
CMSC 449

Malware Analysis

Lecture 1

Introduction to Malware Analysis

Categories of Malware

- Malware can be categorized based on factors such as:
 - How it spreads/persists
 - What it does
 - What kinds of systems it targets

- A single piece of malware can belong to more than one classification within a category
 - Classifications are fuzzy and overlap
 - These are just general guidelines, not a taxonomy

Categories of Malware

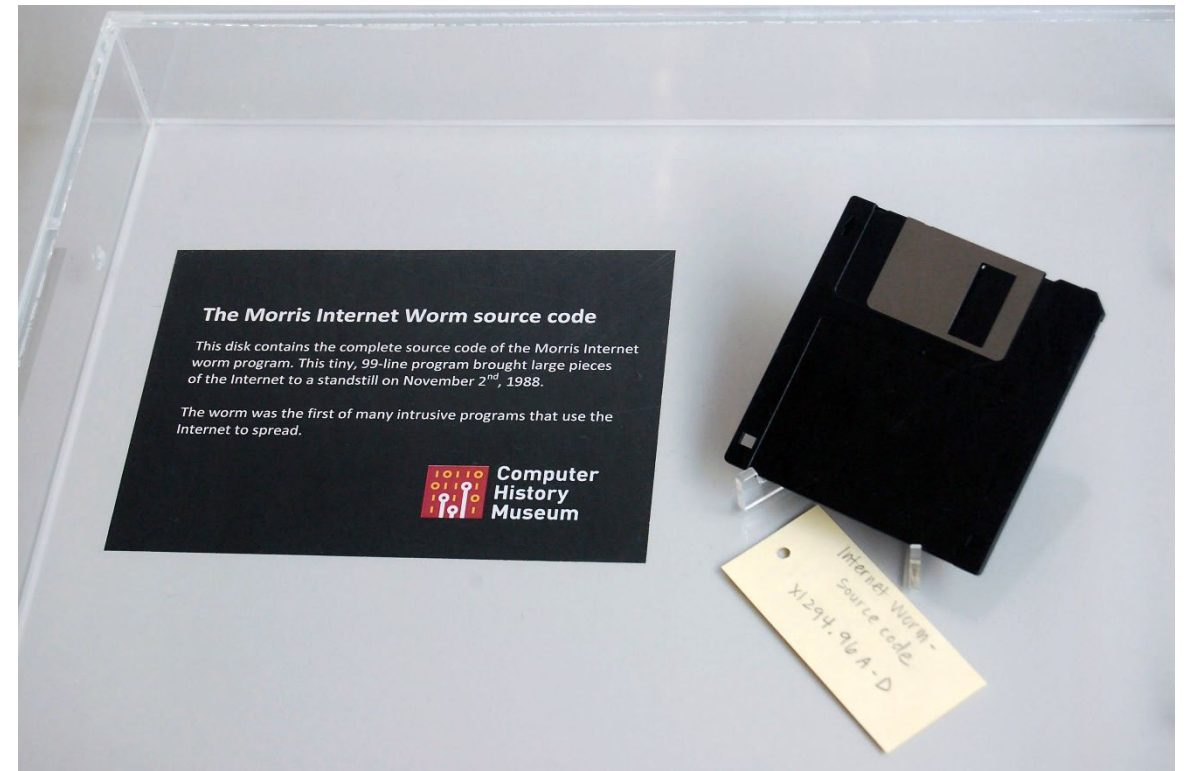
How it Spreads

Worm

- Standalone program
- Replicates itself and spreads automatically
 - Attempt to infect as many computers as possible
- Usually exploits a vulnerability to do so
 - Or uses previously captured authorization credentials

Worm Example: Morris Worm

- Released by grad student Robert Morris in November 1988
 - Claimed it was meant to gauge the size of the Internet
 - Debate over his true intentions
- Infected about 10% of computers connected to the Internet in 1988
- Spreading mechanism led it to re-infect machines, which slowed or crashed them



Worm Example: Morris Worm (cont)

- Once it was on a system, it obtained a list of all known hosts that would allow entry from the current host
- Then tried to gain access to each one, by either
 1. Attempting to log on as a legitimate user, using a simplified brute force method of password cracking
 2. Exploit a bug in the **finger** protocol
 3. Exploit the debug option of the mail receiving program
- Infected systems would respond they were infected
 - 1 out of 7 times, the worm would propagate regardless

File Infector

- Also commonly called a virus
 - (But *not all malware* is a virus! Watch your language!)
- Inserts its own code into executable files to persist and spread
 - Code is now “infected code”
 - When the infected executable is run, the virus also executes
- Virus is spread when the infected executable is copied onto another system or otherwise spread

Trojan (or Trojan Horse)

- Malicious program that appears to have a useful function
- Often spread by social engineering
 - Executing email attachments
 - Clicking on advertisements
- Payloads can be a variety of things, including backdoors, ransomware, etc.



Categories of Malware

What it Does

Banking Trojan

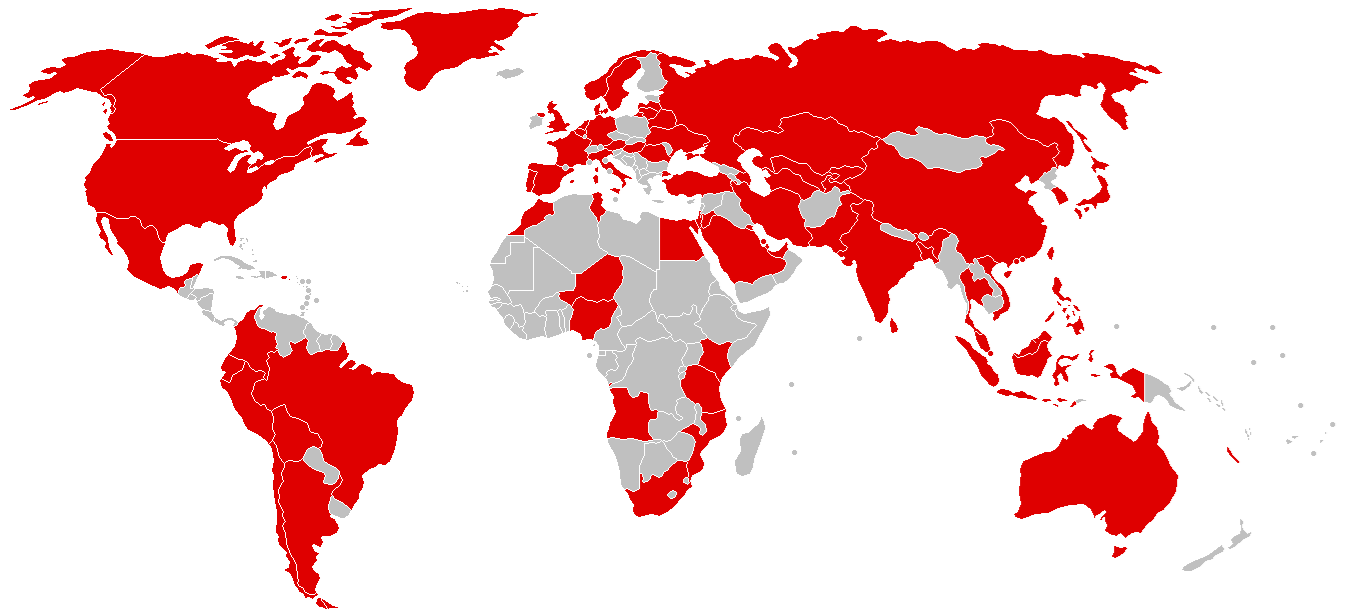
- Trojan that silently “listens” for banking login credentials
- Most famous example:
 - Zeus, which triggered when certain URLs were visited, and inserted JavaScript code into a legitimate bank’s website pages
 - Estimate of over \$100 million in losses/damages since 2007
 - Source code was leaked in 2011
 - Other malware authors used this leaked code to create dozens of variant families that are still active today

Ransomware

- Encrypts data and demands payment to decrypt victim's files
- Often asks for payment in cryptocurrency
 - Cryptocurrency payments are harder to track
- Causes billions of dollars in losses/damages each year
- Quicker and more direct method of making money than banking trojans
 - Don't have to wait for a user to log into their account

Ransomware Example: WannaCry

- Propagated and spread as a worm
- Uses the EternalBlue exploit to propagate
 - Windows released a patch in March 2017
- WannaCry was released worldwide in May 2017
 - Caused billions of dollars in losses and damages



Ransomware Example: WannaCry

- 200,000 computers infected
- \$130,000 paid in ransom
- Multiple sources have pointed to North Korea as the origin
 - Lazarus Group
 - (Also likely responsible for the 2014 Sony email hacks)



Cryptocurrency Miners

- Silently mines cryptocurrency for cybercriminals
- Uses the victim's computer without their knowledge
 - Only obvious sign of infection is slow performance/lagging
- Much stealthier than banking trojans, ransomware
 - And does not require the victim to do anything
- In January 2018, ads on YouTube containing JavaScript were being used to mine the Monero cryptocurrency

Information taken from <https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/>

Backdoor

- Can allow a malicious actor to remotely access a computer that has been infected
- Mainly meant to bypass authentication, often does not have too many additional features

Remote Access Tool/Trojan (RAT)

- Gives actor remote access to, and a high level of control over, the infected computer
 - Backdoor with lots of additional functionality
- Example of RAT:
 - Poison Ivy, which can log keystrokes, spy on the victim's actions, steal password hashes, transfer files, etc.
 - Since 2008, many different APT groups have used Poison Ivy variants in their campaigns
 - Very popular tool, simple to use

Information from <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf>

RAT Example: Poison Ivy

- Screenshot of Poison Ivy use, showing victim's screen within the GUI framework

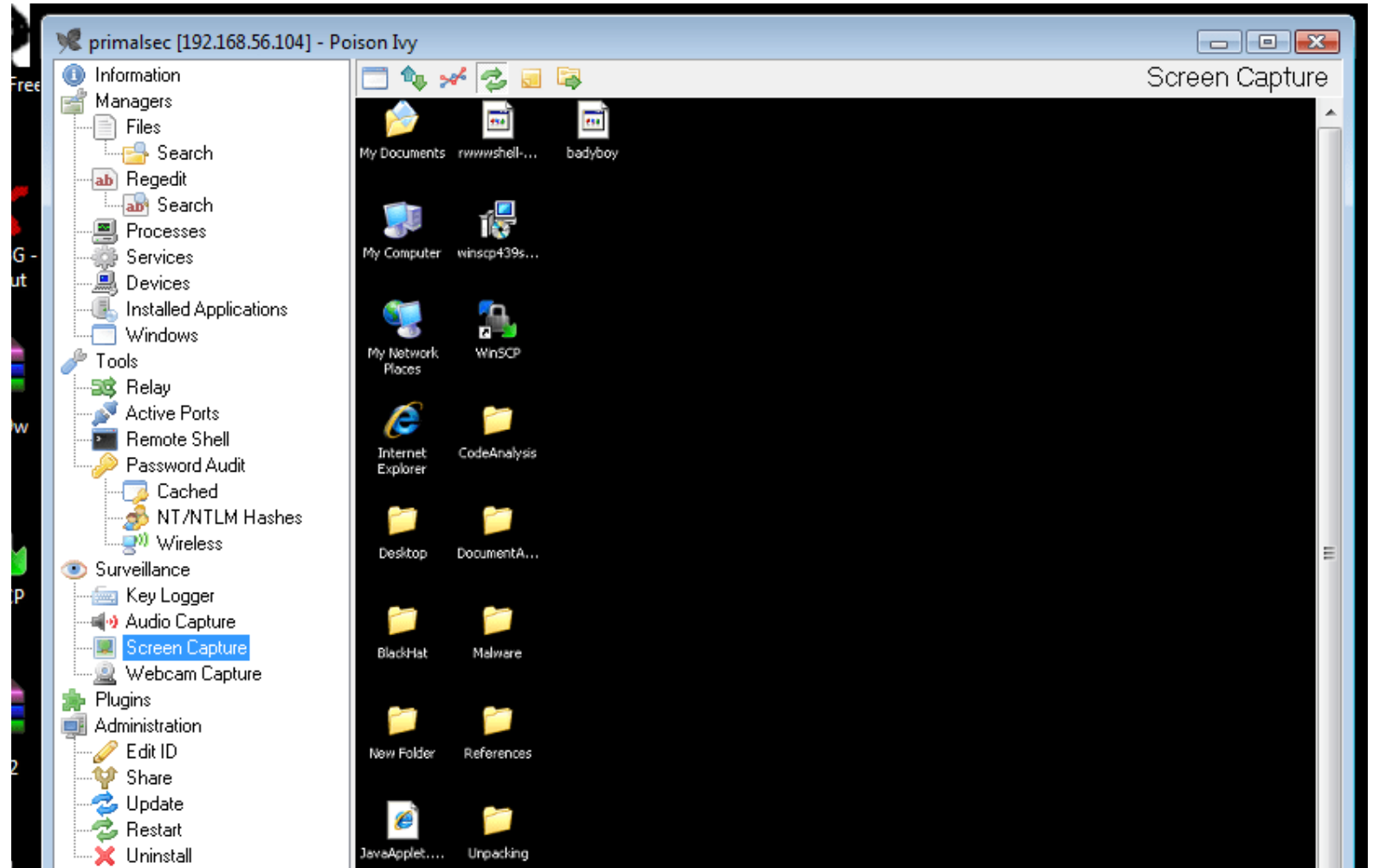


Image from <http://www.primalsecurity.net/poison-ivy-remote-access-tool-rat/>

Botnet

- Refers to a large number of computers being controlled simultaneously by a single actor
 - Anywhere from a few thousand to a few million
- Often used to send spam emails and launch DDoS attacks
- Differs from RAT, where actor has fine control of one computer
- With a botnet, the actor can give commands to many machines
 - Different desired outcomes, different means of achieving them

Credential Stealer

- Attempt to steal the victim's credentials
- Usually done using one of these methods:
 - Keylogging
 - Dumping and extracting from password hashes

Rootkit

- Set of programs that maintains covert access to that system
 - Actively masks its existence within the system
- Two types: user mode and kernel mode
 - User mode runs at same level as other user applications
 - e.g., Intercepts calls to APIs to prevent listing its files in a directory
 - Kernel mode runs with the highest privileges
 - e.g., Adds or replaces portions of the OS itself

Destructive Malware / Disk Wiper

- Wipes the hard drive of the infected system
 - Or otherwise makes the system unusable

- Recent example: NotPetya
 - Originally classified as a ransomware worm that spread by exploiting EternalBlue in 2017
 - Seemed to be a variant of the Petya ransomware
 - Encrypts parts of the master boot record and intentionally makes system unrecoverable, even if the ransom is paid
 - Now classified as a wiper/worm

Wiper Example: NotPetya

- Heavily targeted computers in Ukraine, caused over \$10 billion in damages
 - One of the costliest, if not the costliest cyberattack to date
- Attributed to the Sandworm APT group, which is Russian state-sponsored



Image from https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

Categories of Malware

What it Targets

Mobile Malware

- Malware that targets mobile devices
- Common in 3rd-party app stores
- Growing category of malware and much more prevalent in countries that do not allow access to official app stores
- Antivirus programs are largely ineffective, due to the rapid evolution of mobile malware

Point-of-sale Malware

- Malware that targets PoS devices like cash registers
- Goal is to obtain credit card and debit card information
- Often scrapes RAM of PoS devices to accomplish this
 - Simplest and most evasive way to obtain the data

SCADA Malware

- Stands for “Supervisory Control and Data Acquisition”
- SCADA systems allow high-level process supervising
- Often used for industrial, infrastructure, and facility purposes
 - Manufacturing, power plants, refineries
 - Water treatment, oil pipelines, electric power distribution, etc.
 - Airports, buildings, ships (HVAC, access, etc.)
- Obviously, malware that targets these systems can cause widespread physical damage

SCADA Malware Example: Stuxnet

- SCADA worm that targeted Iran's nuclear program in 2010
 - Centrifuges in nuclear plants spun too fast and tore themselves apart
 - Estimated to have damaged or destroyed approximately 20% of the nuclear plants in Iran
- Was introduced to systems via a USB drive
 - Spreads by exploiting four different zero day exploits
- First known malware that targets industrial systems
 - One of the earliest instances of causing widespread physical damage via malware

Malware Lifecycle

Malware Infection Lifecycle

- Timeline between when malware gets delivered to a system and when it gets done running
- Everyone has their own spin, but here's a simple one:
 1. Initial infection of victim occurs
 - First-stage malware on victim's computer
 2. Payload is delivered
 - Malware takes action
 3. Malware makes contact with actor
 - "Command & Control"

Infection Vector Example: Phishing

- Using email to convince a victim to click a link or download an attachment
- Initial infection occurs via this act

- Spearphishing
 - Phishing of specific, chosen victims
 - Higher rate of success

Infection Vector Example: Exploit Kit

- Compromised website redirects to a malicious website that is hosting the exploit kit
- Exploit kit does what it says on the box:
 - Scans the victim's computer for vulnerabilities
 - Sends an appropriate exploit to the victim's computer
 - Allows delivery of malware
- Patching exploits (allowing updates) is incredibly important
 - When patched, redirects can still happen, but exploit kit won't have anything to exploit

First-Stage Malware

- A full malware payload is rarely delivered directly through the initial infection vector
- The “first-stage” malware gets execution on the victim’s computer, then downloads and runs the payload
 - May be referred to as droppers, loaders, downloaders, etc.
- Most of the time, only first-stage malware is delivered
 - What purpose does this serve?
 - Most email clients don’t allow executable attachments
 - First-stage can be smaller in size, with its limited functionality

First-Stage Example: Malicious Macros

- Files that contain macros that are attached to phishing emails
 - With the intention of the user running the macro and downloading/running the full payload
 - Often Microsoft Office documents, RTF files, or PDFs
- Office documents used to automatically run macros when a user opened the file
 - Now a notification (often including a warning) is shown to the user requiring them to manually enable macros
 - (Many users just click “Enable Content” anyway)

Payloads

- The actual file(s) that perform the malicious actions and achieve the actor's end goal
- We talked about the different categories of payloads
 - Direct actions, like ransomware and cryptojacking
 - End goals, like making the machine part of a botnet, or setting up long-term monitoring with a RAT

Command & Control

- Malware's communication of information with the actor
 - Banking Trojan – send login credentials when seen
 - RAT – constant possible interaction
 - Botnet – centralized C&C (master)
- End of the lifecycle (but this “end” can be very extended)
- Often referred to as C2 or C&C
- Payloads often connect back to a C&C IP address or domain in order to receive instructions from the malware actor