



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

STELLA TSITSOULA

Communications Manager European Cyber Security Challenge

KONSTANTINOS VAVOUSIS

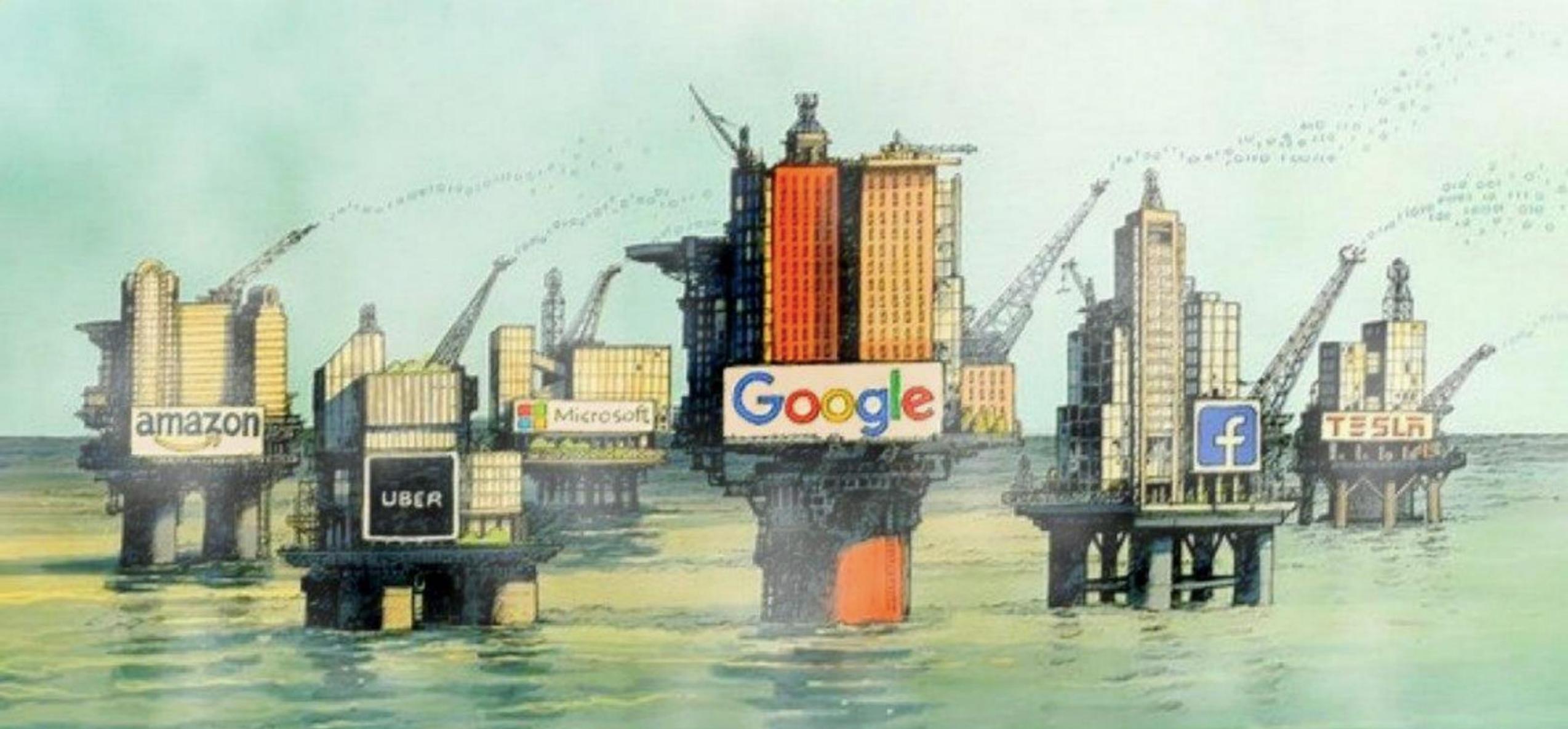
Team Manager European Cyber Security Challenge

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

Member of the European Cyber Security Challenge Steering Committee

Department of Digital Systems, University of Piraeus





The world's most valuable resource is no longer oil, but data.

The Economist - May 2017

David Parkins

Data Volume Growth Continues @ Rapid Clip... % Structured / Tagged (~10%) Rising Fast...

Information Created Worldwide = Expected to Continue Accelerating



**KLEINER
PERKINS**

Source: IDC DataAge 2025 Study, sponsored by Seagate (3/17)
Note: 1 petabyte = 1,000 gigabytes, 1 zeta byte = 1,000 petabytes

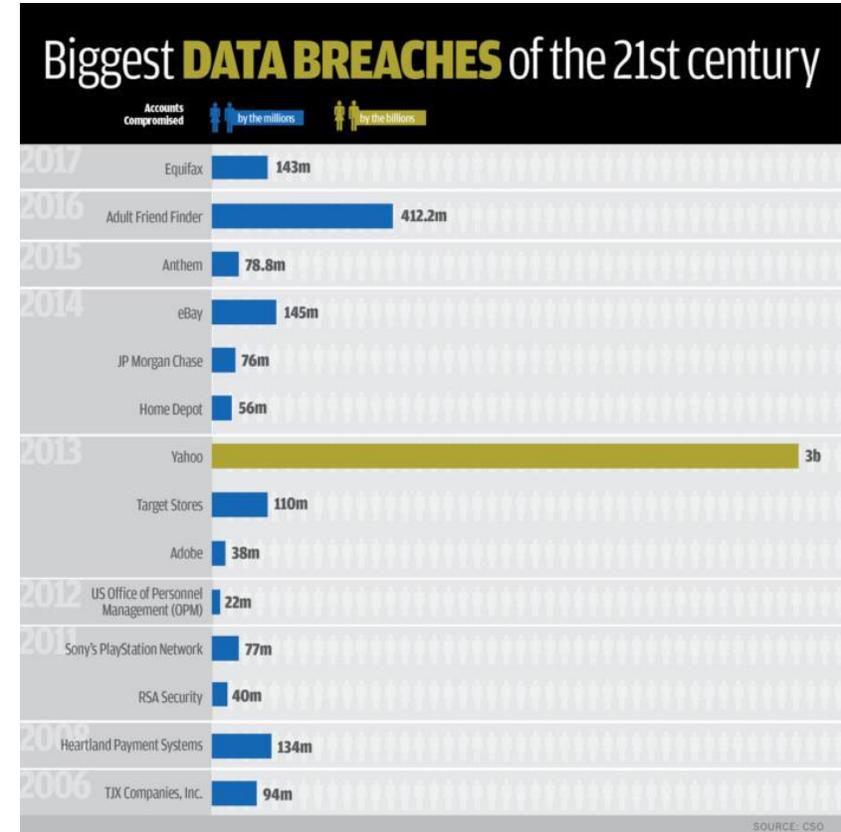
KP INTERNET TRENDS 2017 | PAGE 132



British Airways data breach

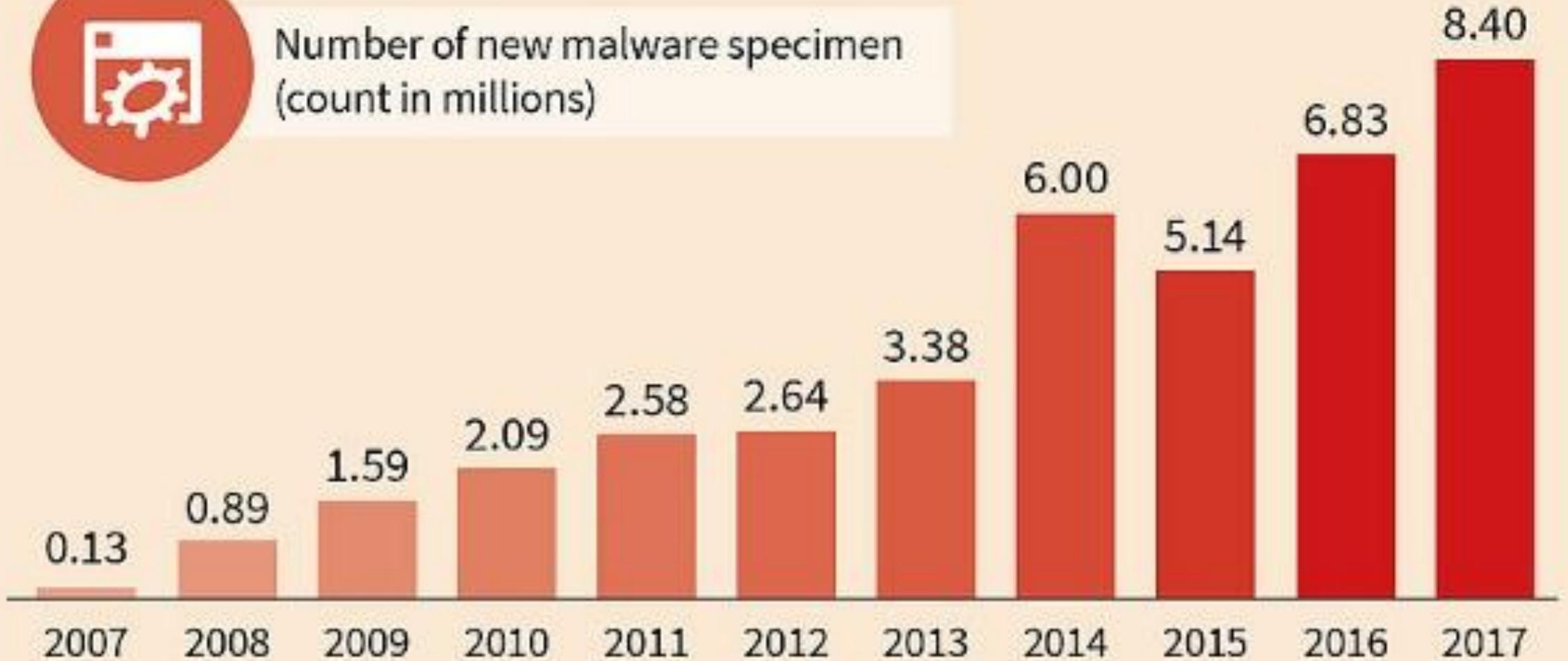
- BA announced that **380,000 card payments** were compromised
- Breach relates to bookings made between 10.58pm on 21 August and 9.45pm on 5 September 2018.

The last 8 years more than 7.1 Billion identities have been exposed in data breaches





Number of new malware specimen
(count in millions)



Web

Percentage of scanned websites with vulnerabilities

2014

76%

2015

78%

2016

76%

Percentage of which were critical

20%

15%

9%

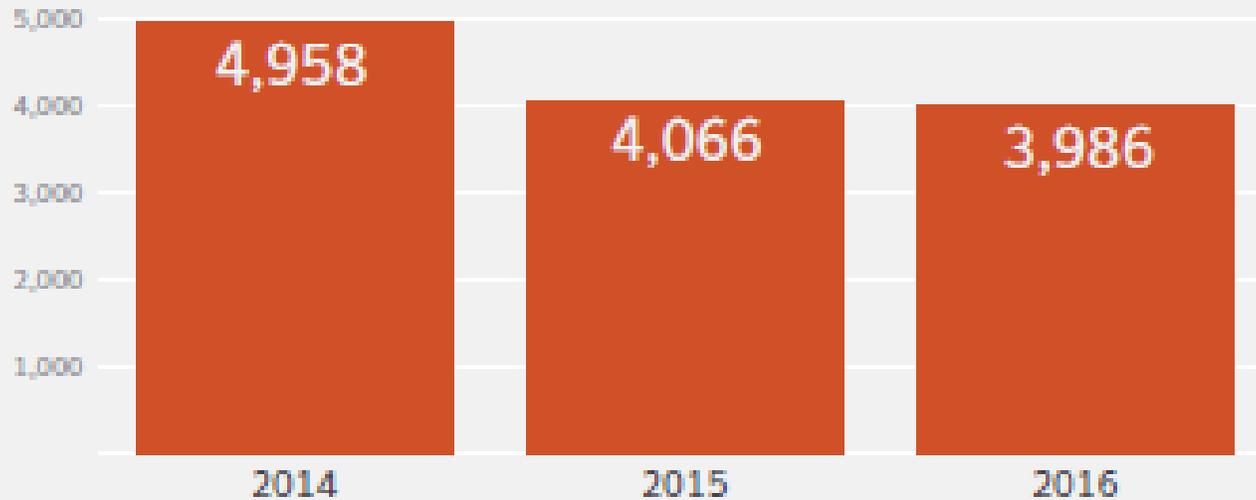
Average number of web attacks blocked per day

2015

340K

2016

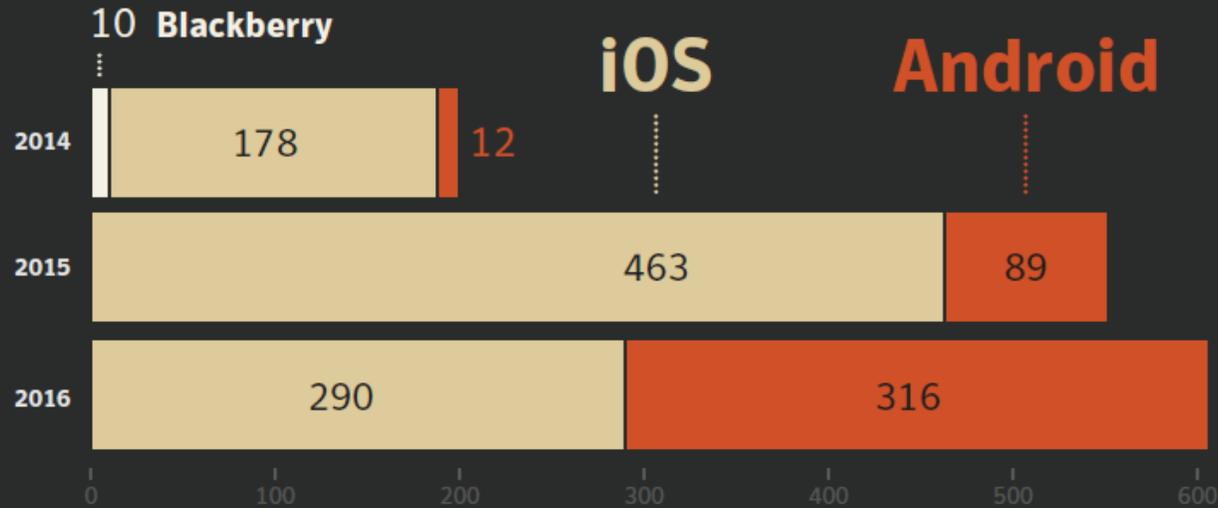
229K



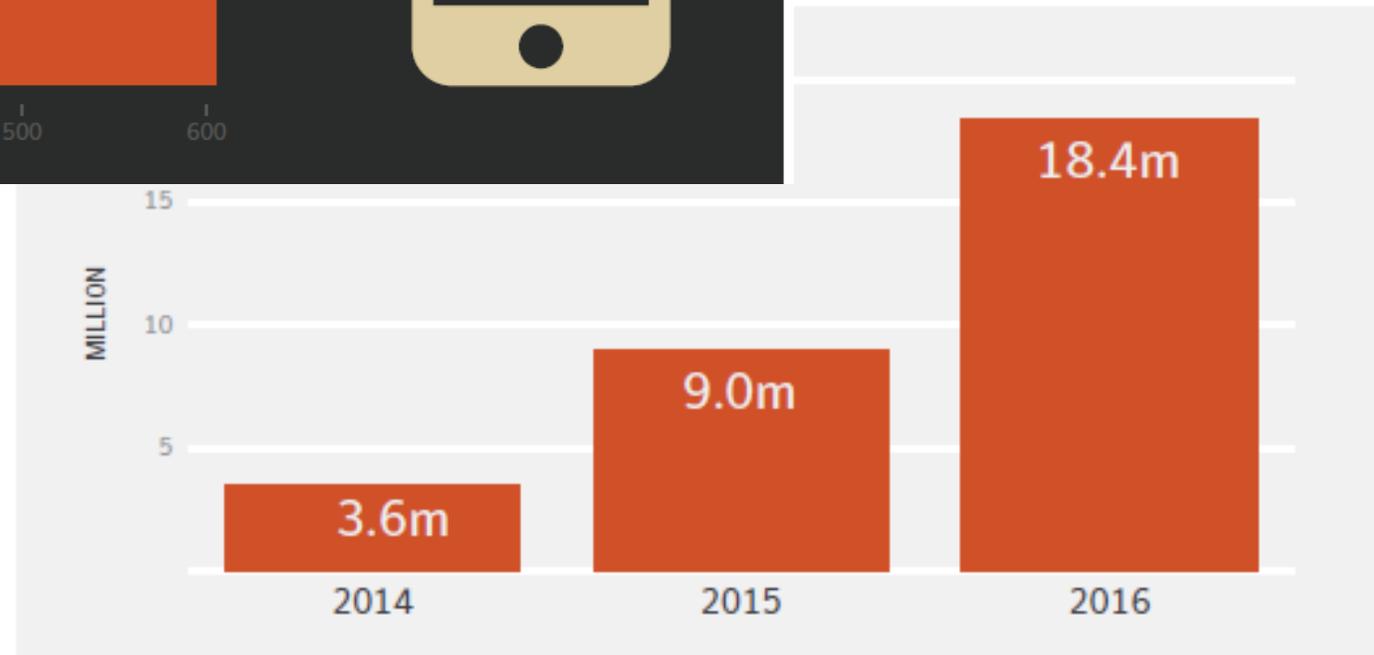
← Zero-day vulnerabilities

Mobile vulnerabilities reported, by operating system

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

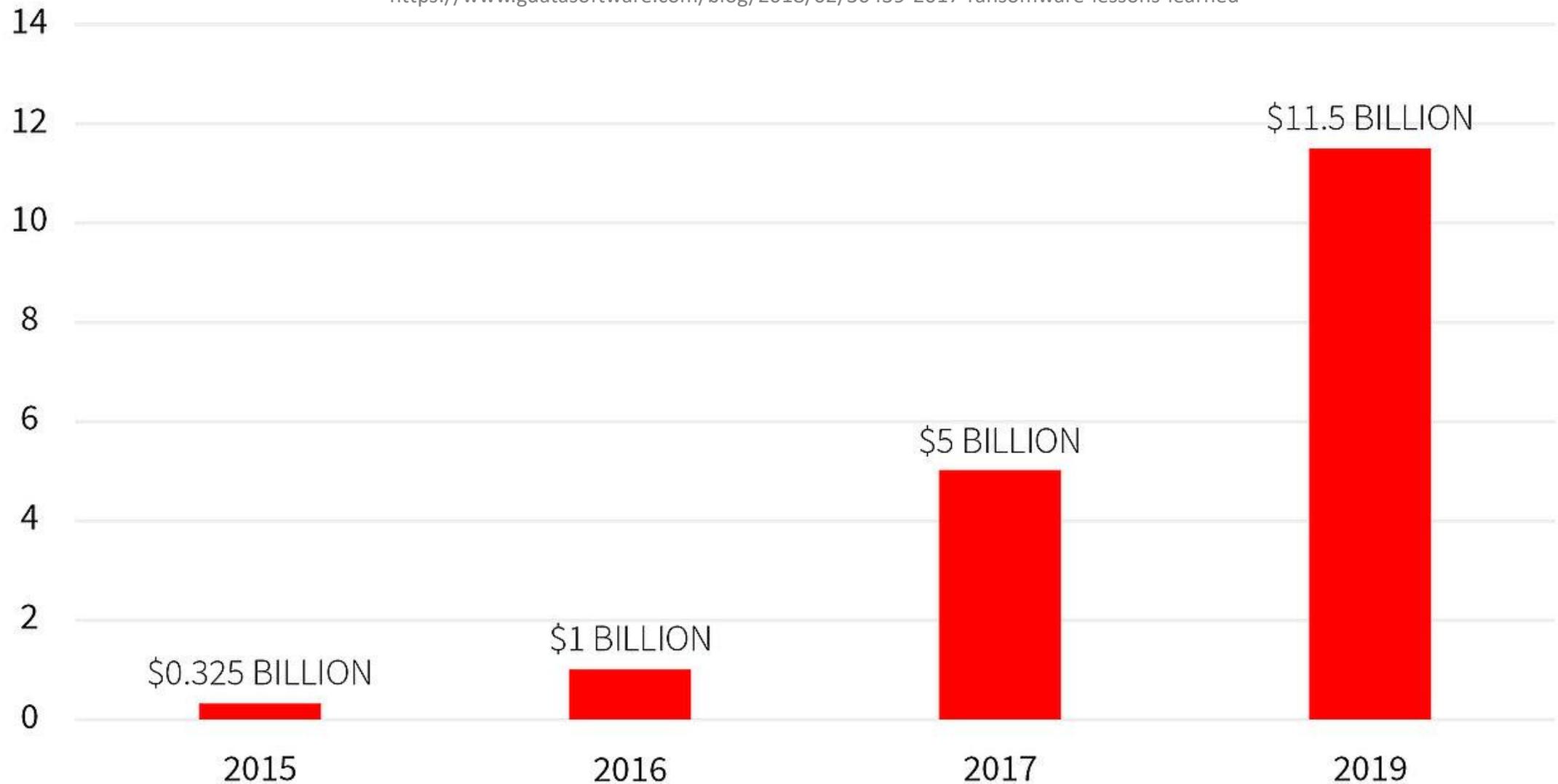


Number of mobile malware detection →



RANSOMWARE: TOTAL DAMAGE COST

<https://www.gdatasoftware.com/blog/2018/02/30439-2017-ransomware-lessons-learned>





The underground marketplace

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

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](#)



TOTAL RESULTS
2,833

TOP COUNTRIES



TOP SERVICES

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

RELATED TAGS: **ufanet**

82.76.209.232
82-76-209-232.rdsnet.ro
RCS & RDS Business
Added on 2018-02-18 07:38:55 GMT
Romania, Bucharest
[Details](#)

HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest qop="auth", realm="IF"

66.247.207.65
66-247-207-65.setardsl.aw
Sibh/setar Aruba
Added on 2018-02-18 07:38:27 GMT
Aruba, Oranjestad
[Details](#)

HTTP/1.1 200 OK
Server: Cross Web Server
Content-length: 2360
Content-type: text/html

```
<html>
<head>
<title>WebCam</title>
<script language="JavaScript">
function msieversion()
{
    var ua = window.navigator.userAgent;
    //alert(window.navigator.userAgent);
    var ms...
```

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](#)

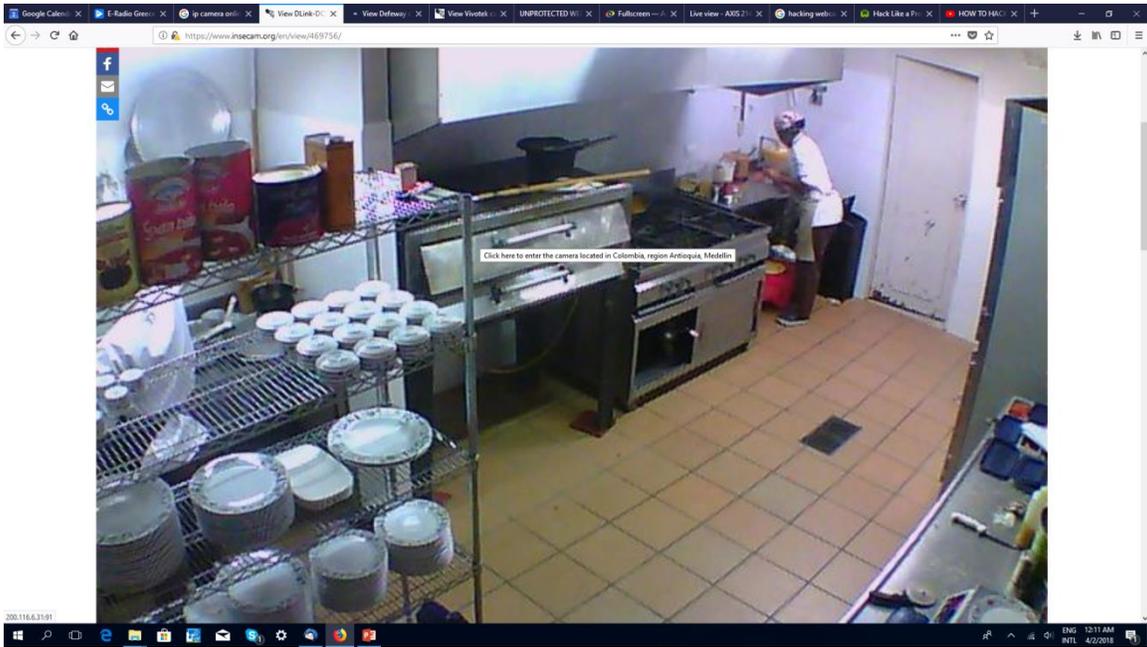


HTTP/1.1 200 OK

Internet of Things

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

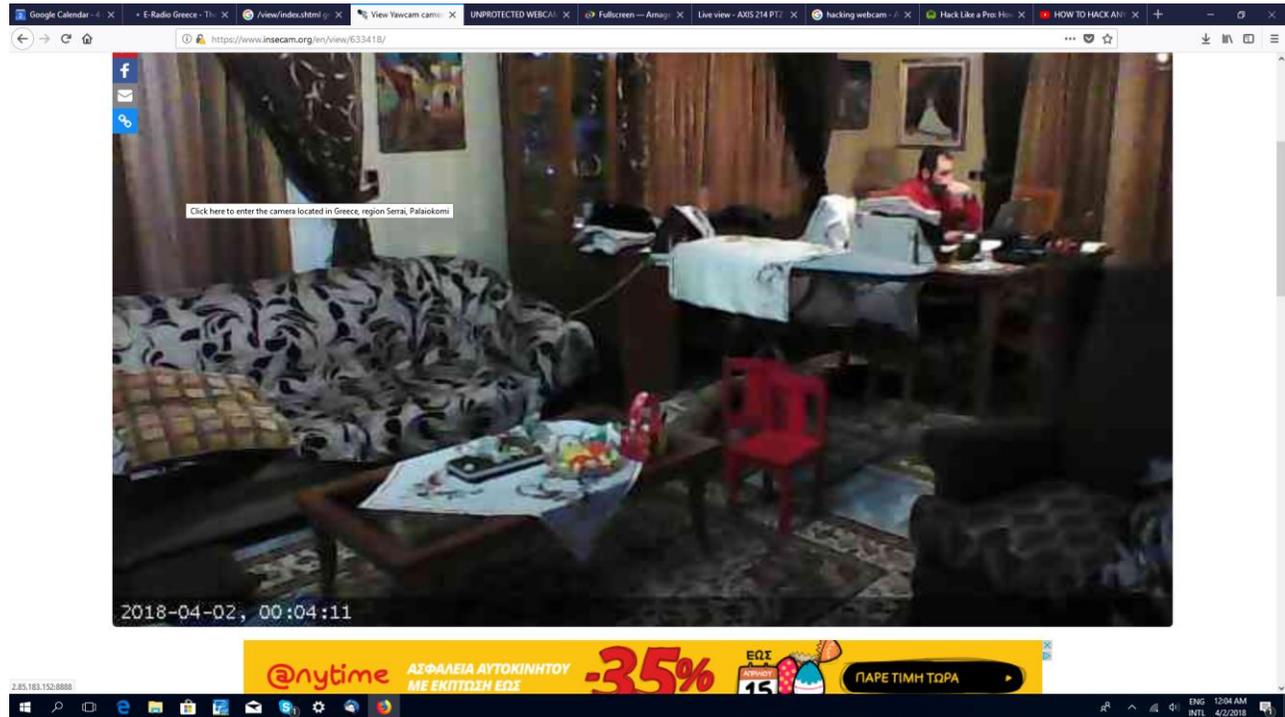
Speed of attack



<https://www.insecam.org/>

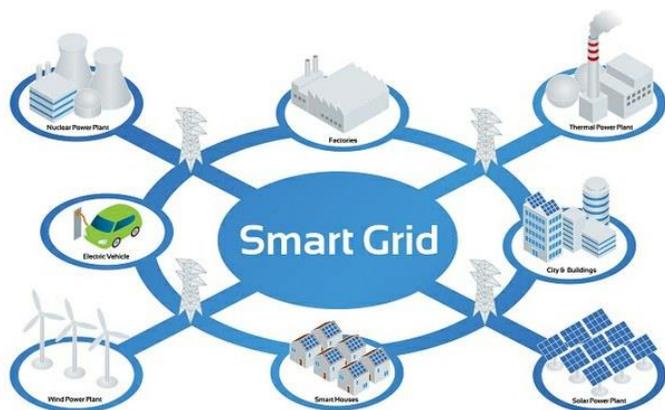


</view/index.shtml> greece



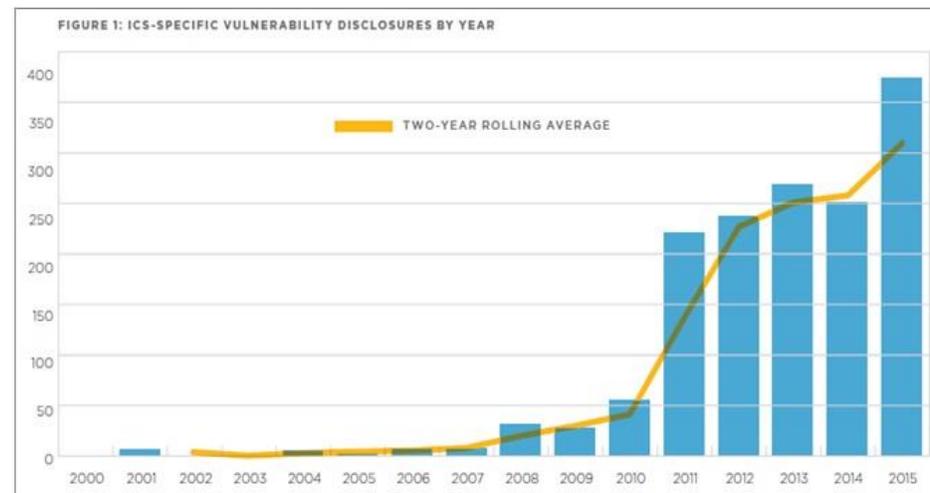
SCADA

- 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 in ICS



85.10.88.37

eu85-10-88-37.adsl.euphony.net.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

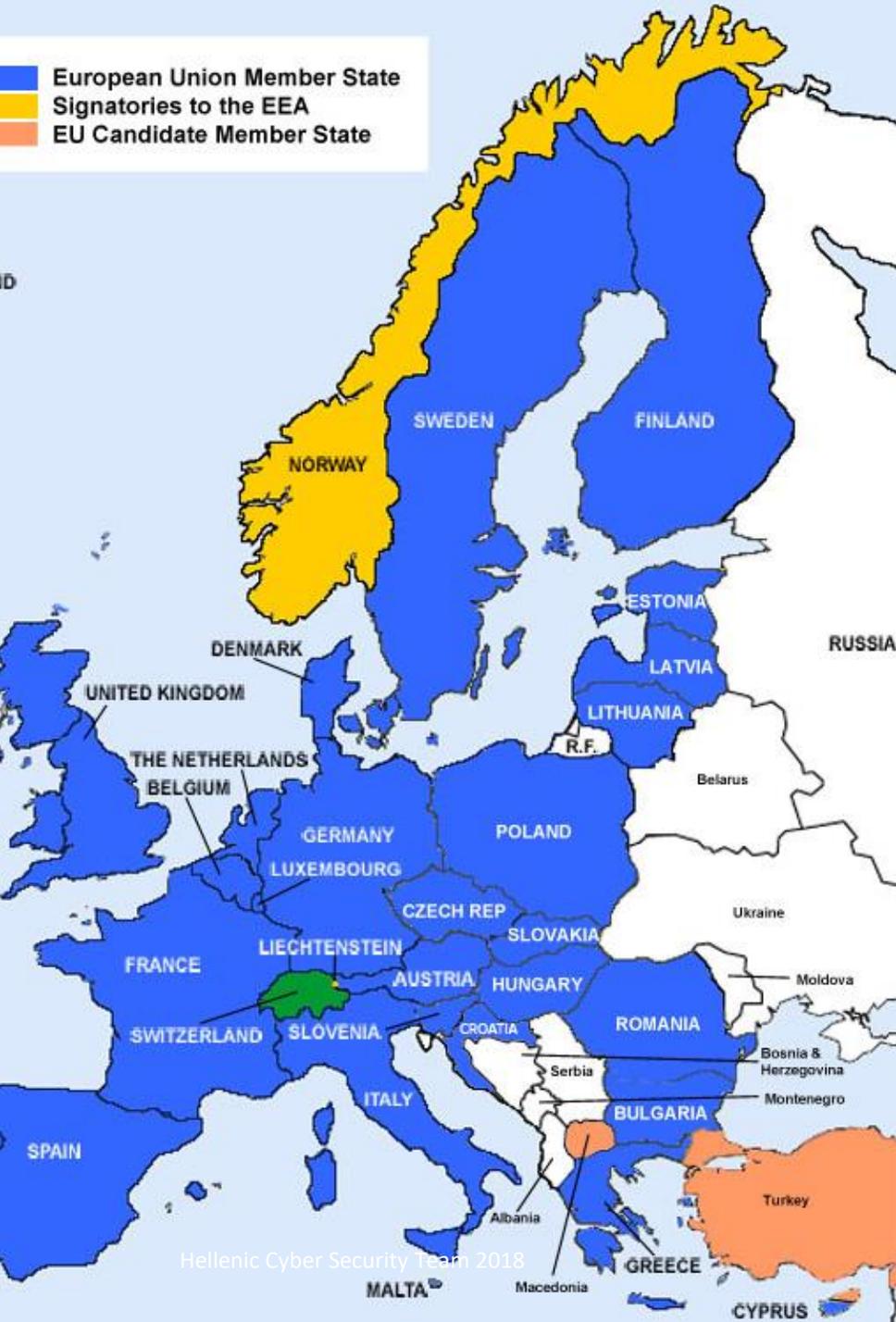


NEWS

Cybersecurity job market to suffer severe workforce shortage

The global [cybercrime epidemic](#) - predicted to cost the world \$6 trillion annually by 2021 - is creating an unprecedented shortage of cybersecurity workers.

- The Palo Alto Research Center and Symantec have both projected the demand for cybersecurity talent would rise to 6 million jobs (total jobs, filled and unfilled) globally by 2019.
- Cybersecurity Ventures predicts there will be [3.5 million unfilled cybersecurity positions globally by 2021](#). Every IT position is also a cybersecurity position now. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure, and people. If that is true, then the cybersecurity workforce shortage is even greater than what the numbers suggest.
- The [cybersecurity unemployment rate](#) was zero percent in 2016, and it's expected to remain there from 2017 to 2021. "The field of cyber security is the least populated of any field of technology," according to John McAfee. "There are two job openings for every qualified candidate."



What ECSC 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**

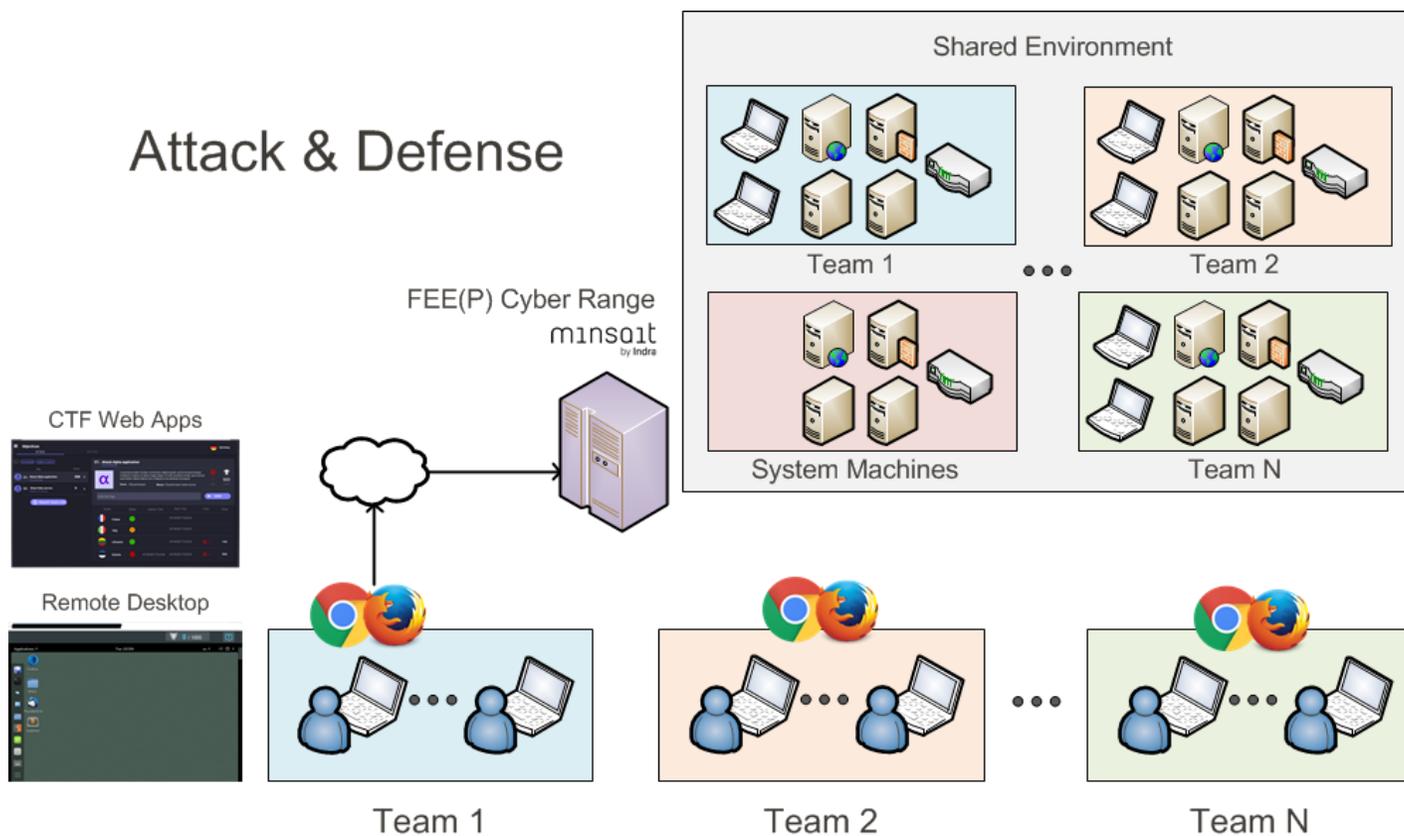
Steve Purser
ENISA Head of Core Operations Department

- **Europe is lacking people with strong cybersecurity skills**
- **Not only do we not have enough people with experience in implementing security in the real world,**
- **We also do not have enough people with an adequate knowledge of security techniques.**
- **That is why we encourage young people to pursue a career in cybersecurity.”**



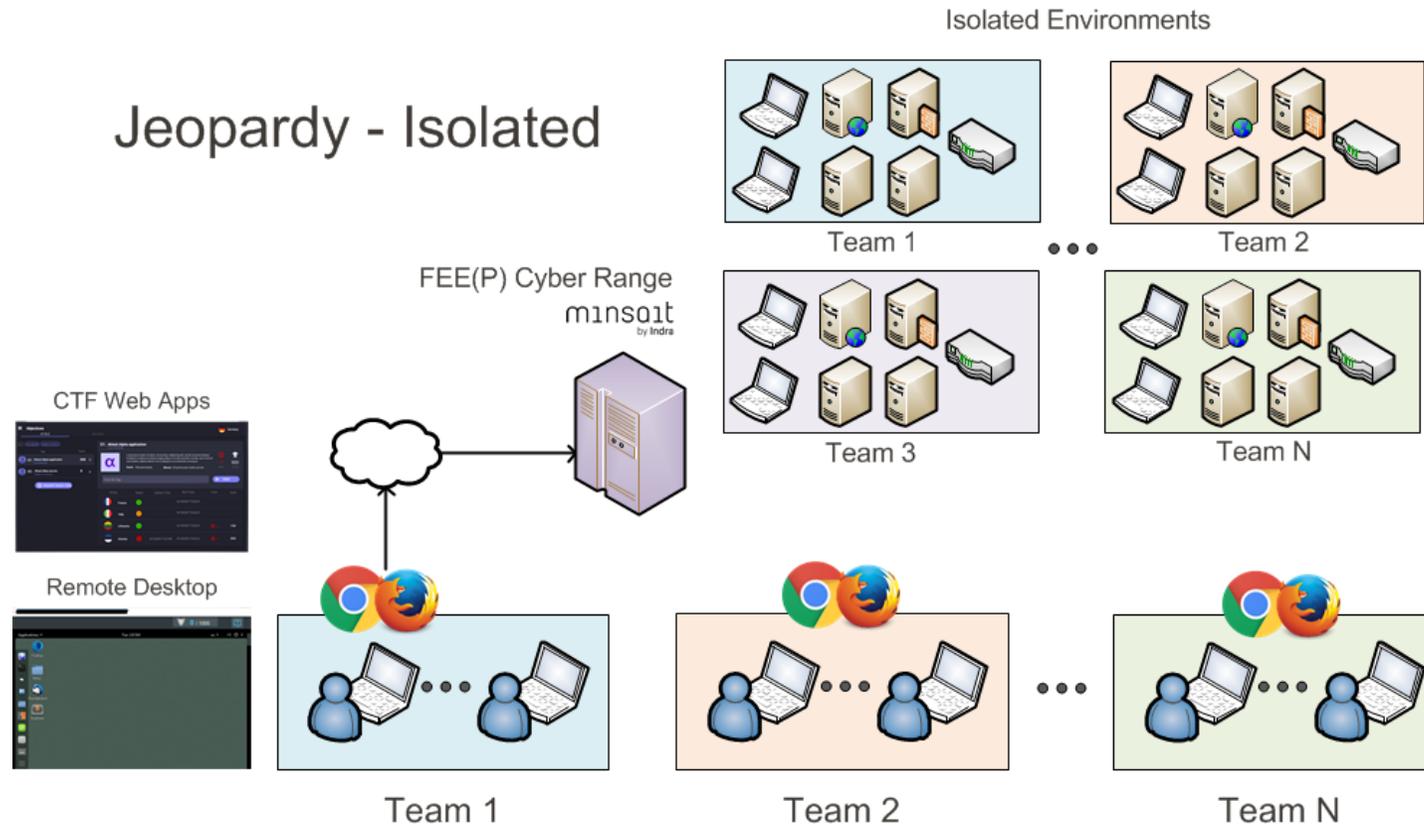
Competition - CTF

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

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**





www.ecsc.gr



@ECSC2017HellenicTeam



European Cyber Security Challenge - Hellenic Team



@ECSCGR



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



**UNIVERSITY
OF PIRAEUS**

Hellenic Cyber Security Team 2018

