Chapter 1
Malware Overview

Mohd Zaki Mas'ud

BITS 3453

Updated 12 10 2020

Topic

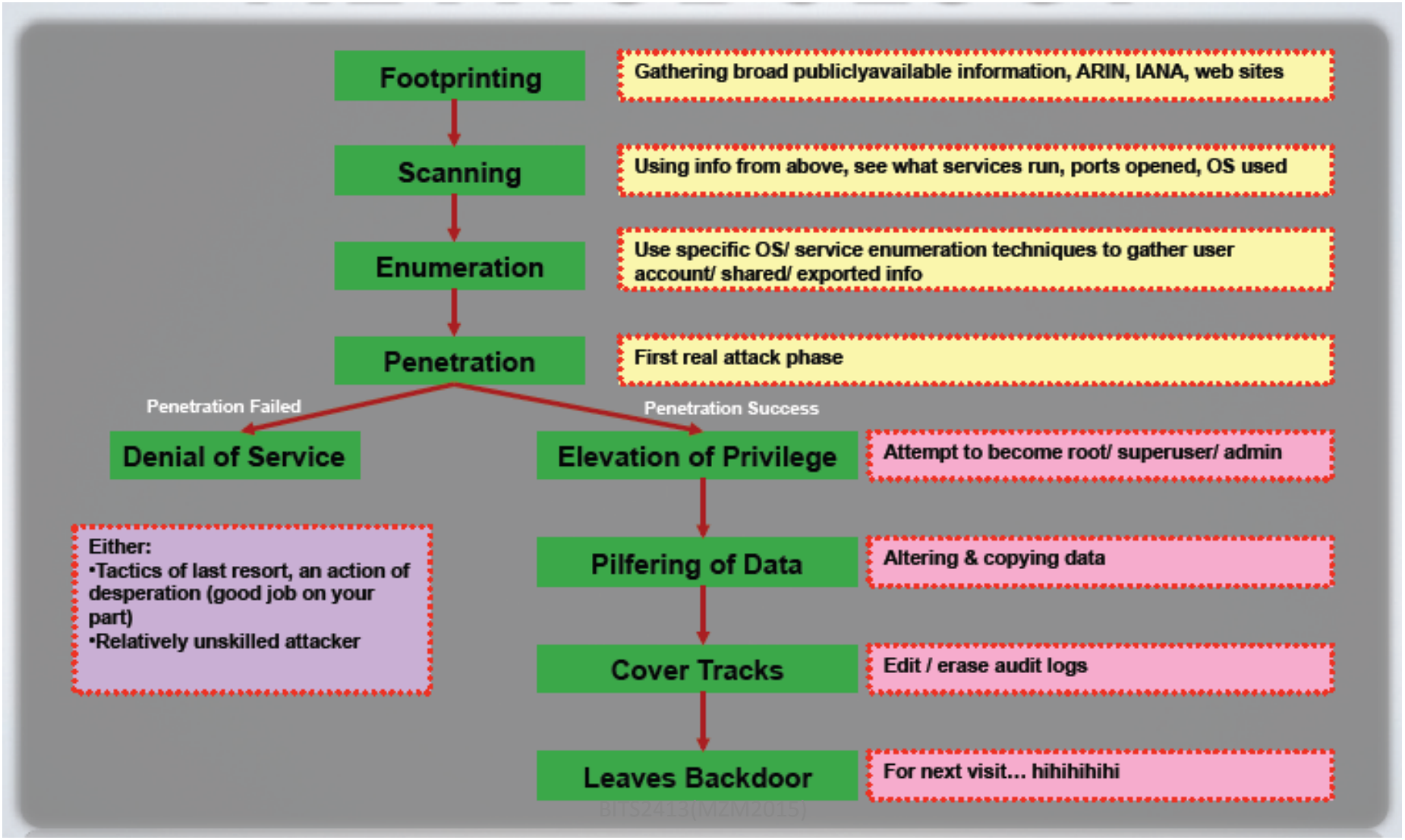
- General classification of computer attack
- Malware definition
- Malware evolution
- Type of Malware
- Target
- How malware embedding itself to program.

DEFINITION

Classification of Computer Attack

- Most of the time Hacker do it manually(info gathering, exploit, launch malicious application, covering attack)……eventually the entire activity can be done automatically using MALWARE….
- Kind of automate attack….

Attack Methodology



Recognizing External Threats

- *Denial-of-Service Attacks*
- *Distributed Denial-of-Service Attacks*
- *Viruses,Worms, and Trojan Horses*
- *BotNet*
- *Software Vulnerabilities*
- *Nontechnical Attacks*

Motivation of Network Attack

	OFFENDER ID	LONE/ GROUP HACKER	TARGET	MOTIVATION/ PURPOSES
Wannabe Lamer	9-16 years old I would like to be hacker but I can't	GROUP	End users	For fashion, it's "cool" → to boast and brag
Script Kiddies	10-18 years The script boys	GROUP (but they act alone)	SME / Specific security flaws	Give vent of their anger, attract mass media
Cracker	17-30 years The destructor, burned the ground	LONE	Business Company	Demonstrate skills, attract mass media attention
Ethical Hacker	15-50 years The "ethical" hacker world	LONE / GROUP (hacking for fun)	Vendor / Technology	For curiosity (learning) & altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized & paranoid attacker	LONE	On necessity	For curiosity (learning) →egoistic purposes
Cyber Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / end users	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI etc	LONE / GROUP	Government / Suspected terrorists / Strategic Company / Individual	Espionage / Counter espionage, Vulnerability test, Activity monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic Company	Monitoring / Controlling / Crashing system

Malware Definition

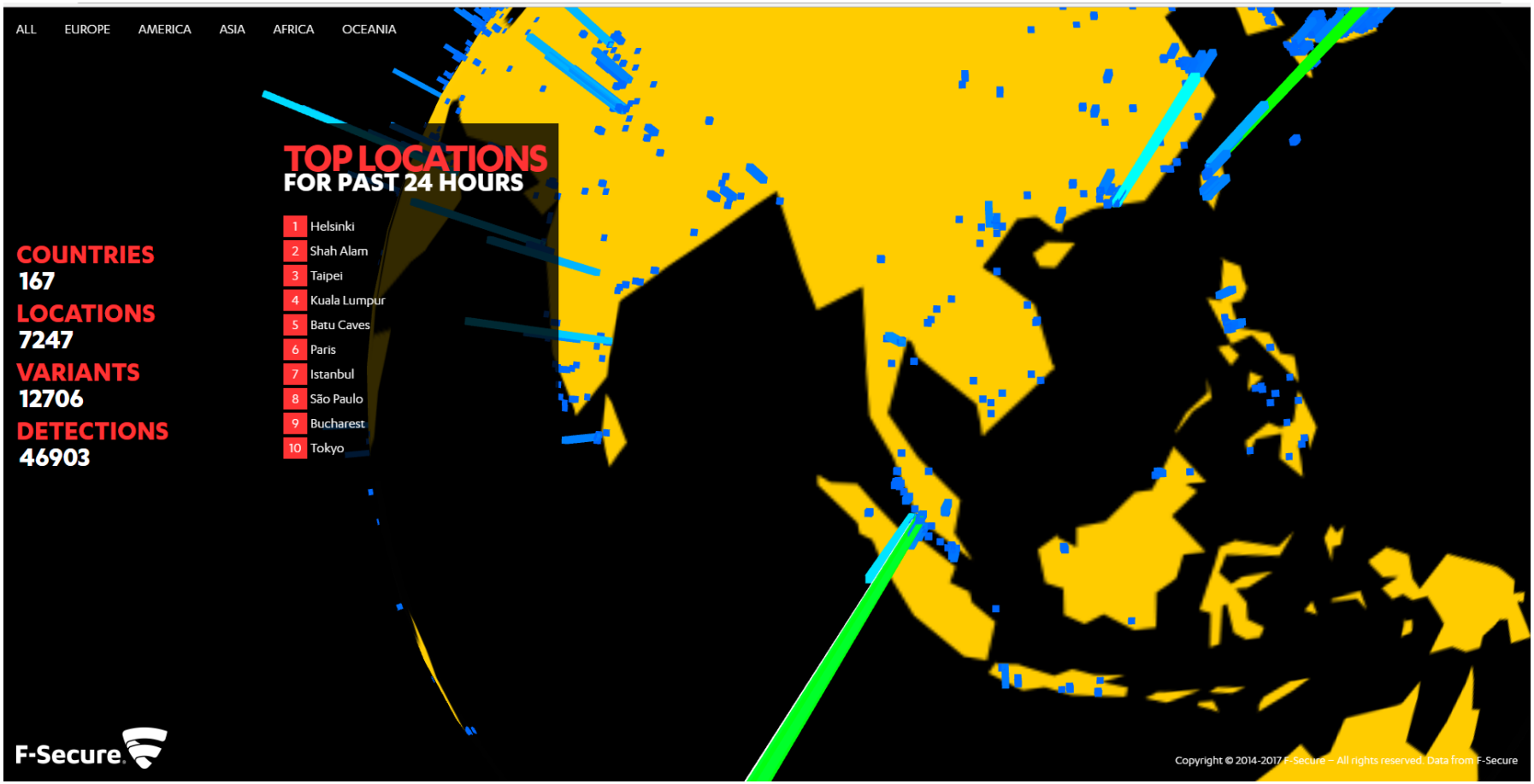
- Any Code that “perform evil Thingy”
- software such as a virus on a computer or computer network that the user does not know about or want. (oxford dictionary)
- Any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems(wikipedia)
- A Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do

General Definition

- Malicious software, or malware, is used by cybercriminals, hacktivists and nation states to disrupt computer operations, steal personal or professional data, bypass access controls and otherwise cause harm to the host system.
- Appearing in the form of executable code, scripts, active content or other software variants, there are many different classes of malware which possess varying means of infecting machines and propagating themselves

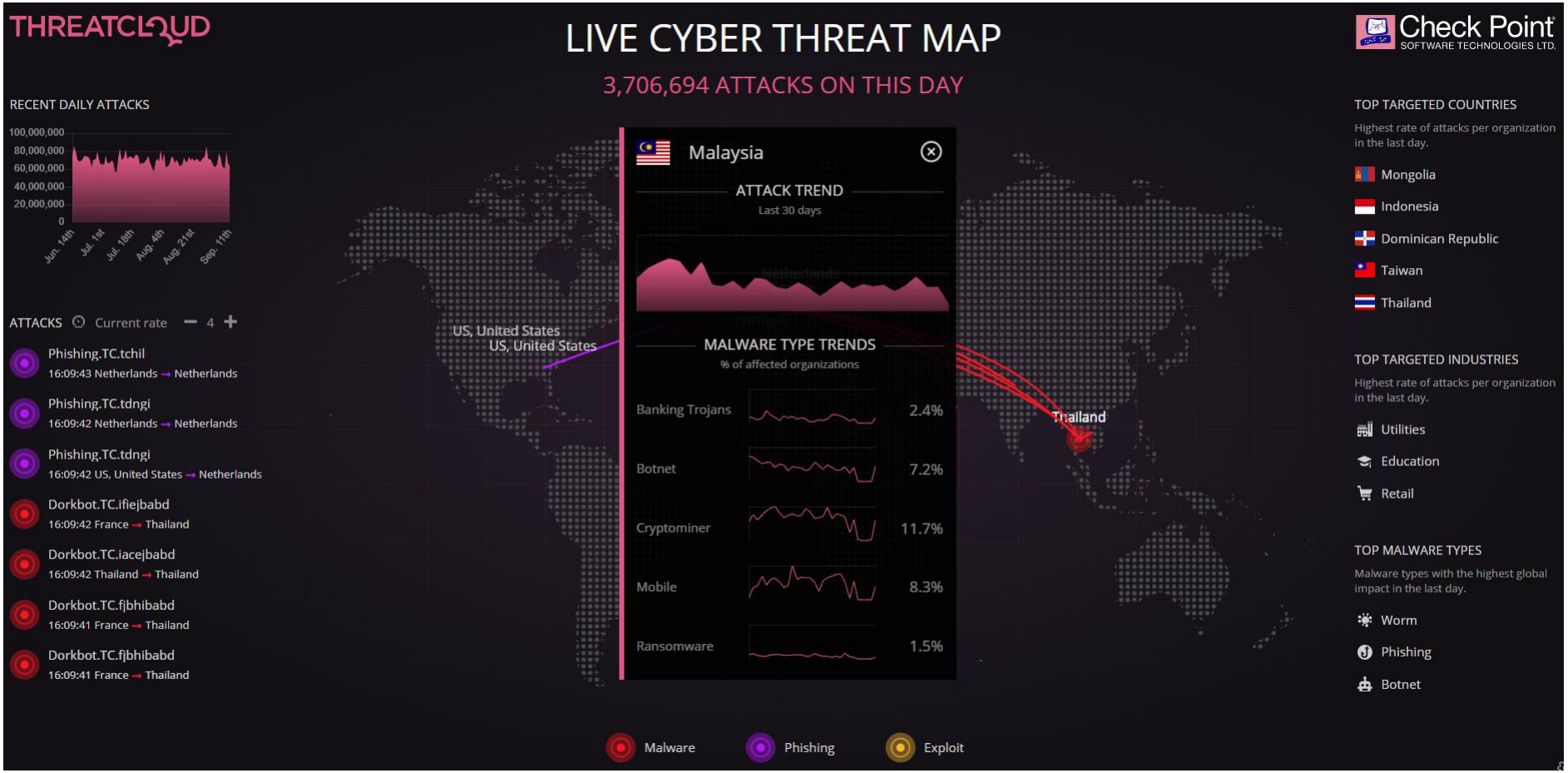
EFFECT & EVOLUTION

11 September 2017



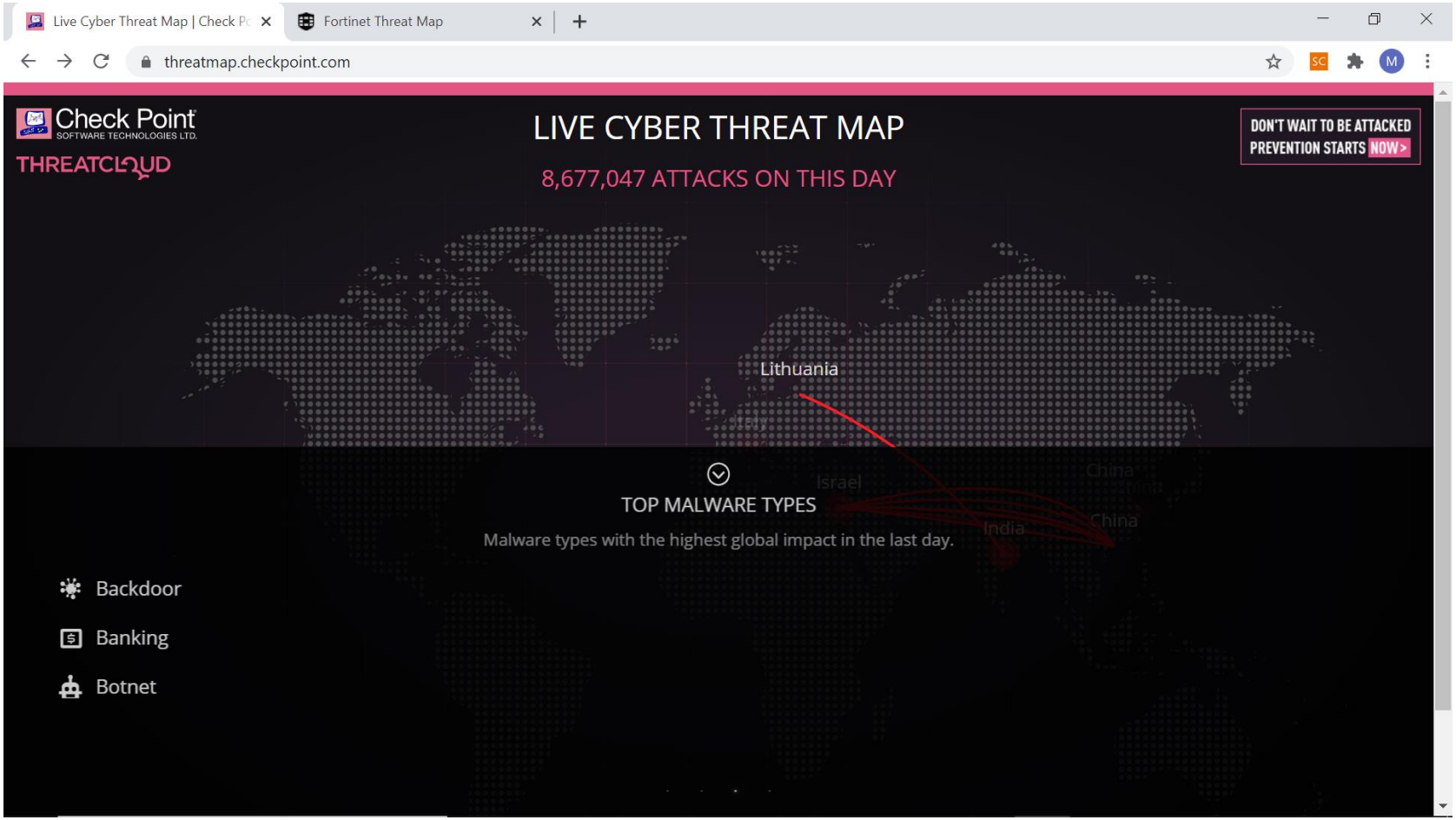
http://globe.f-secure.com/

12 September 2019

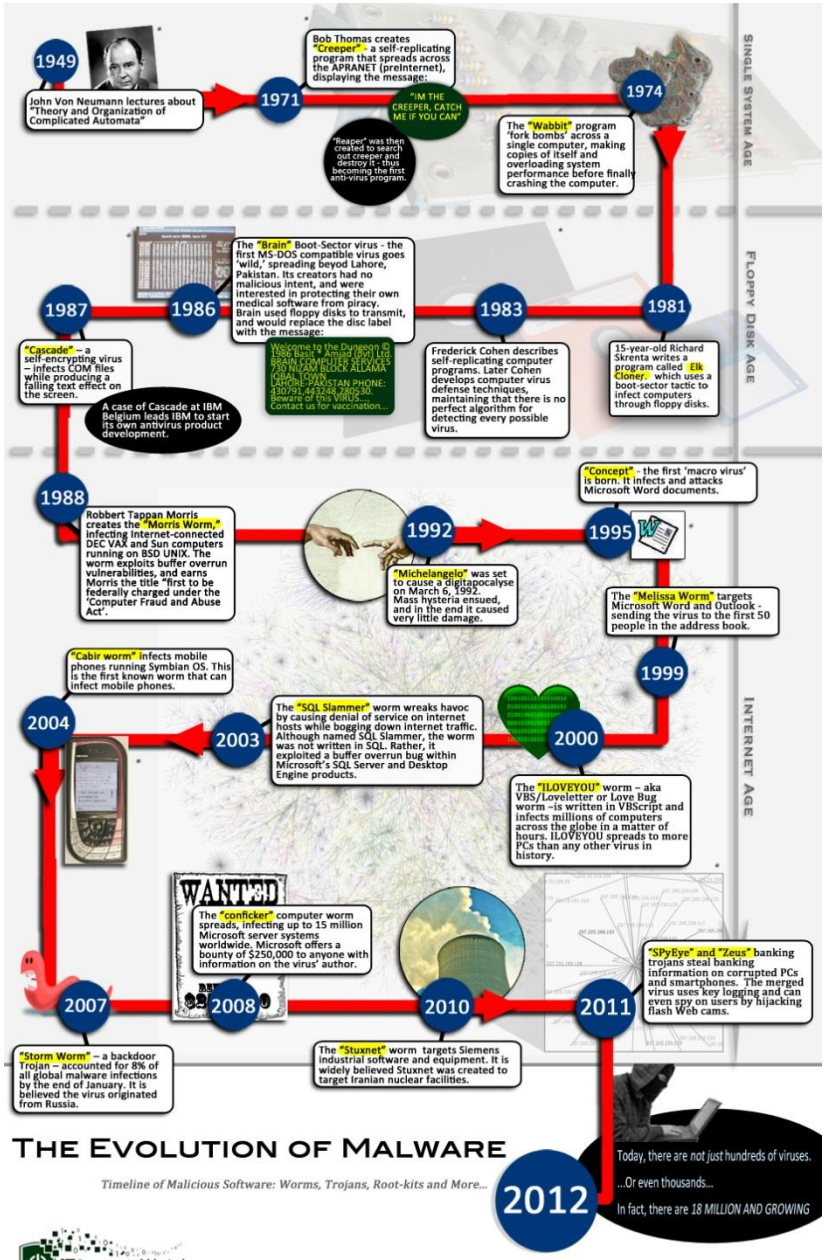


- https://threatmap.checkpoint.com/

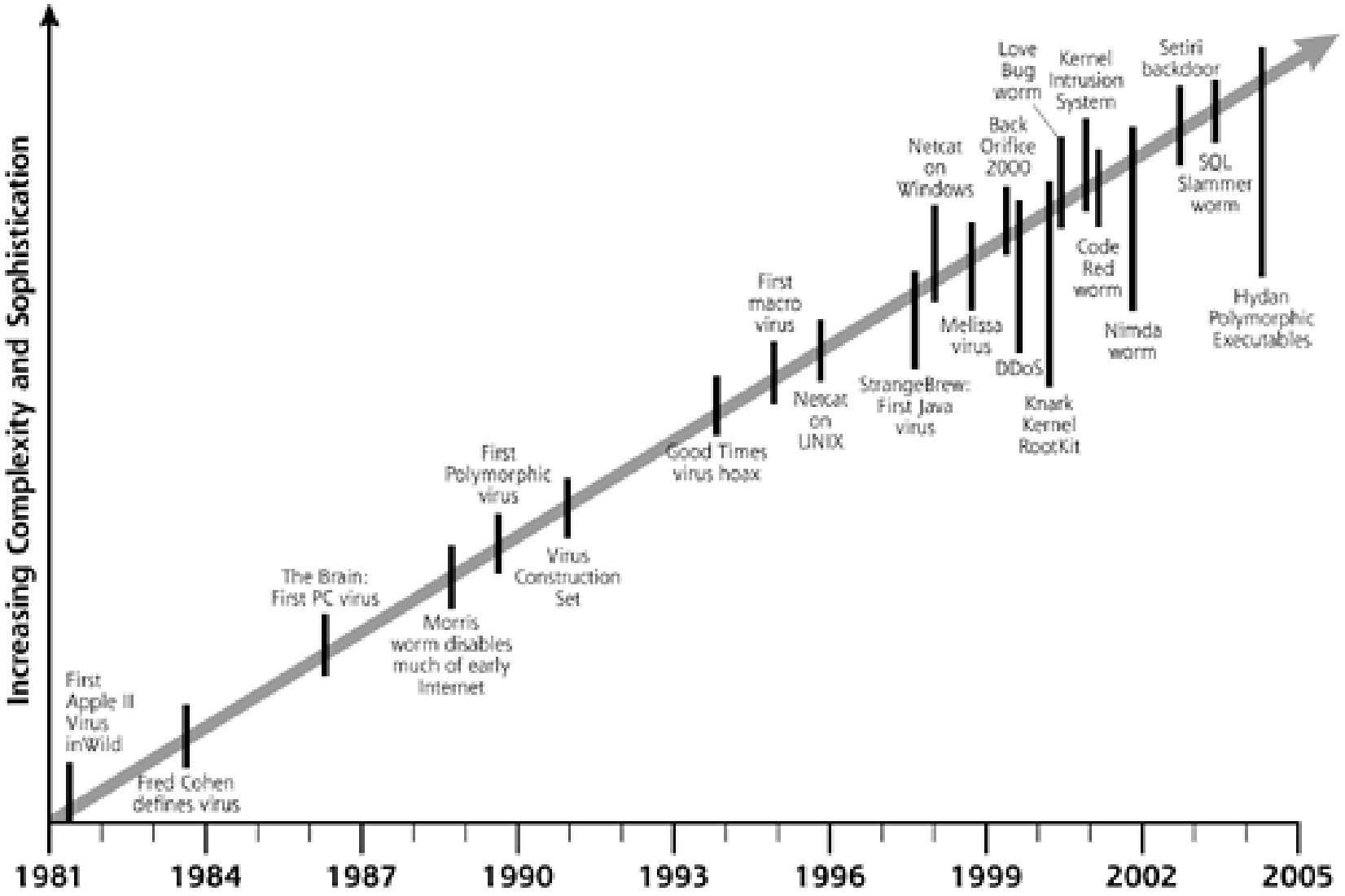
9 Oktober 2020



Malware Evolution


SINGLE SYSTEM AGE
FLOPPY DISK AGE
INTERNET AGE
1949
John Von Neumann lectures about "Theory and Organization of Complicated Automata"
1971
Bob Thomas creates "Creeper" - a self-replicating program that spreads across the APRANET (preInternet), displaying the message:
"IM THE CREEPER, CATCH ME IF YOU CAN"
'Reaper' was then created to search out creeper and destroy it - thus becoming the first anti-virus program.
1974
The "Wabbit" program 'fork bombs' across a single computer, making copies of itself and overloading system performance before finally crashing the computer.
1981
15-year-old Richard Skrenta writes a program called Elk Cloner. which uses a boot-sector tactic to infect computers through floppy disks.
1983
Frederick Cohen describes self-replicating computer programs. Later Cohen develops computer virus defense techniques, maintaining that there is no perfect algorithm for detecting every possible virus.
1986
The "Brain" Boot-Sector virus - the first MS-DOS compatible virus goes 'wild,' spreading beyod Lahore, Pakistan. Its creators had no malicious intent, and were interested in protecting their own medical software from piracy. Brain used floppy disks to transmit, and would replace the disc label with the message:
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...
1987
"Cascade" – a self-encrypting virus – infects COM files while producing a falling text effect on the screen.
A case of Cascade at IBM Belgium leads IBM to start its own antivirus product development.
1988
Robbert Tappan Morris creates the "Morris Worm," infecting Internet-connected DEC VAX and Sun computers running on BSD UNIX. The worm exploits buffer overrun vulnerabilities, and earns Morris the title "first to be federally charged under the 'Computer Fraud and Abuse Act'.
1992
"Michelangelo" was set to cause a digitapocalyse on March 6, 1992. Mass hysteria ensued, and in the end it caused very little damage.
1995
"Concept" - the first 'macro virus' is born. It infects and attacks Microsoft Word documents.
1999
The "Melissa Worm" targets Microsoft Word and Outlook - sending the virus to the first 50 people in the address book.
2000
The "ILOVEYOU" worm – aka VBS/Loveletter or Love Bug worm –is written in VBScript and infects millions of computers across the globe in a matter of hours. ILOVEYOU spreads to more PCs than any other virus in history.
2003
The "SQL Slammer" worm wreaks havoc by causing denial of service on internet hosts while bogging down internet traffic. Although named SQL Slammer, the worm was not written in SQL. Rather, it exploited a buffer overrun bug within Microsoft's SQL Server and Desktop Engine products.
2004
"Cabir worm" infects mobile phones running Symbian OS. This is the first known worm that can infect mobile phones.
2007
"Storm Worm" – a backdoor Trojan – accounted for 8% of all global malware infections by the end of January. It is believed the virus originated from Russia.
2008
WANTED
The "conficker" computer worm spreads, infecting up to 15 million Microsoft server systems worldwide. Microsoft offers a bounty of $250,000 to anyone with information on the virus' author.
2010
The "Stuxnet" worm targets Siemens industrial software and equipment. It is widely believed Stuxnet was created to target Iranian nuclear facilities.
2011
"SPyEye" and "Zeus" banking trojans steal banking information on corrupted PCs and smartphones. The merged virus uses key logging and can even spy on users by hijacking flash Web cams.
2012
Today, there are not just hundreds of viruses.
...Or even thousands...
In fact, there are 18 MILLION AND GROWING
THE EVOLUTION OF MALWARE
Timeline of Malicious Software: Worms, Trojans, Root-kits and More...
ITSecurityWatch
www.ITsecuritywatch.com
Follow Us!
* hover over images for source links.

Almost 30 years of Malware



Some well known malware

- 1981 First reported virus : Elk Cloner (Apple 2)
- 1983 Virus get defined
- 1986 First PC virus MS DOS
- 1988 First worm : Morris worm
- 1990 First polymorphic virus
- 1998 First Java virus
- 1998 Back orifice
- 1999 Melissa virus
- 1999 Zombie concept
- 1999 Knark rootkit
- 2000 love bug
- 2001 Code Red Worm
- 2001 Kernel Intrusion System
- 2001 Nimda worm
- 2003 SQL Slammer worm
- 2004 MyDoom
- 2006 Storm Worm
- 2007 Zeus
- 2013 CryptoLocker
- 2010 Stuxnet
- 2016 Petya
- 2017 WannaCry
- 2020 CovidLock

10 Prolific Malware of All Time

- ILOVEYOU
- CODE RED
- MELISA
- SASSER
- ZEUS
- CONFICKER
- NIMDA
- MY DOOM
- CRYPTOLOCKER
- WANNACRY

Mobile malware evolution

It took only one year for virus writers to adapt their malicious techniques for use on mobiles

Malicious users start stealing money from mobile user accounts

Decline of viruses written purely for vandalism purposes

93.9% of mobile malware targets Android. First mobile botnets on Android devices

10 million malicious Android apps ...and counting

First data theft on mobiles

First FakeAV for mobile

First iPhone malware

ZeuS – first malicious program designed for attacks on online banking customers

First malicious QR codes

First case of cyberespionage (Red October campaign) that collected data via mobile devices

Obad — the most sophisticated Android Trojan to date. Includes three exploits, a backdoor, SMS Trojan and bot capabilities

First backdoor for mobile platforms

First Trojan for mobile devices designed to steal user data

First virus for mobile phones

First Trojan to connect directly to mobile banking account

Malware modifications

Malware families

100 000

10 000

1 000

100

10

514

106

1000

153

6356

331

46415

469

148778

747

170

31

Symbian OS

Android OS

iPhone

iPad

2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

- Virus
- Trojan
- Backdoor

- Spreading via memory cards
- Damaging user data
- Disabling operating system security mechanisms
- Downloading other files from the Internet
- Calling paid services

- Mobile is used in cyberespionage
- Malware targets Android

Malware families

Malware modifications

© 1997 – 2014 Kaspersky Lab ZAO. All Rights Reserved. Industry-leading Antivirus Software KASPERSKY

- Malware remains a dangerous and consistent threat and its success has spawned a host of improved detection and prevention technologies. The resulting arms race means that the technologies of attackers continue to evolve in order to remain ahead of security vendors
- This has resulted in the constant invention of new fraud mechanics to evade existing security solutions, and commoditization in which cutting-edge limited circulation techniques are turned into mainstream capabilities.

What its do

- Steal sensitive information
- Unauthorized access
- Spying on the victims
- Delete files
- Click fraud
- Sending Spam Emails
- Steal software serial numbers
- Use your computer as relay or source of attack
- Locking up computer or files

The Symptom

- Blue Screen
- Increased CPU usage
- Slow computer or web browser speeds
- Problems connecting to networks
- Freezing or crashing
- Modified or deleted files
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs)
- Strange computer behaviour
- Emails/messages being sent automatically and without user's knowledge (a friend receives a strange email from you that you did not send)

Mobile symptom

- While these types of mobile malware differ greatly in how they spread and infect devices, they all can produce similar symptoms. Signs of a malware infection can include unwanted behaviours and degradation of device performance. Stability issues such as frozen apps, failure to reboot and difficulty connecting to the network are also common. Mobile malware can eat up battery or processing power, hijack the browser, send unauthorized SMS messages, freeze or brick the device entirely.

THE IMPACT OF MALWARE TO YOUR COMPUTER AND BUSINESS

Malware short for Malicious Software is used or programmed by attackers to disrupt computer operation, gather sensitive information or gain access to private computer systems

Malware's most common pathway from criminals to users is through the internet, primarily by email and the Worldwide Web

Microsoft reported in May 200 that 1 in 14 downloads from the internet may now contain malware code

32% of the time, Malicious content was hidden within social media behind shortened web links

Risks also increased as mobile devices were used for social media and web surfing more often

Only 1 in 5 emails sent were legitimate spam increased to 76% of email traffic

92% of spam included links to potentially malicious content

Methods that malicious software uses to infect your computer depends on its type

Virus, spyware and Trojan can infect the computer when the user runs the infected program

Malware is downloaded through the Web browser when the user visits an infected website

Worms can be particularly insidious as they can infect the computer without the user doing anything

- The computer becomes unstable
- The computer may crash, reboot, slow down
- The internet connection may become very slow
- Records the keys that you press on the keyboard
- Can damage an operating system so badly

How malware attacks impact businesses

- Disables Microsoft Windows services
- Attacks websites which can lead to big losses
- A potential intruder can access confidential data
- May hammer down a bank's networks
- Paying online poses an increased risk for users to be targeted
- Added repair expenses to infected systems
- Loss of valuable data
- Customer dissatisfaction

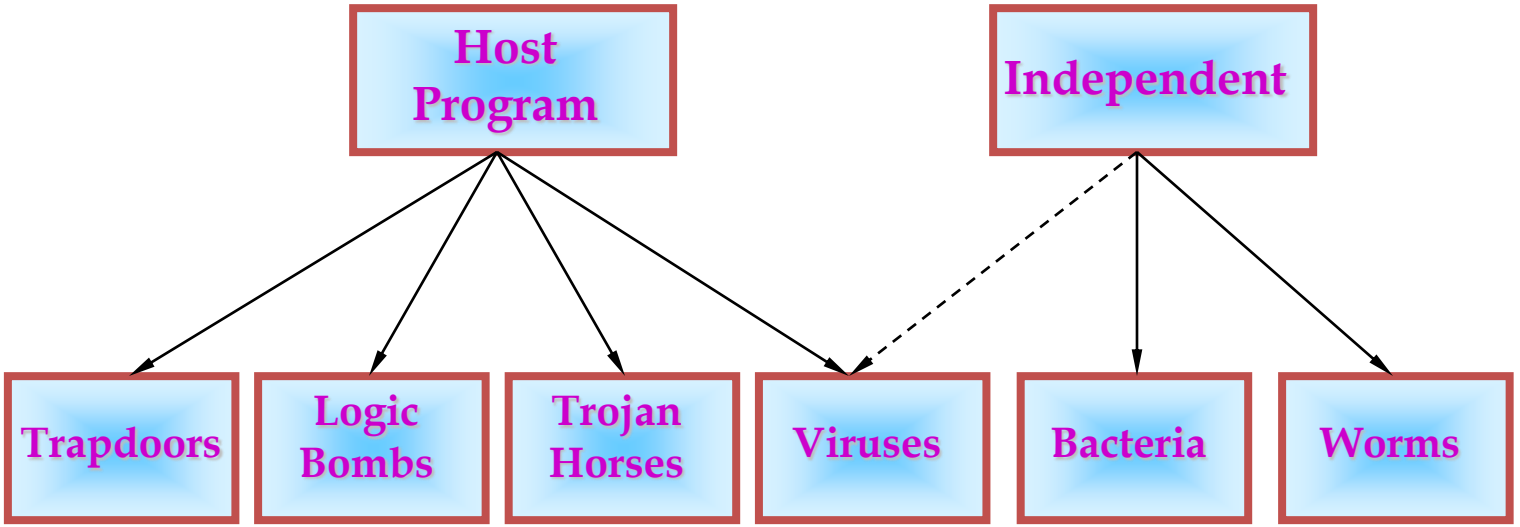
Prevention of Malware

- Avoid downloading and installing anything you do not understand and trust
- Leave the website if you are unsure
- Do not trust spam email and use caution when the message contains links or attachments
- Don't blindly accept disks or flash drives
- Close pop-up windows via Windows Task Manager
- Updated operating system
- Updated browser
- Antivirus software
- Anti-malware software
- Firewall
- Spam filter

DigitalDeliveryDownloads.com

TYPE OF MALWARE

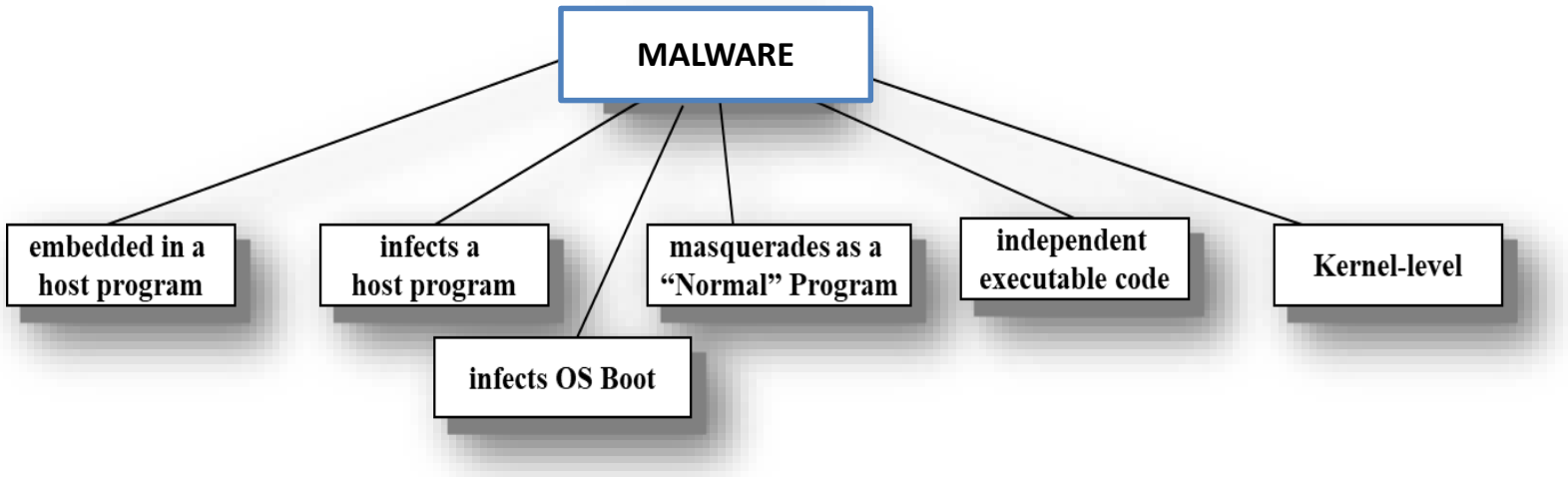
Taxonomy of Malware



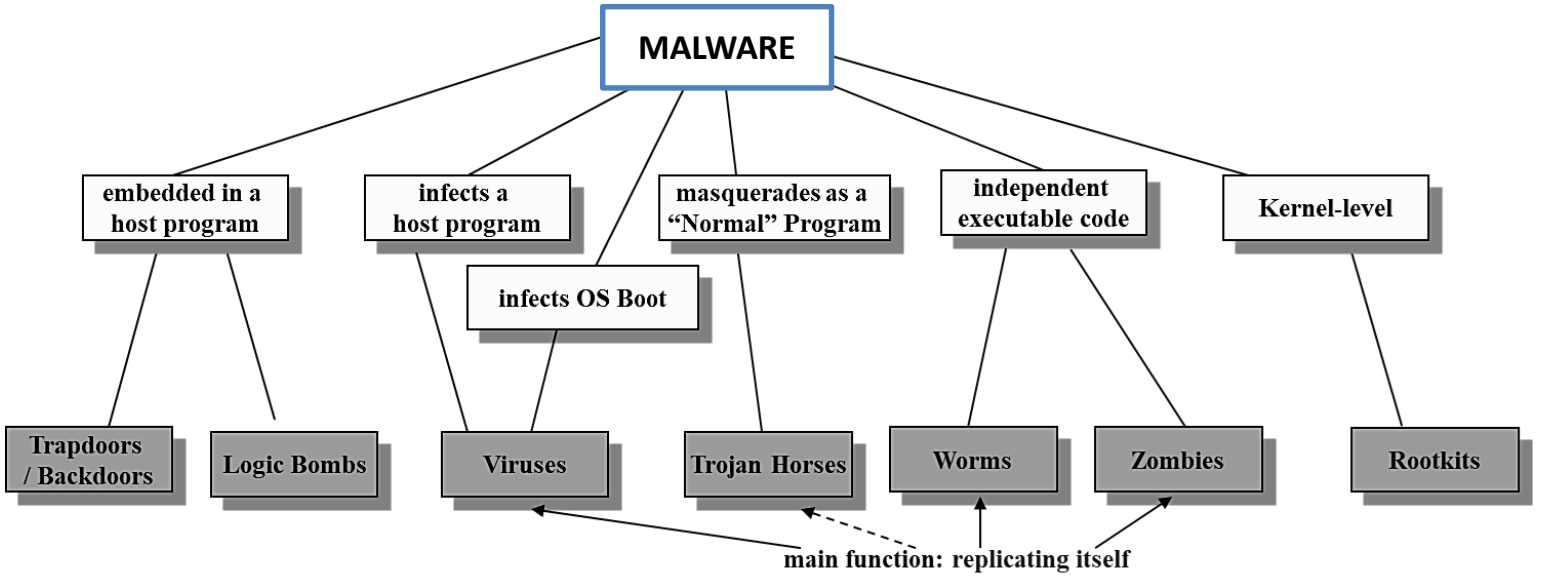
The Malware Type

- Virus
- Backdoor/Rootkit
- Bot/Zombie
- Trojan horse
- Scareware
- Adware
- Worm
- Ransomware
- Downloader or dropper

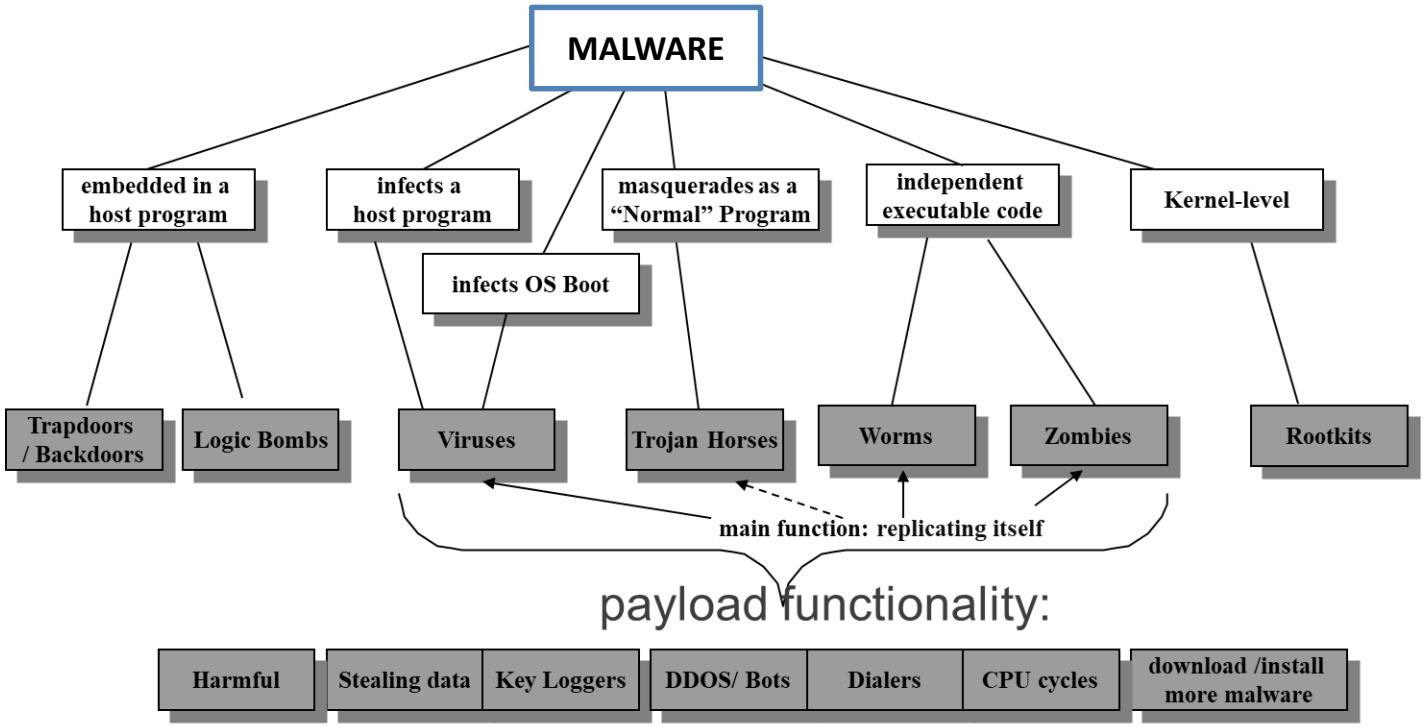
Malware Vector Infection



Malware Vector Infection



Malware Vector Infection + Payload



Virus

- A tiny program that able to exploit and negatively alters the way a computer works
- It have the ability to automatically replicating itself
- Done without user knowledge or intervention but still needs to be activated initially by the user. either time based or activity based
- Viruses often spread to other computers by attaching themselves to various programs and executing code when a
- Viruses can also spread through script files, documents, and cross-site scripting vulnerabilities in web apps.
- Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.

- *a program that can infect other programs by modifying them to include a, possibly evolved, version of itself*

- Fred Cohen 1983

Type of Virus

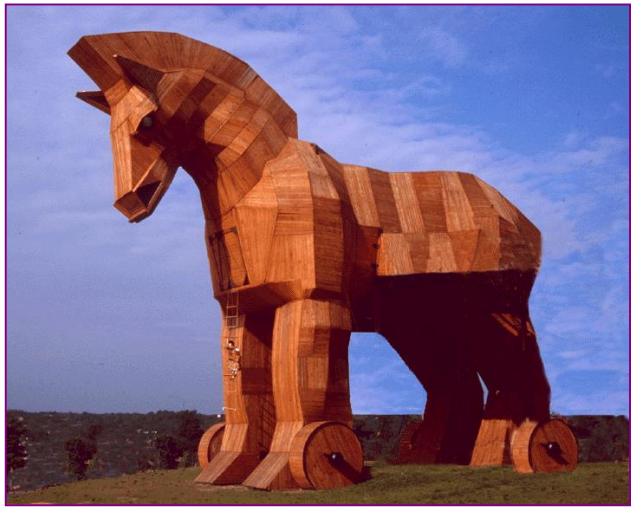
- Polymorphic : uses a polymorphic engine to mutate while keeping the original algorithm intact (packer)
- Metamorphic : Change after each infection

Rootkit/Backdoor

- A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs.
- Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet.
- Rootkit prevention, detection, and removal can be difficult due to their stealthy operation.
- Because a rootkit continually hides its presence, typical security products are not effective in detecting and removing rootkits.
- As a result, rootkit detection relies on manual methods such as monitoring computer behaviour for irregular activity, signature scanning, and storage dump analysis.
- Organizations and users can protect themselves from rootkits by regularly patching vulnerabilities in software, applications, and operating systems, updating virus definitions, avoiding suspicious downloads, and performing static analysis scans.

Trojan Horse

- type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware.
- give a malicious party remote access to an infected computer.
- Once an attacker has access to an infected computer, it is possible for the attacker to steal data (logins, financial data, even electronic money), install more malware, modify files, monitor user activity (screen watching, keylogging, etc), use the computer in botnets, and anonymize internet activity by the attacker.



Trojan is taken from….

- Like the gift horse left outside the gates of Troy by the Greeks, Trojan Horses appear to be useful or interesting to an unsuspecting user, but are actually harmful

Types of Trojans

- erasing or overwriting data on a computer
- corrupting files in a subtle way
- spreading other malware, such as viruses. In this case the Trojan horse is called a 'dropper'.
- setting up networks of zombie computers in order to launch DDoS attacks or send Spam.
- logging keystrokes to steal information such as passwords and credit card numbers (known as a key logger)
- phish for bank or other account details, which can be used for criminal activities.
- installing a backdoor on a computer system.

How can you be infected

- **Websites:** You can be infected by visiting a rogue website. Internet Explorer is most often targeted by makers of Trojans and other pests. Even using a secure web browser, such as Mozilla's Firefox, if Java is enabled, your computer has the potential of receiving a Trojan horse.

- **Instant message:** Many get infected through files sent through various messengers. This is due to an extreme lack of security in some instant messengers, such of AOL's instant messenger.

- **E-mail:** Attachments on e-mail messages may contain Trojans. Trojan horses via SMTP.

Sample Delivery

- Attacker will attach the Trojan to an e-mail with an enticing header
- The Trojan horse is typically a Windows executable program file, and must have an executable file extension such as .exe, .com, .scr, .bat, or .pif. Since Windows is configured by default to hide extensions from a user, the Trojan horse's extension might be "masked" by giving it a name such as 'Readme.txt.exe'. With file extensions hidden, the user would only see 'Readme.txt' and could mistake it for a harmless text file.

Where They Live

- Autostart Folder
  The Autostart folder is located in C:\Windows\Start Menu\Programs\startup and as its name suggests, automatically starts everything placed there.
- Win.ini
  Windows system file using load=Trojan.exe and run=Trojan.exe to execute the Trojan
- System.ini
  Using Shell=Explorer.exe trojan.exe results in execution of every file after Explorer.exe
- Wininit.ini
  Setup-Programs use it mostly; once run, it's being auto-deleted, which is very handy for trojans to restart

Where They Live(con't)

- Winstart.bat
  Acting as a normal bat file trojan is added as @trojan.exe to hide its execution from the user
- Autoexec.bat
  It's a DOS auto-starting file and it's used as auto-starting method like this -> c:\Trojan.exe
- Config.sys
  Could also be used as an auto-starting method for trojans
- Explorer Startup
  Is an auto-starting method for Windows95, 98, ME, XP and if c:\explorer.exe exists, it will be started instead of the usual c:\Windows\Explorer.exe, which is the common path to the file.

What the attacker wants?

- Credit Card Information (often used for domain registration, shopping with your credit card)
- Any accounting data (E-mail passwords, Dial-Up passwords, WebServices passwords, etc.)
- Email Addresses (Might be used for spamming, as explained above)
- Work Projects (Steal your presentations and work related papers)
- Children's names/pictures, Ages (pedophile attacker?!)
- School work (steal your papers and publish them with his/her name on it)

Well Know Trojans

- The Secup Trojan displays fake security related messages. When the user clicks on such a message the Trojan opens malicious web site that quietly installs potentially harmful software. Secup also serves undesirable commercial advertisements.
- Dmsys is a dangerous Trojan that specializes in infecting various instant messengers and stealing user confidential information. By using its keystroke logging technique, Dmsys easily steals user passwords and captures private conversations. This information is written into a log file, which is then sent to the hacker.

VNC

- Remote desktop program freely distributed
- Server executable attached to e-mail and unknowingly installed on your system
- Attacker can use client to uses your system as if he was sitting at the terminal

Bot/Zombie

- Bots are software programs created to automatically perform specific operations.
- While some bots are created for relatively harmless purposes (video gaming, internet auctions, online contests, etc), it is becoming increasingly common to see bots being used maliciously.
- Bots can be used in botnets (collections of computers to be controlled by third parties) for DDoS attacks, as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites.
- Websites can guard against bots with CAPTCHA tests that verify users as human.

The Estonian case

- In April 2007, Estonia which is one of the Baltic States has become one of the victims of such attack, the communication and the online activities of the country were put to a standstill [1]
- Economic losses incurred as online based transactions were disrupted

What Cause it ?

- The attack was cause by a massive distributed denial-of service (DDoS) attack that originated from around the world.
- Those attack origin are coming from thousand of computers that are remotely controlled by a perpetrator that can be located anywhere across the globe
- The computer has been compromised and called as **BOTNET or zombies**

More recent Botnet DDoS

Biggest DDoS attack was directed at Dyn, a major DNS provider, in October of **2016**. This attack was devastating and created disruption for many major sites, including **AirBnB, Netflix, PayPal, Visa, Amazon, The New York TImes, Reddit, and GitHub**. This was done using a **malware called Mirai**. Mirai creates a botnet out of **compromised Internet of Things (IoT)** devices such as cameras, smart TVs, radios, printers, and even baby monitors. To create the attack traffic, these compromised devices are all programmed to send requests to a single victim.

What Botnet do?

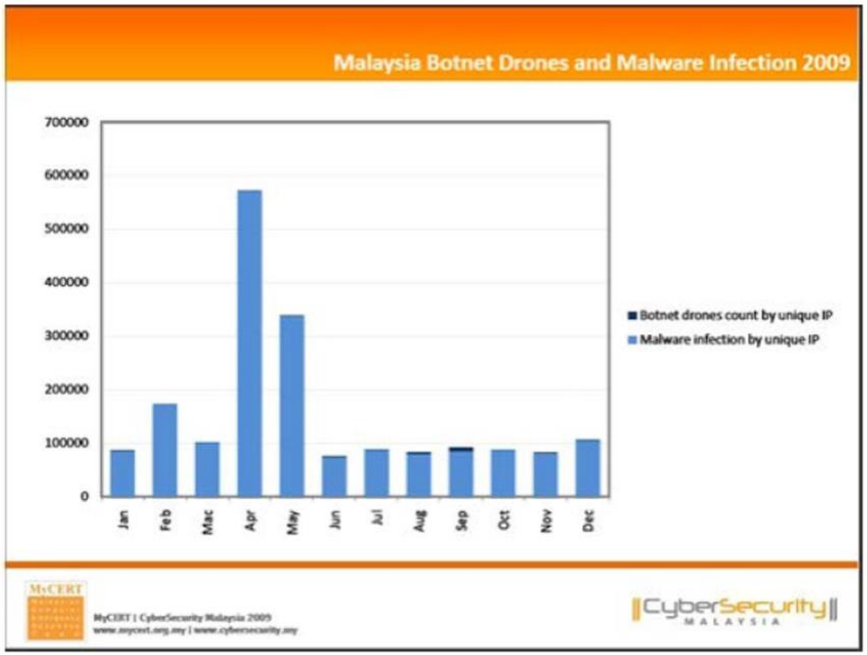
- It is part of malware that exploit and recruit Computer to become army for cyber attack.
- It can be used for [3]:-
  - DDoS attack
  - Distribute Malware
  - Spamming
  - phishing
  - Stealing credential Information
  - Proxies
  - ClickThrough Fraud

In Malaysia

Incidents report by CyberSecurity Malaysia show an increase in Botnet drones from 2009 to 2018

MyCERT Incidence Report

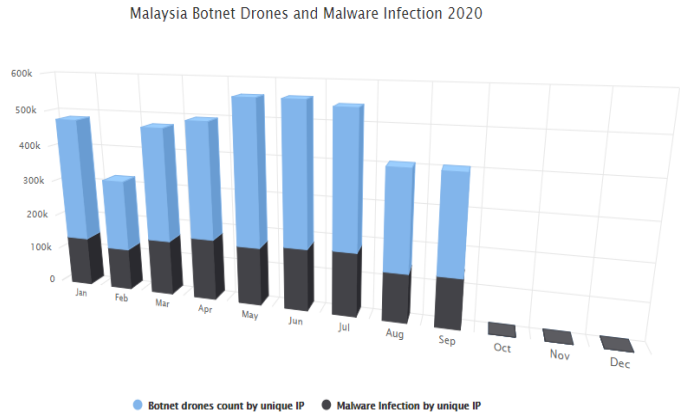
Botnet Drones 2009



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Botnet drones count by unique IP	905	405	268	304	1197	1855	1301	3548	7987	686	937	1497	20890
Malware infection by unique IP	86111	172658	101269	571998	337718	74048	86648	79820	84512	86783	81912	104798	1868275
TOTAL	87016	173063	101537	572302	338915	75903	87949	83368	92499	87469	82849	106295	1889165

20,890 drones

Botnet Drones 2020 until Oct.



#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Botnet drones count by unique IP	339,810	196,358	313,161	320,811	396,133	384,765	367,486	269,594	264,929	0	0	0	2,853,047
Malware infection by unique IP	137,384	117,440	154,712	170,922	160,586	171,490	174,290	133,039	135,957	0	0	0	1,355,820
	477,194	313,798	467,873	491,733	556,719	556,255	541,776	402,633	400,886	0	0	0	4,208,867

2,853,047drones

Worms

- Computer worms are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers. Computer worms can also contain “payloads” that damage host computers. Payloads are pieces of code written to perform actions on affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data, delete files, or create botnets.
- Computer worms can be classified as a type of computer virus, but there are several characteristics that distinguish computer worms from regular viruses. A major difference is that computer worms have the ability to self-replicate and spread independently while viruses rely on human activity to spread (running a program, opening a file, etc). Worms often spread by sending mass emails with infected attachments to users’ contacts.

Worm

- A worm is self-replicating software designed to spread through the network
  - Typically, exploit security flaws in widely used services
  - Can cause enormous damage
    - Launch DDOS attacks, install bot networks
    - Access sensitive information
    - Cause confusion by corrupting the sensitive information

- Worm vs Virus vs Trojan horse
  - A virus is code embedded in a file or program
  - Viruses and Trojan horses rely on human intervention
  - Worms are self-contained and may spread autonomously

Cost of worm attacks

- Morris worm, 1988
  - Infected approximately 6,000 machines
    - 10% of computers connected to the Internet
  - cost ~ $10 million in downtime and cleanup
- Code Red worm, July 16 2001
  - Direct descendant of Morris' worm
  - Infected more than 500,000 servers
    - Programmed to go into infinite sleep mode July 28
  - Caused ~ $2.6 Billion in damages,
- Love Bug worm: $8.75 billion

– Statistics: Computer Economics Inc., Carlsbad, California

Internet Worm (First major attack)

- Released November 1988
  - Program spread through Digital, Sun workstations
  - Exploited Unix security vulnerabilities
    - VAX computers and SUN-3 workstations running versions 4.2 and 4.3 Berkeley UNIX code
- Consequences
  - No immediate damage from program itself
  - Replication and threat of damage
    - Load on network, systems used in attack
    - Many systems shut down to prevent further attack

Some historical worms of note

Worm	Date	Distinction
Morris	11/88	Used multiple vulnerabilities, propagate to “nearby” sys
ADM	5/98	Random scanning of IP address space
Ramen	1/01	Exploited three vulnerabilities
Lion	3/01	Stealthy, rootkit worm
Cheese	6/01	Vigilante worm that secured vulnerable systems
Code Red	7/01	First sig Windows worm; Completely memory resident
Walk	8/01	Recompiled source code locally
Nimda	9/01	Windows worm: client-to-server, c-to-c, s-to-s, …
Scalper	6/02	11 days after announcement of vulnerability; peer-to-peer network of compromised systems
Slammer	1/03	Used a single UDP packet for explosive growth

Kienzle and Elder

Increasing propagation speed

- Code Red, July 2001
  - Affects Microsoft Index Server 2.0,
    - Windows 2000 Indexing service on Windows NT 4.0.
    - Windows 2000 that run IIS 4.0 and 5.0 Web servers
  - Exploits known buffer overflow in Idq.dll
  - Vulnerable population (360,000 servers) infected in 14 hours
- SQL Slammer, January 2003
  - Affects in Microsoft SQL 2000
  - Exploits known buffer overflow vulnerability
    - Server Resolution service vulnerability reported June 2002
    - Patched released in July 2002 Bulletin MS02-39
  - Vulnerable population infected in less than 10 minutes

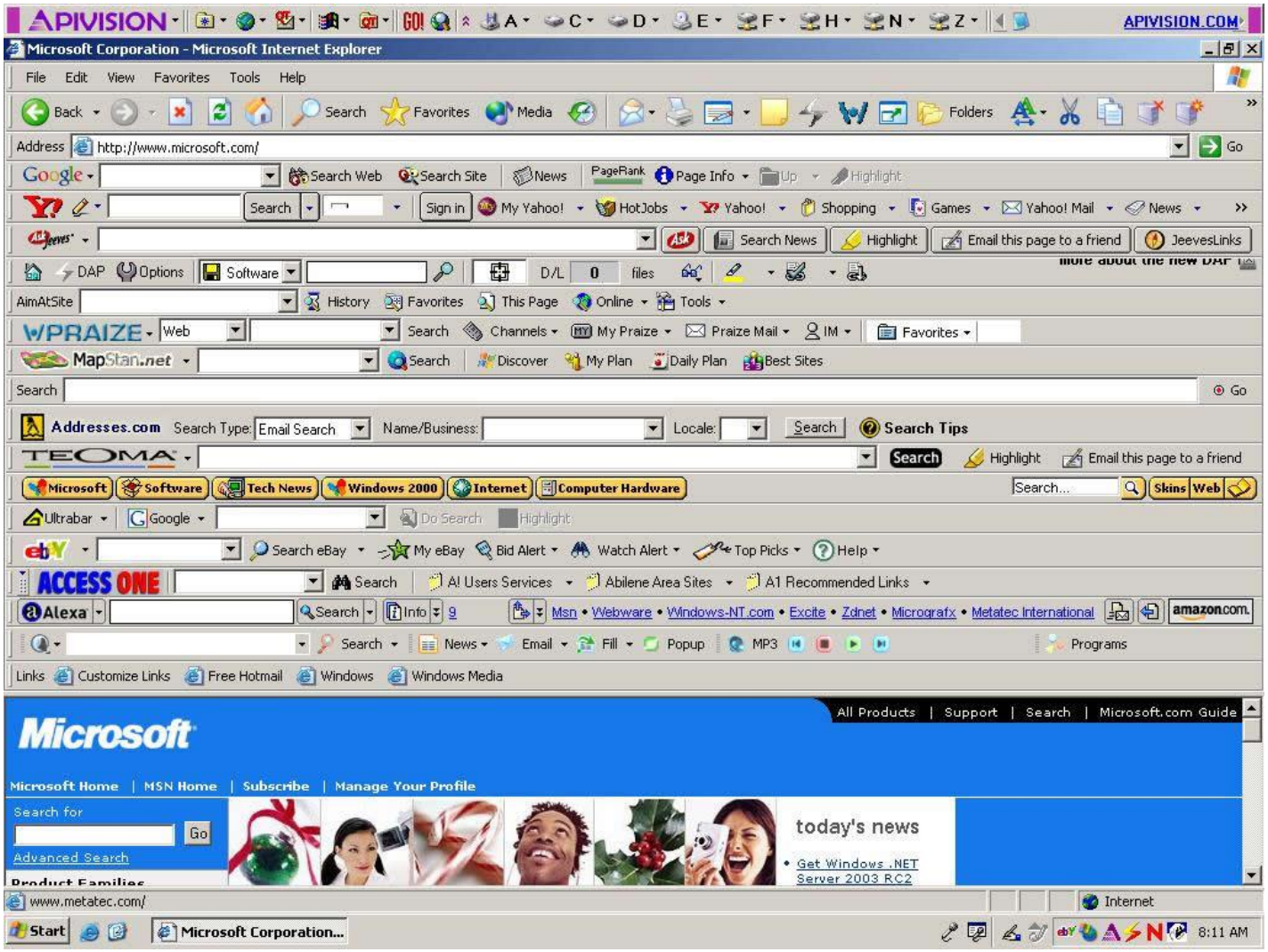
Spyware/Adware

- spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections. Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans.
- Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements. common examples of adware include pop-up ads on websites and advertisements that are displayed by software. Often times software and applications offer “free” versions that come bundled with adware. Most adware is sponsored or authored by advertisers and serves as a revenue generating tool.
- While some adware is solely designed to deliver advertisements, it is not uncommon for adware to come bundled with spyware (see below) that is capable of tracking user activity and stealing information. Due to the added capabilities of spyware, adware/spyware bundles are significantly more dangerous than adware on its own.

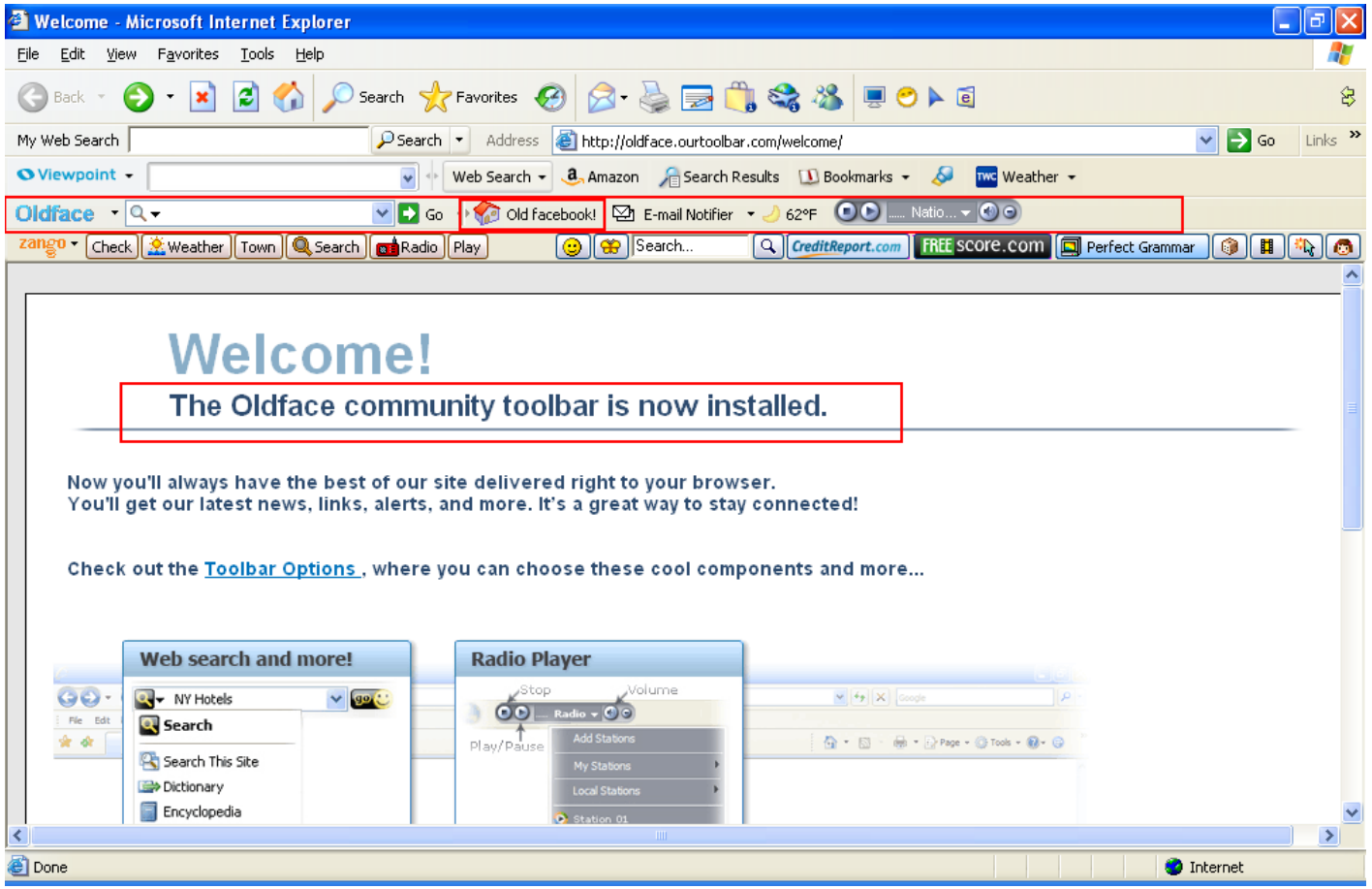
Adware


Free connection
Free modem
Click here to find out more
BT
INSWEB
Lower your insurance costs.
Enter to WIN!
XEROX
WIN an $11,000 USD
Business Upgrade Package
or a Xerox Phaser® 8400
Color Printer
World's fastest color printer
for under $1,000 USD.
Phaser 8400
Color Printer
$999
of coffee,
TRY 2 RISK-FREE ISSUES!
Netscape What's New
Science Proves It: Drinking Causes...
Teen Girls Beware: Popular Boys Do THIS
Look What Was Found in Stone Age Cave
Strange Space Object Mystery Deepens
Did You See What Bush Dared to Wear?
If You Get This E-Mail Scam, Delete It
15 FREE POWER GUIDES
Before you go, did you know....
You can add AOL® for Broadband to any high-speed cable or DSL connection!
Works with and enhances any basic high-speed connection
Built-in protection for you and your family
The best on-demand and exclusive programming online
GET A FREE TRIAL!
Up to 45 days FREE
Click here for details
Home-Owners Click Here
AMERIQUEST MORTGAGE COMPANY®
Are You Paying Too
Rates are at Hist
Get cas
your h
HomeLoanCenter.com
TRAVELZOO
This Week's
on the Interne
Released APRIL 14
Song
CheapCaribbean.c
ReliaQuot
A better way to buy life insura
Take this free test!

Browser Toolbar ...



Toolbar again

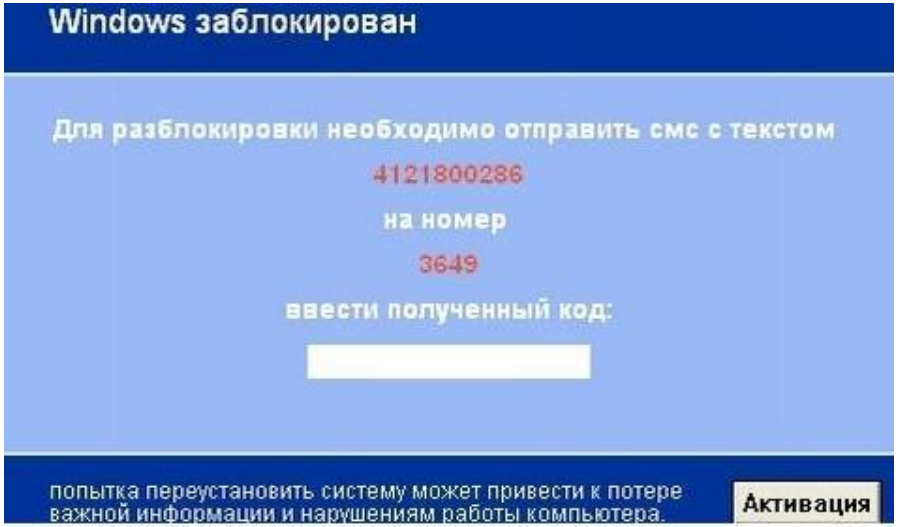


Ransomware

- Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom.
- The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove
- Ransomware typically spreads like a normal computer worm (see below) ending up on a computer via a downloaded file or through some other vulnerability in a network service.

e.g

- Trj/SMSlock.A
- Russian ransomware
- April 2009



To unlock you need to send an SMS with the text4121800286to the number3649Enter the resulting code:Any attempt to reinstall the system may lead to loss of important information and computer damage

- Although ransomware that locks files until victims pay to restore them has existed for many years, it became more prevalent after the Gameover Zeus botnet operators introduced the once widespread but now-defunct CryptoLocker malware in early February 2015.
- An early TeslaCrypt sample was uploaded to the VirusTotal analysis service on November 11, 2014, but TeslaCrypt was not widely distributed until early March 2015.
- The TeslaCrypt operators mimicked CryptoLocker in the warning screen

SPAM

- spam is the electronic sending of mass unsolicited messages.
- The most common medium for spam is email, but it is not uncommon for spammers to use instant messages, texting, blogs, web forums, search engines, and social media.
- While spam is not actually a type of malware, it is very common for malware to spread through spamming. This happens when computers that are infected with viruses, worms, or other malware are used to distribute spam messages containing more malware.
- Users can prevent getting spammed by avoiding unfamiliar emails and keeping their email addresses as private as possible.

Mobile spyware & adware

- Spyware secretly gathers confidential information about the mobile user and then relays this data to a third party. In some cases these may be advertisers or marketing data firms, which is why spyware is sometimes referred to as “adware”. It is typically installed without user consent by disguising itself as a legitimate app (say, a simple game) or by infecting its payload on a legitimate app. Spyware uses the victim’s mobile connection to relay personal information such as contacts, location, messaging habits, browser history and user preferences or downloads. Spyware that gathers device information such as OS version, product ID, International Mobile Equipment Identitiy (IMEI) number, and International Mobile Subscriber Identity (IMSI) number can be used for future attacks.

Mobile trojan

- Mobile Trojans infect user devices by attaching themselves to seemingly harmless or legitimate programs, are installed with the app and then carry out malicious actions. Such programs have been known to hijack the browser, cause the device to automatically send unauthorized premium rate texts, or capture user login information from other apps such as mobile banking. Trojans are closely related to mobile viruses, which can become installed on the device any number of ways and cause effects that range from simply annoying to highly-destructive and irreparable. Malicious parties can potentially use mobile viruses to root the device and gain access to files and flash memory.

Mobile phishing

- Mobile browsing of the internet is growing with smartphone and tablet penetration. Just as with desktop computing, fraudsters are creating mobile phishing sites that may look like a legitimate service but may steal user credentials or worse. The smaller screen of mobile devices is making malicious phishing techniques easier to hide from users less sophisticated on mobile devices than PCs. Some phishing schemes use rogue mobile apps, programs which can be considered “trojanized”, disguising their true intent as a system update, marketing offer or game. Others infect legitimate apps with malicious code that’s only discovered by the user after installing.

Mobile bot

- Mobile malware is getting more sophisticated with programs can operate in the background on the user device, concealing themselves and lying in wait for certain behaviors like an online banking session to strike. Hidden processes can execute completely invisible to the user, run executables or contact botmasters for new instructions. The next wave is expected to be even more advanced, with botnet tendencies to actually hijack and control infected devices.

Advance Persistence Threat (APT)

- Do some Research on this ……..

MALWARE TARGET

What is Malware Targeting

- Executable
- Interpreted file(doc,ppt, pdf,ps)
- Kernel
- Service
- MBR
- Hypervisor

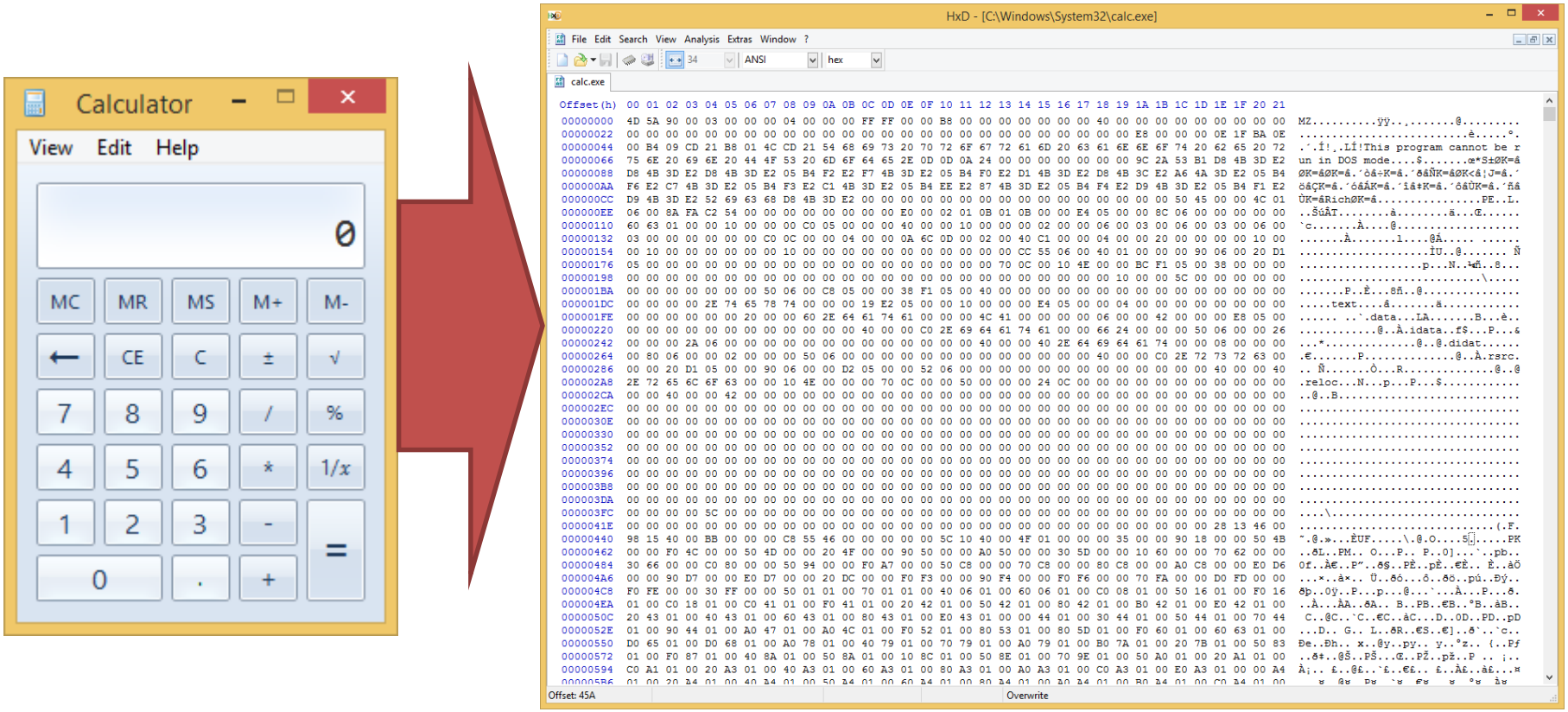
EXECUTABLE FILE FORMAT

An exe file.

- In windows binary file such as .exe or .dll normally called as executable file.
- It is a set of instruction in a machine language.
- To produce an executable file or program or software you'll used

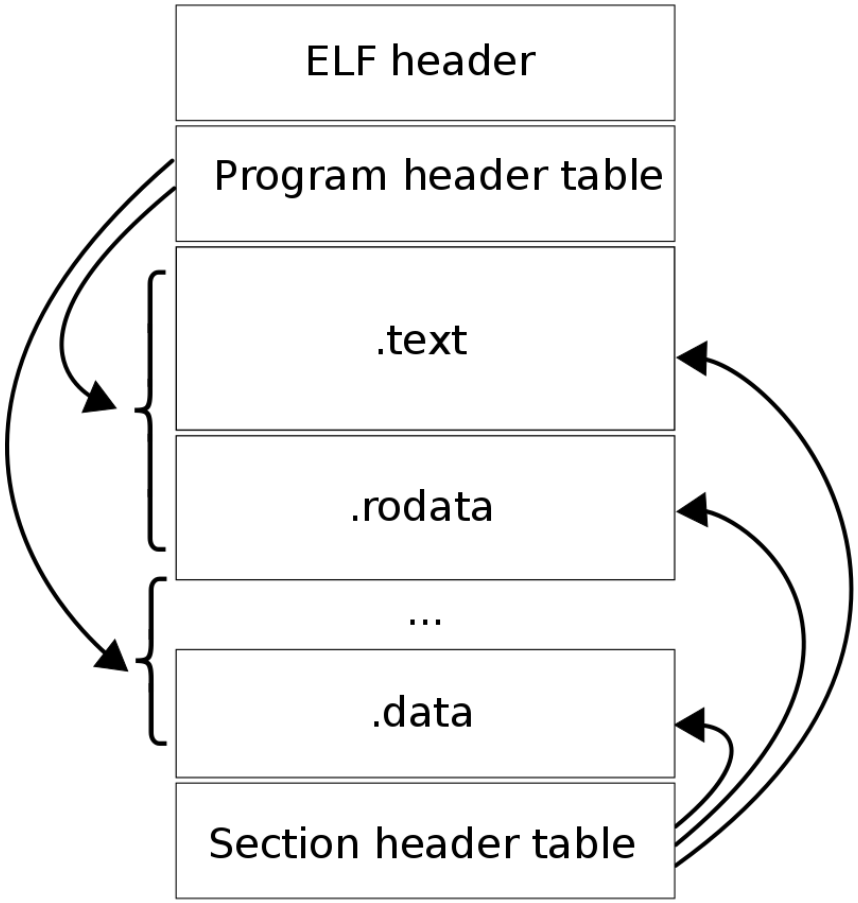
a programming language -> **compile**-> **binary file**

By using HxD editor



PE and ELF

- PE (Portable Executable)
  - "File format for executables, object code and DLLs, used in 32-bit and 64-bit versions of **Windows operating systems**"
- ELF (Executable and Linkable Format)
  - "A common standard file format for executables, object code, shared libraries, and core dumps"
  - Linux, Unix, Apple OS

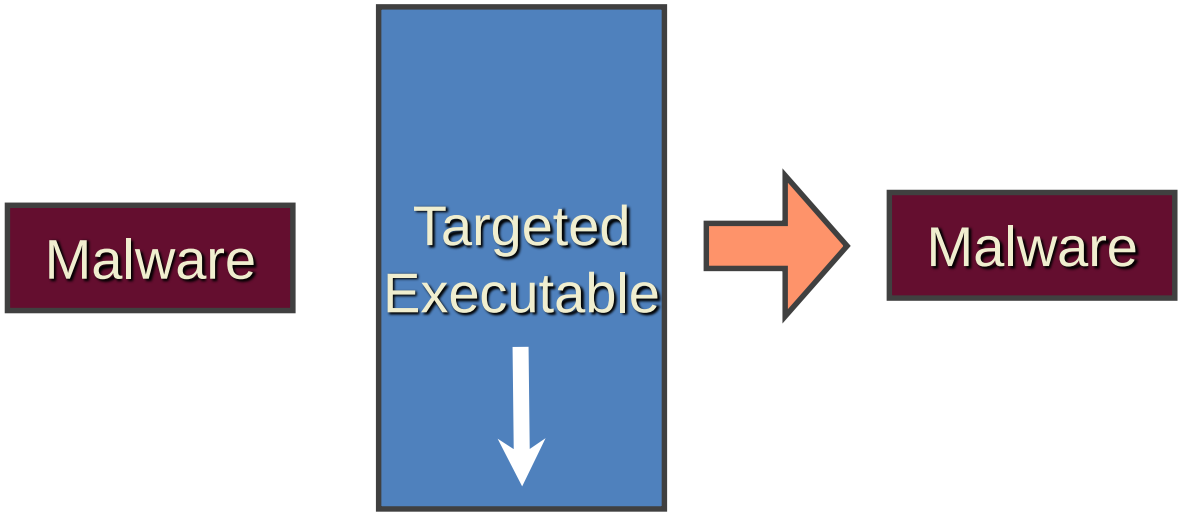


PE File Format

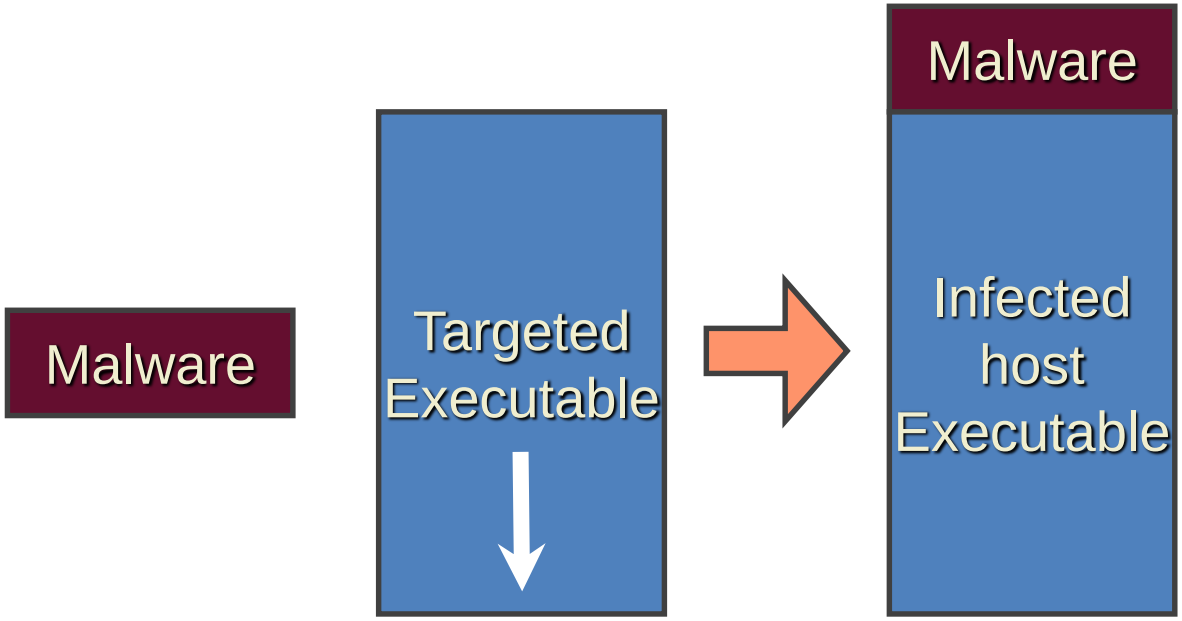
MS-DOS MZ Header
MS-DOS Real-Mode Stub Program
PE File Signature
PE File Header
PE File Optional Header
.text Section Header
.bss Section Header
.rdata Section Header
. . .
.debug Section Header
.text section
.bss Section
.rdata Section
. . .
.debug section

HOW MALWARE IS EMBEDDED IN CODE

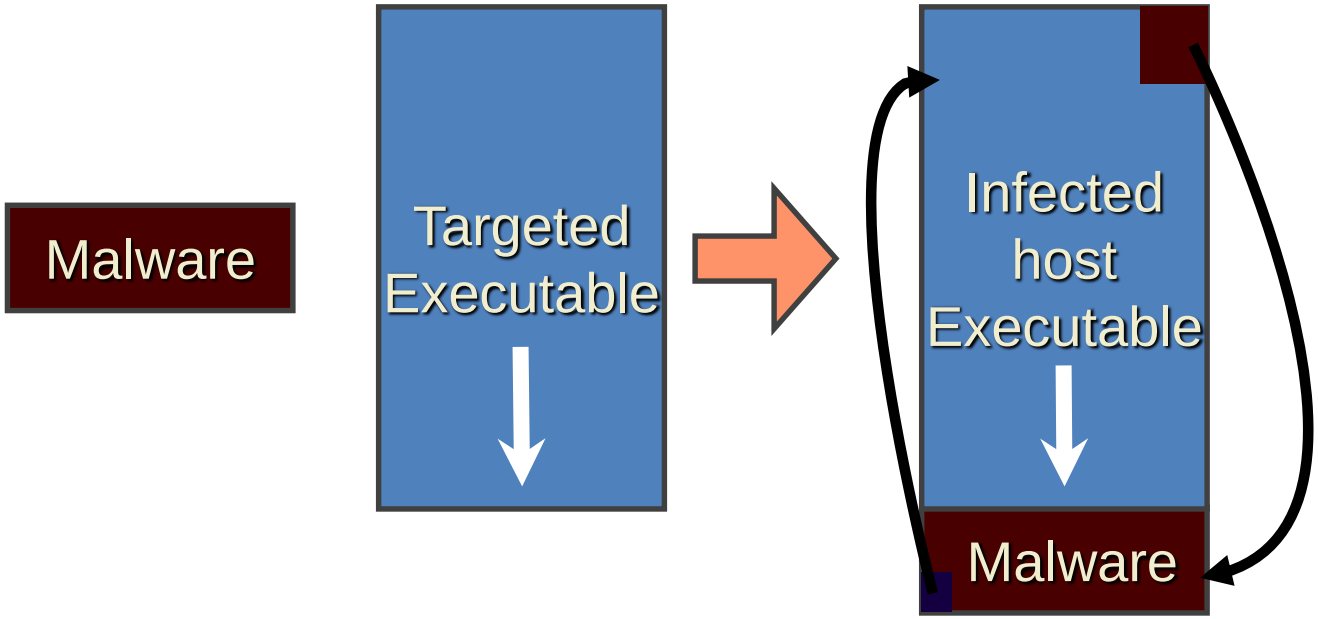
Overwriting malware



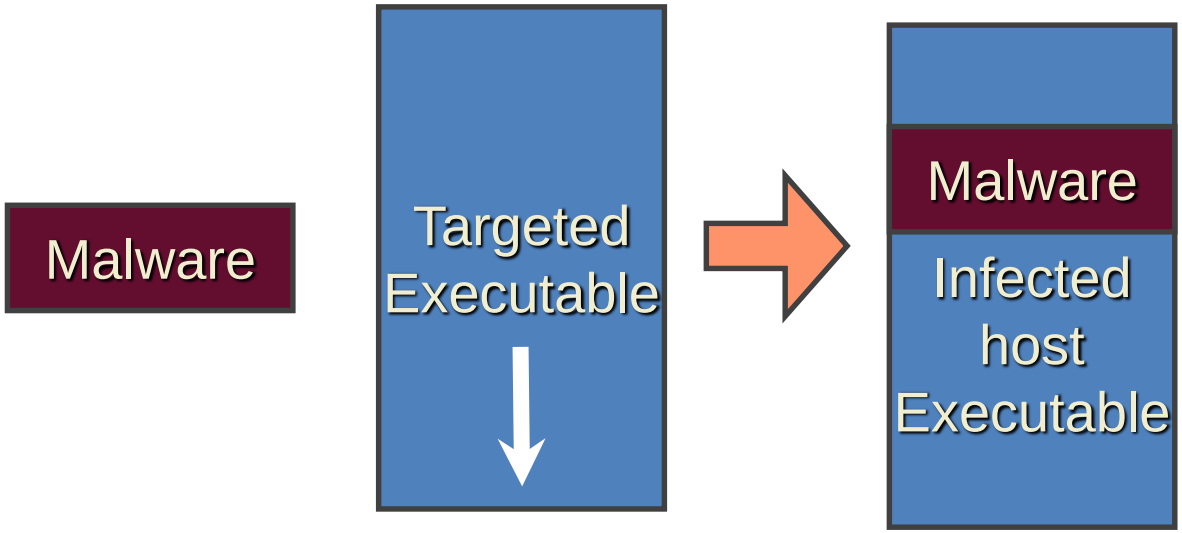
Prepending malware



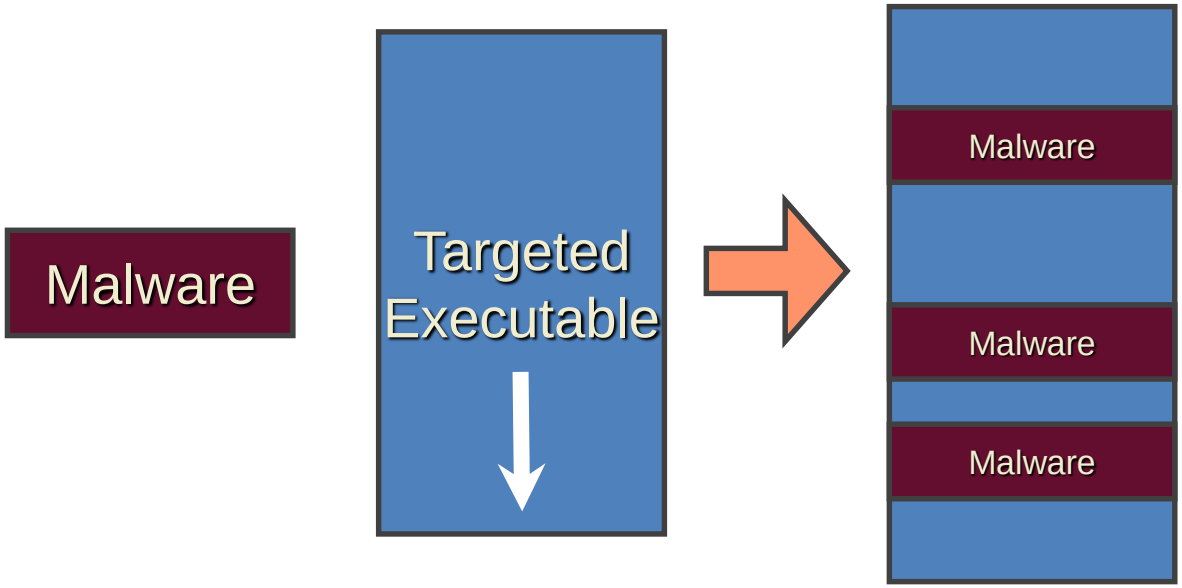
Appending malware



Cavity malware



Multi-Cavity malware



Summary

- Malware stand as Malicious Software, a program that is purposely written for the destruction of the target.
- The evolution of malware is rapid. Nowadays it is more complex and sophisticated
- Virus, Trojan, Rootkit, Botnet, Adware, Ransomware, Spam and worm are types of malware.
- Malware can embed itself to the program in several ways.