CC536
Cyber Security

Spring 2024

Assoc. Prof. Hisham Dahshan
hdahshan@adj.aast.edu

Week8: Malware

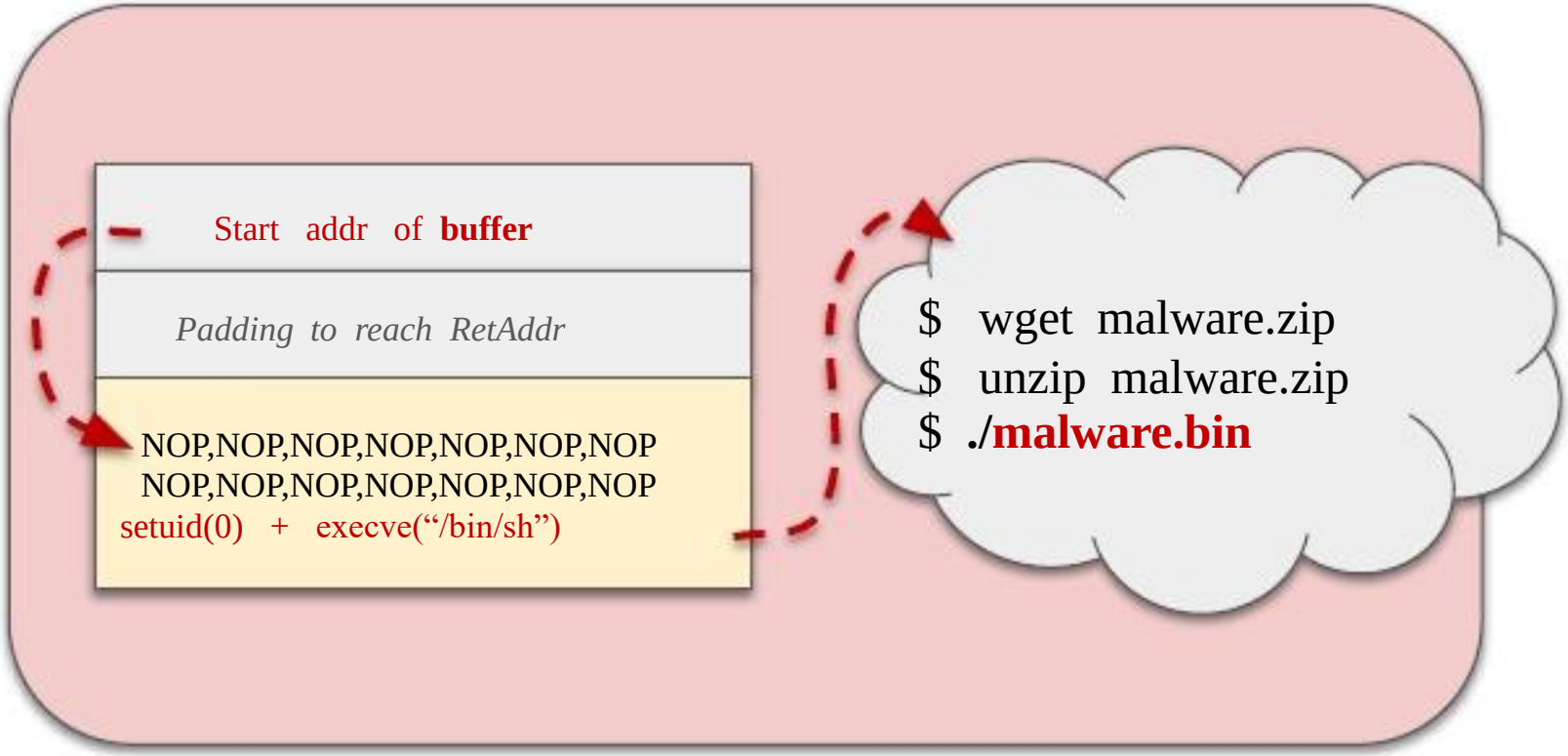
Malware: Malicious Software

- **Definition:** software (more generally, a set of instructions) that runs on a computer it **doesn't have access to** and/or does **something BAD**

- **Goals of Malware:**
  - Steal private data
  - Display ads, send spam
  - Damage local machine
  - Congest a network
  - Attack other systems on the network
  - Commit online fraud
  - Gain, then grant, unauthorized access
  - …

Malware Infection

- **How** does malicious software get on victim computers in the first place?
  - **A local application is exploited to perform arbitrary code execution**



Case Study: the First Malware

- **1988:** The **Morris Worm**
  - First-known computer malware
- Exploited several vulnerabilities
  - UNIX's finger network service
  - UNIX sendmail
  - Weak/default network passwords
- Result: **devastated the internet**
  - Millions of dollars of damages
  - Caused a psychological shift in IT

In Unix, finger is a program you can use to find information about computer users. It usually lists the login name, the full name, and possibly other details about the user you are fingering.

Case Study: The Exploit Grey Market

Case Study: The Exploit Grey Market

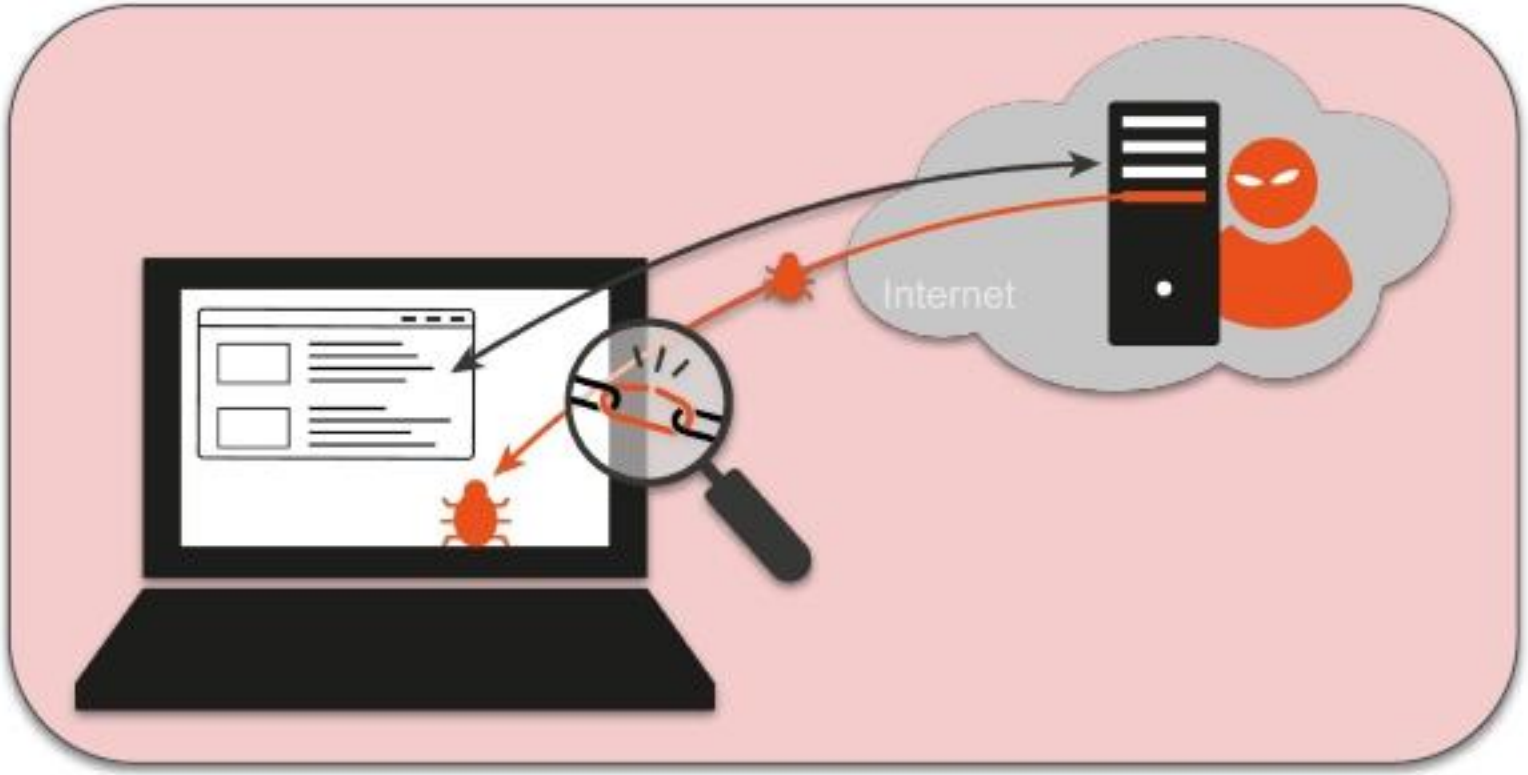
- **Weaponizing and selling exploits**
  - A huge underground economy
    - Nation-state actors
    - Cyber-criminal gangs
- **Don’t participate in this**
  - Likely to end up in bad hands regardless of who brokered it
  - E.g., authoritarian regimes
  - Likely to get people hurt **(or worse)**

Hacks Raise Fear Over N.S.A.’s Hold on Cyberweapons

Pegasus: UAE placed spyware on Khashoggi’s wife's phone months before murder

Malware Infection

- **How else** does malicious software get on victim computers?
  - **Vulnerable client connects to a malicious server/host; drive-by-download**



Case Study: Malvertising

- **Idea:** booby-trap malware in seemingly-benign ads
- **Common target:** browser **content rendering** engines
  - Adobe Flash
  - JavaScript
  - ActiveX
  - Java applets
- Somewhat rare nowadays

Malvertising definition

Malvertising, or malicious advertising, is the term for criminally controlled advertisements within Internet connected programs, usually web browsers (there are exceptions), which intentionally harm people and businesses with all manner of malware, potentially unwanted programs (PUPs), and assorted scams. In other words, malvertising uses what looks like legitimate online advertising to distribute malware and other threats with little to no user interaction required.

Malvertising can appear on any advertisement on any site, even the ones you visit as part of your everyday Internet browsing. Typically, malvertising installs a tiny piece of code, which sends your computer to criminal command and control (C&C) servers. The server scans your computer for its location and what software is installed on it, and then chooses which malware it determines is most effective to send you.

Always keep your software,
plugins, OS, etc. **UP TO DATE!**
Install those updates **ASAP!**

Malware Infection

- **How else** does malicious software get on victim computers?
  - **Social engineering attacks**

What is a social engineering attack?

Social engineering attacks that manipulate people into:

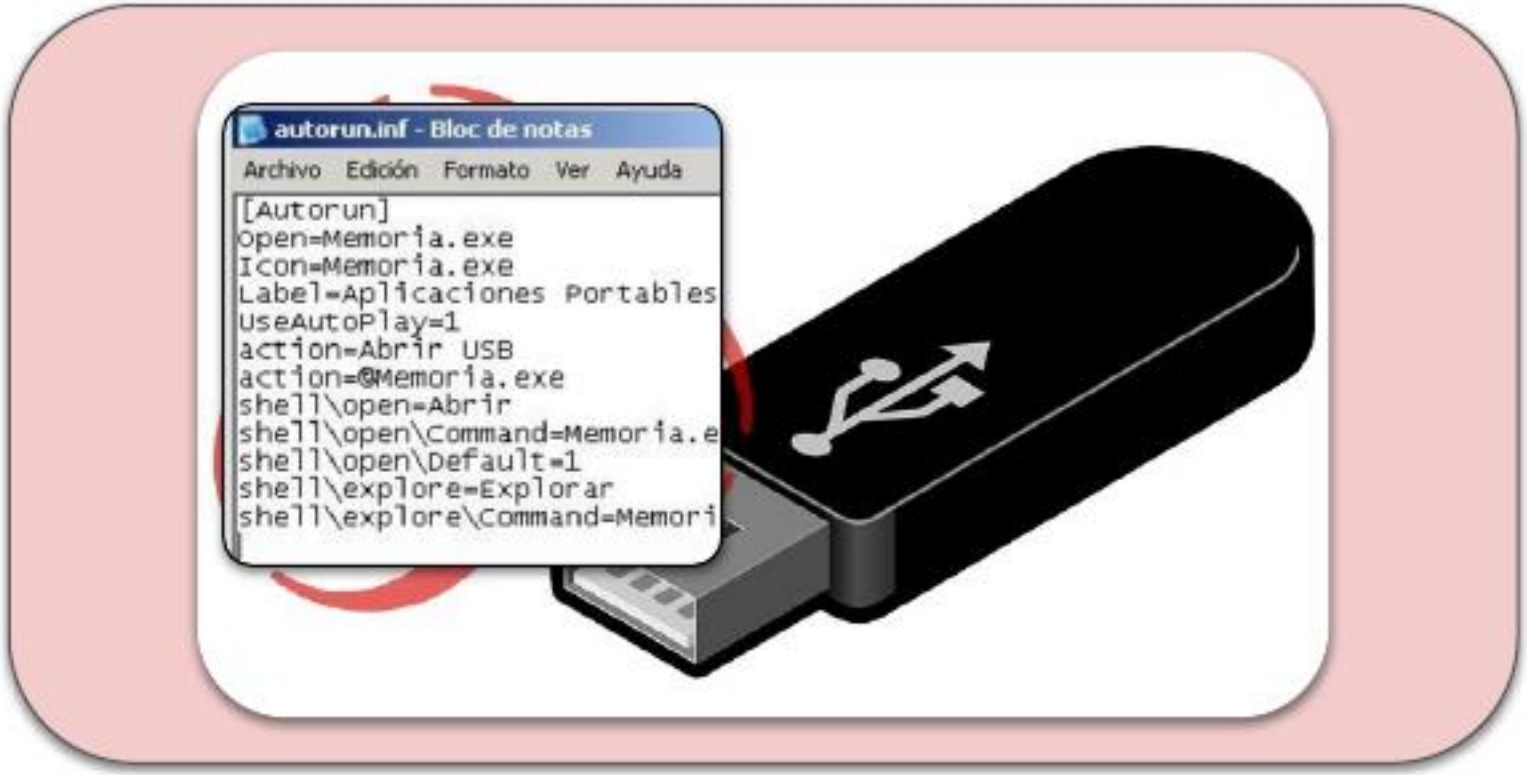
- Sharing information that they shouldn't share,
- Downloading software that they shouldn't download,
- Visiting websites they shouldn't visit,
- Sending money to criminals
- or making other mistakes that compromise their personal or organizational security.

Case Study: Scareware

- **Idea:** trick victim into downloading "anti-virus" software… that itself is really **just a piece of malware**
- Was really common in mid-2000s
- **Common target:** children, elderly, inexperienced computer users, etc.
- Nowadays: **ransomware**

Malware Infection

- **How else** does malicious software get on victim computers?
  - **Malicious hardware plugged-in; automatically executes code**



Case Study: People are Naive

Users Really Do Plug in USB Drives They Find

Matthew Tischer† Zakir Durumeric†‡ Sam Foster† Sunny Duan†

gle, Inc.

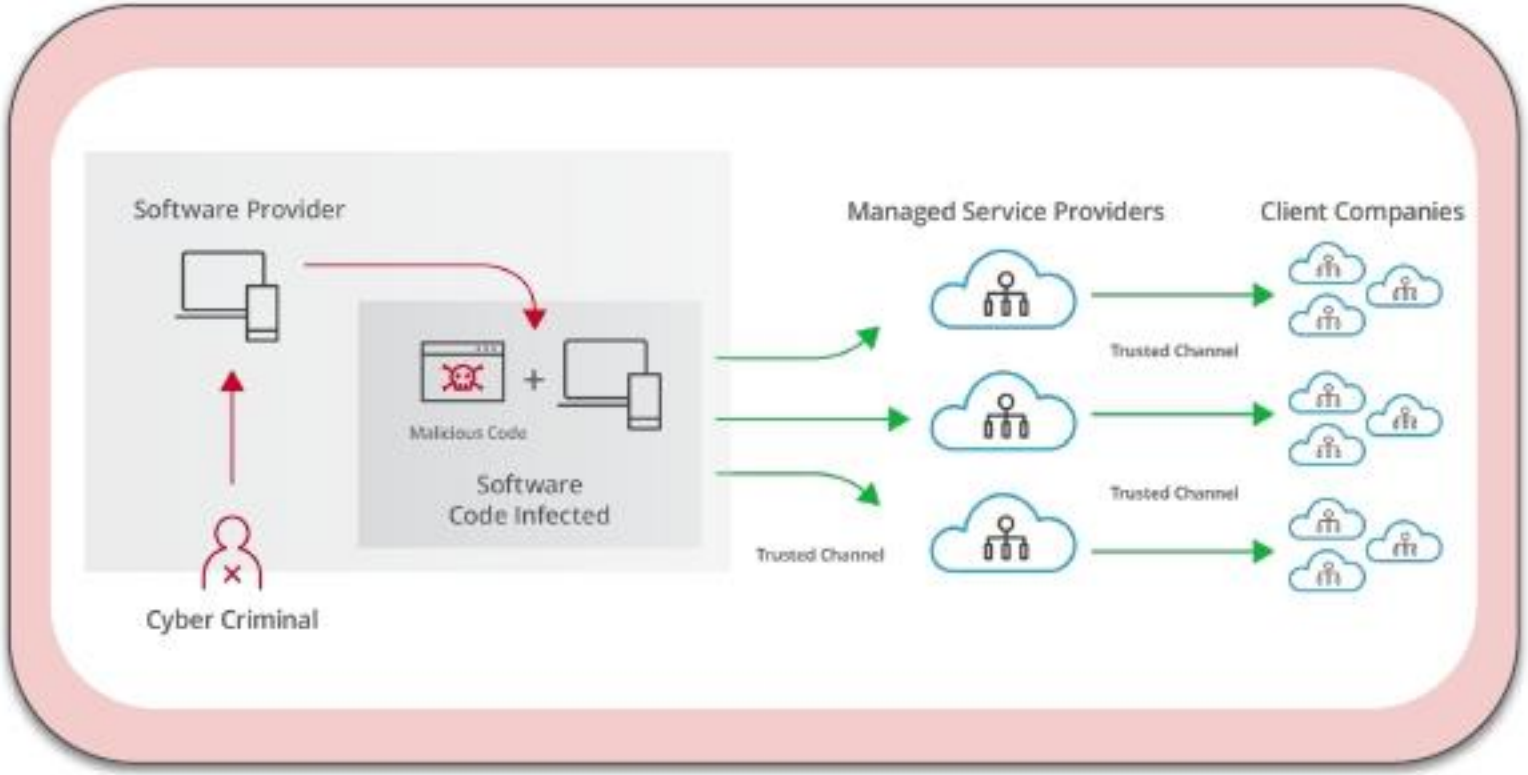
Success rate of people to plugging-in random USB thumb drives: **45–98%**

Abstract—W
will pick up and
a controlled ex
a large universi
with an estimat
the first drive
the types of dr
understand their
a drive's appearance
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

9 hours and the first connection
m when the drive was dropped.
appearance of a drive does not
neone will connect it to their
ect all types of drives unless
g the owner—suggesting that
notivated. 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.

Malware Infection

- **How else** does malicious software get on victim computers?
  - **Supply chain attacks; insider threats**



Case Study: SolarWinds Breach

- **Idea:** infect software provider that serves major targets

solarwinds

SolarWinds provides software for businesses to help manage their networks, systems, and IT infrastructure.
The product is used by more than 300,000 organizations globally including all five branches of the U.S. military, the Pentagon, State Department, Justice Department, NASA, the Executive Office of the President and the National Security Agency.

Partial customer listing:

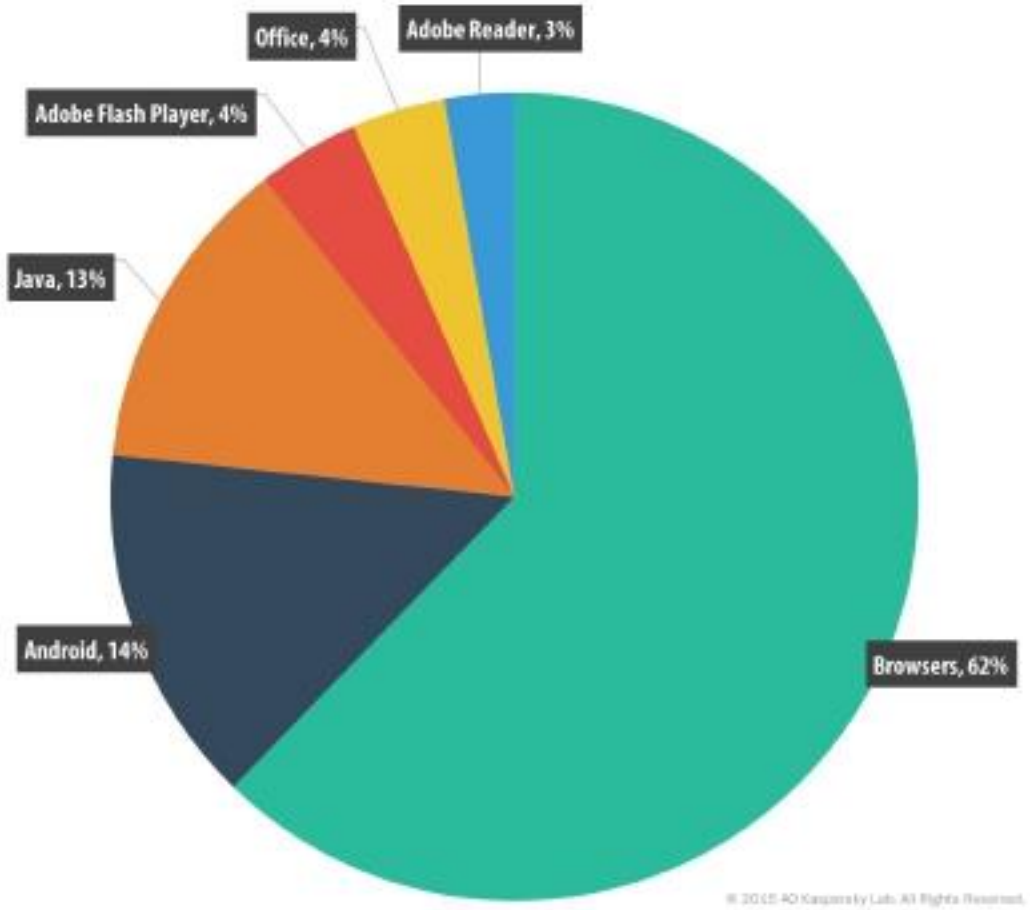
Acxiom	General Dynamics	Sabre
Ameritrade	Gillette Deutschland GmbH	Saks
AT&T	GTE	San Francisco Intl. Airport
Bellsouth Telecommunications	H&R Block	Siemens
Best Western Intl.	Harvard University	Smart City Networks
Blue Cross Blue Shield	Hertz Corporation	Smith Barney
Booz Allen Hamilton	ING Direct	Smithsonian Institute
Boston Consulting	IntelSat	Sparkasse Hagen
Cable & Wireless	J.D. Byrider	Sprint
Cablecom Media AG	Johns Hopkins University	St. John's University
Cablevision	Kennedy Space Center	Staples
CBS	Kodak	Subaru
Charter Communications	Korea Telecom	Supervalu
Cisco	Leggett and Platt	Swisscom AG
CitiFinancial	Level 3 Communications	Symantec
City of Nashville	Liz Claiborne	Telecom Italia
City of Tampa	Lockheed Martin	Telenor
Clemson University	Lucent	Texaco
Comcast Cable	MasterCard	The CDC
Credit Suisse	McDonald's Restaurants	The Economist
Dow Chemical	Microsoft	Time Warner Cable
EMC Corporation	National Park Service	U.S. Air Force
Ericsson	NCR	University of Alaska
Ernst and Young	NEC	University of Kansas
Faurecia	Nestle	University of Oklahoma
Federal Express	New York Power Authority	US Dept. Of Defense
Federal Reserve Bank	New York Times	US Postal Service
Fibercloud	Nielsen Media Research	US Secret Service
Fiserv	Nortel	Visa USA
Ford Motor Company	Perot Systems Japan	Volvo
Foundstone	Phillips Petroleum	Williams Communications
Gartner	Pricewaterhouse Coopers	Yahoo
Gates Foundation	Procter & Gamble	

Case Study: SolarWinds Breach

- **Idea:** infect software provider that serves major targets
- Inject malware within their development process
- When deployed, attacker gets access **to all supplied targets**

Our Vulnerable World

- Kaspersky Lab's 2015 report
- Modern exploits are multi-stage
- Attackers "mastered" non-Windows OSs
  - Linux, MacOS, iOS aren't as safe as you think!

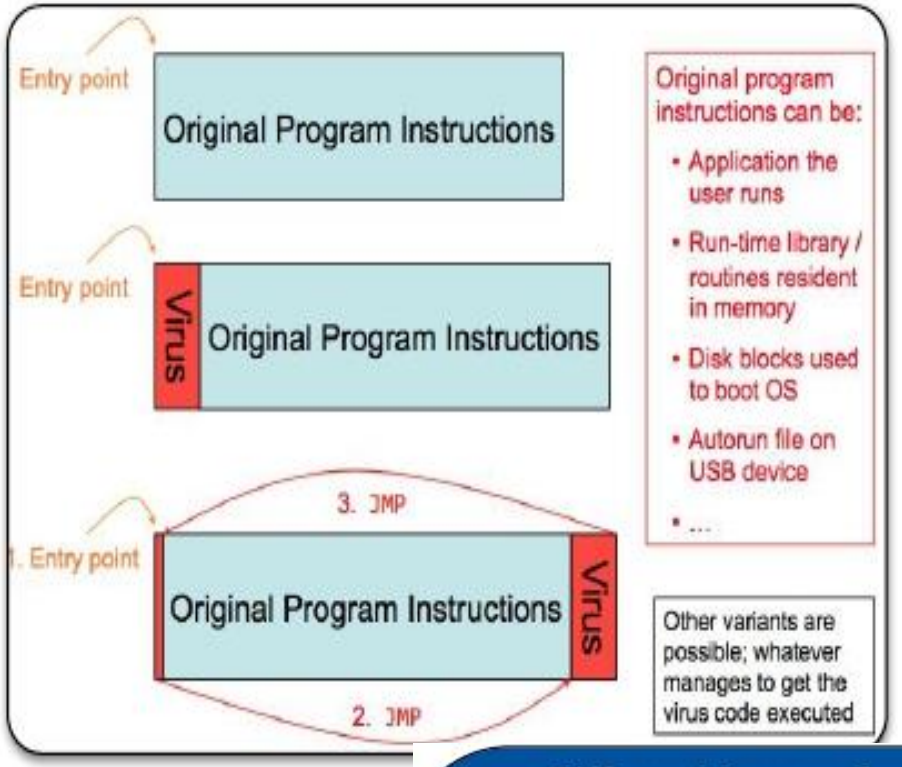


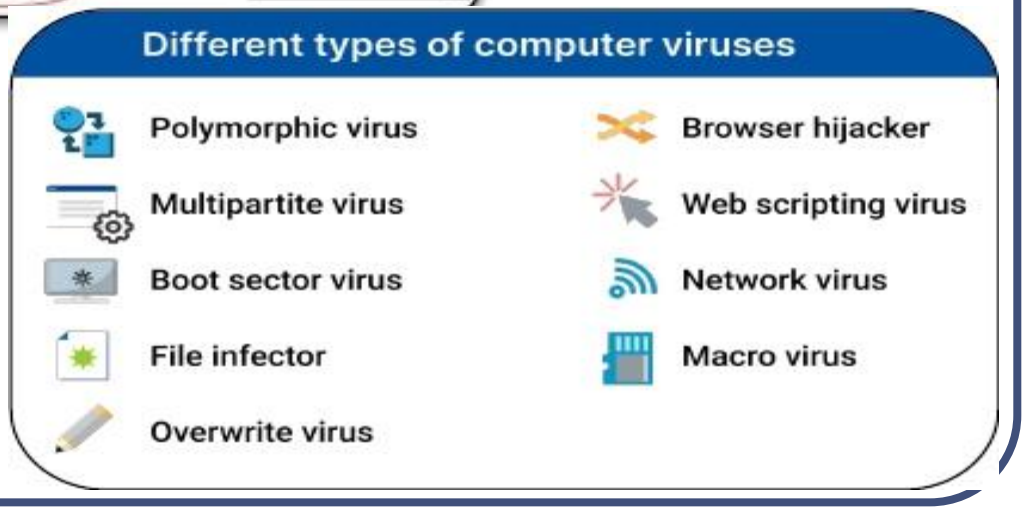
Critical vulnerabilities exist in **every software and system** we use daily

Today’s Malware “Zoo”

Viruses

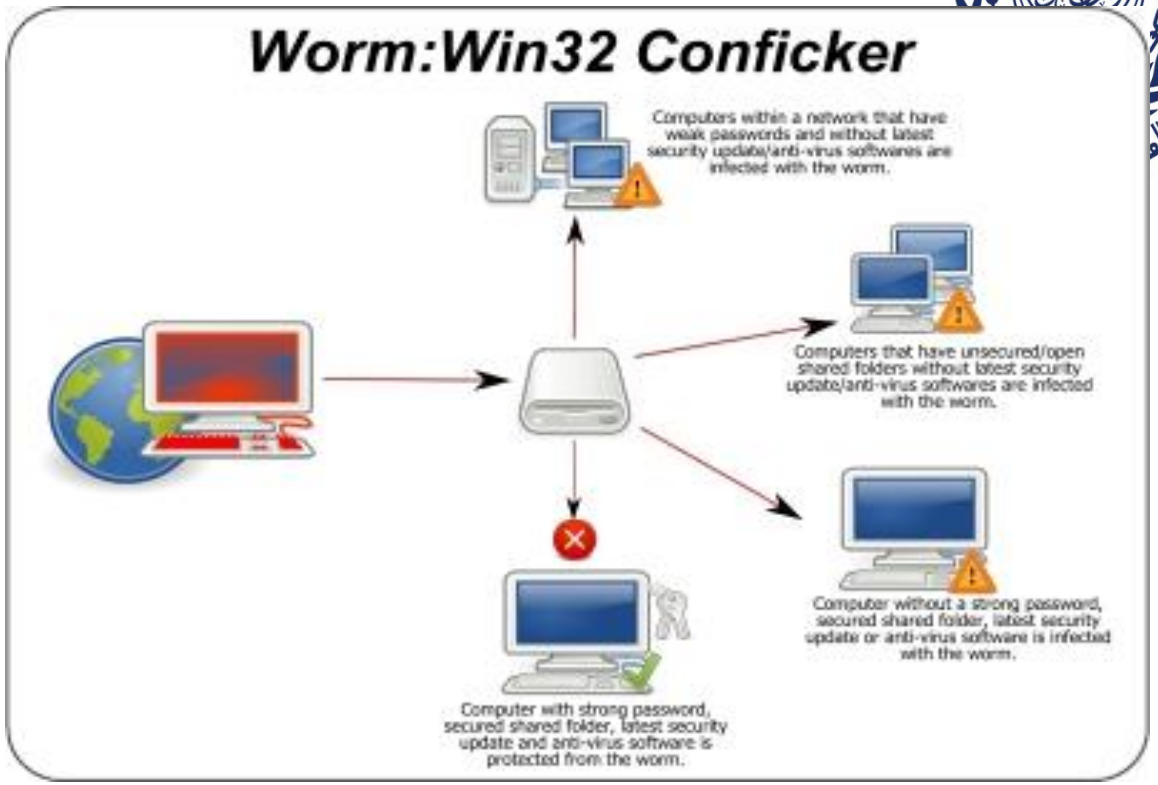
- Analogous to viruses in biology
- **Self-replicating software** that infects other programs by modifying them to inject a version of itself
- Can **mutate to avoid detection** by changing parts of their code
  - E.g., “polymorphic”, “metamorphic” viruses



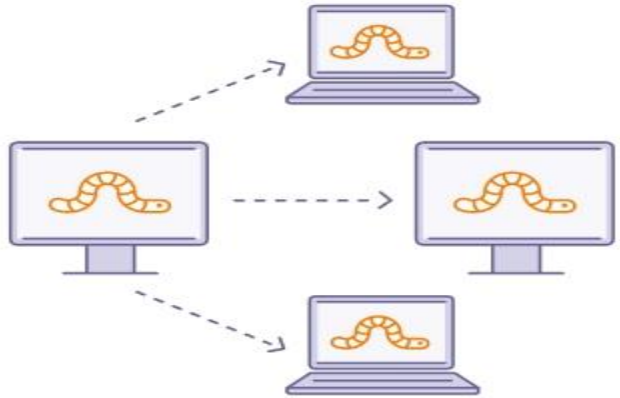


Polymorphic malware can morph itself to change its code using a variable encryption key, whereas metamorphic malware rewrites its code without an encryption key.

Worms



- Self-replicating software that infects **other systems** by automatically spreading over a connected network
- Fast-spreading worms are a big threat (fueled by **software homogeneity**)
- Famous worms (and exploited software):
  - **2003:** Slammer Worm (**Microsoft's SQL Server**)
  - **2008:** Conficker Worm (**Windows NetBIOS**)

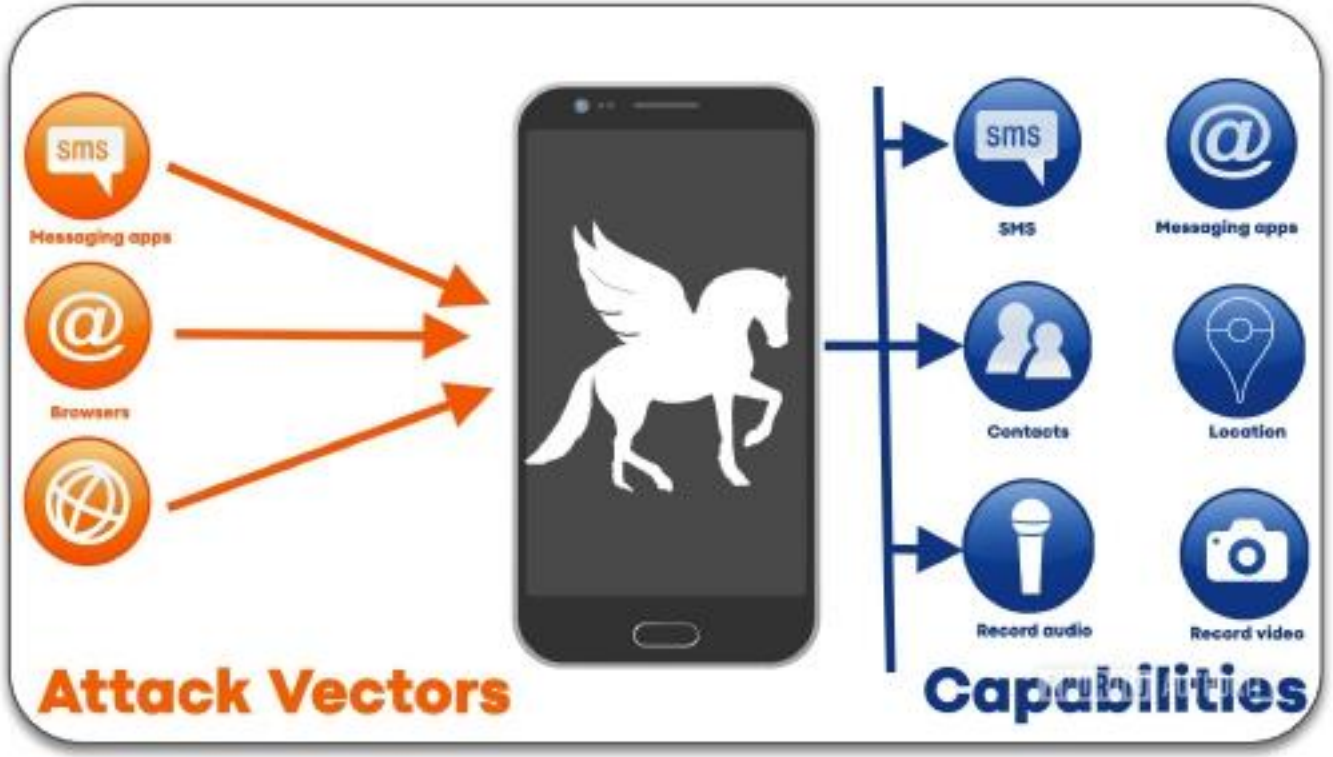


Adware

- Software that incessantly displays **advertisements**
  - Pop-up ads
  - Opening web pages
  - False search engine results
  - Redirecting URL clicks
- Often needs some form of **user interaction** to install

Spyware

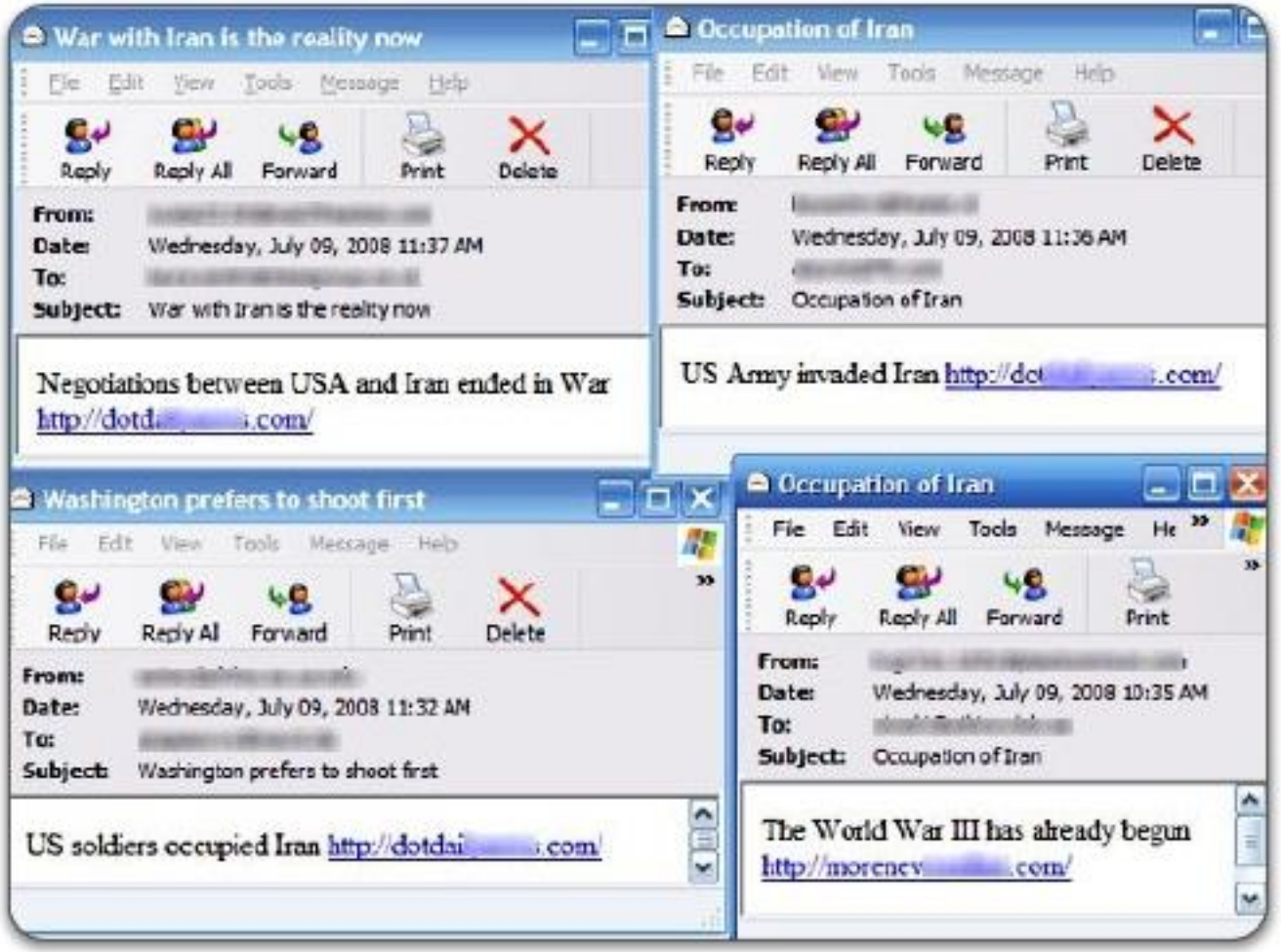
- Software that tracks **sensitive user information**
  - Keystrokes
  - Passwords
  - Web searches
  - GPS Location
  - Installed/accessed apps
- Collects, sends to a third party
  - Parental Control applications
  - Nation-state spyware (Pegasus)



Trojan Horses

- Software that **tricks user into installing** by masquerading as a benign, safe application

- **Common examples:**
  - Adware
  - Malicious attachments
    - E-Cards (Storm Worm)
    - Intriguing links
  - Fake anti-virus applications
  - Ransomware



Trojan Horses

- Software that **tricks user into installing** by masquerading as a benign, safe application

- **Common examples:**
  - Adware
  - Malicious attachments
    - E-Cards (Storm Worm)
    - Intriguing links
  - Fake anti-virus applications
  - Ransomware

Rootkits

- Software designed to **maintain attacker's control** over a system
  - I.e., **root-level access**
- Typically a payload of other malware (e.g., viruses, worms)
- Maintain **stealth**, **undetectability**
- **Stealth Measures:**
  - Intercept system calls responsible listing files, processes, etc.
  - Filter out the malware's files and processes to avoid being seen

Rootkits

- Software designed to **maintain attacker's control** over a system
  - I.e., **root-level access**
- **Stealth Measures:**
  - Intercept system calls responsible listing files, processes, etc.
  - Filter out the malware's files and processes to avoid being seen
- **Incredibly difficult to remove**
  - Can never guarantee system is clean

Sony BMG copy protection rootkit scandal

3 languages

Article Talk | Read Edit View history

From Wikipedia, the free encyclopedia

A scandal erupted in 2005 regarding Sony BMG's implementation of copy protection measures on about 22 million CDs. When inserted into a computer, the CDs installed one of two pieces of software that provided a form of digital rights management (DRM) by modifying the operating system to interfere with CD copying. Neither program could easily be uninstalled, and they created vulnerabilities that were exploited by unrelated malware. One of the programs would install and "phone home" with reports on the user's private listening habits, even if the user refused its end-user license agreement (EULA), while the other was not mentioned in the EULA at all. Both programs contained code from several pieces of copylefted free software in an apparent infringement of copyright, and configured the operating system to hide the software's existence, leading to both programs being classified as rootkits.

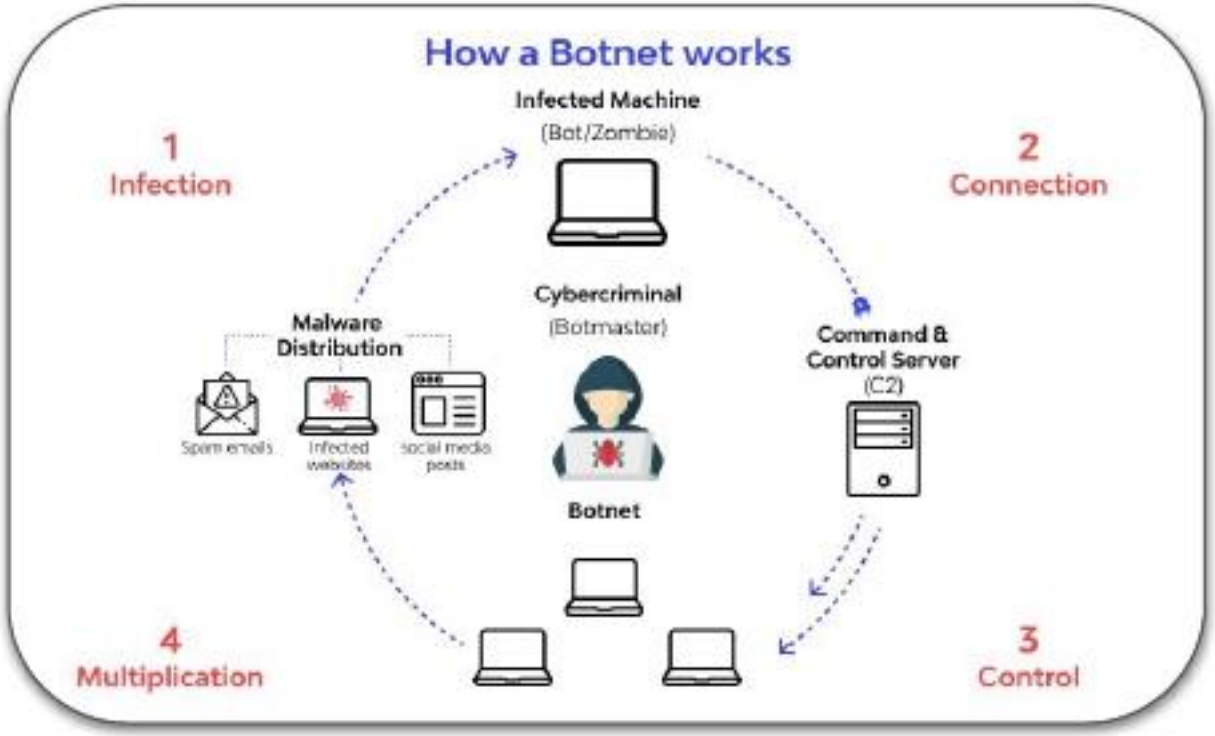
Screenshot of the Sony CD audio player, playing Switchfoot's fifth studio album *Nothing Is Sound*.

Sony BMG initially denied that the rootkits were harmful. It then released an uninstaller for one of the programs that merely made the program's files visible while also installing additional software that could not be easily removed, collected an email address from the user and introduced further security vulnerabilities.

Following public outcry, government investigations and class-action lawsuits in 2005 and 2006, Sony BMG partially addressed the scandal with consumer settlements, a recall of about 10% of the affected CDs and the suspension of CD copy-protection efforts in early 2007.

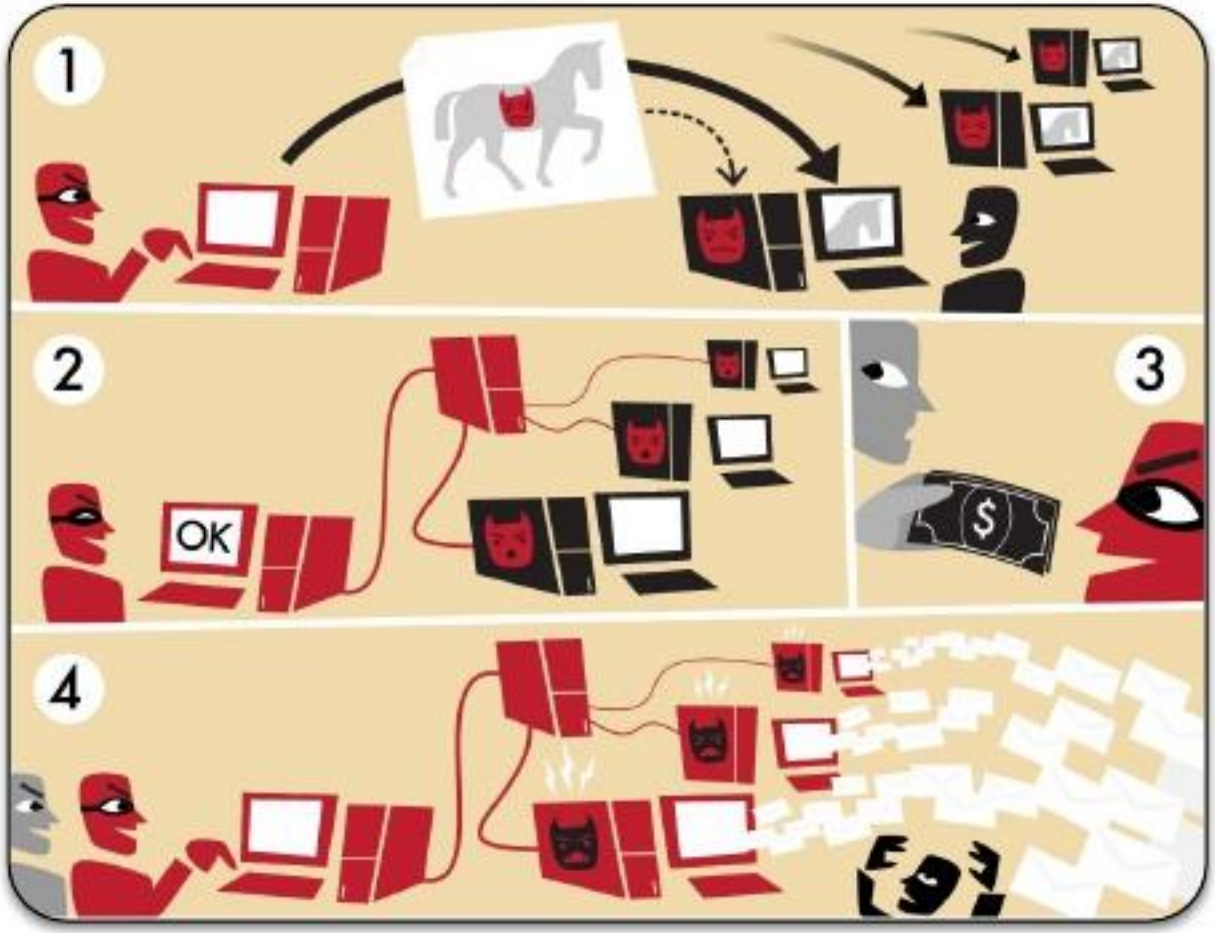
Bots and Botnets

- **Bot:** a victim system remotely under attacker control (e.g., rootkit)
- **Botnet:** a collection of bots
  - Often used for distributed cyber attacks
- **Command and Control Measures:**
  - **Centralized:** **single server** directs bots
    - Simple; easy to detect/disable
  - **Distributed:** bots direct **one another**
    - Complex; hard to detect/disable



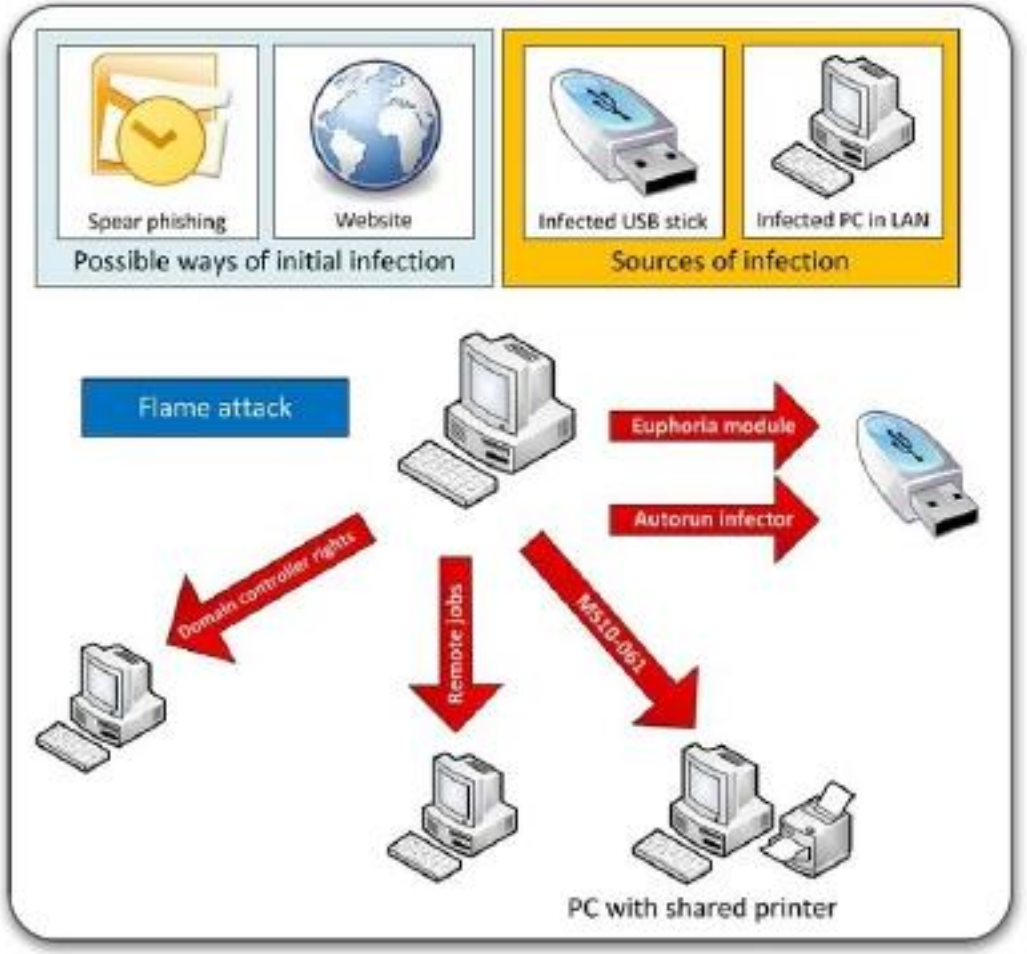
Famous Botnets

- **Mirai Botnet**
  - Propagated by exploiting default passwords in internet-connected household IoT devices
  - Used to DDOS targeted websites
- **Storm Botnet**
  - Propagated by email attachments
  - When infected, each bot spins up an email server and begins mass email spam campaign to propagate itself



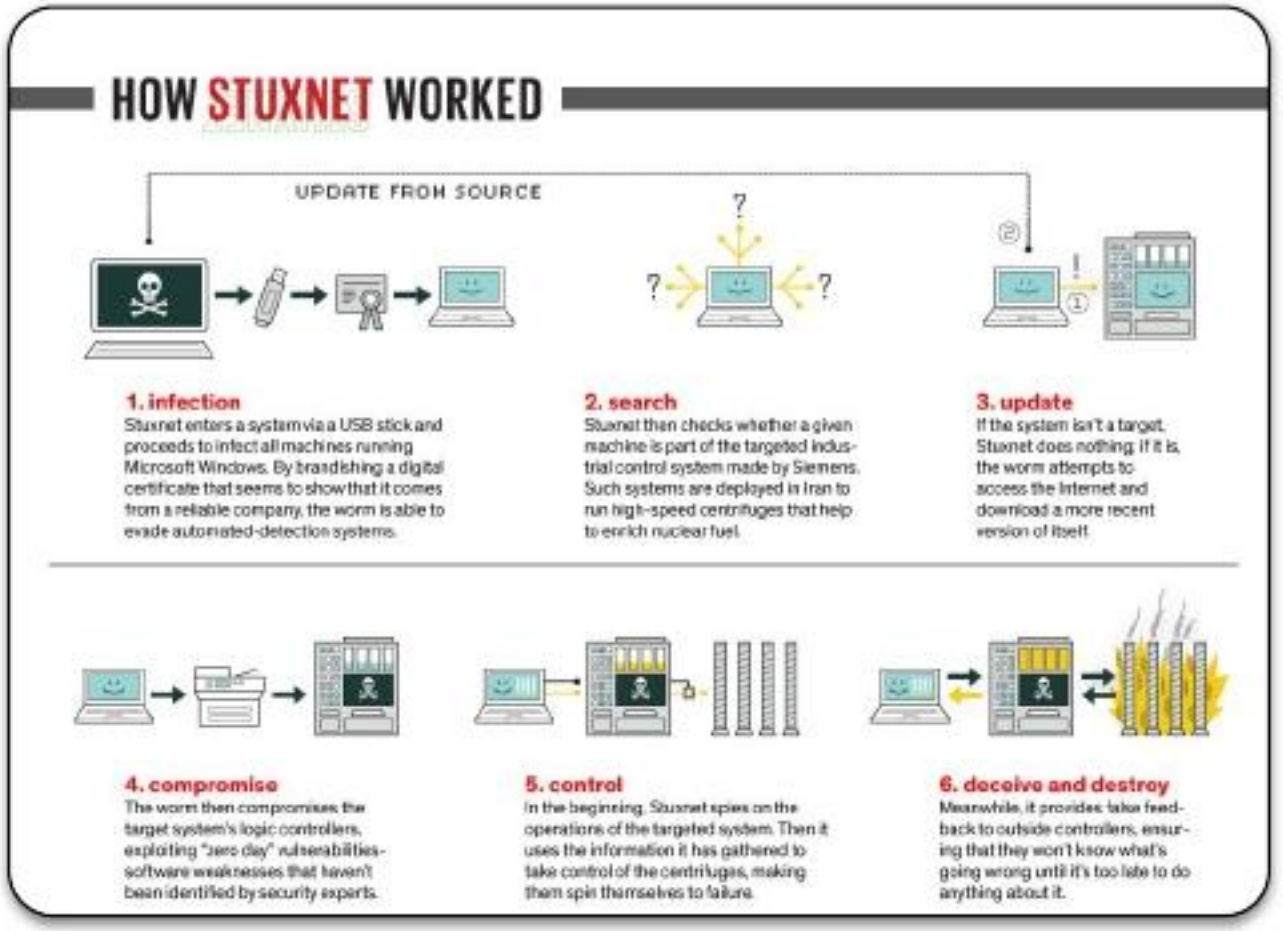
Advanced Persistent Threats (APTs)

- **Combined Threats**
  - Typically a rootkit, spyware, combined with other capabilities
- Extremely sophisticated, stealthy, and target-specific
  - **Insanely complex exploit chains**
- Believed to be developed by **nation-state cyber threat** actors
  - E.g., the NSA, CIA, Mossad, GRU



The Stuxnet APT

- Believed to be developed by USA (NSA) and Israel (Mossad)
- Sophisticated malware designed to infect, destroy ICS computers
  - **Primary target:** uranium enrichment at Iran's Natanz nuclear plant
  - **Payload 1:** make uranium centrifuge spin up so fast that it self-destructs
  - **Payload 2:** feed operators fake data that appears everything is fine
- https://darknetdiaries.com/episode/29/



Summary: Major Malware Types

- **Virus**
  - Self-replicating software that infects other programs, mutates itself to avoid detection
- **Worm**
  - Self-replicating software that spreads over networks to infect programs on other systems
- **Trojans**
  - Appears to perform desirable function, but does something malicious behind the scenes
- **Rootkit**
  - Malware that uses stealth to achieve persistent presence on a machine
- **Botnet**
  - A network of compromised, “Zombie” or “bot” computers that do a botmaster’s bidding

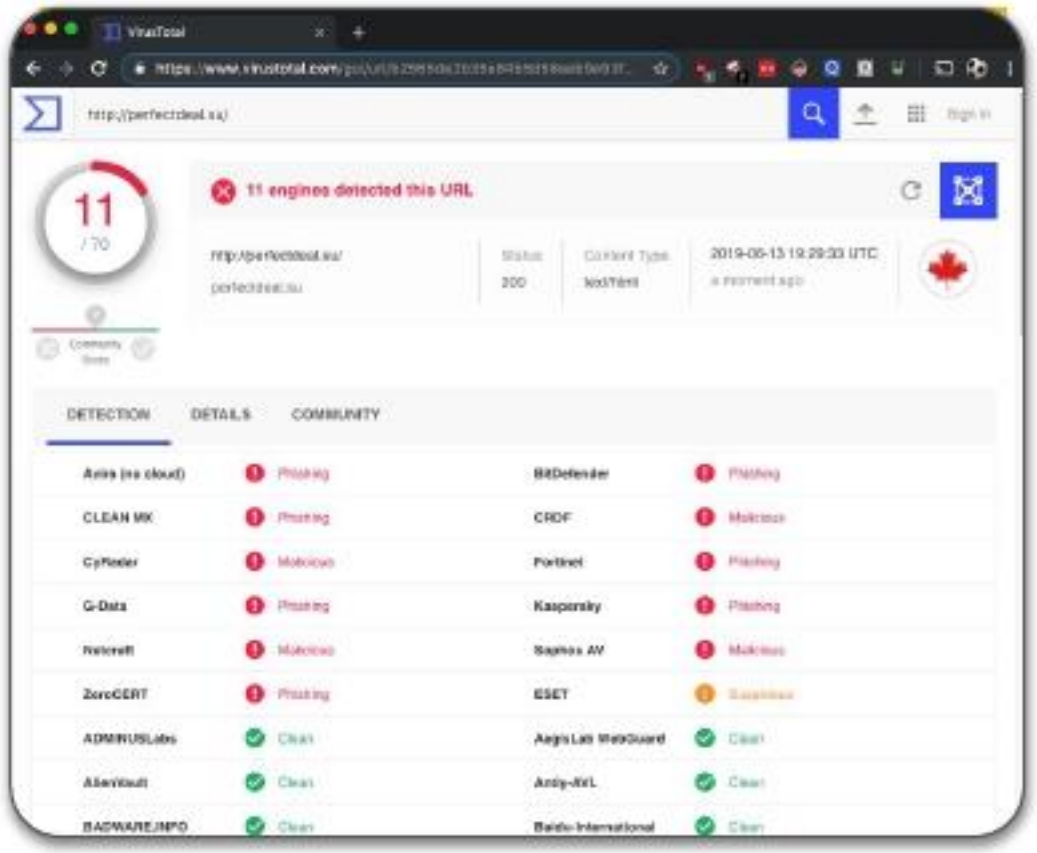
Detecting and Preventing Malware

Detection

- **Anti-virus software**
  - Software for detecting, eliminate malware
  - E.g., Malwarebytes, Avast, McAfee, Symantec
- **Signature-based** anti-virus:
  - Track identifying strings (like a fingerprint)
  - Difficult against mutating viruses
- **Heuristic-based** anti-virus:
  - Analyze program behavior, identify unusual patterns
  - E.g. network access, file deletion, modify boot sector

Detection

- **No anti-virus is perfect!**
  - A constant cat and mouse game
  - Heuristics, signatures need constant updating
- See for yourself: www.virustotal.com
- **Solution:** use **layered defense** approach
  - Use a firewall, anti-virus, sandboxing, etc.
  - **Note:** running multiple AVs may cause issues
    - They may detect and delete one another!



Other Defenses

- **Tripwired Hashes**
  - Keep hash of known system files
  - Periodically re-hash and check
    - **If hash changes, file tampered**

- Be a **security-conscious** citizen
  - Strong passwords, 2-factor authentication
  - Do not access suspicious files or websites
    - **Use your intuition: if it seems too good to be true, it probably is!**
  - Keep software updated and use anti-virus
  - **Teach others!**

Food for Thought

- **Using malware for good?**
  - E.g., would it be ethical to use a worm to patch a ubiquitous security vulnerability?
  - E.g., installing firewalls to censor websites we think are against the common good?

- **Implications of sophisticated malware on public, international policy?**
  - E.g., intercepting everyone's phone records to find a handful of terrorists?
  - E.g., not disclosing critical vulnerabilities so as to stockpile cyberweapons?

Questions?