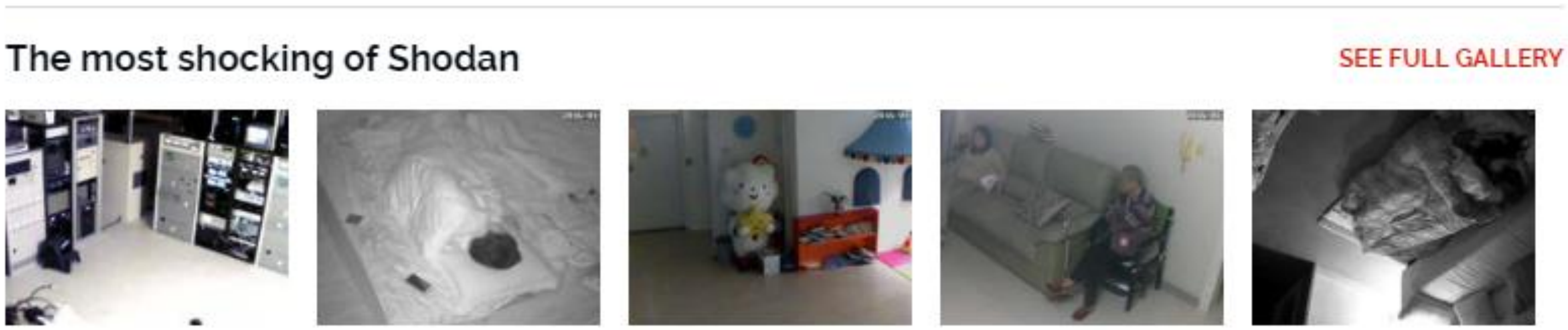




Shodan: The IoT search engine for watching sleeping kids and bedroom antics

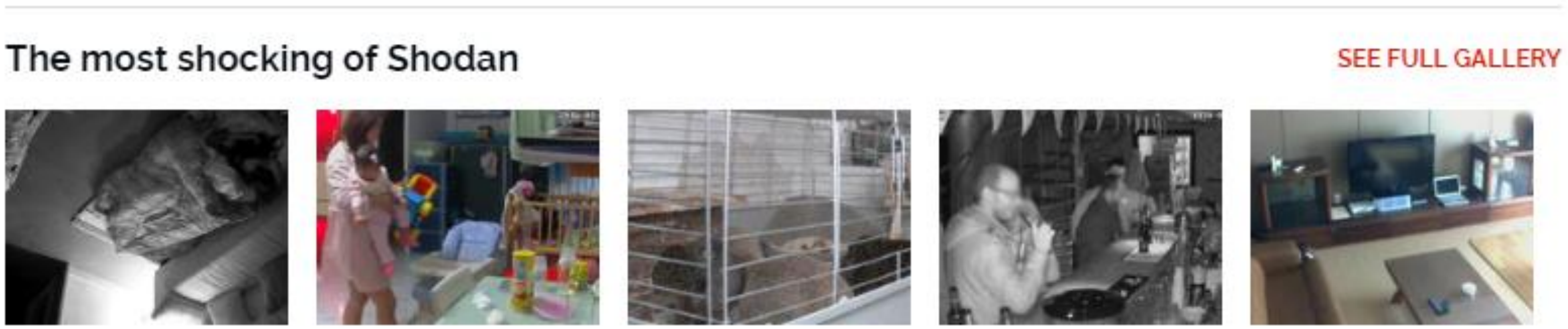
[Opinion] Shodan is not the devil, but rather a messenger which should make us take responsibility for our own security in a world of webcams and mobile devices.

By Charlie Osborne for Zero Day | January 26, 2016 -- 11:43 GMT (11:43 GMT) | Topic: Security



The most shocking of Shodan

SEE FULL GALLERY



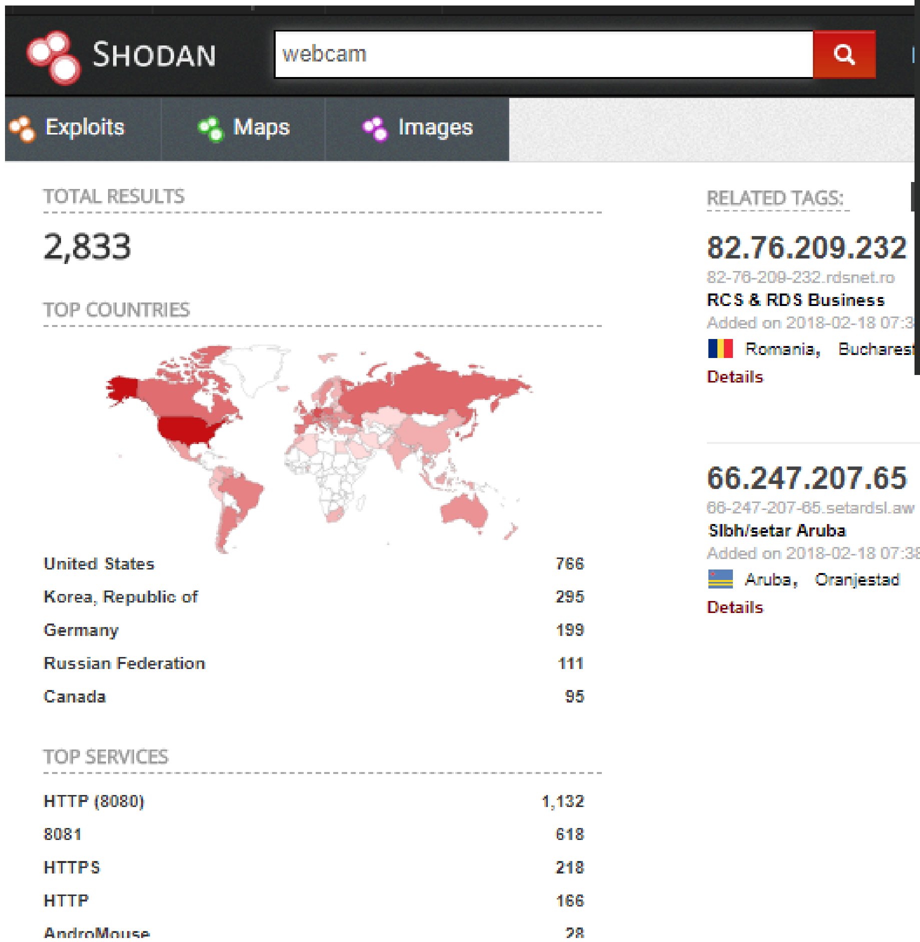
The most shocking of Shodan

SEE FULL GALLERY

Internet of Things

2 minutes:
time it takes for an IoT device to be attacked

Speed of attack



TOTAL RESULTS

2,833

TOP COUNTRIES

United States	766
Korea, Republic of	295
Germany	199
Russian Federation	111
Canada	95

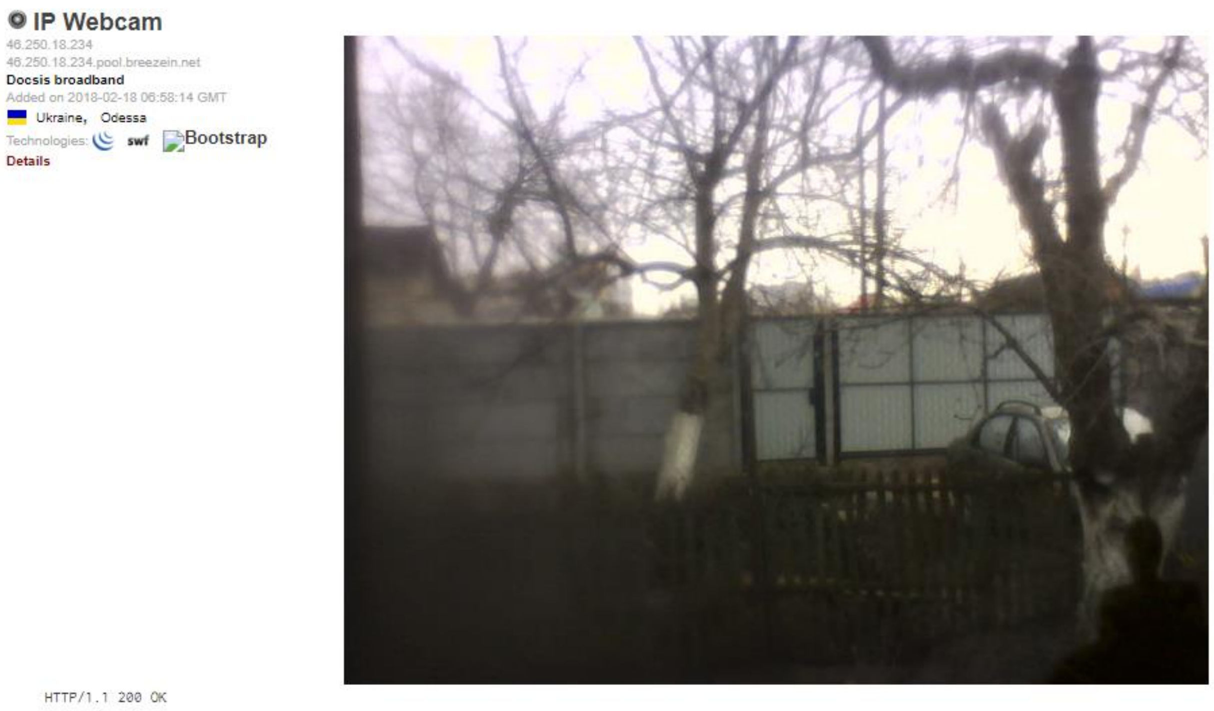
TOP SERVICES

HTTP (8080)	1,132
8081	618
HTTPS	218
HTTP	166
AndroMouse	28

RELATED TAGS:

82.76.209.232
82-76-209-232.rdsnet.ro
RCS & RDS Business
Added on 2018-02-18 07:3
Romania, Bucharest
Details

66.247.207.65
66-247-207-65.setardsl.aw
Slbh/setar Aruba
Added on 2018-02-18 07:38:27 GMT
Aruba, Oranjestad
Details

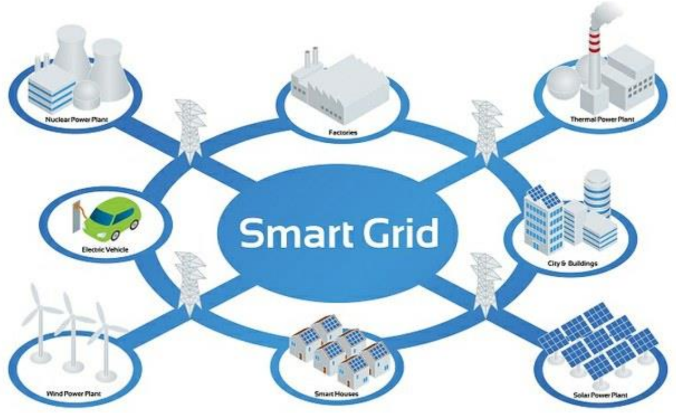


IP Webcam
46.250.18.234
46.250.18.234.pool.breezein.net
Docsis broadband
Added on 2018-02-18 06:58:14 GMT
Ukraine, Odessa
Technologies: swf Bootstrap
Details

HTTP/1.1 200 OK

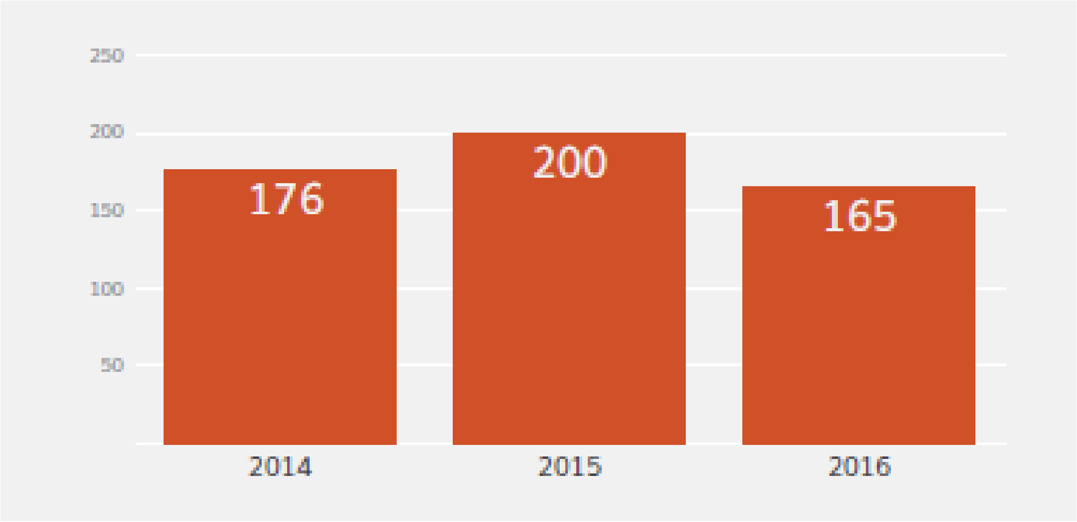
SCADA

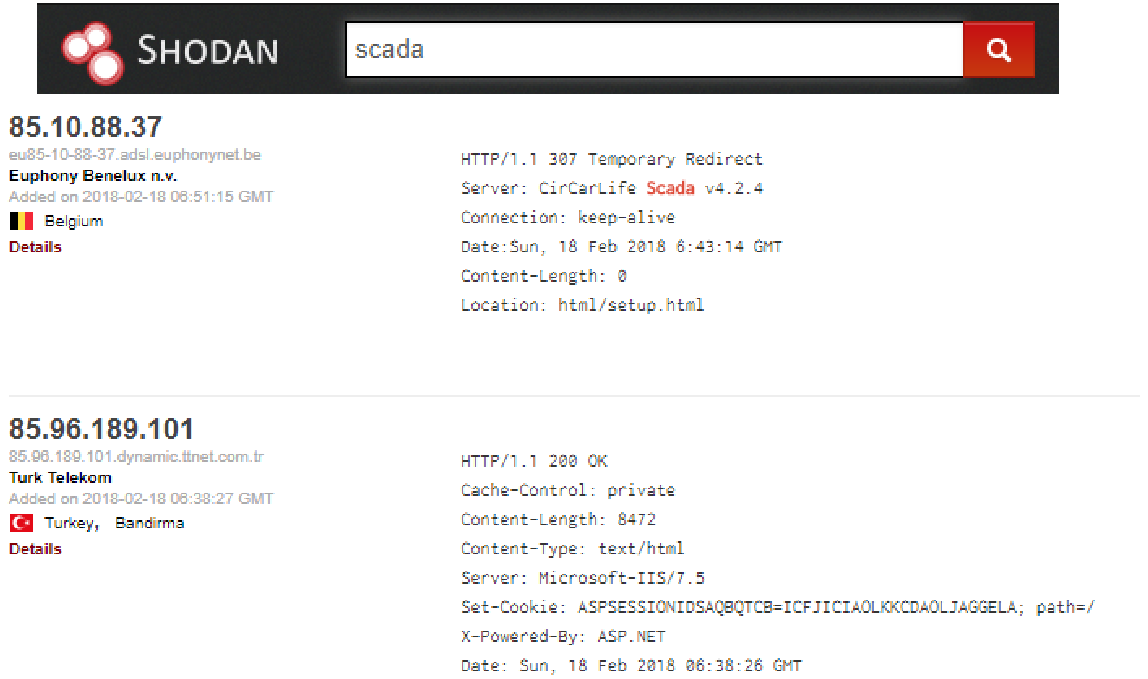
- In **2016** attacks have been reported in **Israel, Turkey** & **Finland**
- In **2015** a malware in **Ukraine** trigger an **hours-long blackout** affecting about **80,000 people**



"Every component in the grid that has become digitized is becoming an attack point"

Vulnerabilities discovered in ICS





85.10.88.37
eu85-10-88-37.adsl.euphonynet.be
Euphony Benelux n.v.
Added on 2018-02-18 06:51:15 GMT
Belgium
Details

```
HTTP/1.1 307 Temporary Redirect
Server: CirCarLife Scada v4.2.4
Connection: keep-alive
Date:Sun, 18 Feb 2018 6:43:14 GMT
Content-Length: 0
Location: html/setup.html
```

85.96.189.101
85.96.189.101.dynamic.ttnet.com.tr
Turk Telekom
Added on 2018-02-18 06:38:27 GMT
Turkey, Bandirma
Details

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 8472
Content-Type: text/html
Server: Microsoft-IIS/7.5
Set-Cookie: ASPSESSIONIDSAQBQTCB=ICFJICIAOLKKCDAOLJAGGELA; path=/
X-Powered-By: ASP.NET
Date: Sun, 18 Feb 2018 06:38:26 GMT
```

Cellular Networks

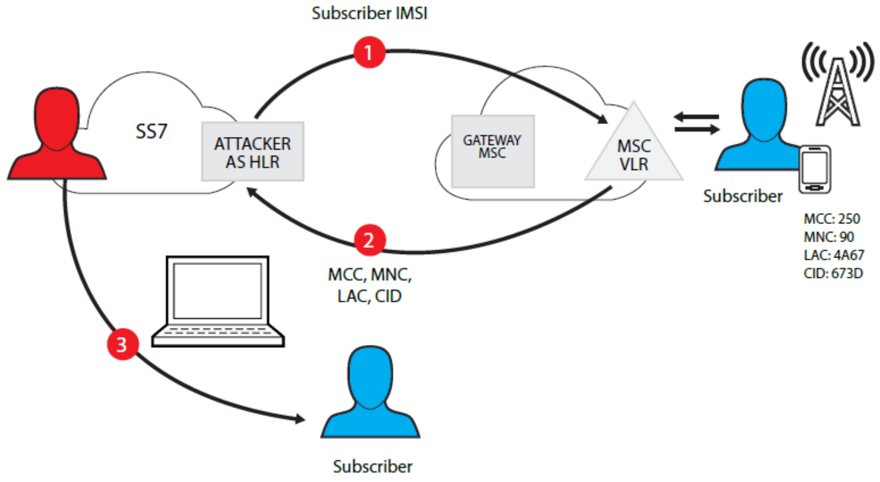
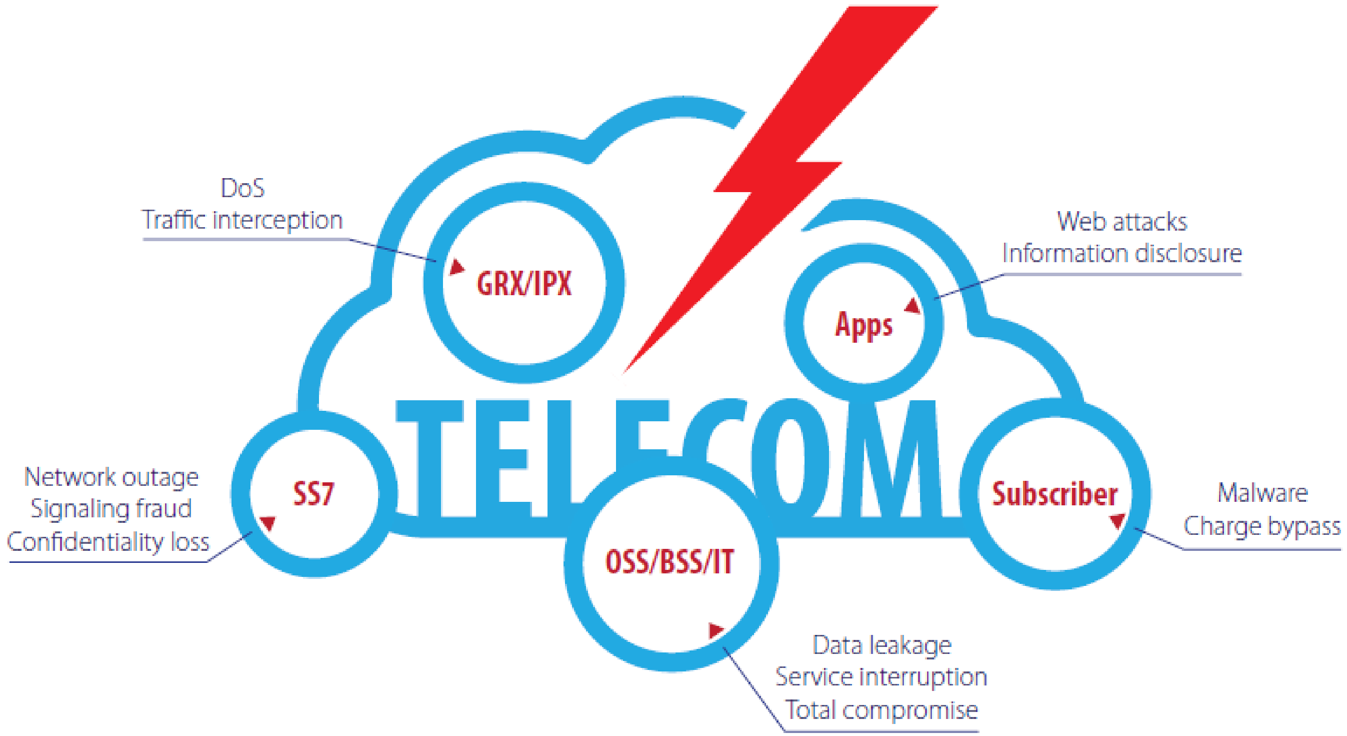


Figure 2. Determining a subscriber's location



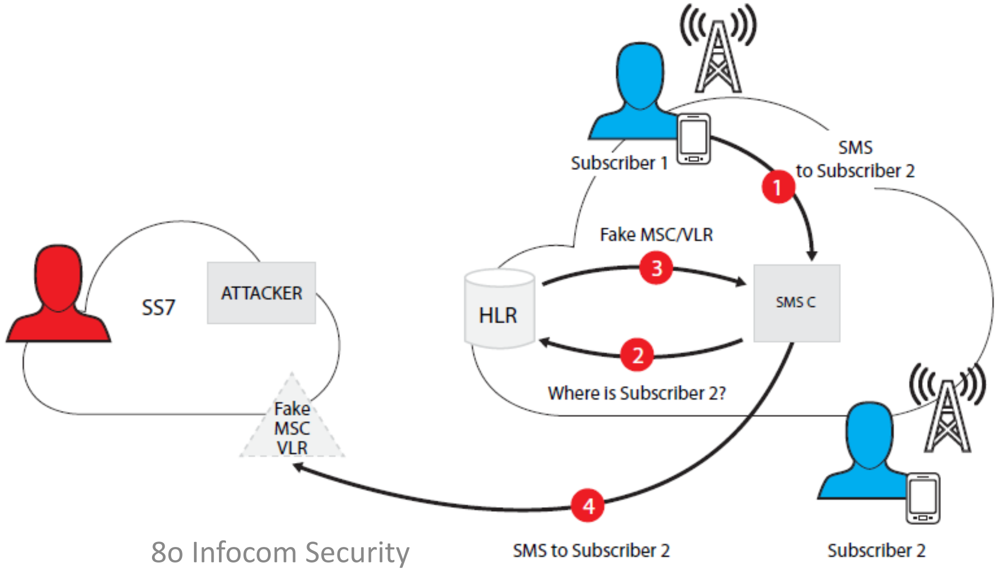


Figure 4. Intercept incoming SMS messages

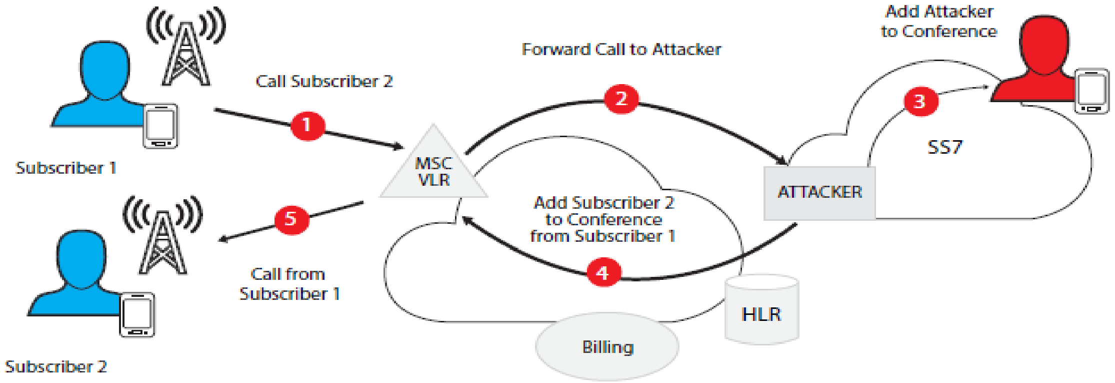
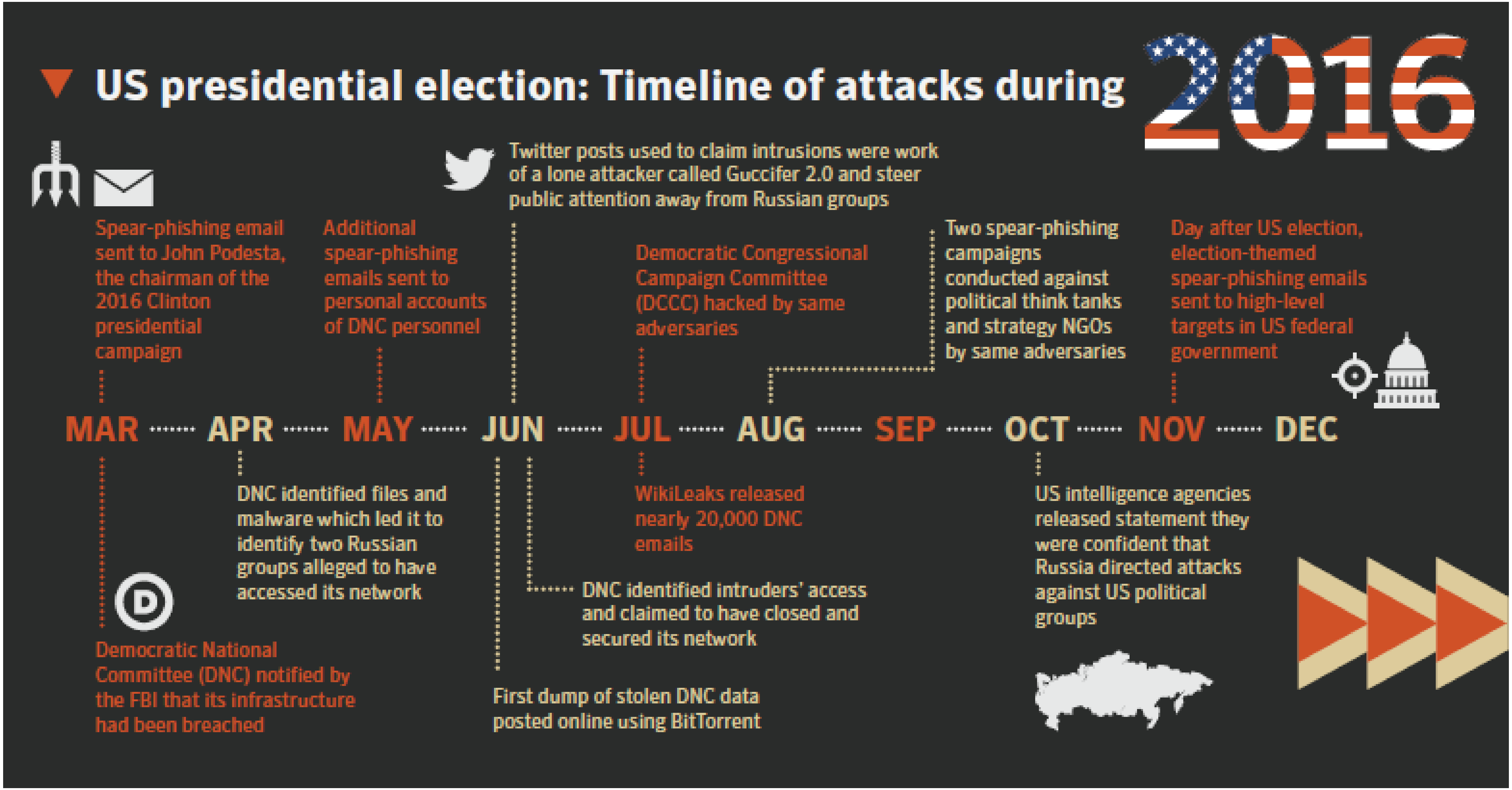


Figure 7. Interceptiing outgoing calls



US presidential election: Timeline of attacks during 2016

MAR ······· APR ······· MAY ······· JUN ······· JUL ······· AUG ······· SEP ······· OCT ······· NOV ······· DEC

Spear-phishing email sent to John Podesta, the chairman of the 2016 Clinton presidential campaign

Democratic National Committee (DNC) notified by the FBI that its infrastructure had been breached

DNC identified files and malware which led it to identify two Russian groups alleged to have accessed its network

Additional spear-phishing emails sent to personal accounts of DNC personnel

Twitter posts used to claim intrusions were work of a lone attacker called Guccifer 2.0 and steer public attention away from Russian groups

First dump of stolen DNC data posted online using BitTorrent

DNC identified intruders' access and claimed to have closed and secured its network

Democratic Congressional Campaign Committee (DCCC) hacked by same adversaries

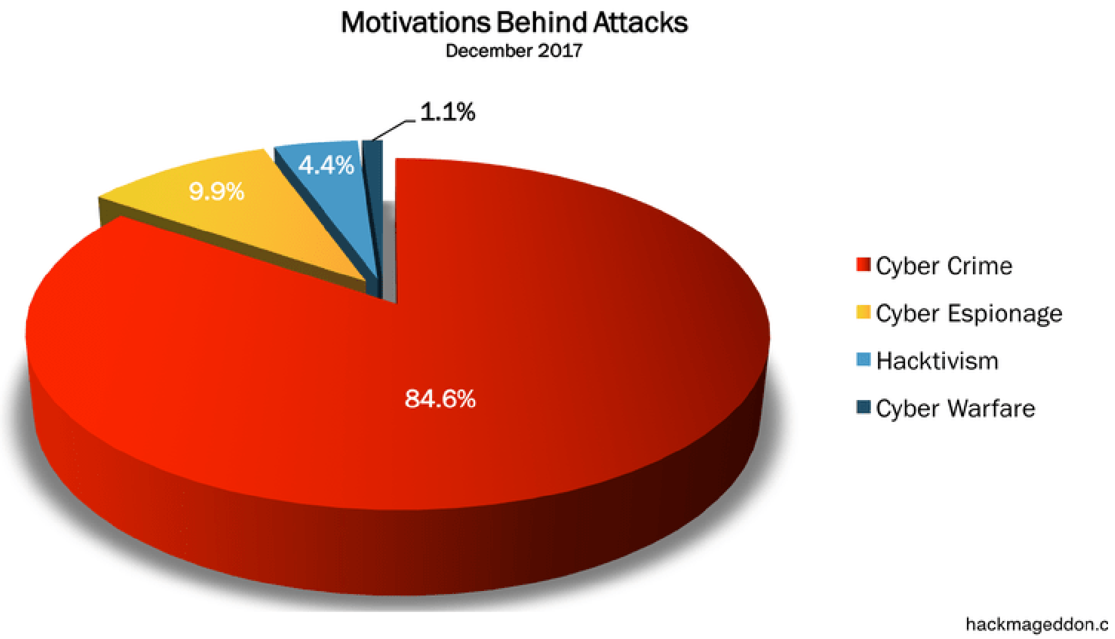
WikiLeaks released nearly 20,000 DNC emails

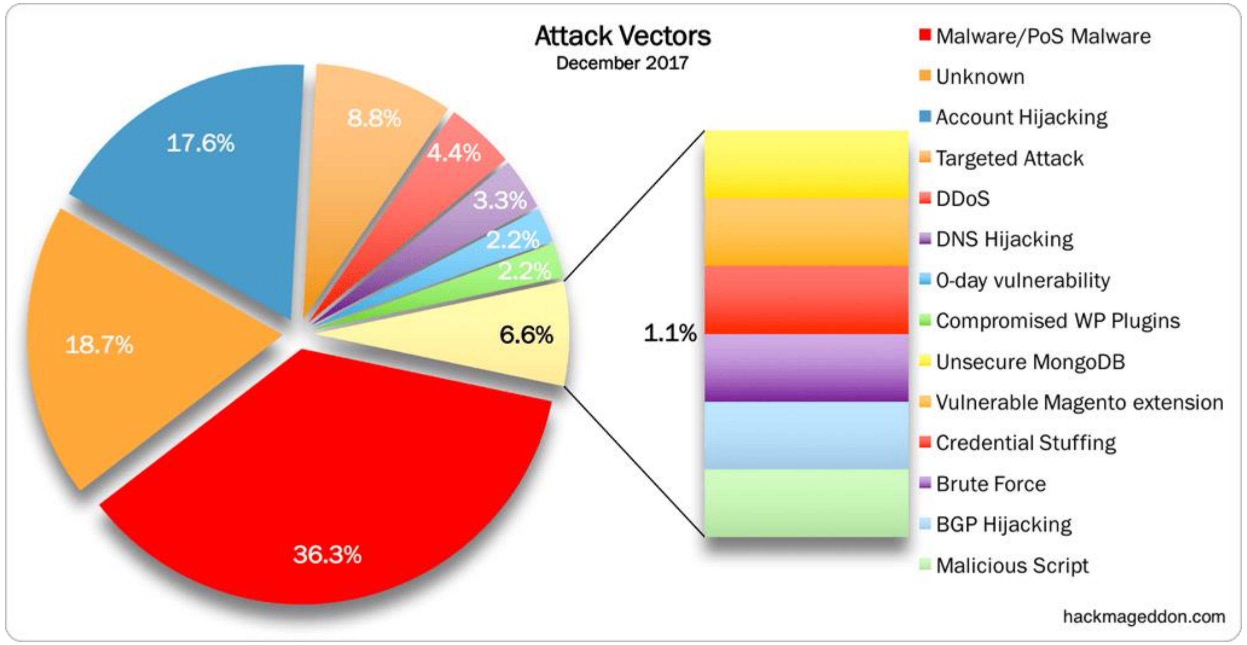
Two spear-phishing campaigns conducted against political think tanks and strategy NGOs by same adversaries

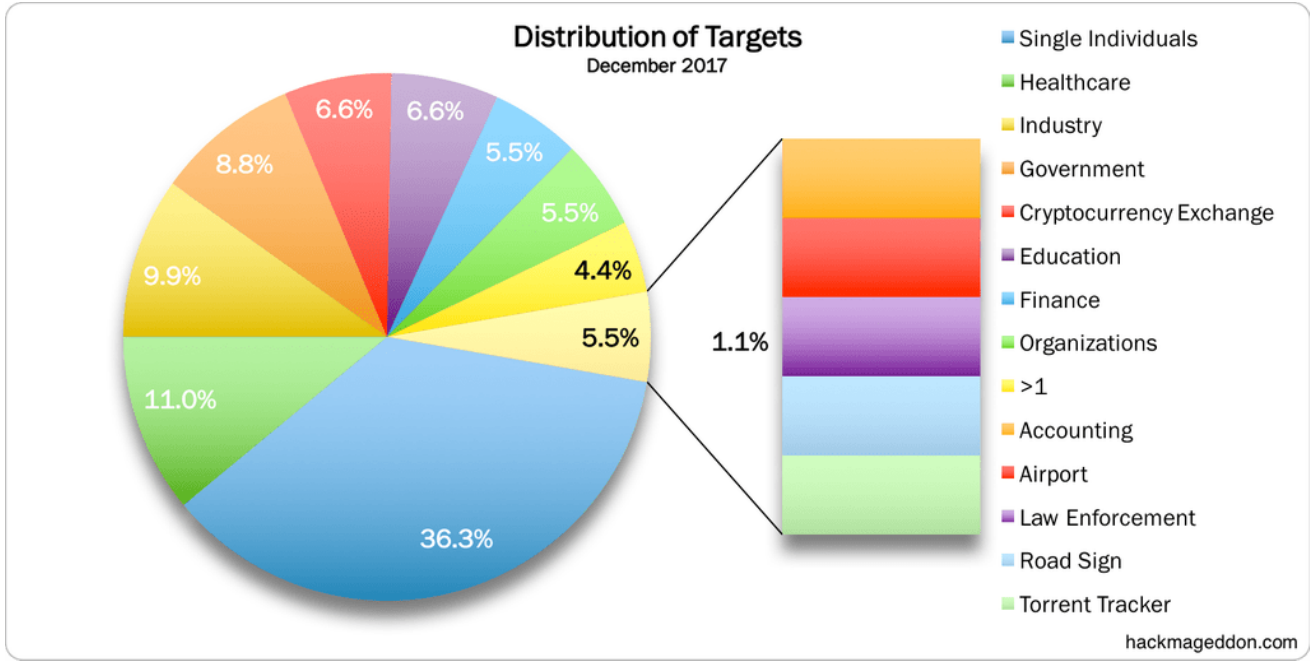
US intelligence agencies released statement they were confident that Russia directed attacks against US political groups

Day after US election, election-themed spear-phishing emails sent to high-level targets in US federal government

https://www.symantec.com/security-center/threat-report


Motivations Behind Attacks
December 2017
84.6%
9.9%
4.4%
1.1%
Cyber Crime
Cyber Espionage
Hacktivism
Cyber Warfare
hackmageddon.c


Attack Vectors
December 2017
36.3%
18.7%
17.6%
8.8%
4.4%
3.3%
2.2%
2.2%
6.6%
1.1%
Malware/PoS Malware
Unknown
Account Hijacking
Targeted Attack
DDoS
DNS Hijacking
0-day vulnerability
Compromised WP Plugins
Unsecure MongoDB
Vulnerable Magento extension
Credential Stuffing
Brute Force
BGP Hijacking
Malicious Script
hackmageddon.com


Distribution of Targets
December 2017
36.3%
11.0%
9.9%
8.8%
6.6%
6.6%
5.5%
5.5%
4.4%
5.5%
1.1%
Single Individuals
Healthcare
Industry
Government
Cryptocurrency Exchange
Education
Finance
Organizations
>1
Accounting
Airport
Law Enforcement
Road Sign
Torrent Tracker
hackmageddon.com

General Data Protection Regulation – GDPR

Cybercrime can no longer be considered as an acceptable 'running cost' of business

Harmonization & geographical reach

20 MEUR or 4%

Data portability

May 2018

Breach notification

Right to be forgotten

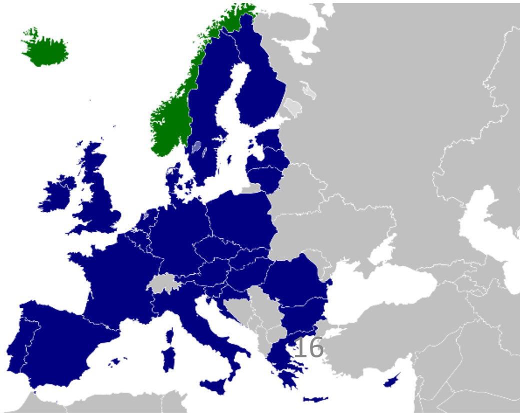
Data security

What do we need to protect our world ?

PERSONNEL
HOW COULD YOU HAVE THIRTY YEARS EXPERIENCE WHEN YOU'RE ONLY TWENTY ?
LOTS OF OVERTIME!!!
CARTOONSTOCK .com
Search ID: ear0485
ledgar wgo

What is about

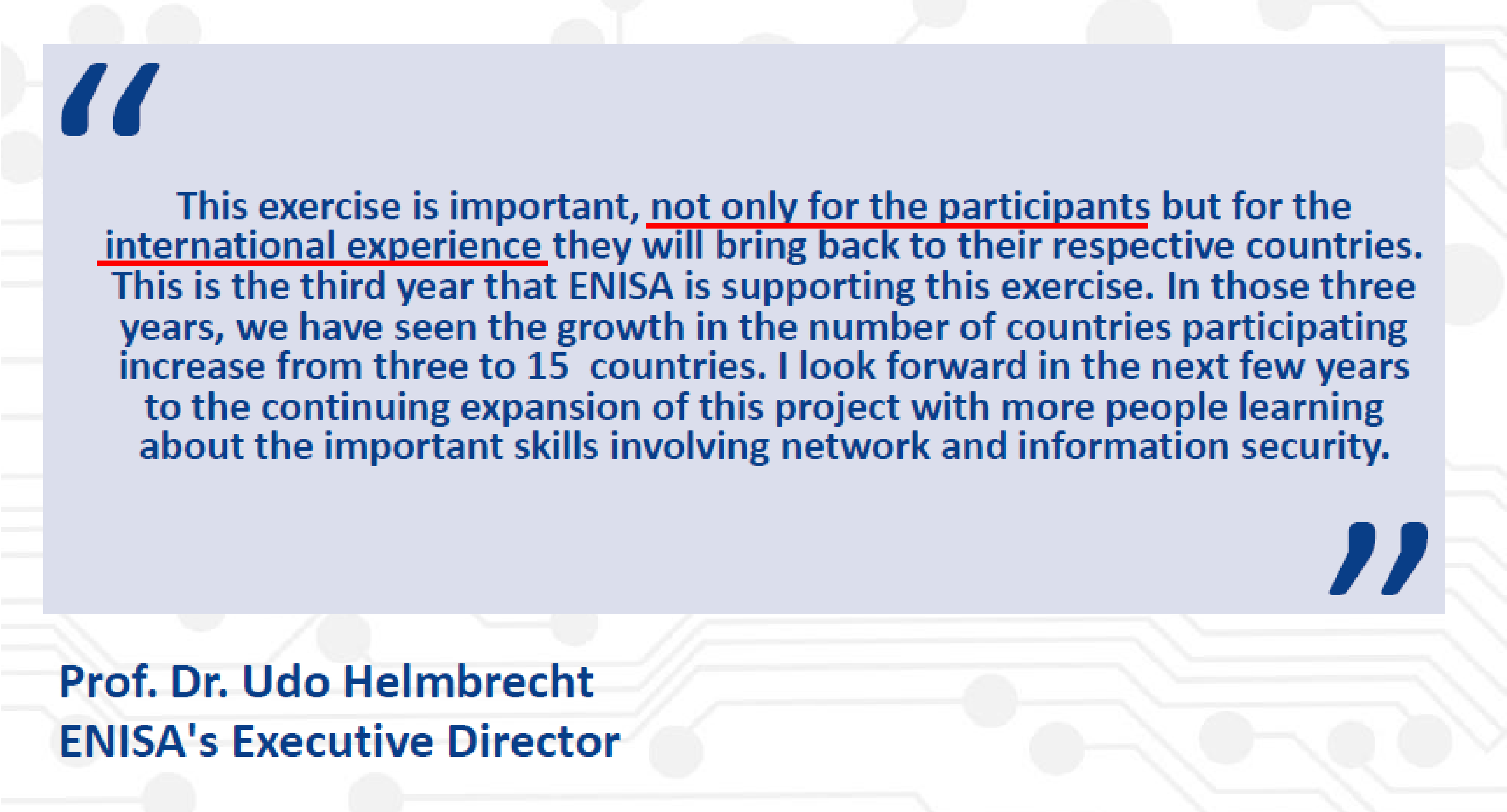
- It **is acknowledged** that there is a growing need for **IT security professionals** worldwide
- To mitigate **this shortage**, many countries launch **National Cyber Security Competitions**
- The **aim** of these competitions are:
    1. Find **new** and **young talents** in **cyber security**
    2. **Encourage** young people to **pursue a career** in **cyber security**
- The **European Cyber Security Challenge – ECSC** adds a **Pan-European layer** on these **National Competitions**



The European Cyber Security Challenge - ECSC

- It is an initiative of the **European Commission** supported by **ENISA**
- **Annually**, the competition brings together **young talents** from **European Countries** to have fun and **compete in cyber security**
- The goal of **ECSC** is to place **Cyber Security** at the **service of humankind**
- **Promoting:**
  - **An open, safe and secure cyberspace**
  - **A peaceful society with democratic values**
  - **Free and critical thinking**
- A **Cyber Security championship**

EUROPEAN CYBER SECURITY CHALLENGE
LONDON, UNITED KINGDOM 2018



“This exercise is important, not only for the participants but for the international experience they will bring back to their respective countries. This is the third year that ENISA is supporting this exercise. In those three years, we have seen the growth in the number of countries participating increase from three to 15 countries. I look forward in the next few years to the continuing expansion of this project with more people learning about the important skills involving network and information security.”

Prof. Dr. Udo Helmbrecht
ENISA's Executive Director

History of the contest

ECSC 2015

- Edition: 1st
- Place: Austria
- Participating teams: 6
- Competitors per team: 10
- Winner: Austria

ECSC 2016

- Edition: 2nd
- Place: Germany
- Participating teams: 10
- Competitors per team: 10
- Winner: Spain

ECSC 2017 hosted in Spain

- In 2017, the competition was hosted in **Malaga**, by **Spanish National Cyber Security Institute** (INCIBE)
- **30th October – 3rd November 2017**
- **Participated Teams: 15**
- **Competitors per Team: 10**

EUROPEAN CYBER SECURITY CHALLENGE

MALAGA, SPAIN, 2017

National Teams that will participate

Austria

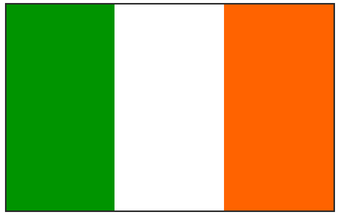
Cyprus

Denmark

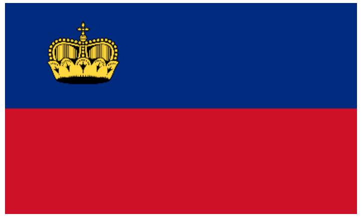
Estonia

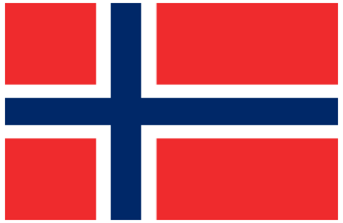
Germany

Greece


Ireland

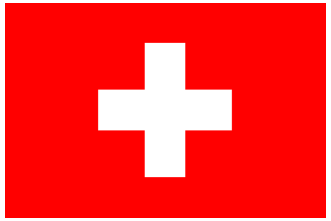
Italy


Liechtenstein

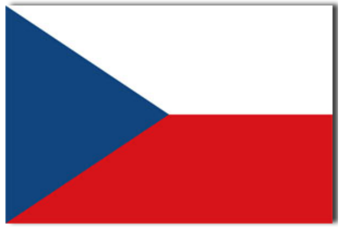

Norway

Romania

Spain


Switzerland

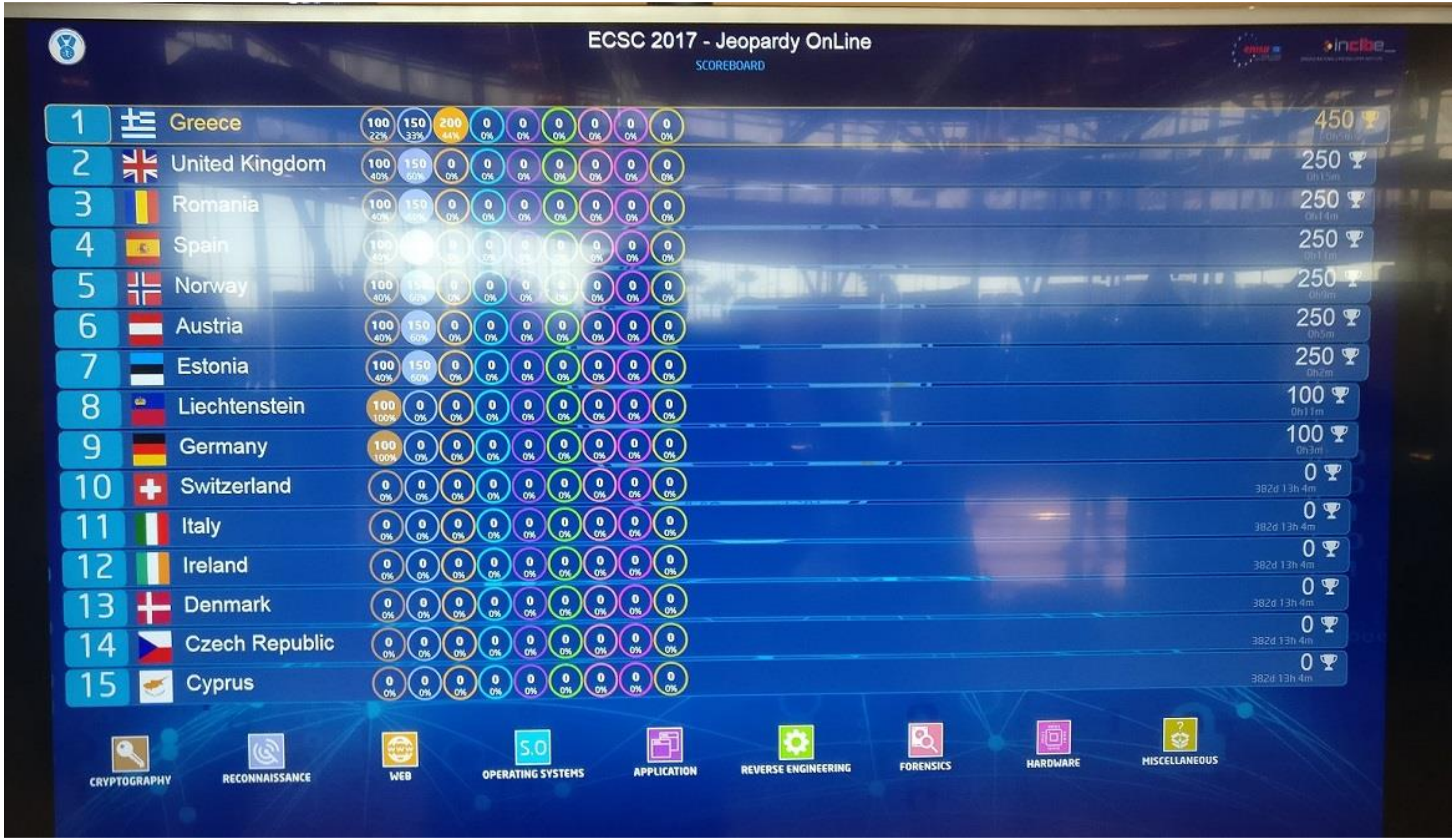
United Kingdom


Czech

The Hellenic Cyber Security Team 2017

OPEAN
ER SECURITY CHALLENGE 2017
EUROPEAN
CYBER SECURITY CHALLENGE 2017
Información y Registro
Information and Registration
ADACOM

Most of the time Greece was first !!

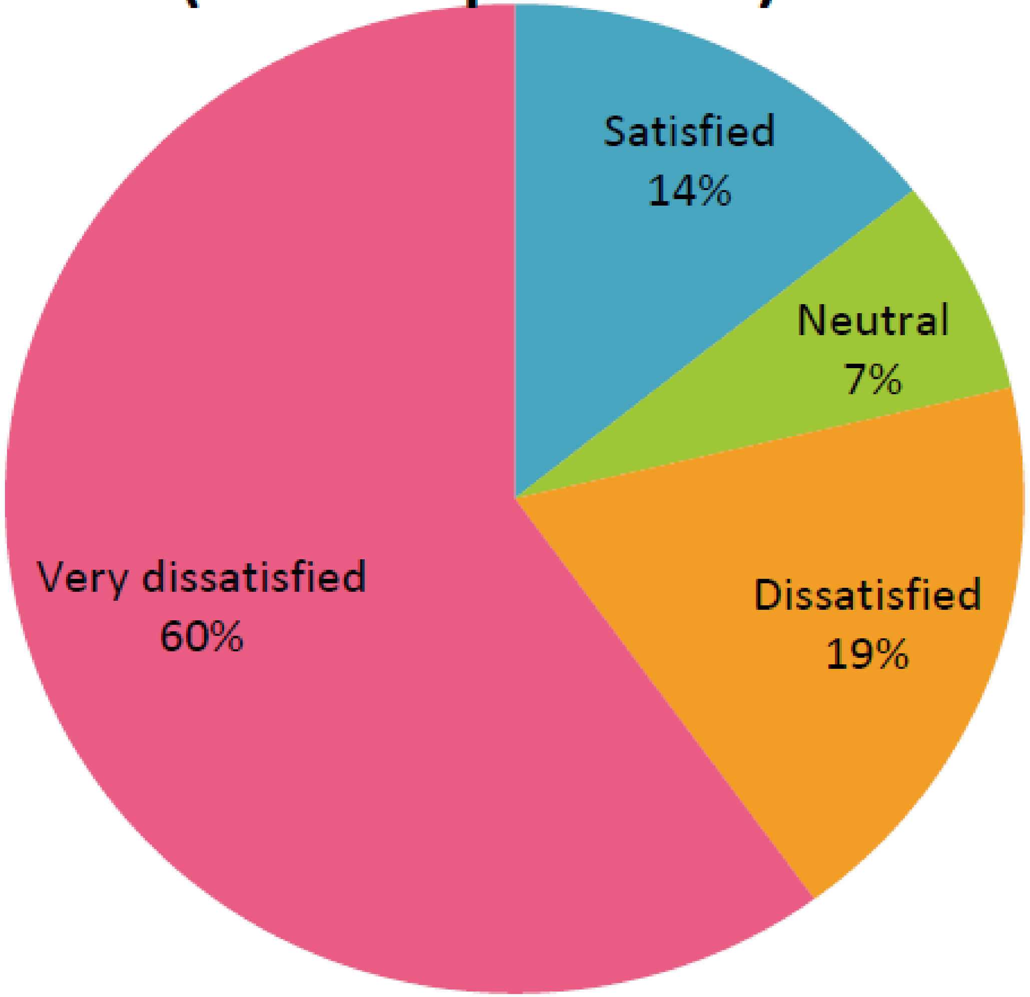


ECSC 2017 - Jeopardy OnLine

SCOREBOARD

1	Greece	100 22%	150 33%	200 44%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	450 0h5m
2	United Kingdom	100 40%	150 60%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	250 0h15m
3	Romania	100 40%	150 60%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	250 0h14m
4	Spain	100 40%	[illegible]	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	250 0h11m
5	Norway	100 40%	150 60%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	250 0h9m
6	Austria	100 40%	150 60%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	250 0h5m
7	Estonia	100 40%	150 60%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	250 0h2m
8	Liechtenstein	100 100%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	100 0h11m
9	Germany	100 100%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	100 0h3m
10	Switzerland	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 382d 13h 4m
11	Italy	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 382d 13h 4m
12	Ireland	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 382d 13h 4m
13	Denmark	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 382d 13h 4m
14	Czech Republic	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 382d 13h 4m
15	Cyprus	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 382d 13h 4m

How satisfied were you with the design of the challenge (i.e. CTF platform)?



3. Campaign key statistics: what we achieved

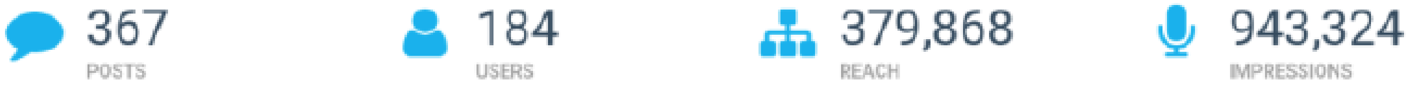
- ENISA and INCIBE showed to be the most influential online, real AMBASSADORS of the ECSC brand
- More active participating countries

- Note that other THIRD COUNTRIES like i.e. US, China, Argentina, Canada engaged and show support of the ECSC

Facts and figures

- In the last 10 days we had: 15,755 unique site visitors.

- In the past 30 days, ENISA's effort generated significant visibility of the ECSC2017 in the social media channels popular with the primary audience of the competition (i.e. young cyber talent)



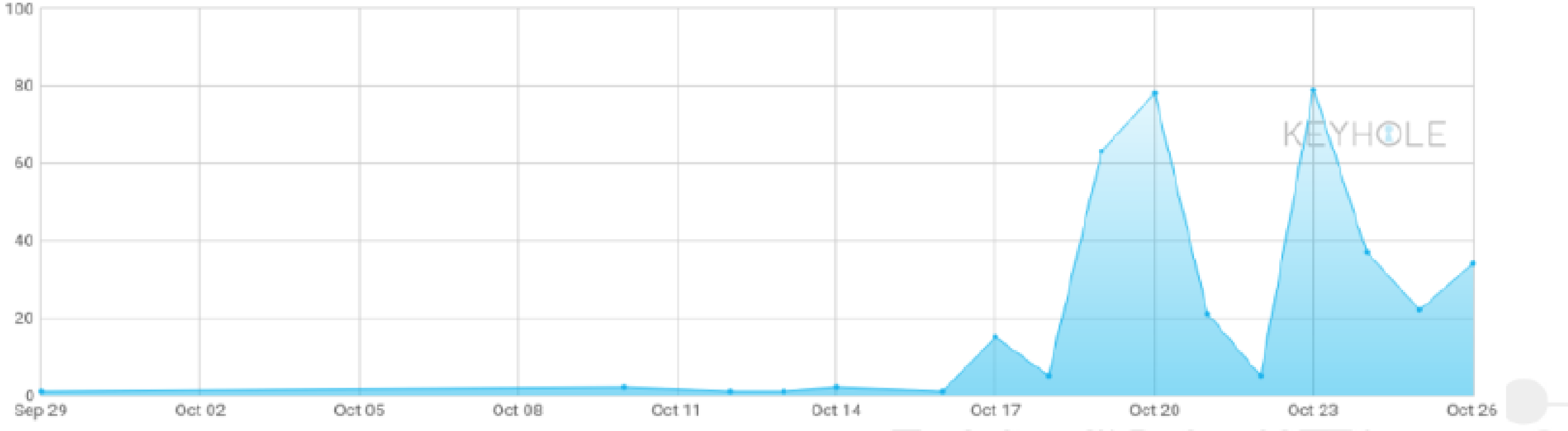
367 POSTS

184 USERS

379,868 REACH

943,324 IMPRESSIONS

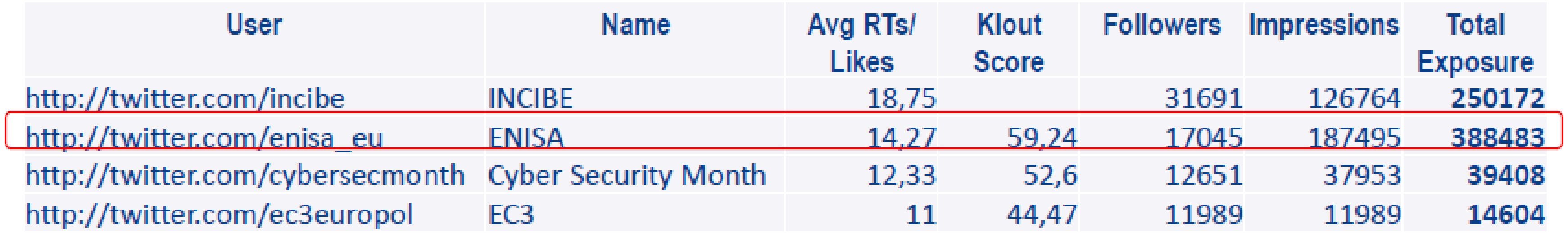
Note: Twitter impact in the past 30 days



Note: Twitter posts on #ECSC2017 in the past 30 days

Key influencers

- Based on the analysis of social media analytics, it is evident that ENISA's support to the ECSC 2017 media campaign is instrumental for creating the impact

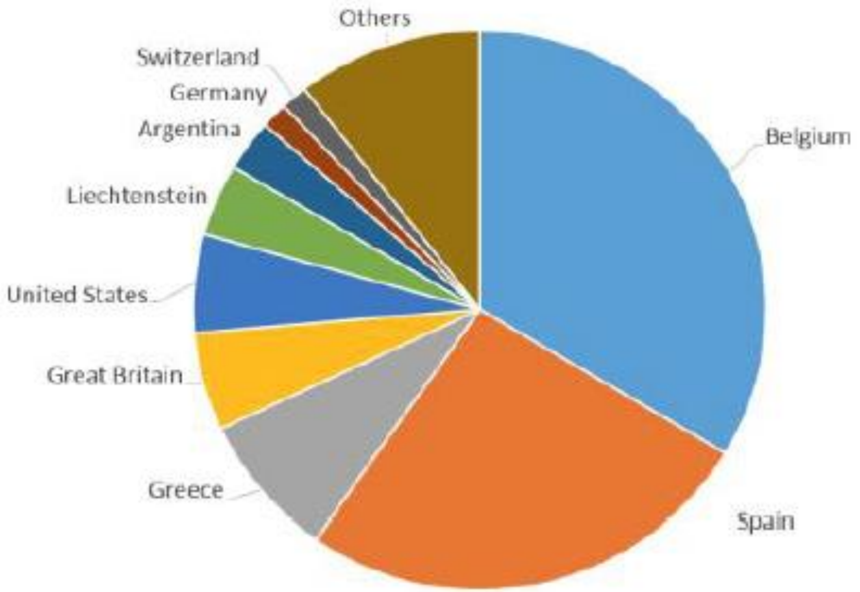


User	Name	Avg RTs/ Likes	Klout Score	Followers	Impressions	Total Exposure
http://twitter.com/incibe	INCIBE	18,75		31691	126764	**250172**
http://twitter.com/enisa_eu	ENISA	14,27	59,24	17045	187495	**388483**
http://twitter.com/cybersecmonth	Cyber Security Month	12,33	52,6	12651	37953	**39408**
http://twitter.com/ec3europol	EC3	11	44,47	11989	11989	**14604**

- 3 out of 4 top impact media drivers are EU institutions (ENISA, EC3, EC – see above)

Lessons learned - countries

- Majority of visibility and impact of ECSC 2017 campaign was reaching European countries
- Interest was triggered in other geographies too:
  - United States
  - Argentina
  - China, etc.



- Participating teams could spread the message, share and engage more.

Funding is solely based on sponsorships

Diamond Sponsors

Funding is solely based on sponsorships

Platinum Sponsors

MediaMarkt®

Quest GROUP

Info Quest TECHNOLOGIES

uni.systems

Gold Sponsors

NEUROsoft

UBITECH
ubiquitous solutions

Silver Sponsor

EXUS®

Funding is solely based on sponsorships

Supporters

netsquare

THALES

ReCRED

ATHENS
INTERNATIONAL AIRPORT
ELEFTHERIOS VENIZELOS

Equipment Supporters

alcatel
enjoy.now

devolo

SENCOR

Media Sponsors

BIZtech.gr

επιχειρώ
www.epixeiro.gr

PROFESSIONAL
it security

NetFAX

netweek

PC MAGAZINE
ΕΛΛΗΝΙΚΗ ΕΚΔΟΣΗ
gr.pcmag.com

TECH MATRIX

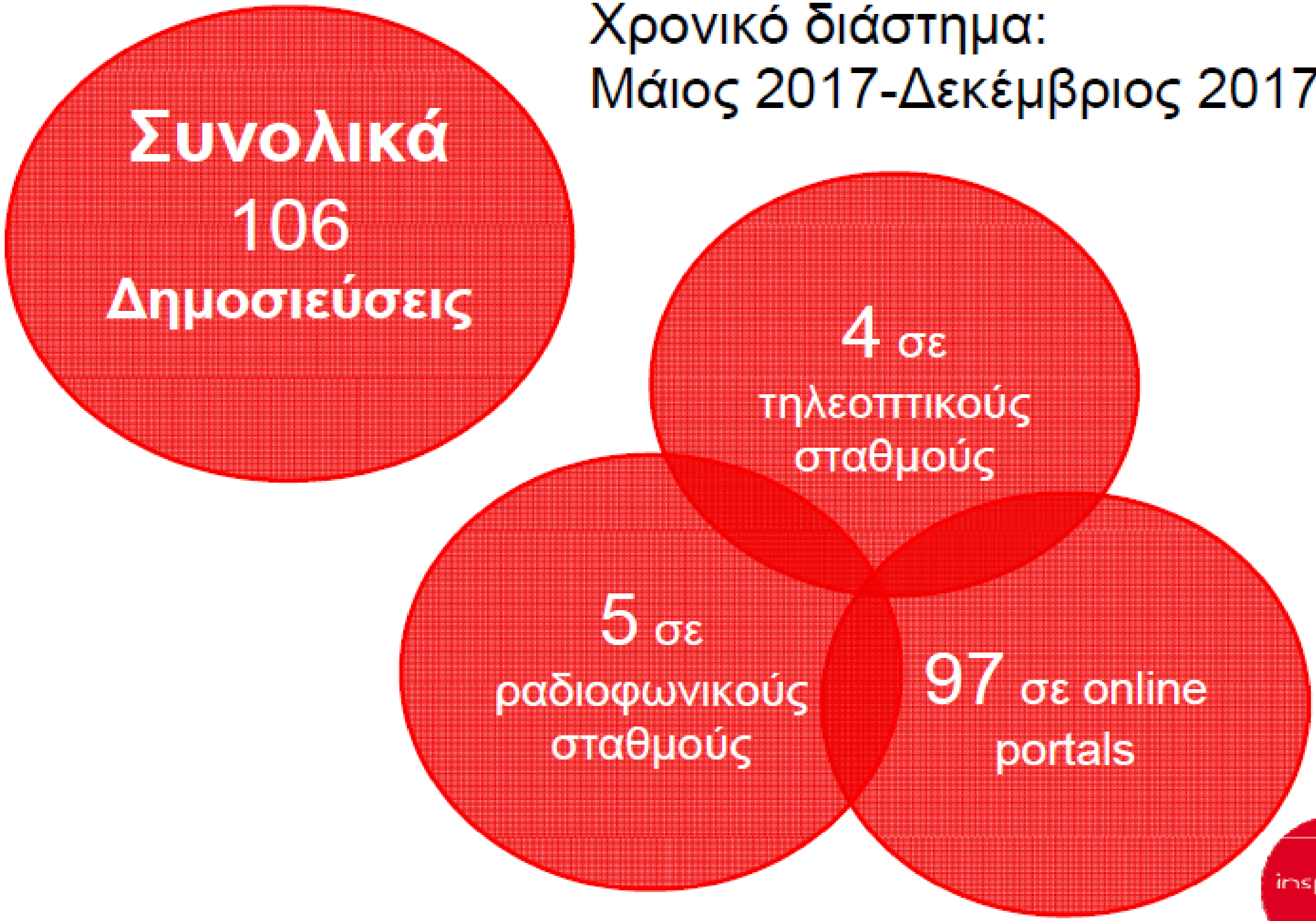
HUFFPOST

SpoudaZO.gr
Το Νο.1 Φοιτητικό Site

In Depth IT News
SecNews

Η δημοσιότητα του ECSC 2017

Χρονικό διάστημα:
Μάιος 2017-Δεκέμβριος 2017



Συνολικά
106
Δημοσιεύσεις

4 σε
τηλεοπτικούς
σταθμούς

5 σε
ραδιοφωνικούς
σταθμούς

97 σε online
portals

Χρονικό διάστημα:
Μάιος 2017-Δεκέμβριος 2017

13
Συνεντεύξεις

5
ραδιοφωνικές

5
σε online
portals

3
τηλεοπτικές

The 2018 European Cyber Security Challenge will be held in London…

2018 Competition Dates

October 15th – 19th 2018

Cyber Security Challenge UK

The Greek Participation

EUROPEAN CYBER SECURITY CHALLENGE

- The **leadership** for the **Greek participation** in **ECSC 2018** was appointed to the **Systems' Security Laboratory** of the **Department of Digital Systems** of the **University of Piraeus**
  - Constitution of the **Greek Team**
  - Organization of the **Greek participation**
  - Financial administration – Sponsorship
  - Dissemination
- The **Steering Committee** members are:
  - Prof. Christos Xenakis
  - Prof. Costas Lambrinoudakis

HELLENIC
CYBER SECURITY
TEAM

University of Piraeus
Department of Digital Systems

The Hellenic Cybersecurity Team

- **10 Persons - Contestants**
  - Should be selected by a **National Competition**
  - **Five person (14-20)** and **five person (21 – 25)** who legally reside in **Greece**
- Three **coaches** (an additional may act as alternative) who is responsible for
  - **Well-being** and **behavior** of the **Greek Team**
  - Making sure that **essential information** reaches the **Team** and is **understood**
  - **Organizing the Team’s strategy**
- **A Jury representative**
  - One from each country that assess the **performance**

Constitution of the Greek Team

Hack the box

- A **National on line Competition** will take place on **April – May 2018**.
- We focus on high participation **> 100 persons**.
- The Hellenic Team of 2017 will be actively involved

- **Pavlos Kolios (Team leader)**
- **Giorgos David Tsekalas**
- **Anastasios Tsimpoukis**
- **Petros Lazaros Karolos Mantos**
- **Lefteris Touloumtzidis**
- **Giannis Zaxarioudakis**
- **Marios Gyftos**
- **Efstratios Kaplanelis**
- **Nikos Kamarinakis**
- **Fanis Dimakis**

HELLENIC CYBER SECURITY TEAM

- **Charis Mylonas – Greunion**
- **Thomas Tompoulis - Greunion**
- **Charis Pylarinos - Greunion**

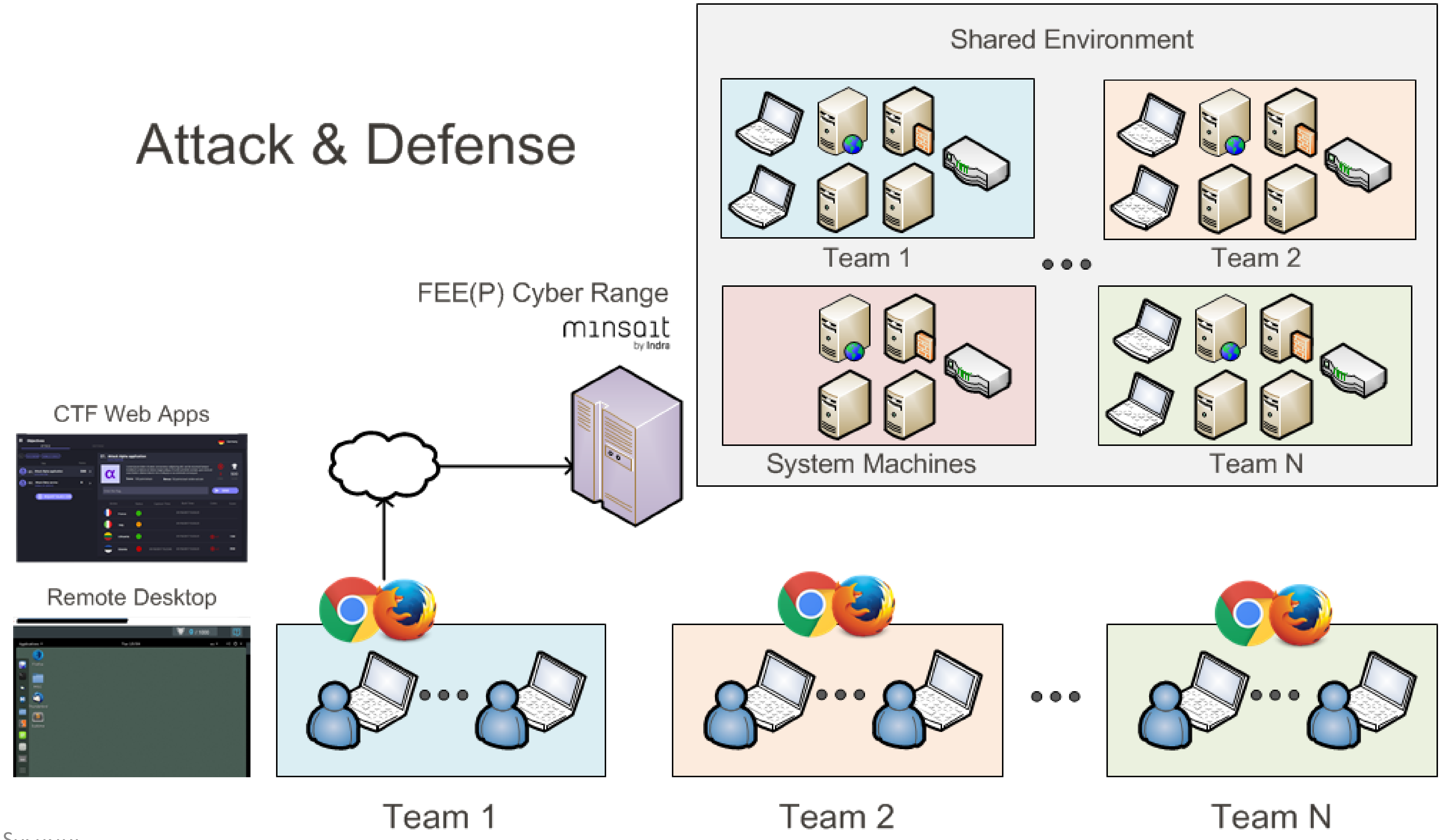
- **Kostantinos Vavousis - Unipi**
- **Alexandra Dritsa – Unipi**
- **Stella Tsitsioula – Red Comm**

Competition

- It will be based on the **educational exercise Capture-The-Flag (CTF),** which gives the participants experience in:
    - **Securing** a **machine** or an **application**
    - **Conducting** and **reacting** to **attacks** found in the **real world**
- Challenges will include:
    - **Reverse engineering, network sniffing, protocol analysis**
    - **System administration, programming, cryptoanalysis**
    - **Web security, forensics, mobile security**
- In both styles: (a) **attack/defense** and (b) **Jeopardy**

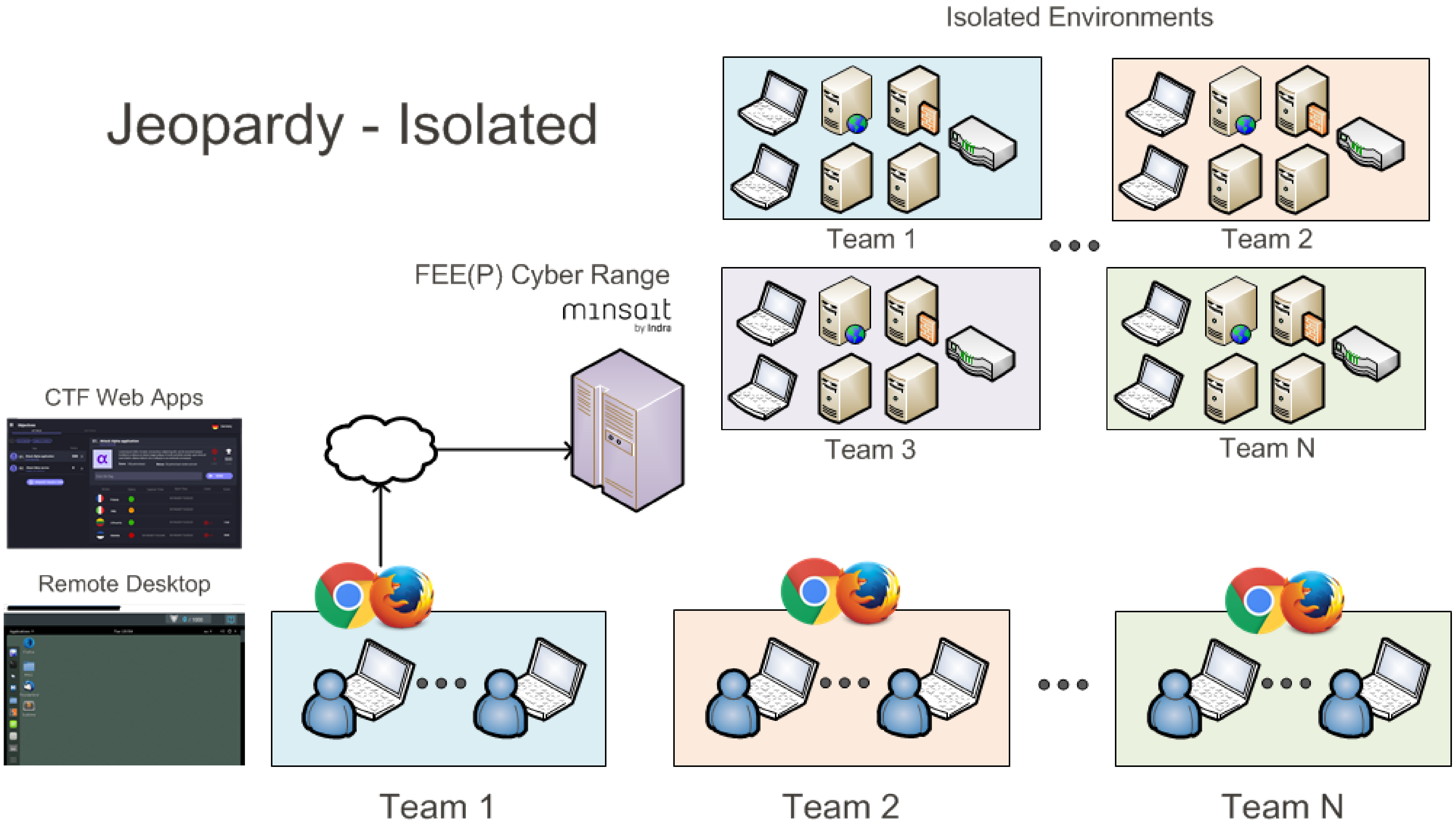
Competition - CTF

Attack & Defense



Competition - Isolated

Jeopardy - Isolated



Competition - Required skills

- Operating Systems
- Forensic Analysis
- Web Hacking
- Crypto Puzzles
- Malware Analysis
- Reverse Engineering
- Social Engineering
- Mobile Security
- Esteganography
- Database Security
- Code Analysis
- Cryptography
- Secure Programming
- Penetration Testing
- Network Security
- Miscellaneous

Objectives for the Hellenic Team in 2018

- Attract more than **> 100 participant** at the **National Competition**
- Constitute a team of more than **> 20 persons** of the two age sets **(14- 20) & (21 – 25)**
- **Create a Hellenic Cyber Security Academy**
  - Contestants, Coaches, Supporters, Professionals, Researcher, etc.
- **Attract more Sponsors**
- **Higher impact** and **exposure** to **the media / society**
- Become more **self-funded** by providing:
  - **Professional services**
  - **Cyber training**

EUROPEAN CYBER SECURITY CHALLENGE

LONDON, UNITED KINGDOM 2018

HELLENIC CYBER SECURITY TEAM

enisa

European Network and Information Security Agency

http://www. www.ecsc.gr

@ECSC2017HellenicTeam

European Cyber Security Challenge - Hellenic Team

@ECSCGR

xenakis@unipi.gr stet@ssl-unipi.gr ecsc@unipi.gr

UNIVERSITY OF PIRAEUS

UNIVERSITY OF PIRAEUS RESEARCH CENTER