Malware: Malicious Software

CSE 565 - Fall 2025
Computer Security

Hongxin Hu (hongxinh@buffalo.edu)

Updates

- **Project 2 SQL Injection Attack**
  - Deadline: Tuesday, Oct 7
- **Assignment 2**
  - Deadline: Thursday, Oct 9
- **Midterm Exam**
  - Deadline: Thursday, October 16

Viruses, Worms, Trojans, Rootkits

- Malware can be classified into several categories, depending on propagation and concealment
- Propagation
  - Virus: human-assisted propagation (e.g., open email attachment)
  - Worm: automatic propagation without human assistance
- Concealment
  - Rootkit: modifies operating system to hide its existence
  - Trojan: provides desirable functionality but hides malicious operation

Insider Attacks

- An **insider attack** is a security breach that is caused or facilitated by someone who is a part of the organization that controls or builds the asset that should be protected.
- In the case of malware, an insider attack refers to a security hole that is created in a software system by one of its programmers.

Backdoors

- A **backdoor,** which is also sometimes called a **trapdoor,** is a hidden feature or command in a program that allows a user to perform actions he or she would not normally be allowed to do.
- When used in a normal way, this program performs completely as expected and advertised.
- But if the hidden feature is activated, the program does something unexpected, often in violation of security policies, such as performing a privilege escalation.

Logic Bombs

- A **logic bomb** is a program that performs a malicious action as a result of a certain logic condition.
- A classic example combines a logic bomb with a backdoor, where a programmer puts in a logic bomb that will crash the program on a certain date.

The Omega Engineering Logic Bomb

- An example of a logic bomb that was actually triggered and caused damage is one that programmer Tim Lloyd was convicted of using on his former employer, Omega Engineering Corporation. On July 31, 1996, a logic bomb was triggered on the server for Omega Engineering's manufacturing operations, which ultimately cost the company millions of dollars in damages and led to it laying off many of its employees.

The Omega Bomb Code

- The Logic Behind the Omega Engineering Time Bomb included the following strings:
  - 7/31/96
    - Event that triggered the bomb
  - F:
    - Focused attention to volume F, which had critical files
  - F:\LOGIN\LOGIN 12345
    - Login a fake user, 12345 (the back door)
  - CD \PUBLIC
    - Moves to the public folder of programs
  - FIX.EXE /Y F:*.*
    - Run a program, called FIX, which actually deletes everything
  - PURGE F:\/ALL
    - Prevent recovery of the deleted files

Defenses against Insider Attacks

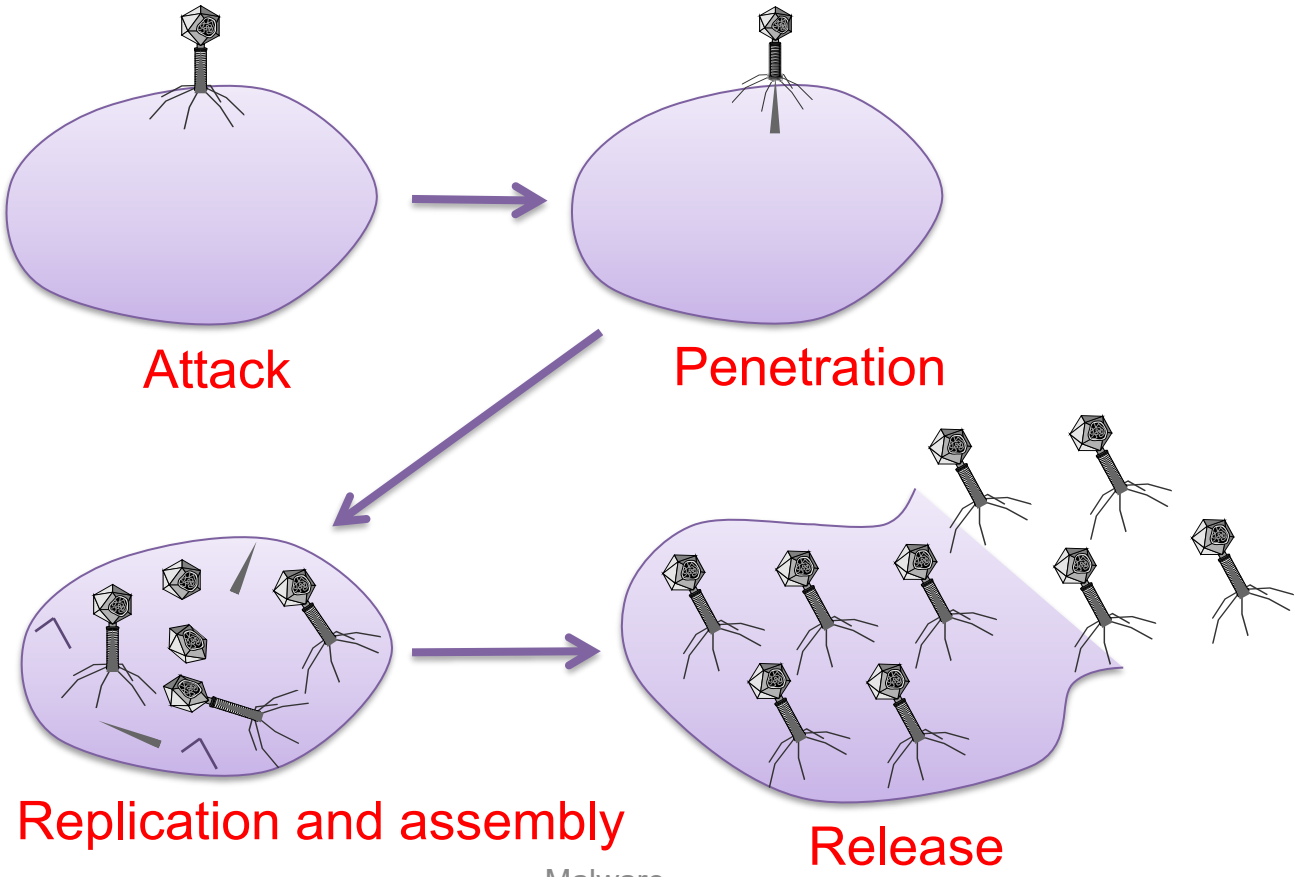
- Avoid single points of failure.
- Use code walk-throughs.
- Use archiving and reporting tools.
- Limit authority and permissions.
- Physically secure critical systems.
- Monitor employee behaviors.
- Control software installations.

Computer Viruses

- A **computer virus** is computer code that can replicate itself by modifying other files or programs to insert code that is capable of further replication.
- This self-replication property is what distinguishes computer viruses from other kinds of malware, such as logic bombs.
- Another distinguishing property of a virus is that replication requires some type of user assistance, such as clicking on an email attachment or sharing a USB drive.

Biological Analogy

- Computer viruses share some properties with Biological viruses

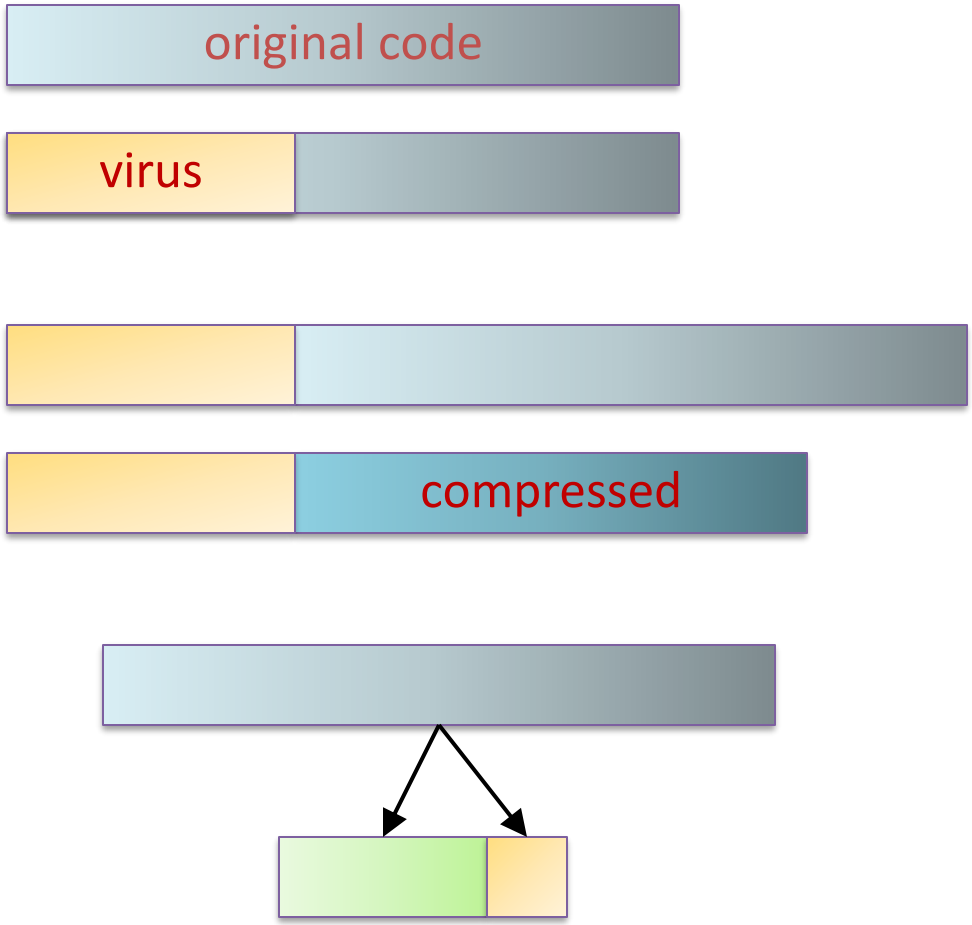


Virus Phases

- **Dormant phase.** During this phase, the virus just exists—the virus is laying low and avoiding detection.
- **Propagation phase.** During this phase, the virus is replicating itself, infecting new files on new systems.
- **Triggering phase.** In this phase, some logical condition causes the virus to move from a dormant or propagation phase to perform its intended action.
- **Action phase.** In this phase, the virus performs the malicious action that it was designed to perform, called **payload.**
  - This action could include something seemingly innocent, like displaying a silly picture on a computer's screen, or something quite malicious, such as deleting all essential files on the hard drive.

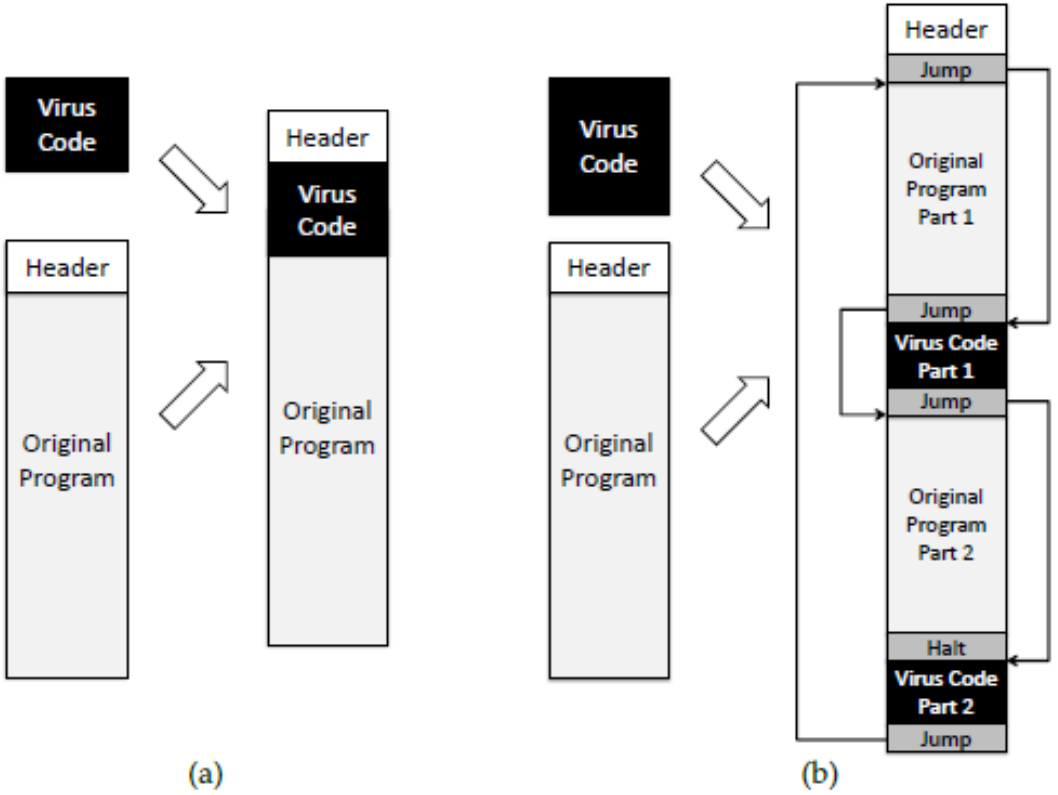
Infection Types

- Overwriting
  - Destroys original code
- Pre-pending
  - Keeps original code, possibly compressed
- Infection of libraries
  - Allows virus to be memory resident
  - E.g., kernel32.dll
- Macro viruses
  - Infects MS Office documents
  - Often installs in main document template



Degrees of Complication

- Viruses have various degrees of complication in how they can insert themselves in computer code.



Concealment

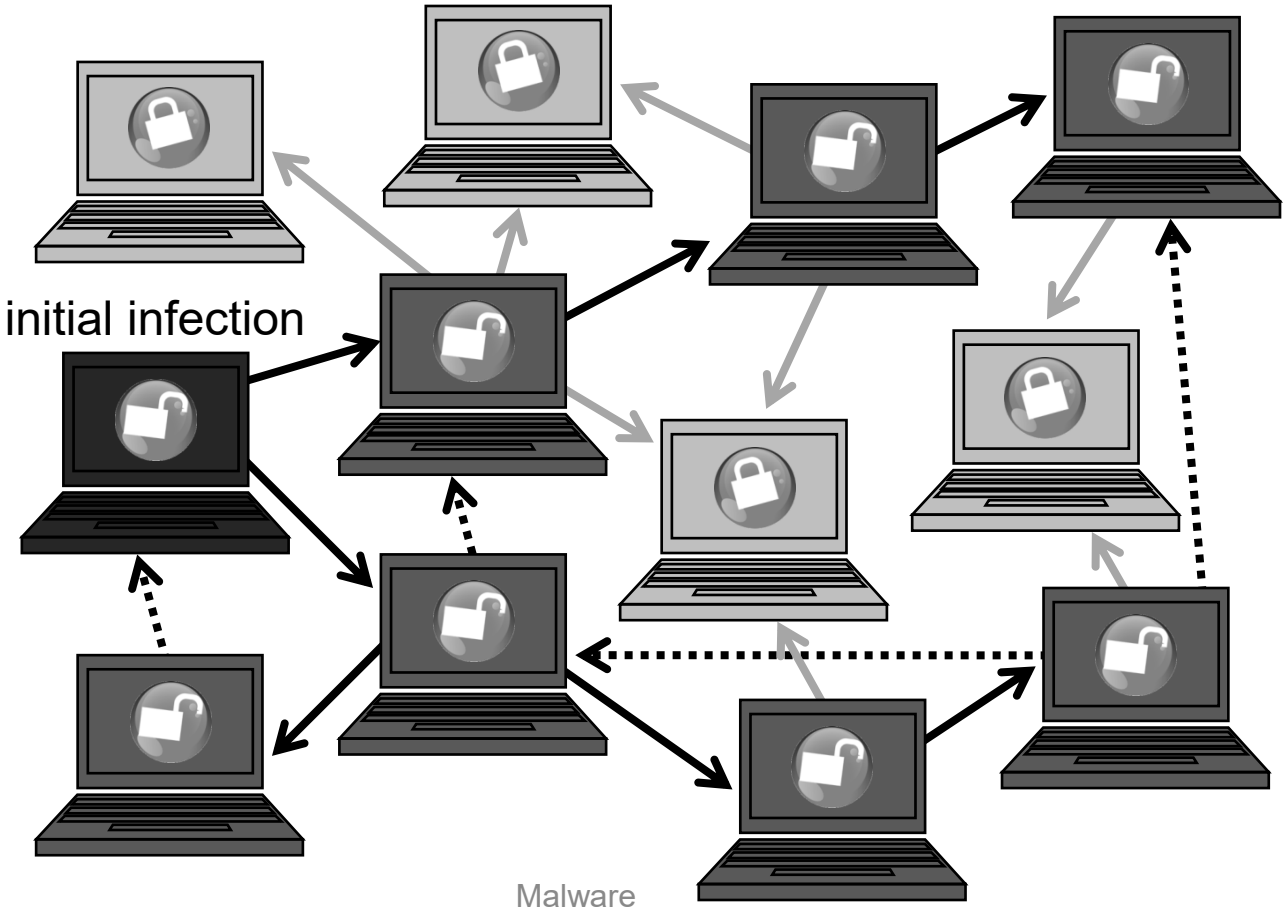
- Encrypted virus
  - Decryption engine + encrypted body
  - Randomly generate encryption key
  - Detection looks for decryption engine
- Polymorphic virus
  - Encrypted virus with random variations of the decryption engine (e.g., padding code)
  - Detection using CPU emulator
- Metamorphic virus
  - Different virus **bodies**
  - Approaches include code permutation and instruction replacement
  - Challenging to detect

Computer Worms

- A **computer worm** is a malware program that spreads copies of itself without the need to inject itself in other programs, and usually without human interaction.
- Thus, computer worms are technically not computer viruses (since they don't infect other programs), but some people nevertheless confuse the terms, since both spread by self-replication.
- In most cases, a computer worm will carry a malicious payload, such as deleting files or installing a backdoor.

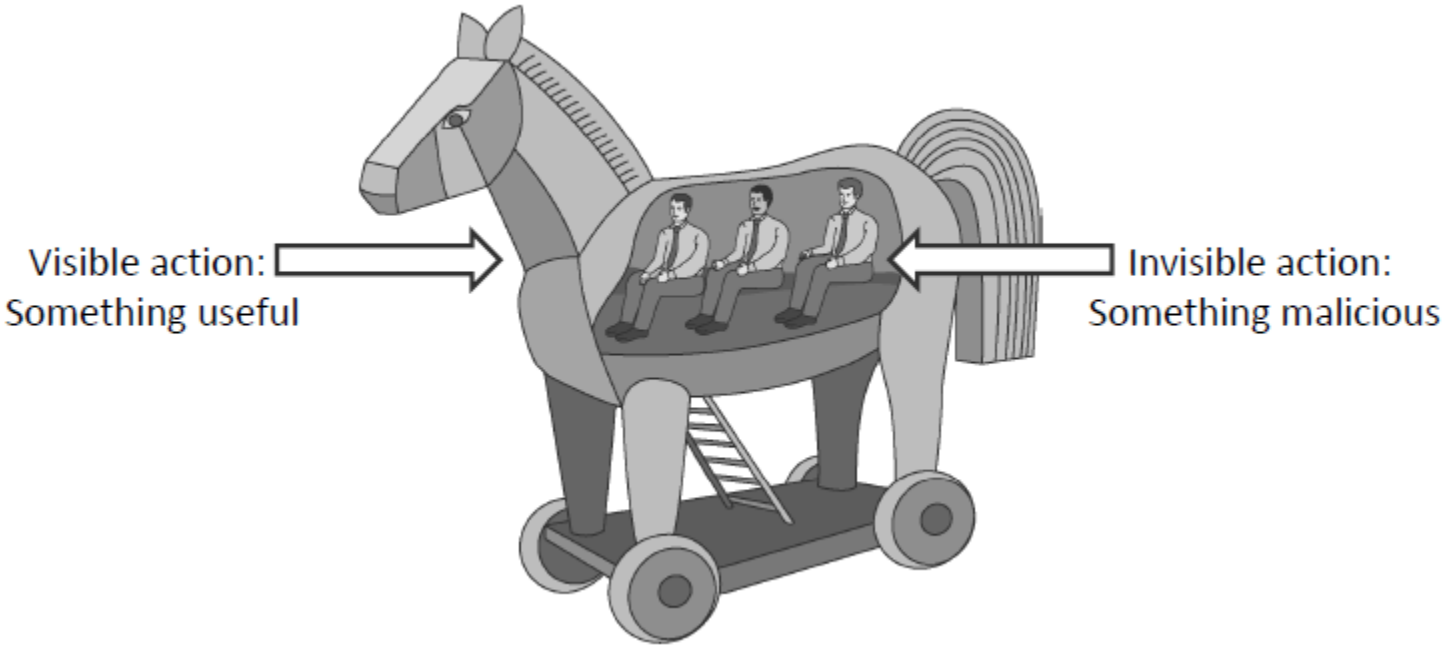
Worm Propagation

- Worms propagate by finding and infecting vulnerable hosts.
  - They need a way to tell if a host is vulnerable
  - They need a way to tell if a host is already infected.



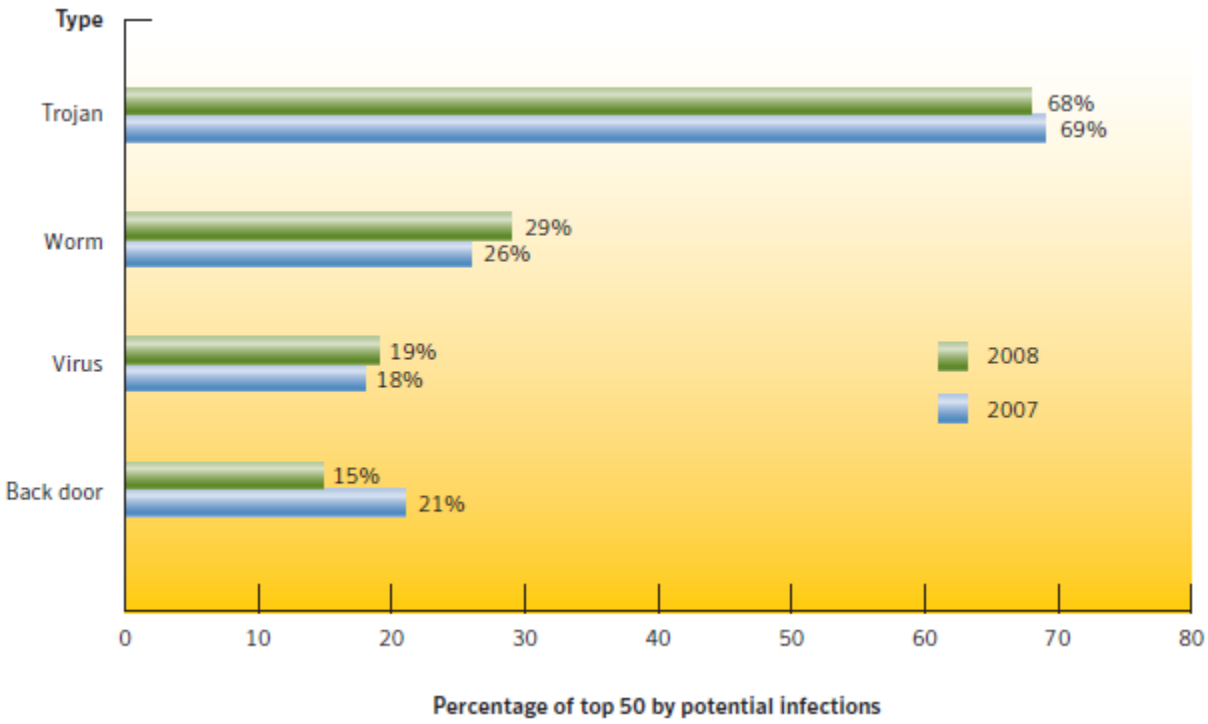
Trojan Horses

- A **Trojan horse (or Trojan)** is a malware program that appears to perform some useful task, but which also does something with negative consequences (e.g., launches a keylogger).
- Trojan horses can be installed as part of the payload of other malware but are often installed by a user or administrator, either deliberately or accidentally.



Trends

- Trojans currently have largest infection potential
  - Often exploit browser vulnerabilities
  - Typically used to download other malware in multi-stage attacks



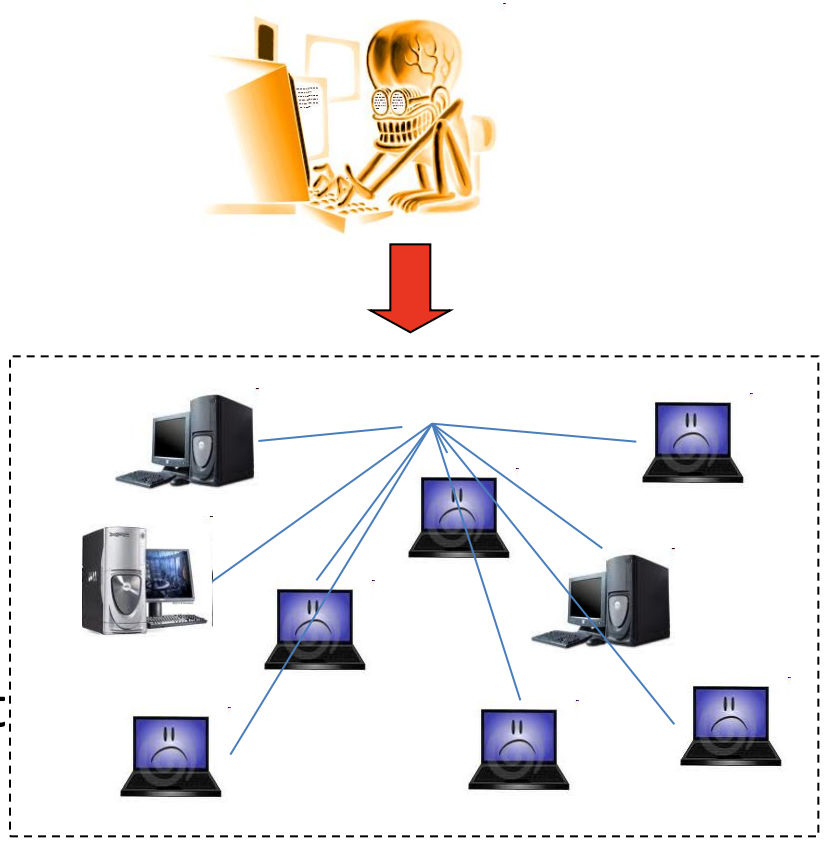
Source:
Symantec Internet Security Threat Report, April 2009

Rootkits

- A rootkit modifies the operating system to hide its existence
  - E.g., modifies file system exploration utilities
  - Hard to detect using software that relies on the OS itself
- **RootkitRevealer**
  - By Bryce Cogswell and Mark Russinovich (Sysinternals)
  - Two scans of file system
  - High-level scan using the Windows API
  - Raw scan using disk access methods
  - Discrepancy reveals presence of rootkit
  - Could be defeated by rootkit that intercepts and modifies results of raw scan operations

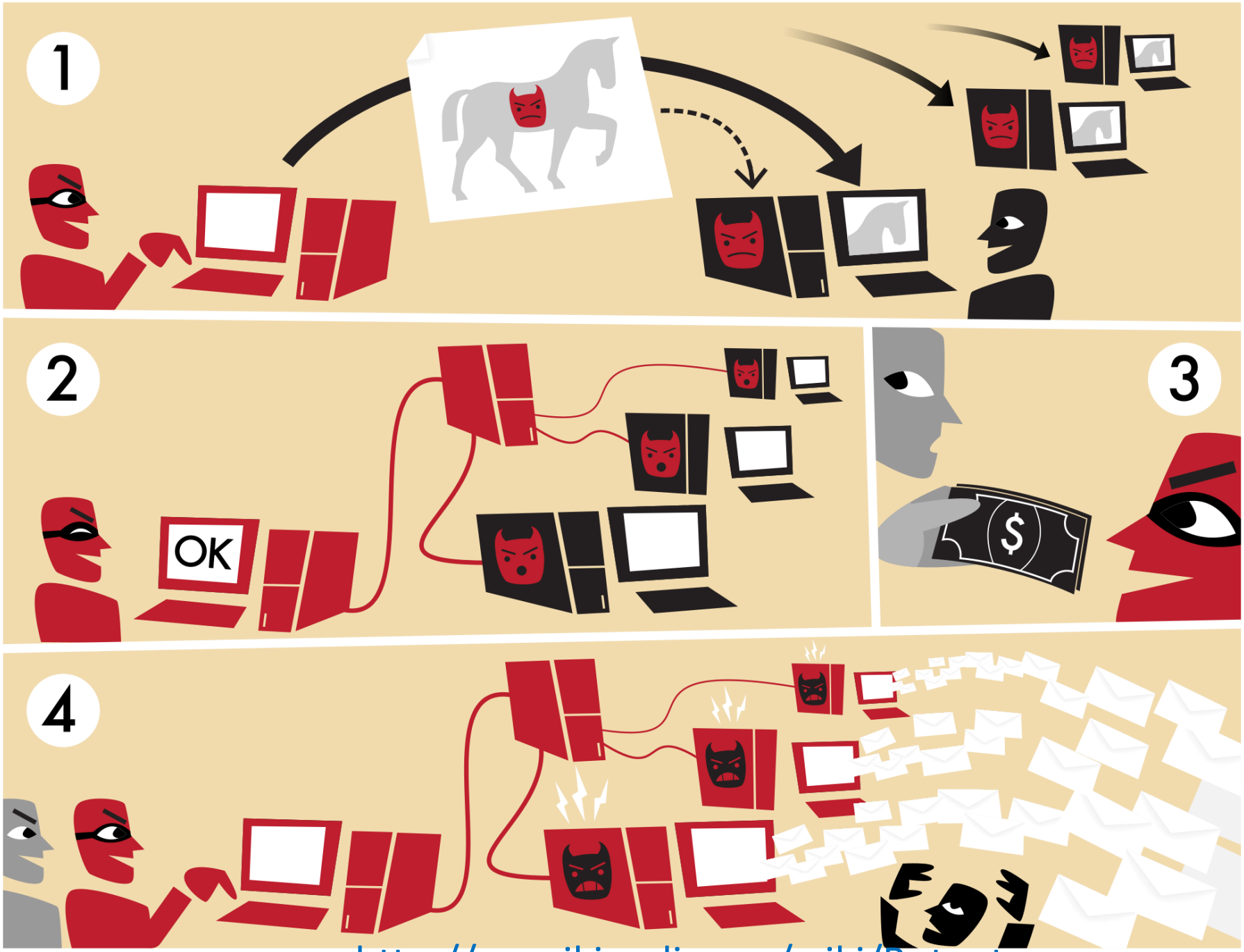
Botnet

- Botnet: a “network” of infected machines
- Infected machines are “bots”
  - Victim is unaware of infection (stealthy)
- Botmaster controls botnet
  - Generally, using IRC
  - P2P botnet architectures exist
- Botnets used for…
  - Spam, DoS attacks, keylogging, ID theft, etc.



Bot

- *Bot - a small program to remotely control a computer*
- Characterized by
  - Remote control & communication (C&C) channels to command a victim
    - *For ex., perform denial-of service attack, send spam*
  - The implemented remote commands
    - *For ex., update bot binary to a new version*
  - The spreading mechanisms to propagate it further
    - *For ex., port scanning, email*



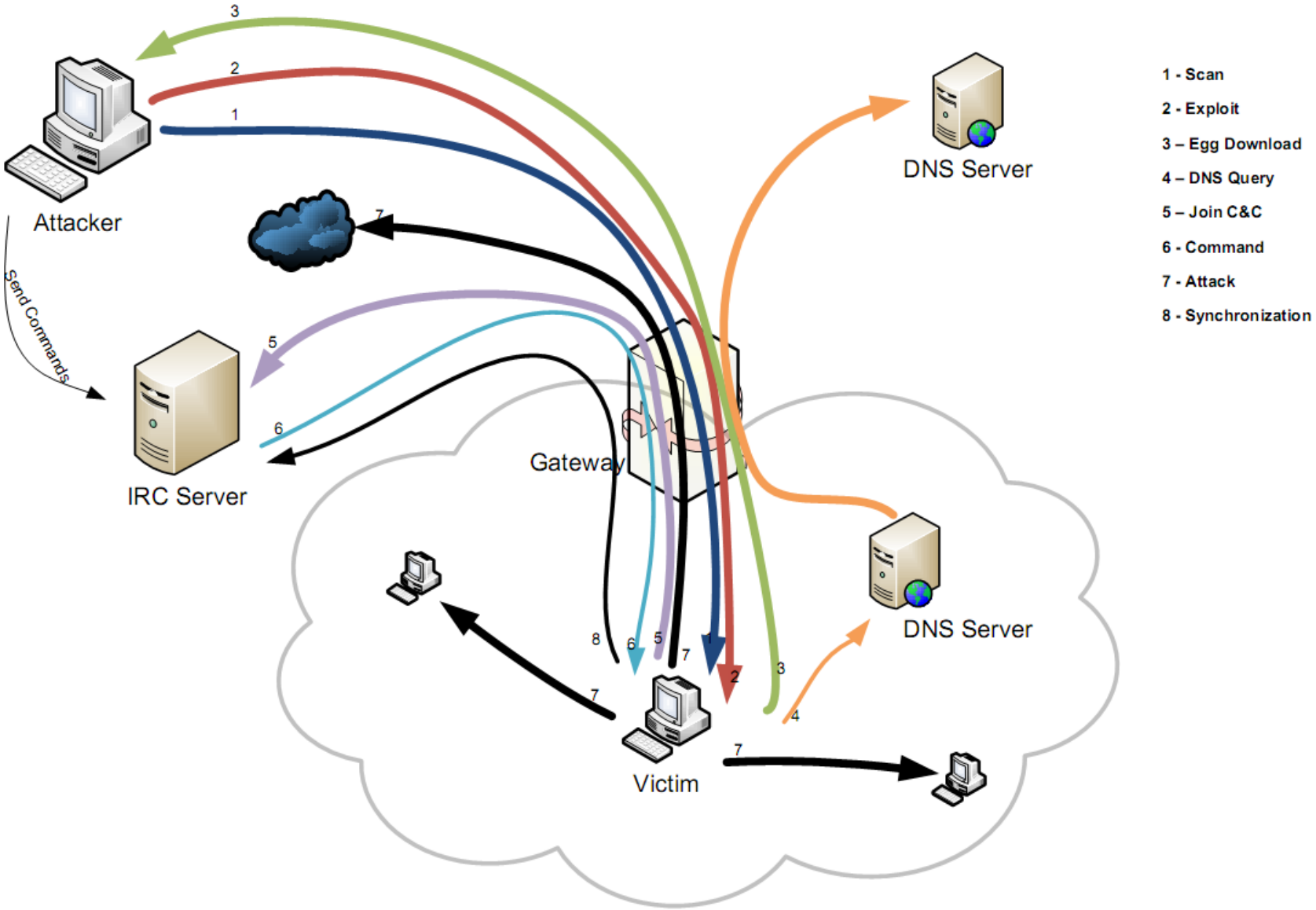
http://en.wikipedia.org/wiki/Botnet

C&C channel

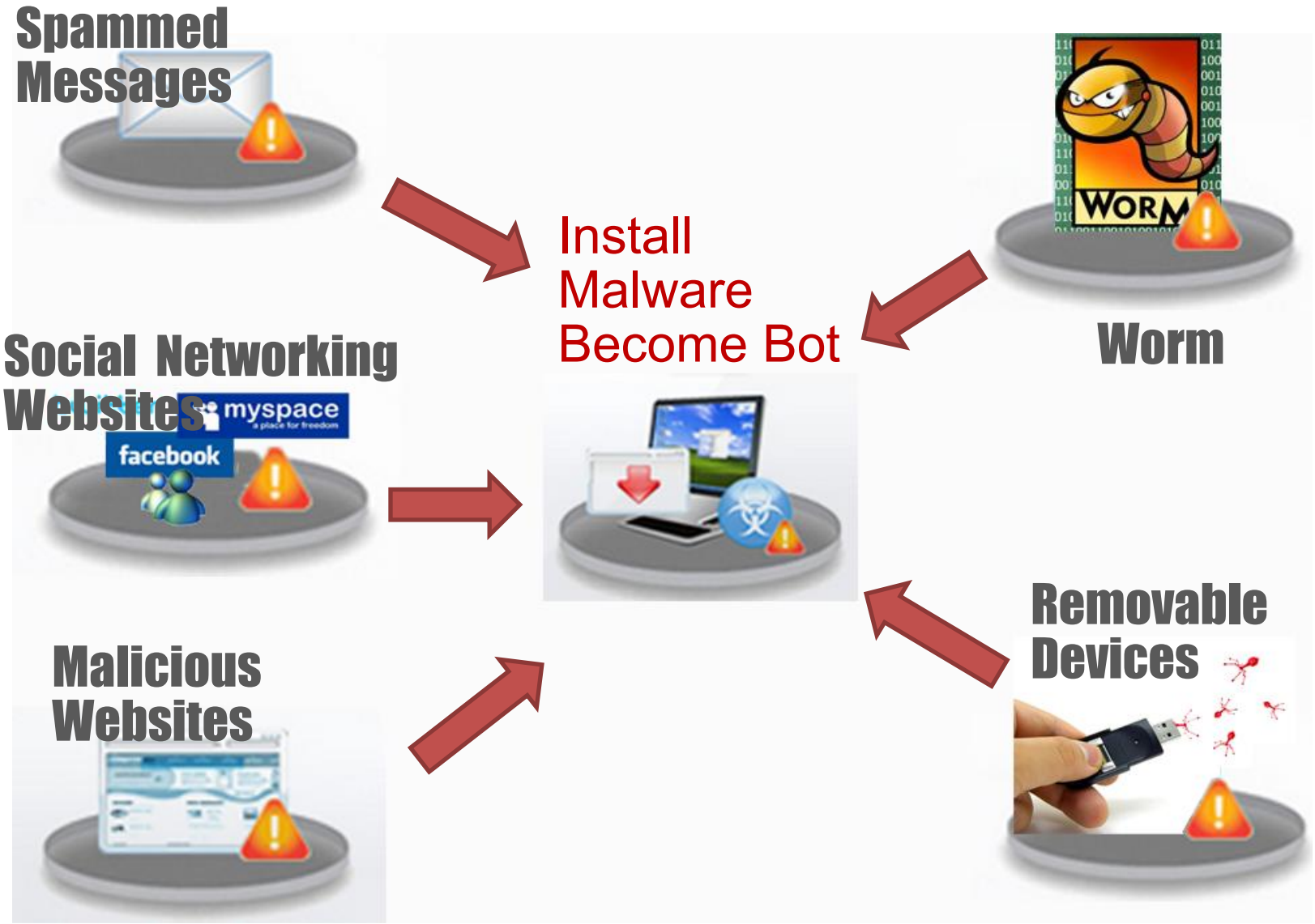
- Means of receiving and sending commands and information between the botmaster and the zombies.
- Typical protocols
  - IRC
  - HTTP
  - Overnet (Kademlia)

- Protocols imply (to an extent) a botnet's communication topology.
  - The topology provides trade-offs in terms of bandwidth, affectivity, stealth, and so forth.

Botnet Infection Stages - Centralized

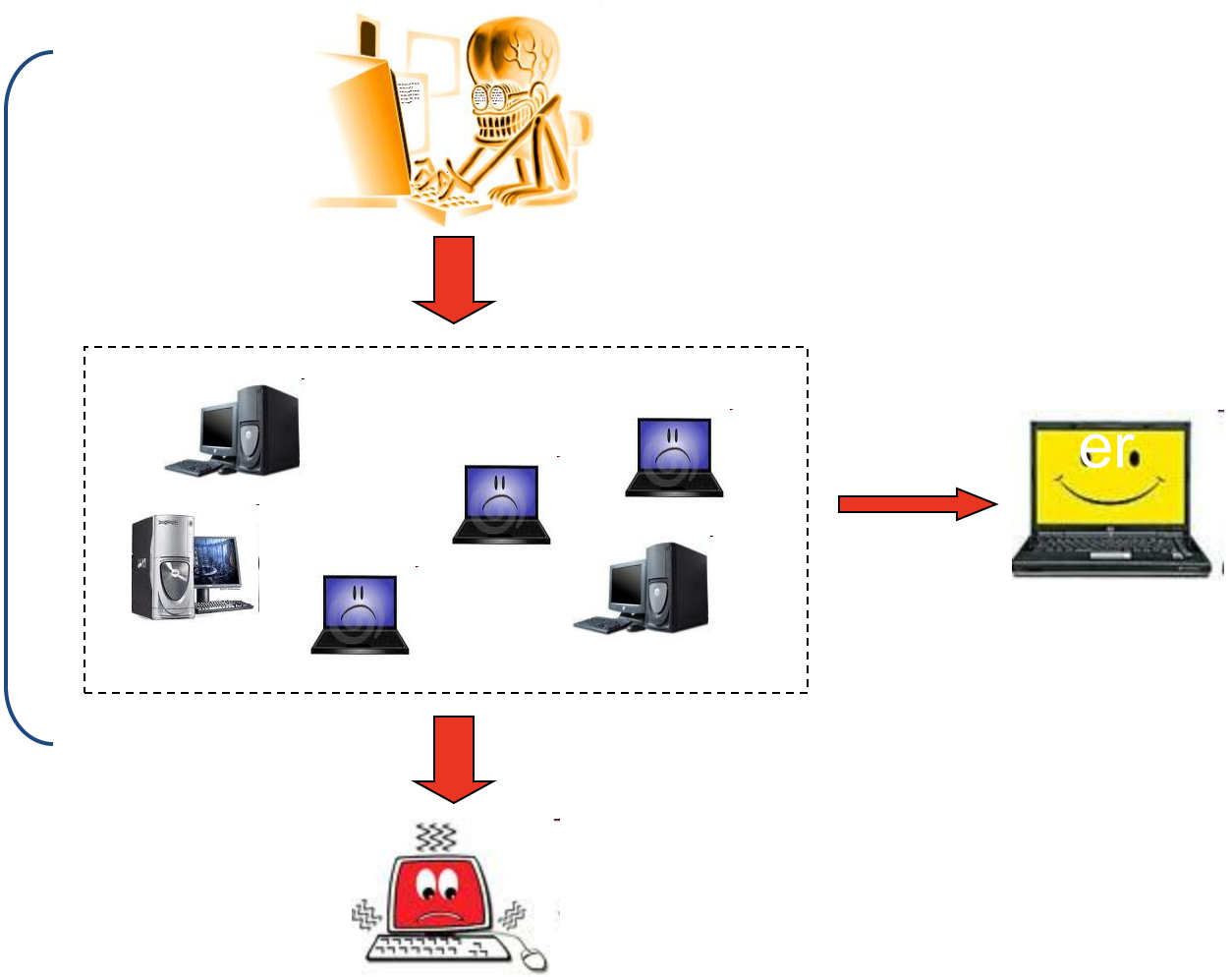


Popular Botnets Propagation Methods



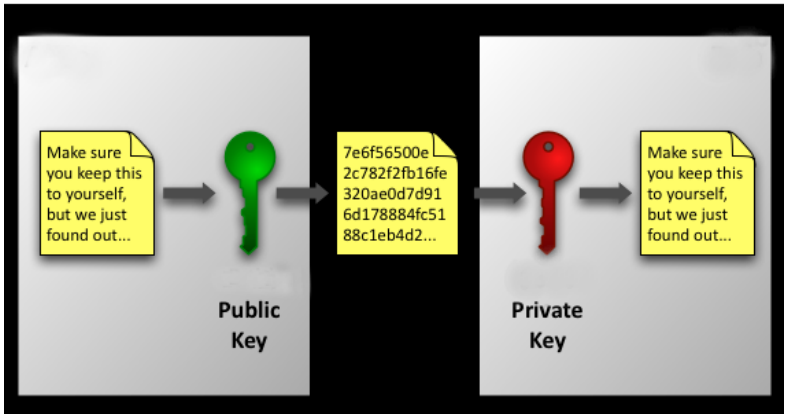
Traditional botnet

Botnet topology mainly refers to the organization of C&C channels between zombies and an attacker.



How do they hide?

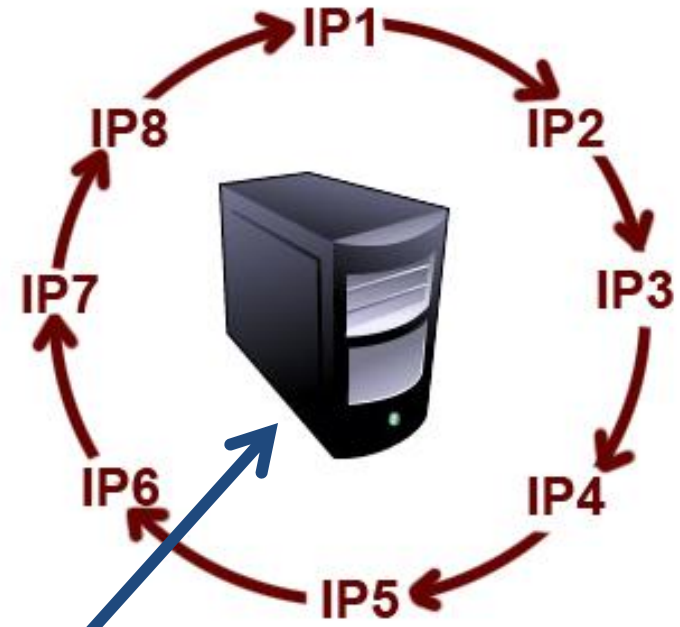
Encryption



Fast Flux

Rootkit

Fast Flux



[QUESTION] Website name:
www.lijg.ru

[ANSWER] IP Addresses:
www.lijg.ru → 68.124.161.76
www.lijg.ru → 69.14.27.151
www.lijg.ru → 70.251.45.186
www.lijg.ru → 71.12.89.105
www.lijg.ru → 71.235.251.99
www.lijg.ru → 75.11.10.101
www.lijg.ru → 75.75.104.133
www.lijg.ru → 97.104.40.246
www.lijg.ru → 173.16.99.131
……

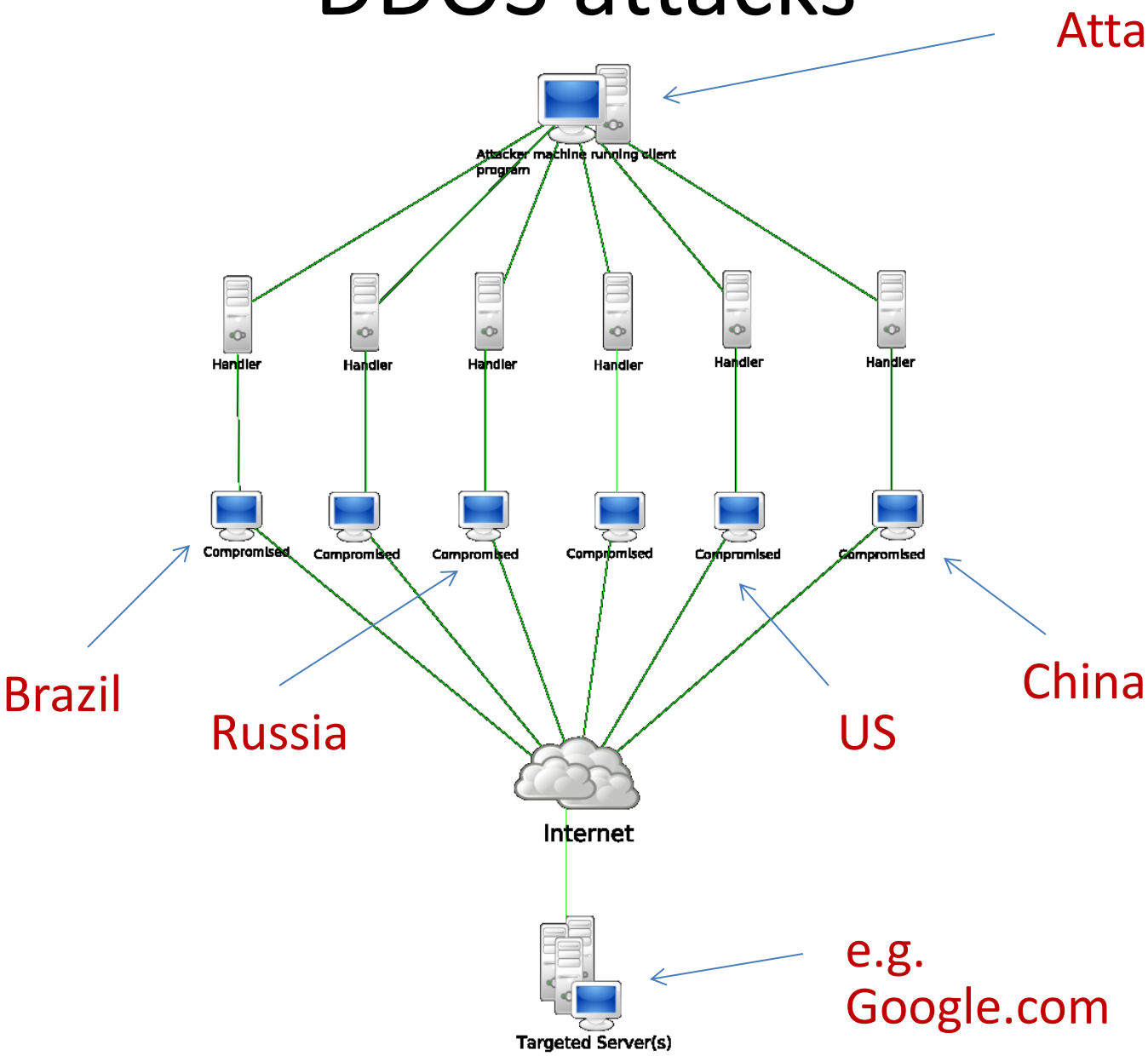
Botnet Activities

The least damage caused by Botnets:
Bandwidth Consumption

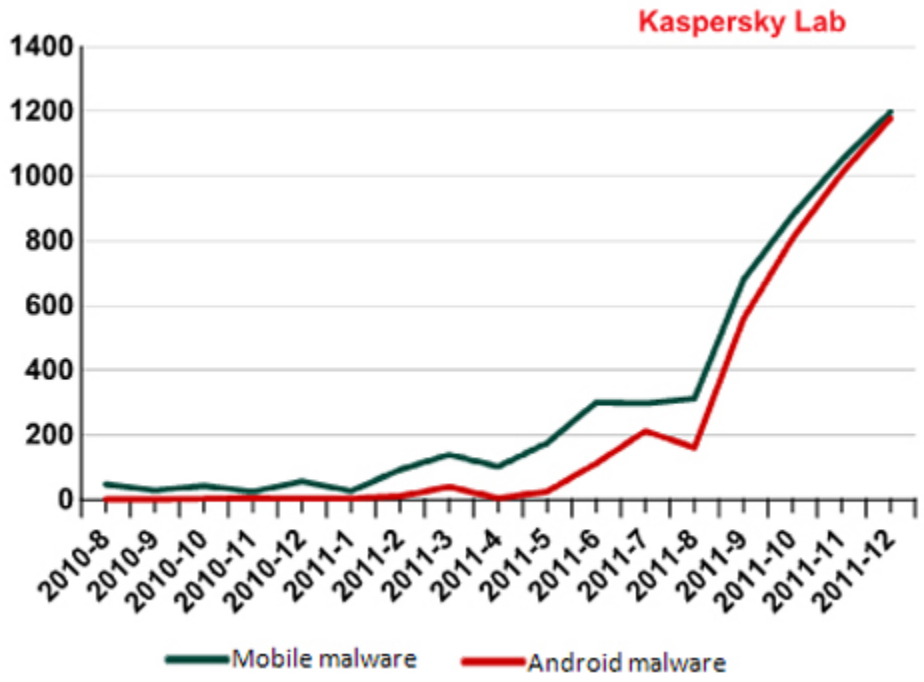
Other things:

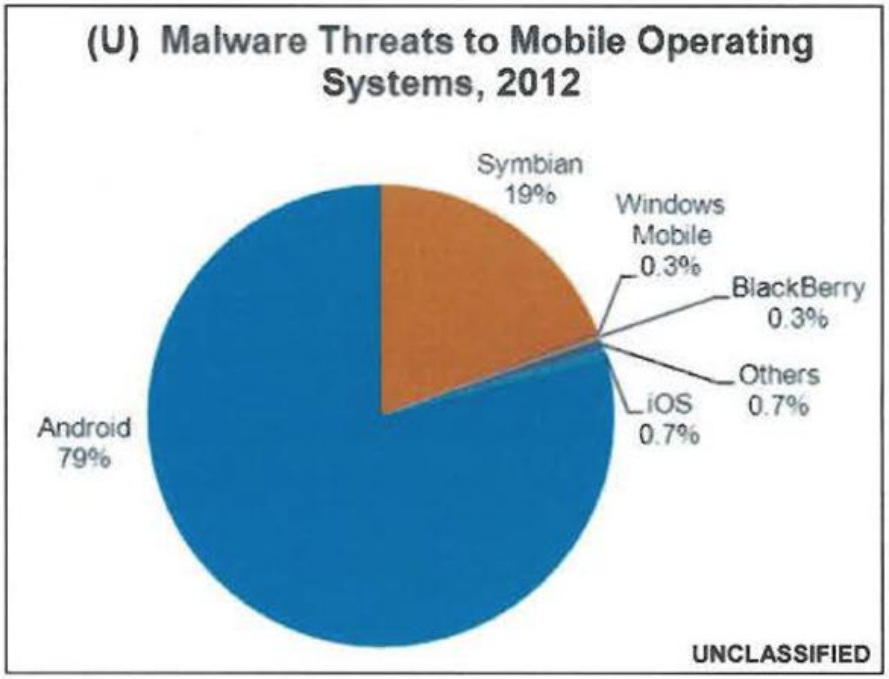
- DDOS attacks
- Spam
- Click Fraud
- Data Theft
- Phishing
- Mistrustful services

DDOS attacks



Mobile Malware





Mobile Malware Delivery

Malware Detection

- Three common detection methods
  - Signature detection
  - Change detection
  - Anomaly detection
- We briefly discuss each of these
  - And consider advantages…
  - …and disadvantages

Signature Detection

- A **signature** may be a string of bits in exe
  - Might also use wildcards, hash values, etc.
- For example, W32/Beast virus has signature

  83EB 0274 EB0E 740A 81EB 0301 0000
  - That is, this string of bits appears in virus
- We can search for this signature in all files
- If string found, have we found W32/Beast?
  - Not necessarily - string could appear elsewhere
  - A very small chance

Signature Detection

- Advantages
  - Effective on “ordinary” malware
  - Minimal burden for users/administrators
- Disadvantages
  - Signature file can be large (10s of thousands)…
  - …making scanning slow
  - Signature files must be kept up to date
  - ***Cannot detect unknown viruses***
  - Cannot detect some advanced types of malware
- The most popular detection method

Change Detection

- Viruses must live somewhere
- If you detect a file has changed, it might have been infected
- How to detect changes?
  - Hash files and (securely) store hash values
  - Periodically re-compute hashes and compare
  - If hash changes, file **might** be infected

Change Detection

- Advantages
  - Virtually no false negatives
  - Can even detect previously unknown malware
- Disadvantages
  - Many files change — and often
  - Many false alarms (false positives)
  - Heavy burden on users/administrators
  - If suspicious change detected, then what?
  - Might fall back on signature-based system

Anomaly Detection

- Monitor system for anything "unusual" or "virus-like" or potentially malicious or …
- Examples of "unusual"
  - Files change in some unexpected way
  - System misbehaves in some way
  - Unexpected network activity
  - Unexpected file access, etc., etc., etc., etc.
- But, we must first define "normal"
  - Normal can (and must) change over time

Anomaly Detection

- Advantages
  - Chance of detecting unknown malware
- Disadvantages
  - No proven track record (cannot point out exact virus names)
  - Trudy can make abnormal look normal (go slow)
  - Must be combined with another method (e.g., signature detection)
- Also popular in intrusion detection (IDS)
- Difficult unsolved (unsolvable?) problem
  - Reminds me of AI…

Future of Malware

- Recent trends
  - Encrypted, polymorphic, metamorphic malware
  - Fast replication/Warhol worms
  - Flash worms, slow worms
  - Botnets
  - Malicious apps for smart phones
  - Ransomware
    - Encrypting your files (e.g. WannaCry)
  - IoT malware (Linux Malware)
- The future is bright for malware
  - Good news for the bad guys…
  - …bad news for the good guys
- Future of malware detection?

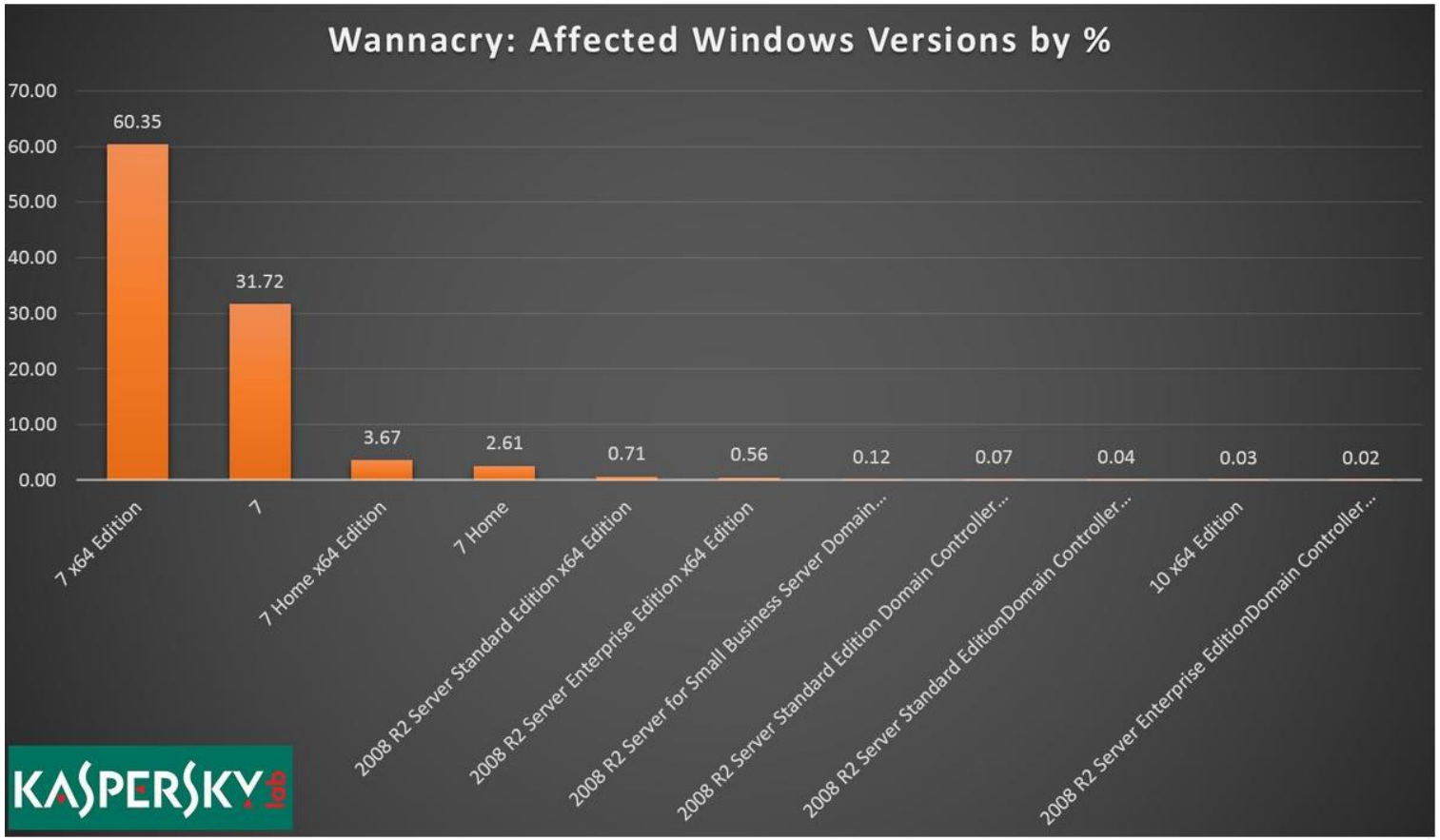
Ransomware - WannaCry

Ransomware – WannaCry (cont…)

- How does it work?
  - Used existing (but unknown) exploit called EternalBlue to attack older versions of Windows
  - Malicious code injected via SMB port
  - DoublePulsar, a backdoor is installed on victim's machine
  - WannaCry installed using backdoor

Ransomware – WannaCry (cont…)

- Affected victims found to be using old versions of Windows



Ransomware – WannaCry (cont…)

- How could it have been prevented?
  - Update!
    - Windows 7 still the most used Windows version
  - Disable unnecessary protocols
    - SMB not needed by majority machines
  - Don’t hide exploits
    - NSA hid the EternalBlue exploit
  - Network segmentation
    - Splitting networks into small chunks