
# Software Security

Pr. Dr. Yves ROUDIER
I3S – CNRS – UCA

Yves.Roudier@unice.fr
Yves.Roudier@i3s.unice.fr

# Software Security

- This is an introductory class about software security
  - High-level concepts
  - Hands-on experience on some attacks and protection approaches
- We will also consider network and hardware security to some extent
  - Software is distributed, mobile, or embedded today.
- Now that you know how to write code, we will see how to break it and how to secure it!
  - Understand software vulnerabilities
  - Concepts of security requirements engineering and security architectures

# A word of warning

- Don’t do this on others’ systems!
- Don’t do this on Polytech systems …
- Don’t do this in the wild neither for fun nor profit!

- Hacking/Cracking is illegal (and often unethical)
- This course discusses vulnerabilities in order to make you aware of the attack vectors that must be countered to secure software

- … you’ve been warned !!!!

- ***Le contenu de cet enseignement a un objectif strictement pédagogique. Toute personne utilisant son contenu hors de ce cadre s’expose à rendre des comptes devant des juridiques !***

# Developing your security awareness

- **Theory:** how the attacks work, what are software protection principles and mechanisms, etc.
- **Practice:** run a few attacks, write secure code, manipulate security libraries and tools for security testing
- **Mindset:** learn to think as an attacker, not just as a developer : you need to understand how to break a system before being able to create a secure design

# (Tentative) Course Outline

- Malware and Attacks: an introduction
- Software exploits 1: Web Apps
- Software exploits 2: Low level attacks
- Secure Software Development Life-Cycle
  - Security requirements, risk assessment, and model-driven engineering for security architectures, primer on cryptography
- Secure Programming
  - Security objectives and architectures, access control, security and cryptographic libraries
- Pentesting (Security testing): reverse engineering, static & dynamic analysis
- Secure execution environments, Trusted Computing (integrity and confidentiality), Secure Software Deployment

# About the course

- Slides and labs: available on the LMS Moodle (Securite logicielle - EIIN727)

- Grading
  - Written evaluations (60 min)
    - Oct 6th : 30%
    - Dec 1st : 40%
  - paper presentations : 30%
    - Papers will be presented by groups of 3-4 students
- Labs will NOT be graded

- Communications
  - Get in touch through Slack or email
  - Virtual meetings are preferred (COVID-19 …)

# Capture The Flag (CTF) contest

- Online or local CTF
  - Ph0wn: January, 2021

# After this course …

- CASPAR
  - https://www.dropbox.com/s/d5y2wxq4ej3a2on/CASPAR.pdf?dl=0
  - SI5 / Master 2 (Apprenticeship)
- Security Courses:
  - Cryptographie et Sécurité
  - Cybersecurité
  - Preuves en Cryptographie
  - Security and Privacy 3.0
  - Sécurité dans les réseaux
  - Sécurité des applications web

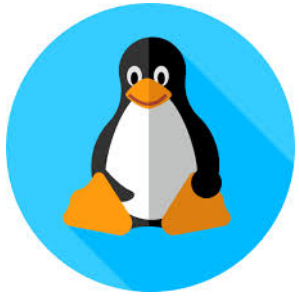
# Security: Why should you care?

- Security impacts on our daily lives
- You have to become a security-aware user
  - Make wise and informed decision when using software
- You want to become a security-aware developer or security consultant
  - Design and build secure software and systems
- You may like to become a security researcher
  - Find security flaws and propose original solutions

# Security is hard to capture

- Network Security
  - Perimeter protection  (authentication & more)
  - Protecting communications
- System Security
  - Security policies (Rights management, access control/usage)
- Hardware Security
  - Physical attacks over processors and memory
- Software Security
  - Software Vulnerabilities
  - Information flow protection
  - IPR protection (obfuscation, fingerprinting …)

# Software is everywhere (everyware?)




Operating Systems

Native Applications

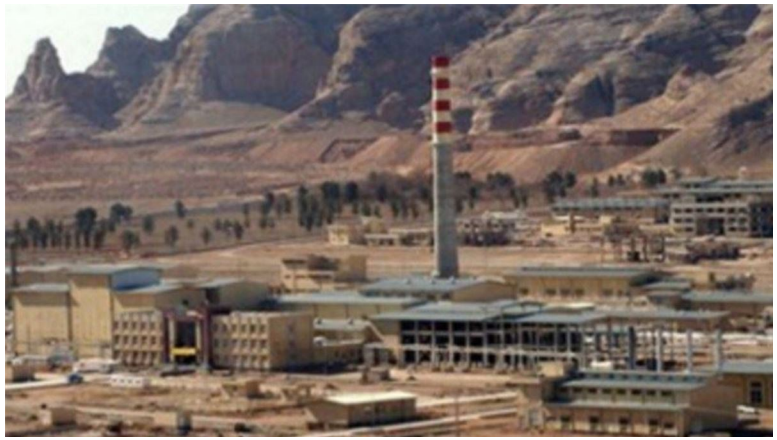

Web Applications

# Software is everywhere (everyware?)



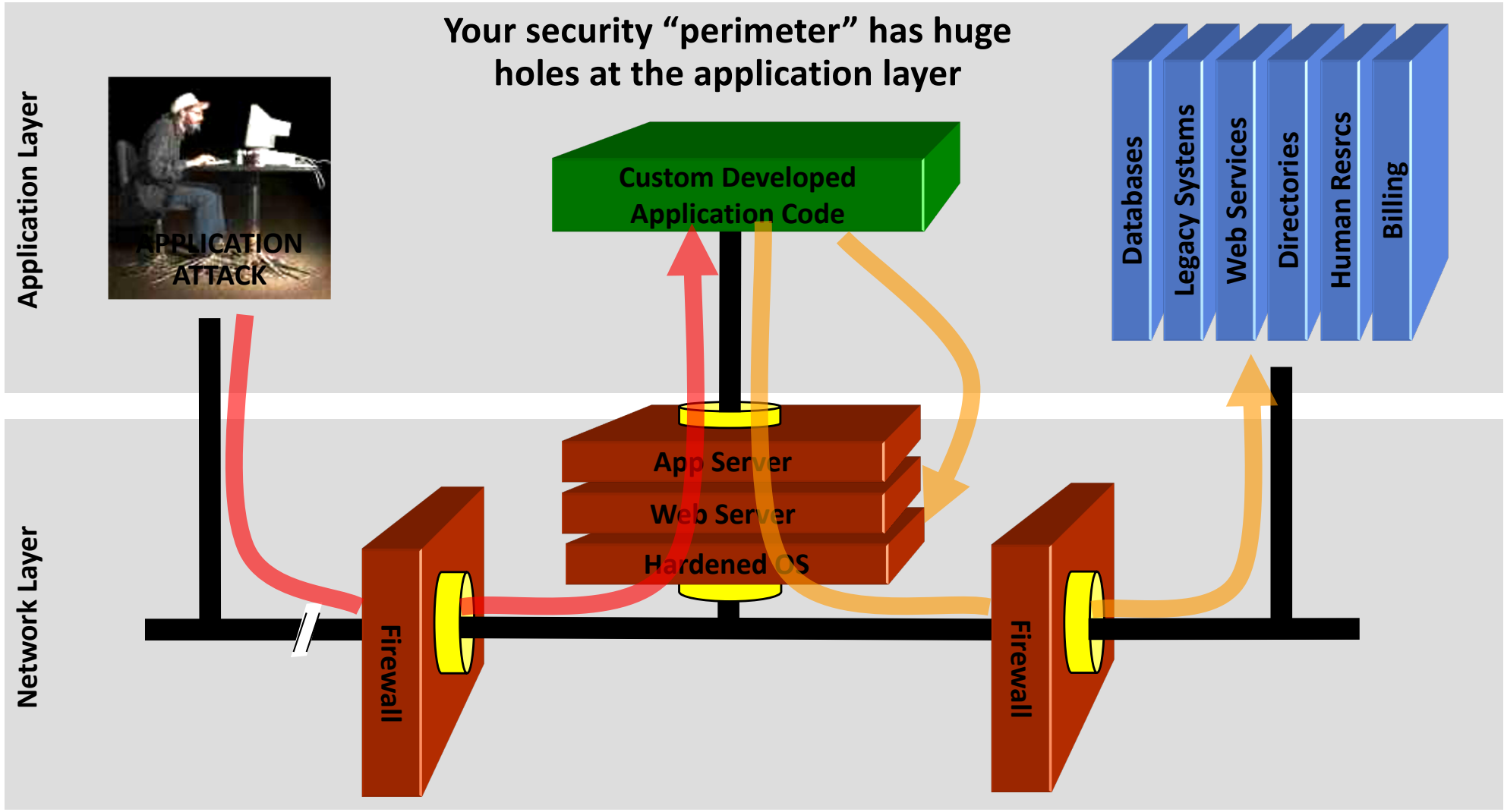
Network stacks


Security systems (smartcards, firewalls)

Cyber-Physical Systems (IoT, vehicles, plants)

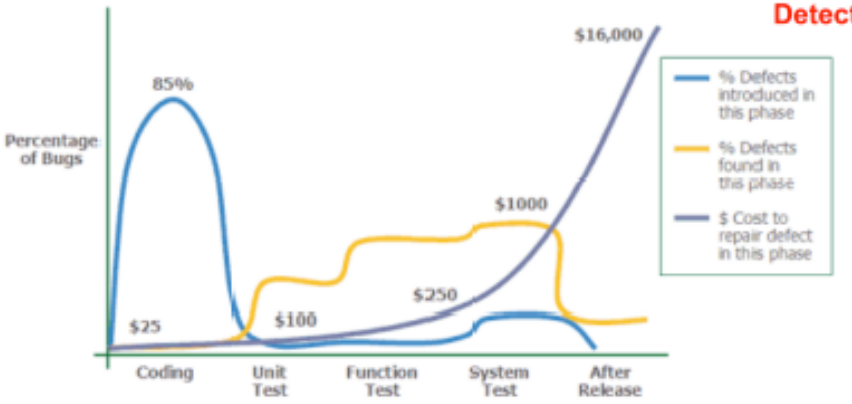
# Blurred Lines: Your Code is Part of Your Security Perimeter




**You can't use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks**

# Software and Security Engineering

- Multiple actors
- Separation of responsabilities
- Secure SDLC


"applied software measurement"
Capers Jones 1996

# Vulnerable Software

- Computer systems still have many vulnerabilities
  - Vocabulary: Human error -> fault (bug or unwanted access) -> security failure (vulnerability) -> exploitation (compromise)
- Technical factors
  - It's complex!
  - Wrong configuration vs. logical faults
- Organizational factors
  - Security = cost center!
  - Deadline pressure
- Human factors
  - Designer mindset
  - Environment

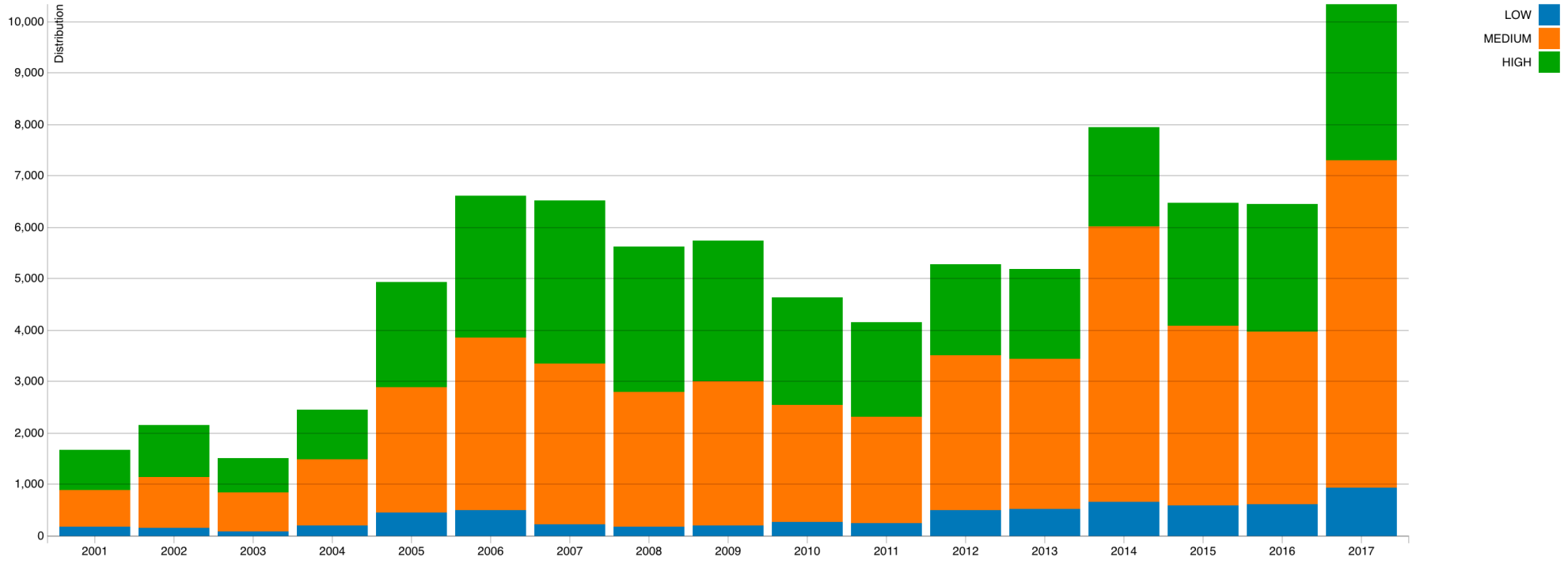
*Bruce Schneier's law (according to Cory Doctorow): "Any person can invent a security system so clever that he or she can't imagine a way of breaking it."*

# Vulnerable Software

- Exploitation is as old as remote access
  - Major issue as computer systems become more ubiquitous
  - Exposure to remote access (e.g. the Internet) leads to exploitation
  - 1973 - Bob Metcalfe's *RFC 602: "The Stockings Were Hung by the Chimney with Care" (about security issues in the ARPANET)*
    - "Many people still use passwords which are easy to guess: their first names, their initials, their host name spelled backwards, a string of characters which are easy to type in sequence"

# Software Flaws

https://web.nvd.nist.gov/view/vuln/statistics



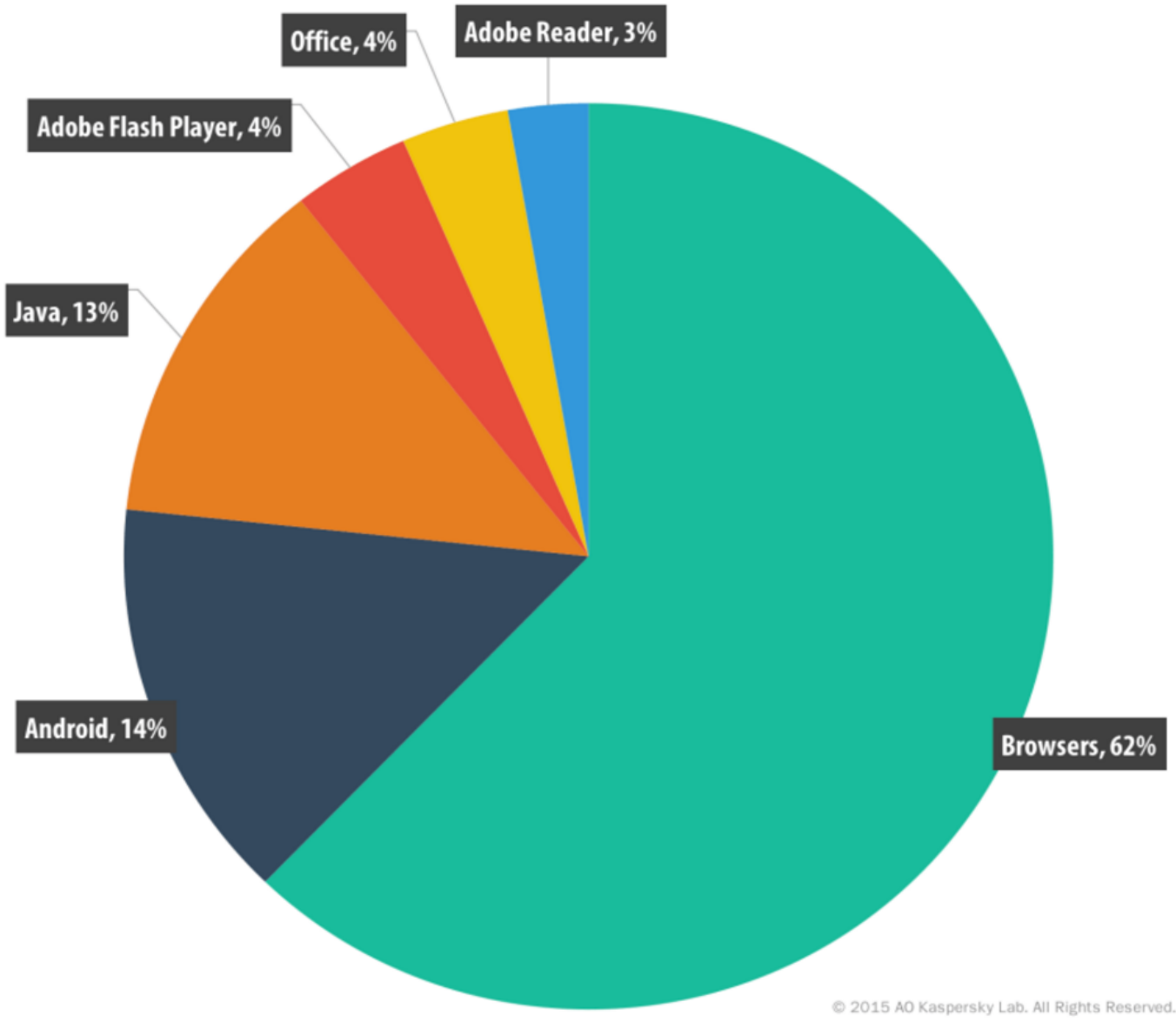

- CVSS Severity Distribution Over Time

# Vulnerability disclosures (2015)

| | Product Name | Vendor Name | Product Type | Number of Vulnerabilities |
|---|---|---|---|---|
| 1 | Mac Os X | Apple | OS | 385 |
| 2 | Iphone Os | Apple | OS | 376 |
| 3 | Flash Player | Adobe | Application | 313 |
| 4 | Air Sdk | Adobe | Application | 246 |
| 5 | AIR | Adobe | Application | 246 |
| 6 | Air Sdk & Compiler | Adobe | Application | 246 |
| 7 | Internet Explorer | Microsoft | Application | 231 |
| 8 | Chrome | Google | Application | 187 |
| 9 | Firefox | Mozilla | Application | 178 |
| 10 | Windows Server 2012 | Microsoft | OS | 155 |
| 11 | Ubuntu Linux | Canonical | OS | 152 |
| 12 | Windows 8.1 | Microsoft | OS | 151 |

source: www.cvedetails.com/top-50-products.php?year=2015

# Vulnerable applications being exploited

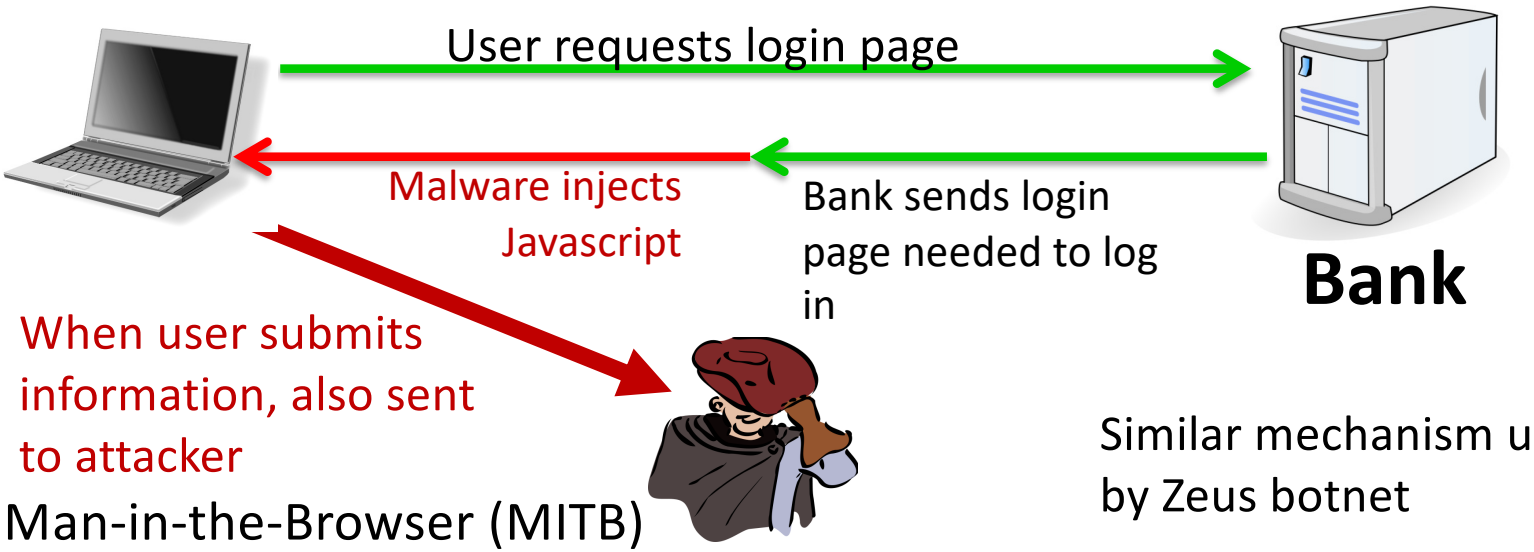



Source: Kaspersky Security Bulletin 2015

# Malware and Attacks

# Malware: Malicious Software

- Malware = malicious software (software as attack vector)
  - Spam
  - Denial of Service
    - Services: 1 hour (20$), 24 hours (100$)
  - Click Fraud
  - Stealing credentials and passwords
    - Example: Target attack (2013), ≈ 140M CC numbers stolen




Similar mechanism used by Zeus botnet

# Malware: Malicious Software

- Terminology
  - Trojan horse: allows remote access to unauthorized users
  - Virus: computer program designed to spread (requires human intervention)
  - Worm: does not require human intervention
  - Adware: ads when application is running
  - Spyware: monitors & collects information to be transmitted to a third party without user knowledge/consent
  - Ransomware: asks for a ransom to prevent deletion of data (encrypted and/or transferred to some other disk)
  - Botnets: network of (ro)bot / zombie computers under the control of attackers and used for perpetrating attacks or sending other vectors

# Malware: a few trends

- Viruses, worms and bots are more stealthy today
  - 2008-2009 Conficker infected 2-15 million windows servers
- Ransomware is on the rise
  - Originally weak threat (encryption keys recovered from software)
  - Now use up to date asymmetric encryption techniques
- Mobile malware is exploding
  - Banking applications, notably
- Drive by download from mainstream websites
- Dynamic and highly obfuscated malware
- Browser plugins
- Misleading applications

# Malware: a few trends

- SQL injection on mainstream websites
- Malvertisements: users redirected to malicious websites
- Malware is more prevalent than ever, leading to an underground economy
  - "MPack is sold as commercial software (costing $500 to $1,000 US), and is provided by its developers with technical support and regular updates of the software vulnerabilities it exploits."
  - Botnets of up to several million computers – their control is also disputed among hackers
  - Exponential increase in unique and targeted malware samples

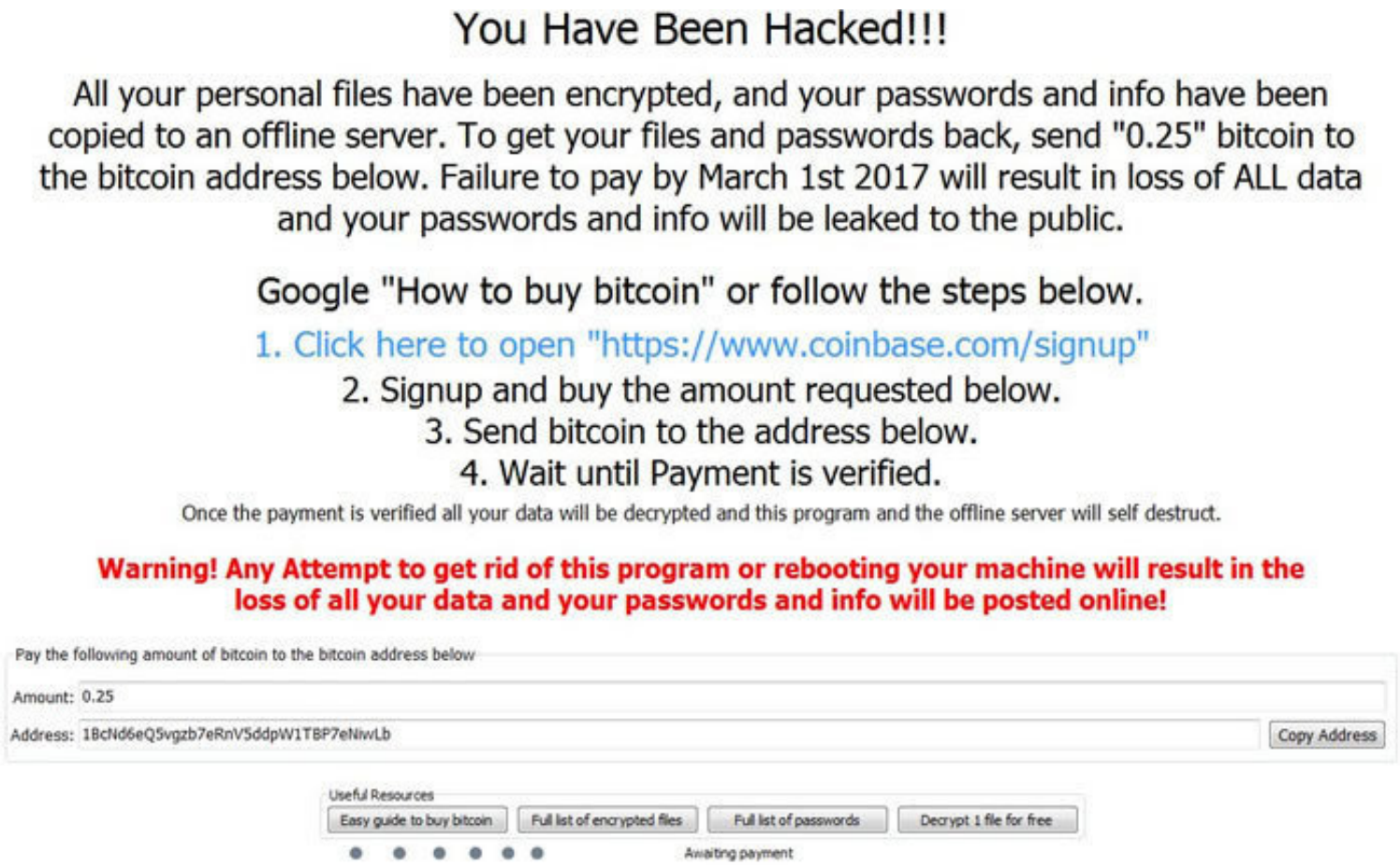
# Lots of financial malware

| | |
|---|---|
| 1 | Trojan-Downloader.Win32.Upatre |
| 2 | Trojan-Spy.Win32.Zbot |
| 3 | Trojan-Banker.Win32.ChePro |
| 4 | Trojan-Banker.Win32.Shiotob |
| 5 | Trojan-Banker.Win32.Banbra |
| 6 | Trojan-Banker.Win32.Caphaw |
| 7 | Trojan-Banker.AndroidOS.Faketoken |
| 8 | Trojan-Banker.AndroidOS.Marcher |
| 9 | Trojan-Banker.Win32.Tinba |
| 10 | Trojan-Banker.JS.Agent |

- size: 3.5 KB
- spread via email attachments
- also found on home routers

Source: Kaspersky Security Bulletin 2015

# Ransomware


You Have Been Hacked!!!
All your personal files have been encrypted, and your passwords and info have been copied to an offline server. To get your files and passwords back, send "0.25" bitcoin to the bitcoin address below. Failure to pay by March 1st 2017 will result in loss of ALL data and your passwords and info will be leaked to the public.
Google "How to buy bitcoin" or follow the steps below.
1. Click here to open "https://www.coinbase.com/signup"
2. Signup and buy the amount requested below.
3. Send bitcoin to the address below.
4. Wait until Payment is verified.
Once the payment is verified all your data will be decrypted and this program and the offline server will self destruct.
Warning! Any Attempt to get rid of this program or rebooting your machine will result in the loss of all your data and your passwords and info will be posted online!
Pay the following amount of bitcoin to the bitcoin address below
Amount: 0.25
Address: 1BcNd6eQ5vgzb7eRnV5ddpW1TBP7eNiwLb
Copy Address
Useful Resources
Easy guide to buy bitcoin
Full list of encrypted files
Full list of passwords
Decrypt 1 file for free
Awaiting payment

# Ransomware

## Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

## Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5

## What we did?

We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world (Encryption -Wikipedia). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.

## Why we do that?

We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. **I personally have lost both my parents and my little sister in 2015.** The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. (Syria War in Wikipedia)

Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people. We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.

# Why own machines: 3. **Ransomware**

| | |
|---|---|
| 1 | Trojan-Ransom.HTML.Agent |
| 2 | Trojan-Ransom.JS.Blocker |
| 3 | Trojan-Ransom.JS.InstallExtension |
| 4 | Trojan-Ransom.NSIS.Onion |
| 5 | Trojan-Ransom.Win32.Cryakl |
| 6 | Trojan-Ransom.Win32.Cryptodef |
| 7 | Trojan-Ransom.Win32.Snocry |
| 8 | Trojan-Ransom.BAT.Scatter |
| 9 | Trojan-Ransom.Win32.Crypmod |
| 10 | Trojan-Ransom.Win32.Shade |

CryptoWall (2014-)

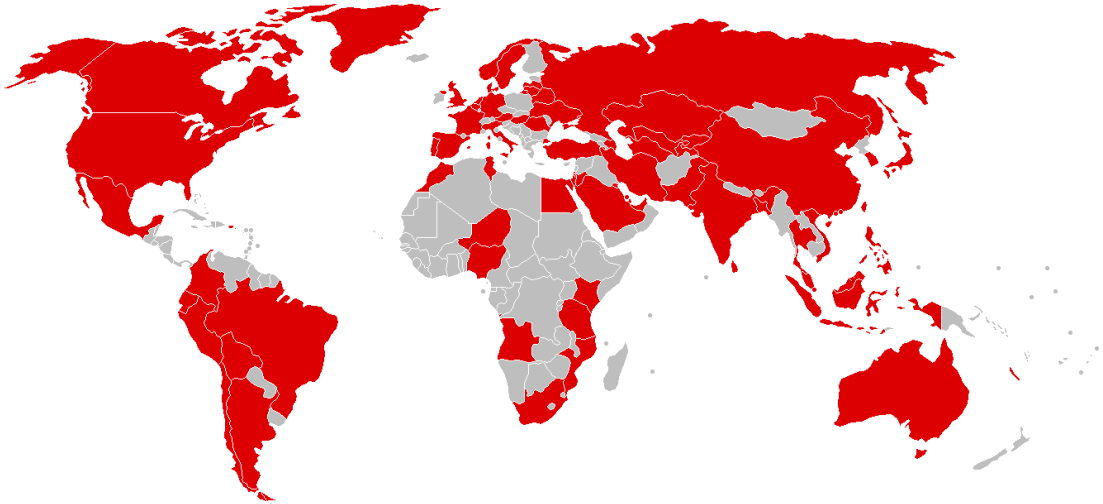
- targets Windows
- spread by spam emails

≈ 200,000 machines in 2015

A worldwide problem.

# Wannacry (May 2017)

- Worldwide Cyberattack on Windows
- infected more than 230,000 computers in over 150 countries
- NHS (UK), Renault (France), Deutsche Bahn (Germany), Telefonica (Spain) …
- Kill Switch URL discovered by security researcher Marcus Hutchins



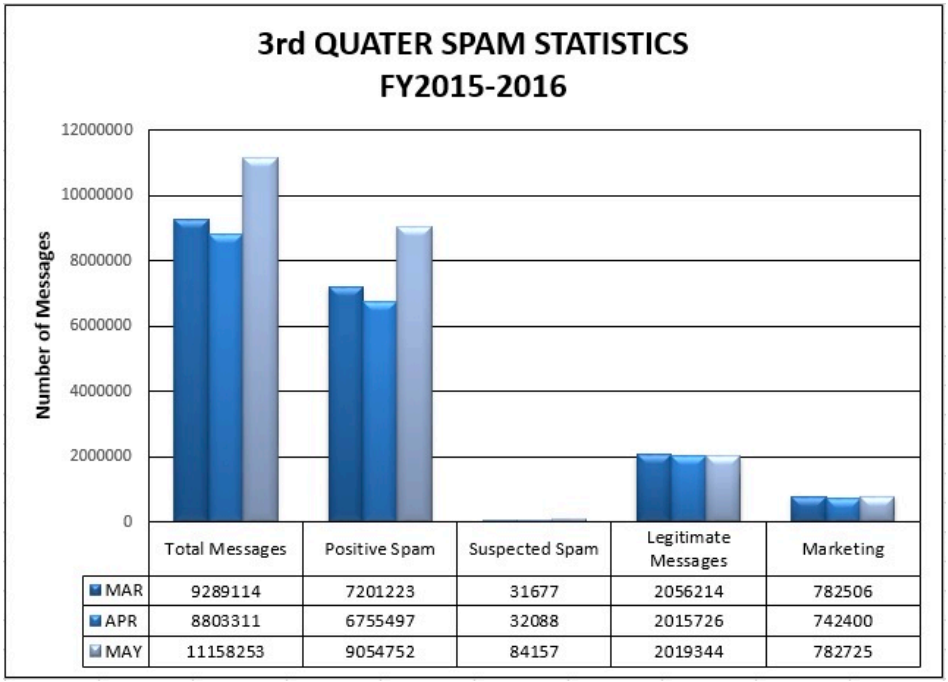
# A few more figures

- “The Business of Rogueware”, PandaLabs, 2010
- “The Business of Cybercrime”, PandaLabs, 2008
- “Web Based Attacks”, Symantec, 2009

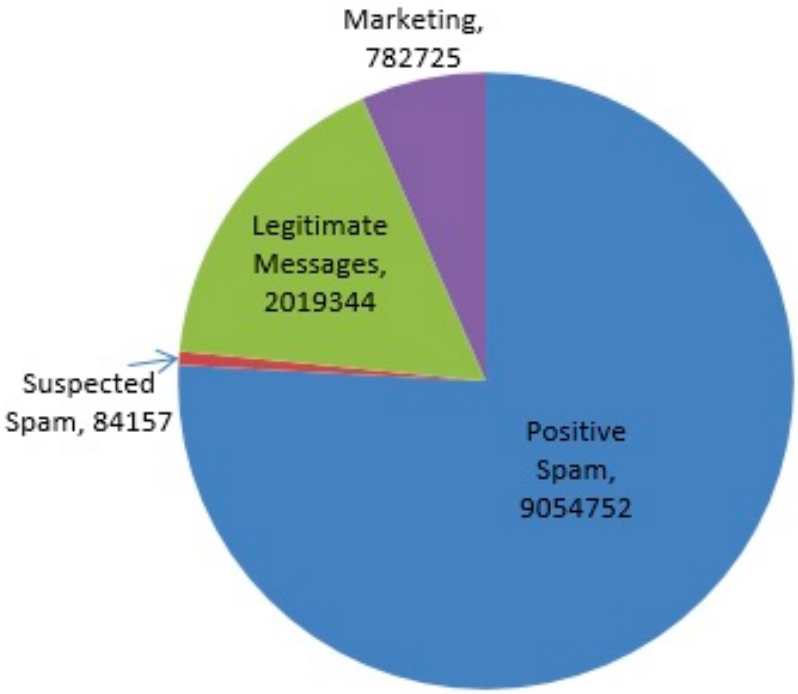
- Adware industry is worth 2 billion dollars per year
- Malware industry is worth 105 billion dollars per year
- > 80% of the e-mail traffic out there is (or was) spam
- 50%-80% of computers connected to Internet infected with spyware
- Some people make 20 thousand dollars (!) per month using botnets (i.e., compromised computers)
- A 26 year-old made 20 million dollars with spam before being caught
- 2 billion dollars were lost to phishers four years ago

# SPAM Statistics (May 2016)

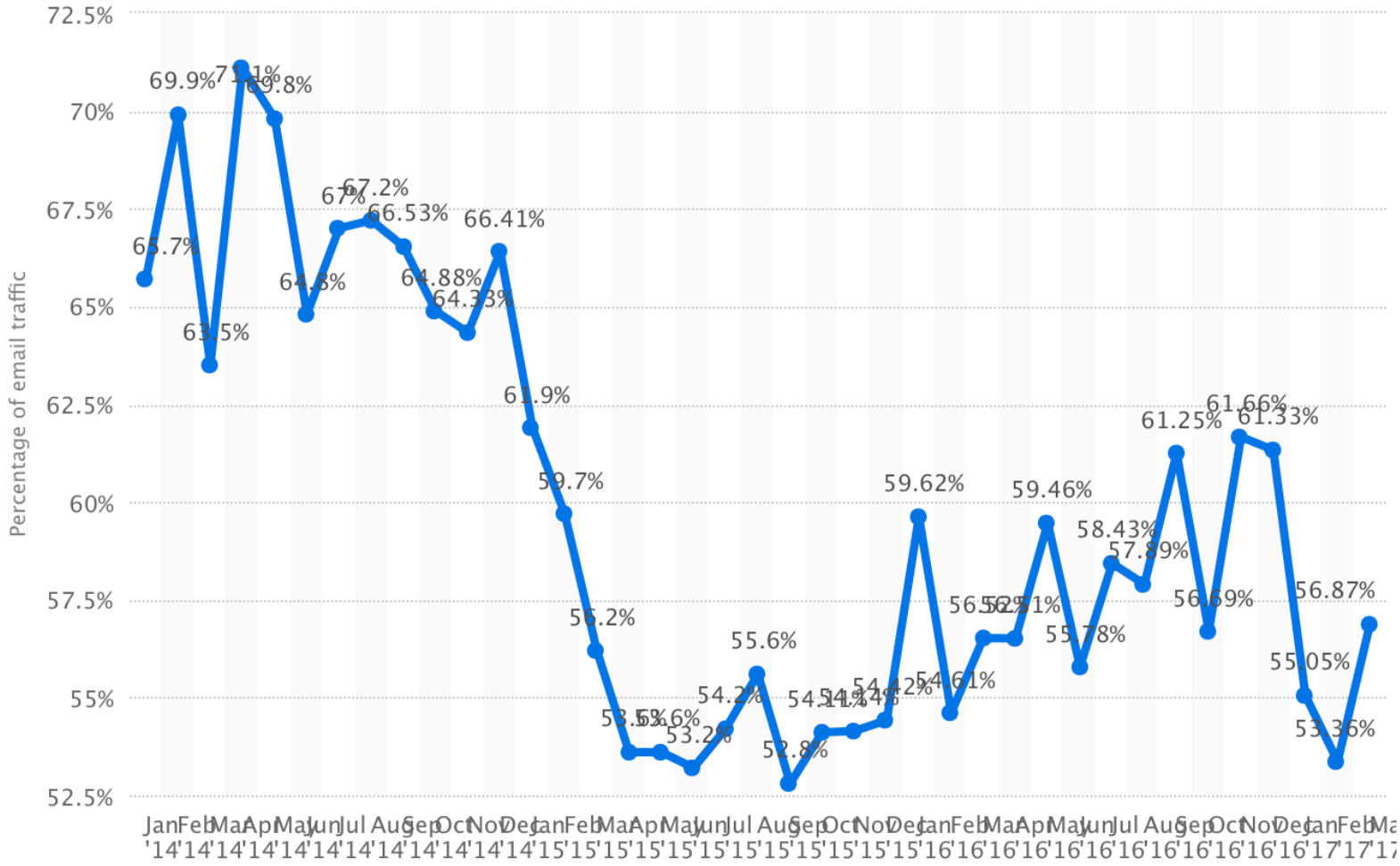
- Information Security Office (Univ. El Paso)




| | Total Messages | Positive Spam | Suspected Spam | Legitimate Messages | Marketing |
|---|---|---|---|---|---|
| MAR | 9289114 | 7201223 | 31677 | 2056214 | 782506 |
| APR | 8803311 | 6755497 | 32088 | 2015726 | 742400 |
| MAY | 11158253 | 9054752 | 84157 | 2019344 | 782725 |



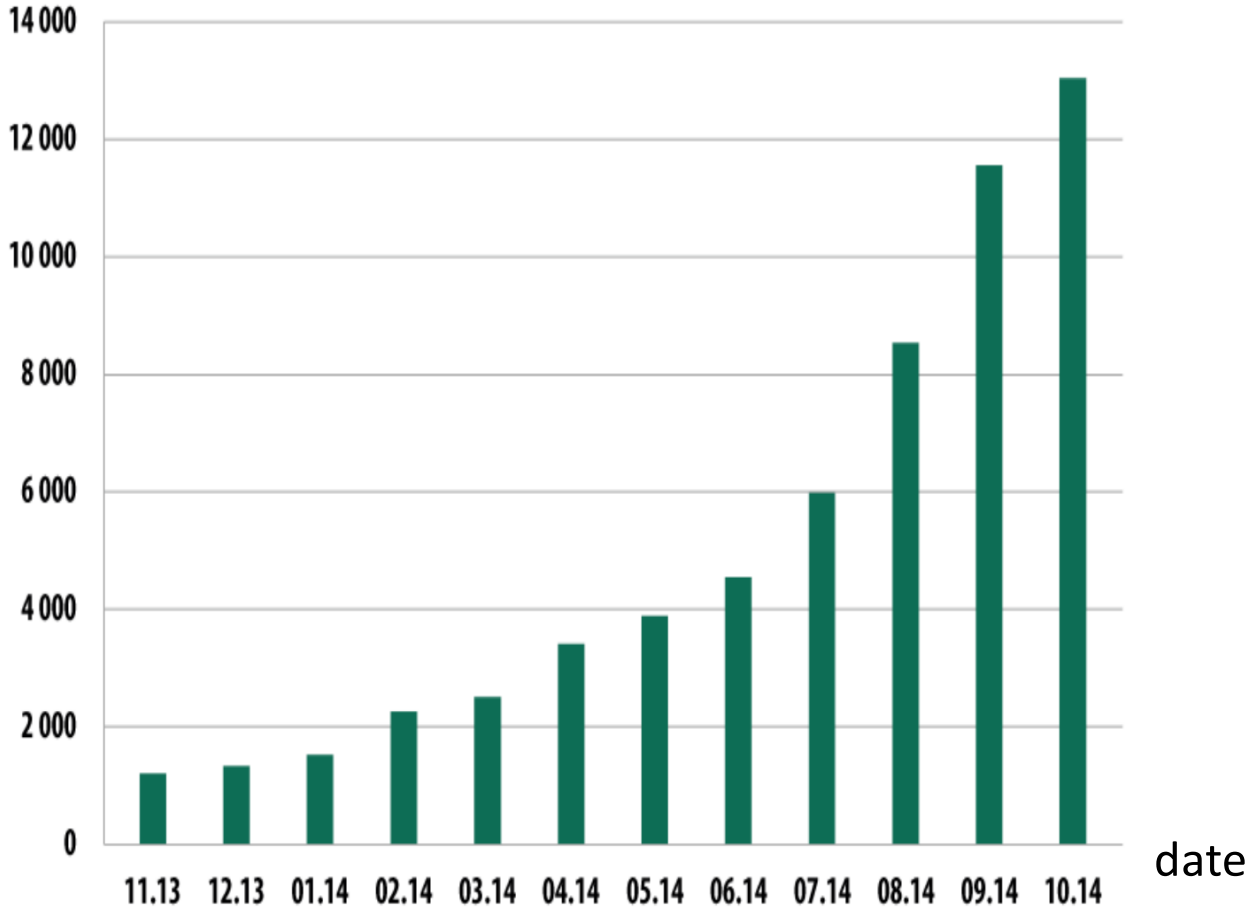
# SPAM volume as percentage of email traffic




Data visualized by tableau

© Statista 2017

# Mobile malware (Nov. 2013 – Oct. 2014)




The rise of mobile banking Trojans (Kaspersky Security Bulletin 2014)

# An unprecedented scale (IoT)

## EXTRA-LARGE DENIAL OF SERVICE ATTACK USES DVRS, WEBCAMS

by: Elliot Williams

46 Comments

September 26, 2016

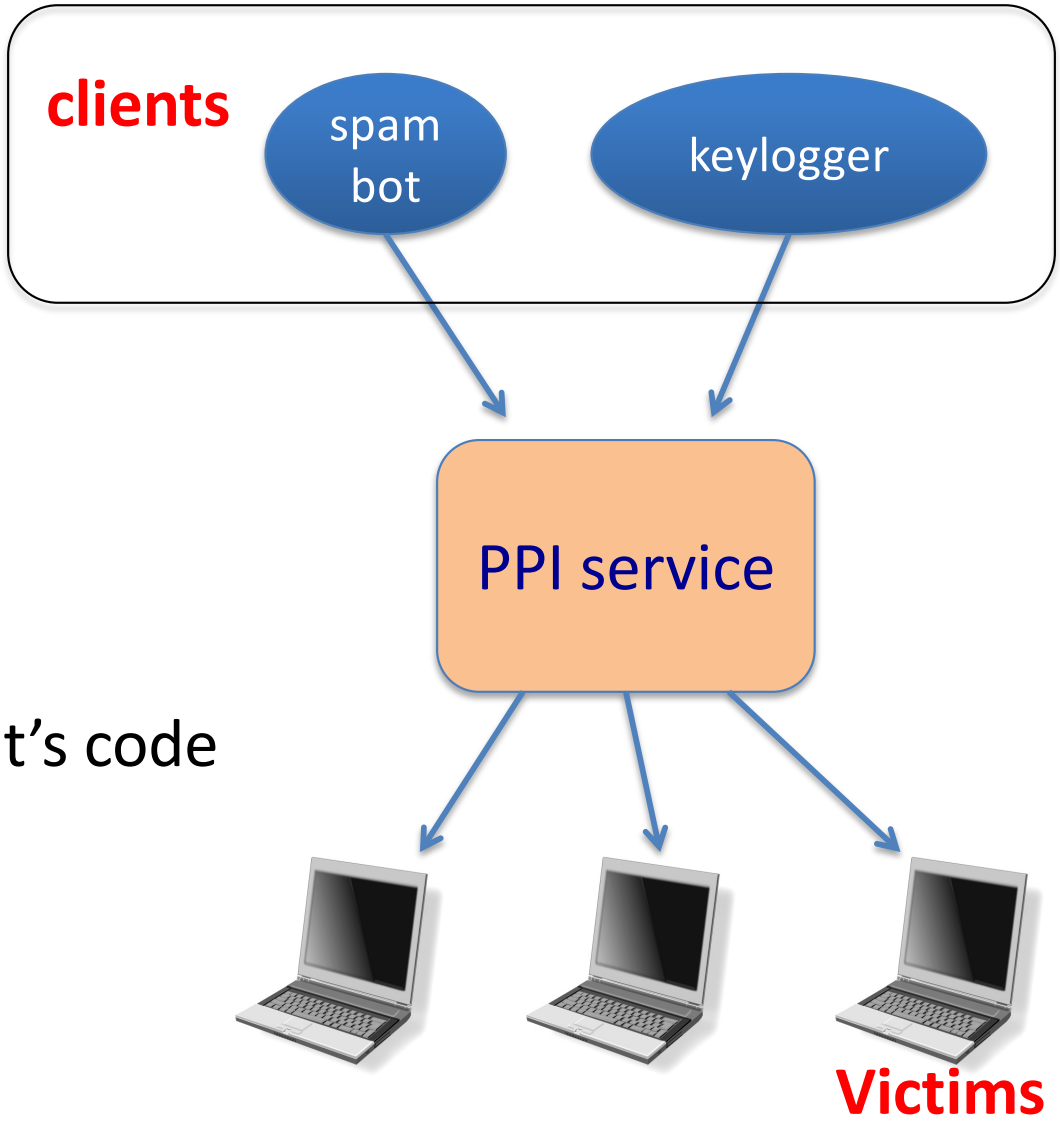
Brace yourselves. The rest of the media is going to be calling this an "IoT DDOS" and the hype will spin out of control. Hype aside, the facts on the ground make it look like an extremely large distributed denial-of-service attack (DDOS) was just carried out using mostly household appliances (145,607 of them!) rather than grandma's old Win XP system running on Pentiums.

# Advanced Persistent Threats (APT)

- Low-frequency & high-impact
- Targeted attacks, strategy
- Sophisticated and coordinated
- Stealthy attack (under the radars)
- Financial or industrial gain is not necessarily immediate
- Attack vectors
  - Remote (traditional vectors)
  - Local (USB keys, shared disks, MITM attacks …)
  - Human (spear phishing, forums, social networks …)

# Hackers deploy their own infrastructures

# Marketplace for owned machines



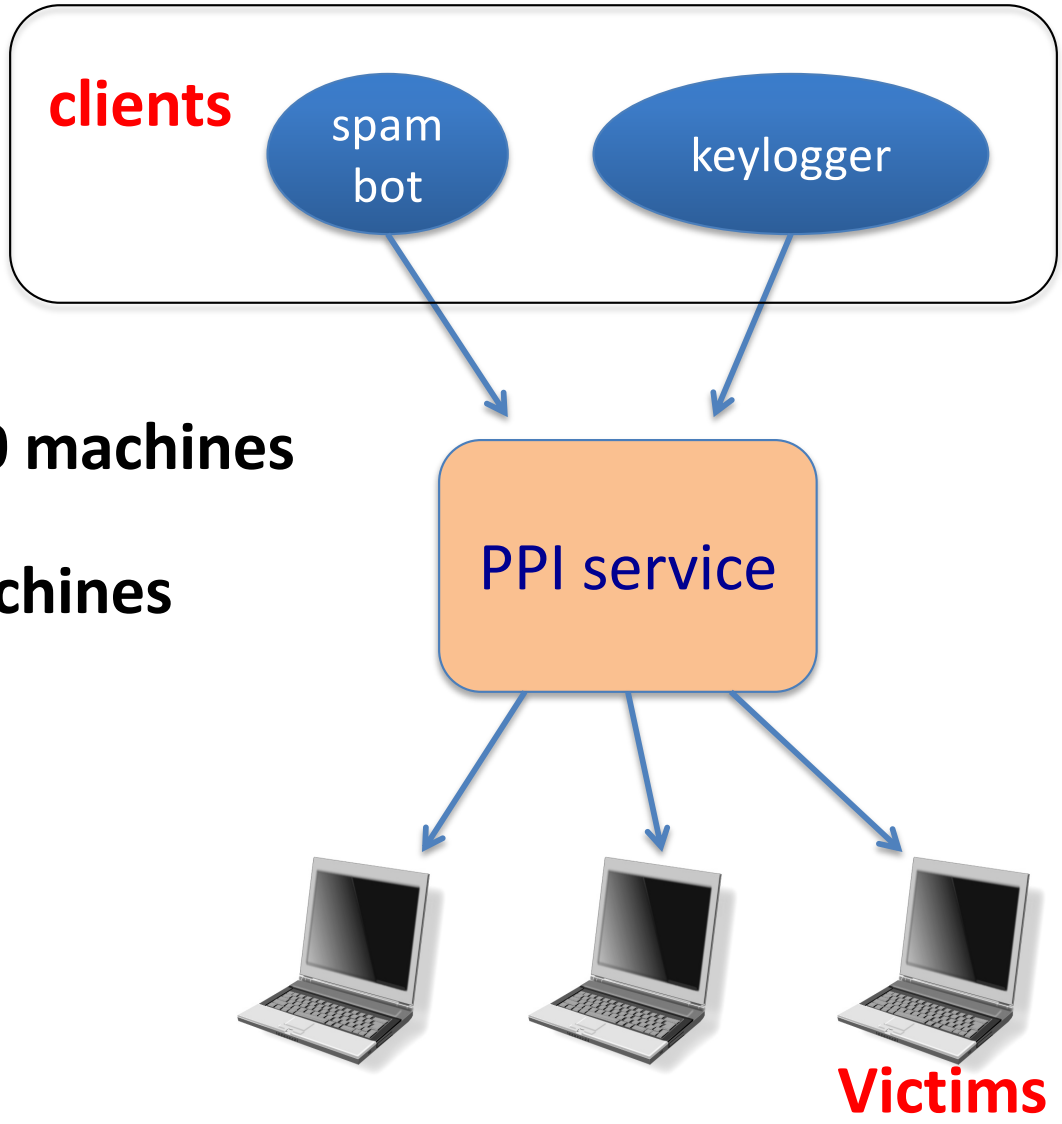

Pay-per-install (PPI) services

**PPI operation:**

1. Own victim's machine
2. Download and install client's code
3. Charge client

Source: Cabalerro et al. (www.icir.org/vern/papers/ppi-usesec11.pdf)

# Marketplace for owned machines




Cost: **US - 100-180$ / 1000 machines**

**Asia - 7-8$ / 1000 machines**

Source: Cabalerro et al. (www.icir.org/vern/papers/ppi-usesec11.pdf)

# Marketplace for Vulnerabilities

**Option 1**: bug bounty programs (many)

- Google Vulnerability Reward Program: up to $20K
- Microsoft Bounty Program: up to $100K
- Mozilla Bug Bounty program: $7500
- Pwn2Own competition: $15K

**Option 2**:

- Zero day initiative (ZDI), iDefense: $2K – $25K

# Example: Mozilla

| Novel vulnerability and exploit, new form of exploitation or an exceptional vulnerability | High quality bug report with clearly exploitable critical vulnerability[1] | High quality bug report of a critical or high vulnerability[2] | Minimum for a high or critical vulnerability[3] | Medium vulnerability |
|---|---|---|---|---|
| $10,000+ | $7,500 | $5,000 | $3,000 | $500 - $2500 |

# A few references

- Books:
  - Gildas Avoine, Pascal Junod, Philippe Oechslin, Sylvain Pasini. Sécurité informatique, Cours et exercices corrigés. Vuibert.
  - Ross Anderson. Security Engineering. Wiley. (http://www.cl.cam.ac.uk/~rja14/book.html)
- Conferences:
  - Academic: Security&Privacy (Oakland), CCS, Usenix Security, NDSS, ESORICS, RAID, ACSAC, DSN
  - Non-academic:  DefCon, BlackHat, SSTIC, GreHack