

TK2100: Informasjonssikkerhet

Lesson 04: Malware

Dr. Andrea Arcuri
Westerdals Oslo ACT
University of Luxembourg

Goals

- Learn bases of how malwares work and distribute
- Learn bases of how to protect from them
- Note: writing and analyzing malware is quite complex, as you need to have a good grasp of C language (which at this point in time you likely do not have) and low level details of OS... as such, this class is mainly on the “*theoretical*” side...

What Is Malware?

- Malware means **Malicious Software**
- Software that performs unauthorized and (most often) harmful actions
- If you haven't watched yet, highly recommended to see "*2001: a Space Odyssey*"



Malware Classification

- We can categorize malware into different types based on how it is spread and how it hides.
- Spreading
 - Virus: human-assisted spread (eg opening of email attachments and memory sticks)
 - Worm: Automatic spread from machine to machine over the net
- Hiding
 - Rootkit: Changes OS to hide presence
 - Trojans: Utility program that conceals malicious operations (eg keylogger)

How common is malware (2017)?

- 1 out of 131 emails contains attached malware
- 357 **M**illion variants
- Source: Symantec Internet Security Threat Report (ISTR) 2017

Insider Attacks

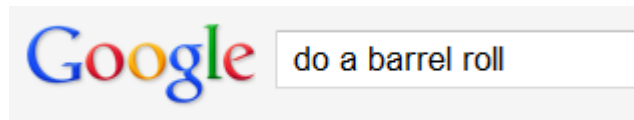
- *“In the case of malware, an insider attack refers to a security hole that is created in a software system by one of its programmers”*
- Different kinds of *Insider Attacks*:
 - Backdoors
 - Easter Eggs
 - Logic Bombs

Backdoors

- Hidden features, activated with special commands
 - eg, a way to bypass authentication, eg access online banking of different users
- Deliberately added by a developer
- *Debugging*: sometimes backdoors added during development to simplify testing/debugging
 - eg, skip authentication
 - should never end up in production configurations
- *Bug*: backdoors are not always obvious... often deliberate bugs that can be exploited as backdoors (eg buffer-overflow)... if malicious developer get caught, can just claim ignorance...

Easter Eggs

- Similar to backdoors, these are hidden features that can be activated with secret passwords or unusual sets of inputs
- Usually harmless, just done for “fun”
- Eg, try typing “*do a barrel roll*” on Google Search



Logic Bombs



- A program that performs a malicious action as a result of a certain logic condition
 - Eg, erase all data one month after an employee has been fired
 - Eg, disable authentication checks at certain time during the day
- *Extortion*: once logic bomb activated, provide solution via a backdoor after an extortion payment

Insider Attack Prevention

- No 100% solutions, but can reduce risk
- Avoid single points of failure, eg only one employee handling critical systems / backups
- Code-reviews: code written by a developer should be reviewed by a second one
- Static analyses: exist tools that can automatically check source code for some types of backdoors
- Etc.

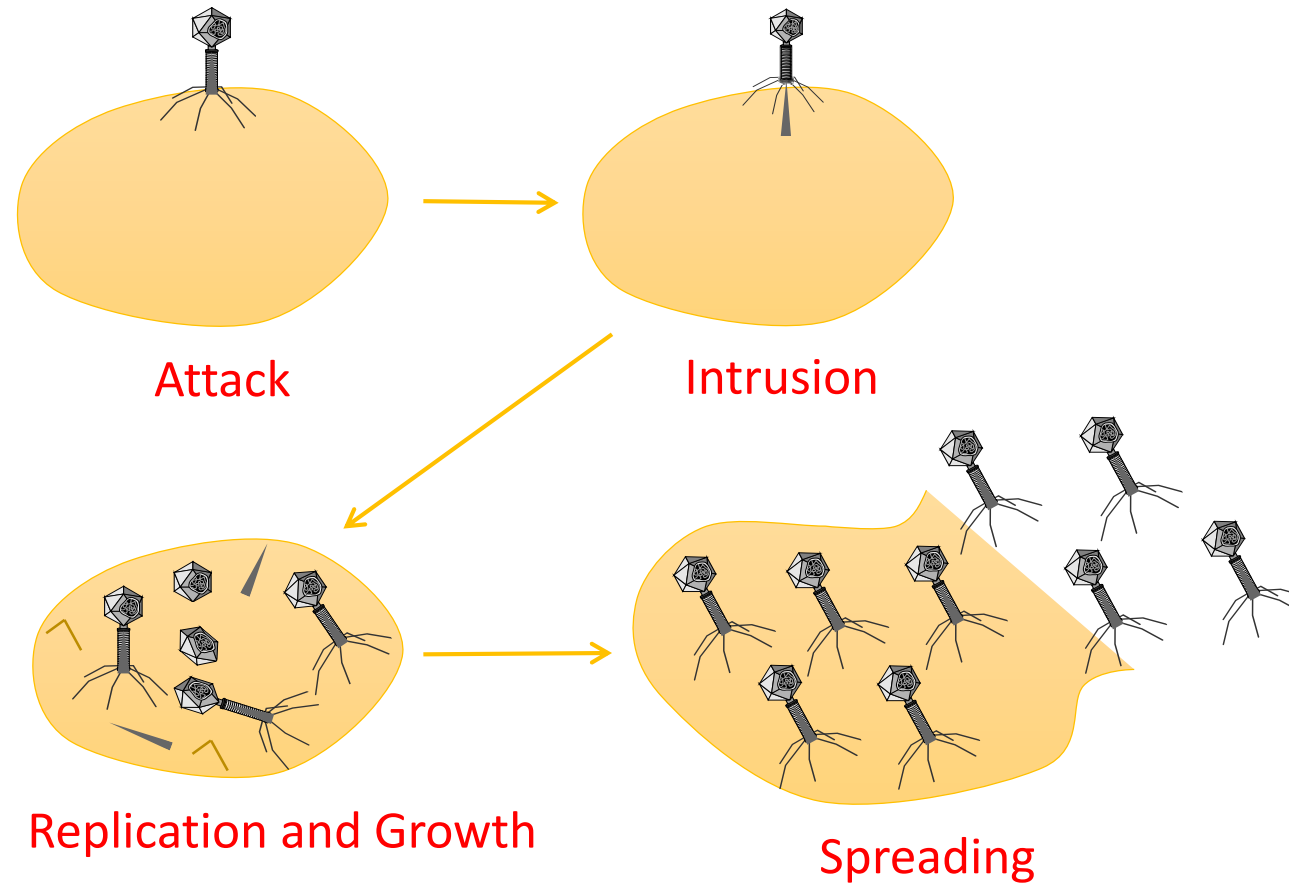
Computer Viruses



What is a Computer Virus?

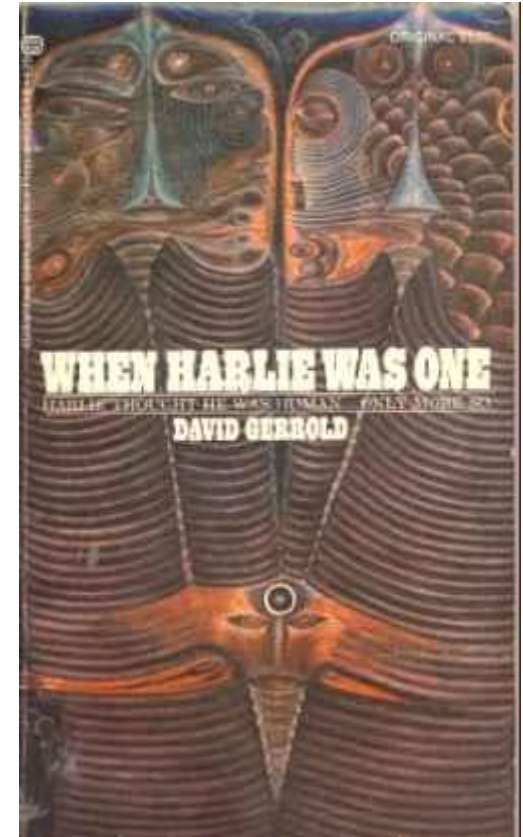
- A program that can replicate itself
 - by changing other files / programs
 - by infecting them with code
 - can modifying itself further
- The ability to infect existing files/programs is what separates viruses from other types of malware
- Generally requires initial user interaction
 - Click on a link and start installation
 - Open an email attachment
 - Share a memory stick, or other USB device

Similar to a Biological Virus



History

- In David Gerrold's AI novel "When HARLIE was One" (1971), the program VIRUS reproduces itself
- Adleman (The A in the RSA Encryption Algorithm) suggested the term (1984) for Fred Cohen, who wrote his PhD on the theory behind
- The first PC viruses observed in the 1980s were typically "boot-virus" that infected the boot sector on floppy disks and (eventually) hard disks.

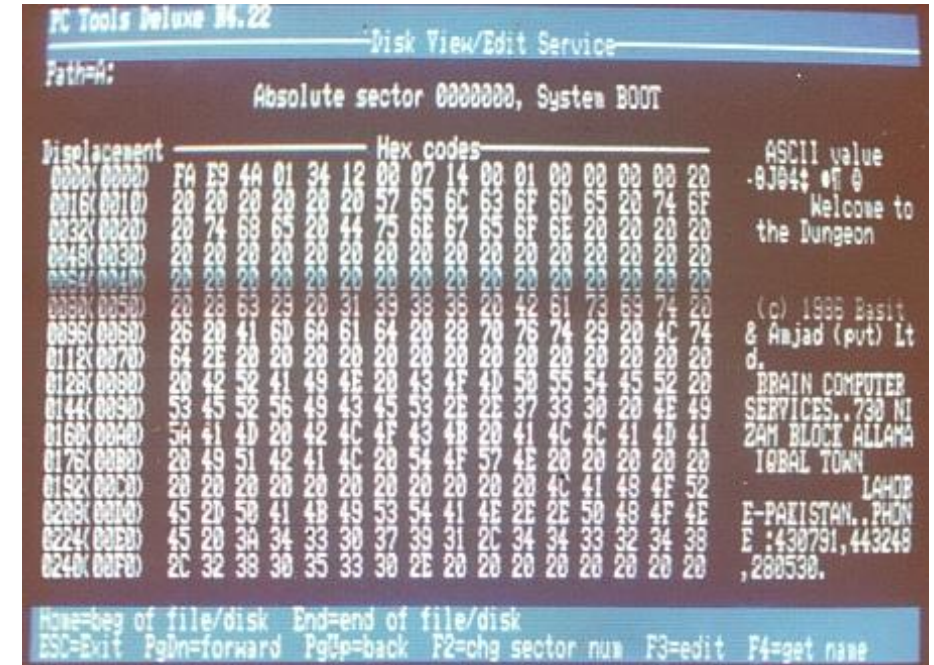


Traditional Viruses

- Today Worms and Trojans are more common
 - malicious files that are able to live an independent life without a host process
- Has existed longer than PCs, and first registered malware came in 1971 and is called "The Creeper Program" and spread over ArpaNet
- Brain is credited as the world's first "PC virus" (1986), and later that year, for the first time, it was possible to infect ".exe" files with Suriv-02
 - ".exe" files were initially considered a safe format because it was so complex that no one could manage to infect them, unlike other execution files that were using clear machine code ...
 - Some credit Old Yankee as the first ".exe" file infector
- Several dangerous viruses came out at this time:
 - AIDS Trojan (1989); encrypted your entire disk
 - Dark Avenger (1989); overwritten random parts of the disk 1/16 times the virus ran
 - Jerusalem (1987); Deleting files on machine on Friday 13th ...

Brain

- ©Brain – January 1986
- Written by two brothers in Pakistan to protect copyright on the program of a heart monitoring device they were selling
- Contained their phone number
- Spread via floppy disks



The screenshot shows the boot screen of the Brain virus. At the top, it says 'PC Tools Deluxe V6.22' and 'Disk View/Edit Service'. Below that, it says 'Fath=A:' and 'Absolute sector 0000000, System BOOT'. The main display is a table with three columns: 'Displacement', 'Hex codes', and 'ASCII value'. The table contains 16 rows of data. The ASCII value column shows the text 'Welcome to the Dungeon' and copyright information for Basit & Amjad (pvt) Ltd. At the bottom, there is a legend for keyboard shortcuts: Home=begin of file/disk, End=end of file/disk, ESC=Exit, PgDn=forward, PgUp=back, F2=chg sector num, F3=edit, F4=get name.

Displacement	Hex codes	ASCII value
0000(0000)	FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 20	·8J94: *T 0
0016(0010)	20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F	Welcome to
0032(0020)	20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20	the Dungeon
0048(0030)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0064(0040)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0080(0050)	20 20 63 23 20 31 39 38 36 20 42 61 73 69 74 20	(c) 1986 Basit
0096(0060)	26 20 41 60 6A 61 64 20 28 70 76 74 29 20 4C 74	& Amjad (pvt) Lt
0112(0070)	64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20	d.
0128(0080)	20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20	BRAIN COMPUTER
0144(0090)	53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49	SERVICES..730 NI
0160(00A0)	54 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41	2AM BLOCK ALLAMA
0176(00B0)	20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20	IQBAL TOWN
0192(00C0)	20 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52	LAHORE
0208(00D0)	45 20 50 41 48 49 53 54 41 4E 2E 2E 50 48 4F 4E	E-PAKISTAN..PHON
0224(00E0)	45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38	E :430791,443248
0240(00F0)	2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20	,280530.

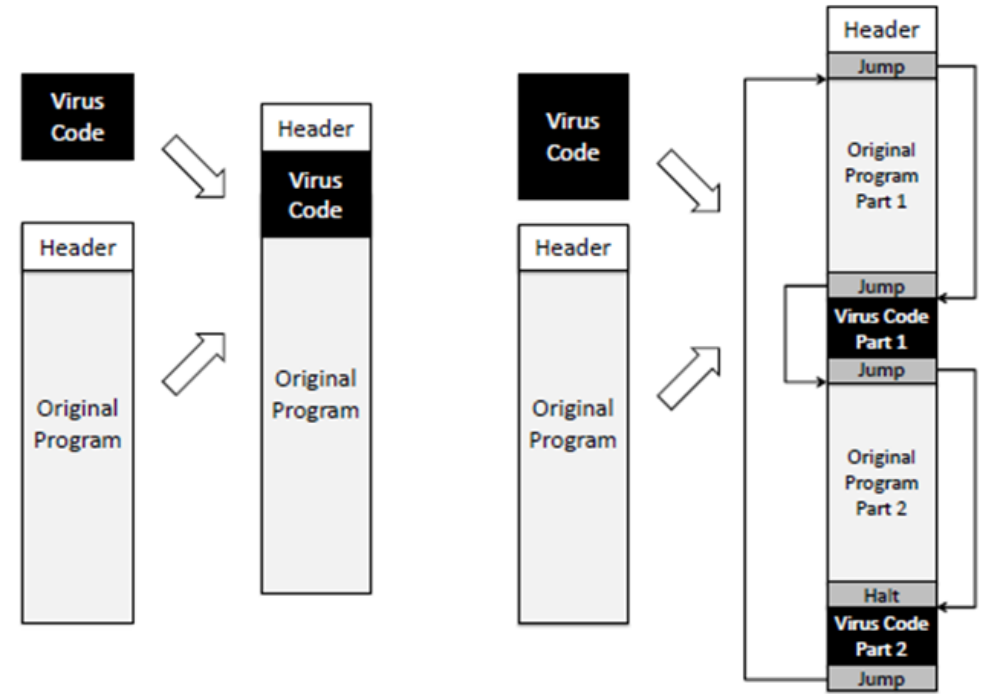
Welcome to the Dungeon © 1986 Basit * Amjad (pvt) Ltd. BRAIN
COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-
PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS....
Contact us for vaccination...

Virus Phases

1. *Dormant*: virus laying down to avoid detection (eg, from an Antivirus software)
2. *Propagation*: replicates itself, infecting new files in new systems
3. *Triggering*: logical condition causes switch from dormant to propagation phase
4. *Action*: do a malicious action, usually called *payload*
 - eg, delete/encrypt files

Types of Viruses

- Program Virus
 - Injecting itself inside the code of an existing program
- Macro Virus
 - Injecting documents like Words, which does support scripting code, usually called “macros”
- Boot Sector Virus
 - Infecting “boot sector”, which is what first run the OS starts



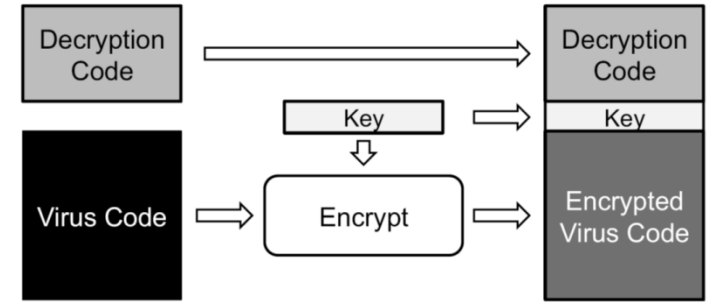
Virus Protection

- Simply, use an AntiVirus program... which needs to be updated often...
 - Why updates? Why often? How does it work?
- *Virus Signature*: once a virus is spread and known, can analyze its characteristics (eg special sequences of malicious instructions it uses), and then use *pattern-matching* to check if a file contains such instructions
 - As new viruses come up all the time, need to update the list of virus *signatures* in the antivirus program

Arms-Race

- Antiviruses use virus signatures to detect the viruses
- Virus developers try to find new ways to *hide* the presence of the viruses
- Antiviruses “evolve” to be able to handle these cases, and so on in an “arms-race”

Hiding Techniques



- Encrypt part of the code of the virus, and then decrypt and execute those parts at runtime when the infected program is running
 - A program that does decryption is hence “suspicious”
- *Polymorphic* virus: uses encryption, but each time it replicates, uses a different key
 - so signature of encrypted code is different
- *Metamorphic* virus: no encryption, but *code obfuscation* at each replication via code reordering and adding non-used instructions

Worms

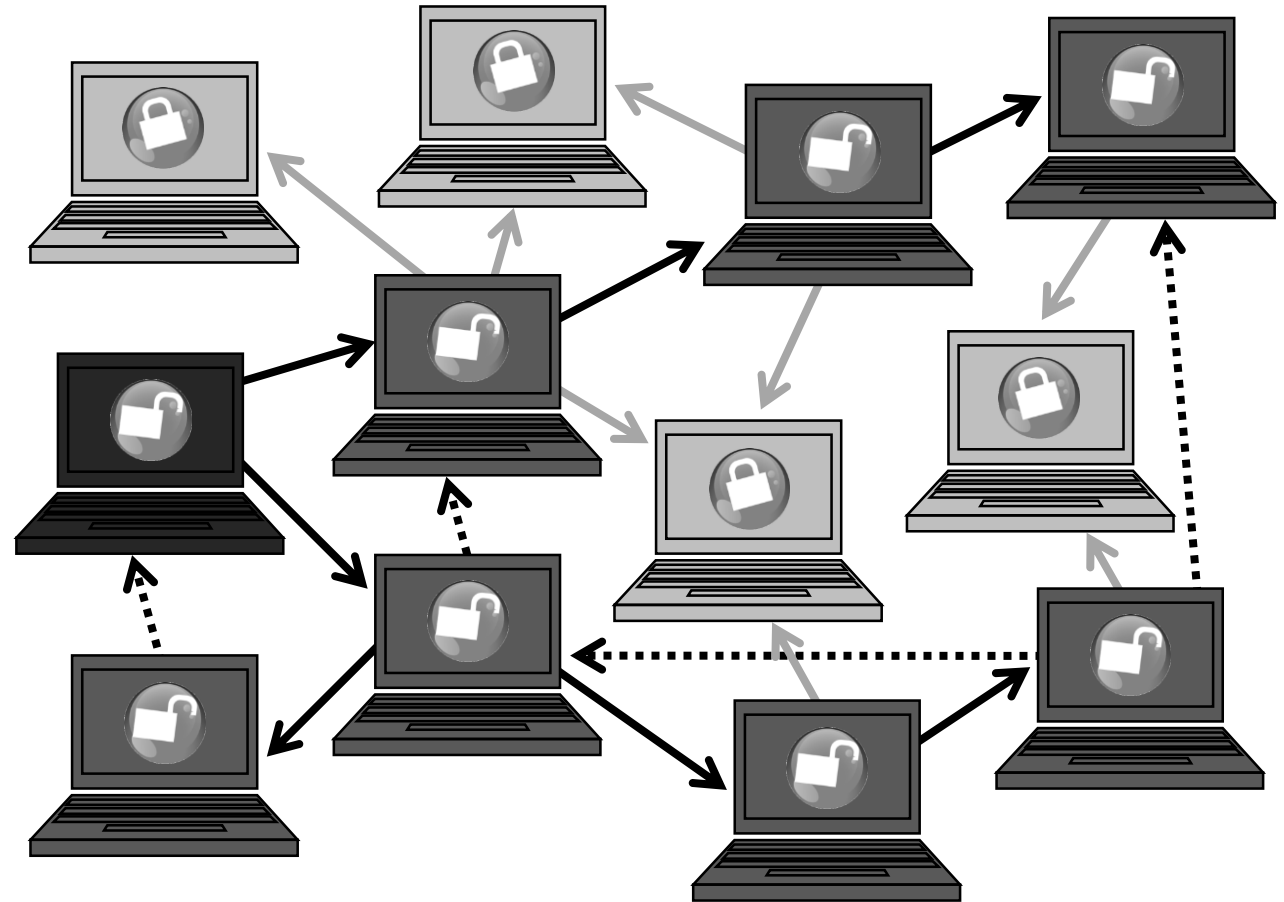


What is a Computer Worm?

- A malware that can replicate itself
- Does not need to inject its code inside other programs/files
 - I.e., this is contrast to viruses
- Usually does not need manual intervention (like opening an attachment in an email)
 - eg, exploiting security holes in existing programs, like a buffer overflow in web servers

Spreading of Worms

- Worms spread by finding and identifying vulnerable host machines
 - eg, having known security hole
- It must determine if the machine is vulnerable
- It must be able to check if the machine is already infected



History



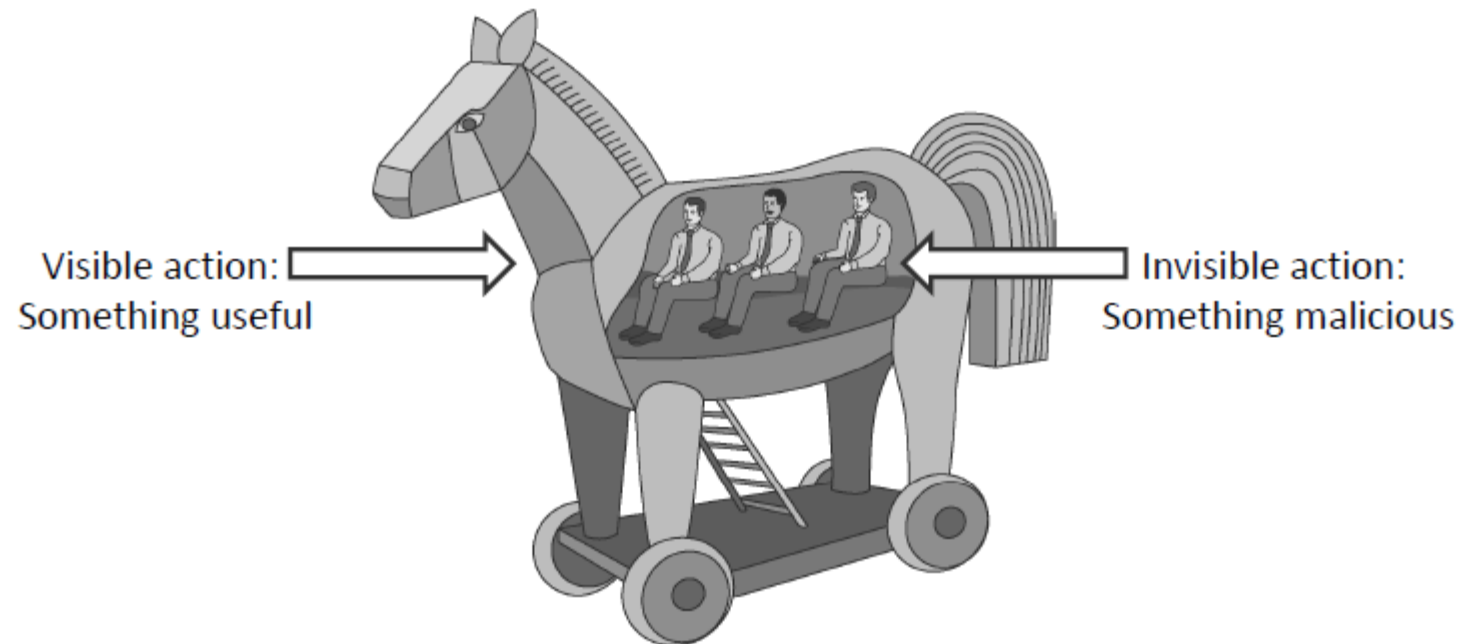
- First Worm program was in 1988, by Robert Morris, a student at that time, for research purposes
- No malicious payload, just replicating itself
- Propagation by exploiting for example a buffer overflow in a networking program
- Checking if machine was already infected, but not trusting results 1/7 of times, and replicating anyway in such case
- Ended up many running many copies on same machine, consuming CPU resources, becoming an involuntary DOS attack
- Spread on 10% of all machines on internet at that time...
- Large unintended damage, ie wasted time in cleaning the infected machines
- Morris was convicted: 3 years if probation, 400 hours of community service, plus fine...

Other Kinds of Malware

Trojans, Rootkits, Botnets, etc.

Trojan Horses

- Reference to a Greek myth in *Aeneid*
- Program that does something useful (eg a music player), but also hide malicious code (eg steal your passwords / secrets)



Rootkits

- Malware that is installed at administrative level (ie, “root” user in Unix) of the OS, and alter the OS itself
- Very difficult to detect, because altering the functionalities of OS
- Might need to wipe out the hard-drive, and re-install the OS
- **Sony** 2005: most famous case, where Sony had rootkit malware in their CDs to alter Windows OS to install secret anti-copy protection software



Zero-Day Attacks

- A virus/worm to propagate needs to exploit an existing vulnerability in software (eg buffer overflow)
- Software can have bugs and security “holes” (eg, a buffer overflow vulnerability) not known to its developers
- Once a hole/bug is detected, the software can be *patched*, and a new release distributed
 - And that is why it is important to update software...
- A “Zero-Day” attack is an attack that exploits a vulnerability that is not known yet

Botnets

- Once machine infected with a worm, can be controlled remotely
- *Zombie*: an infected machine, which can receive commands from a *bot herder*
- *Botnets*: there can networks of millions of compromised machines (typically IoT devices) that can be controlled by a herder
- Uses: massive DDOS (distributed-denial-of-service) attacks and sending spam emails

Adware

- Privacy-invasive software
- Display advertisements *without* user consent
- Eg, typically as pop-up message
- Can hide, and show pop-ups like they were coming from browser



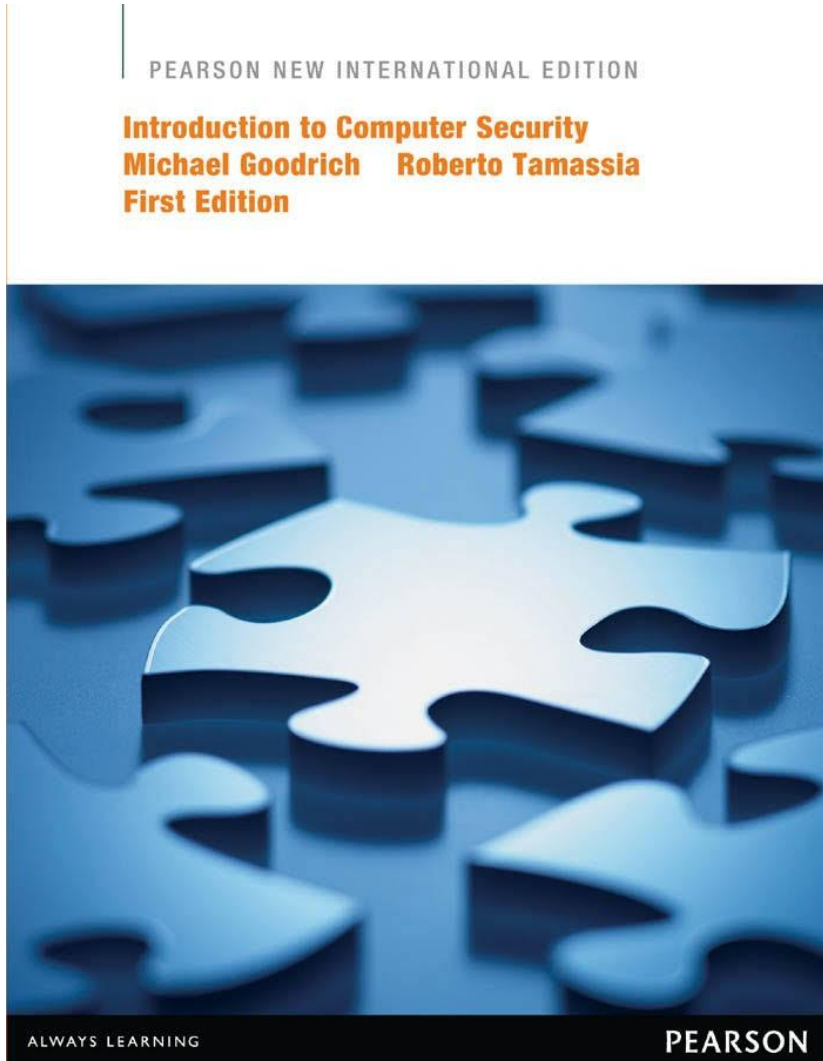
Spyware

- Privacy-invasive software that collects data from user and send it to a malicious third-party
- *Keylogging*: record actions on keyboard, eg typing of passwords
- *Screen Capturing*: take snapshots of screen
- Detection: user would likely not notice the presence of spyware, as only direct negative effect would be just some CPU overhead of spyware running in background

Countermeasures

- Install an antivirus
 - Not only for Windows, but Mac also...
 - Not just for viruses, but also for worms, Trojans, etc
- Eg, never open email attachments that are programs, or activate macros in Word documents
- Eg, beware of P2P networks, as often containing worms...
- Common sense: in general, never trust *unsolicited* files sent to you, *even from friends*
 - their machines could have been compromised

For Next Week



- Book pages: 174-214
- Note: when I tell you to **study** some specific pages in the book, it would be good if you also *read* the other pages in the same chapter at least once
- Note: no exercises this week