CMSC 426
Principles of Computer Security

Malware Categories

Last Class We Covered

- Malware
- Threat actors
  - APT groups and others
- Attribution
- Threat actor examples

Any Questions from Last Time?

Today's Topics

- Types of malware
- Well-known malware families
  - Gratuitous examples of malware

Categorizations

- Malware is categorized based on
  - How it spreads/persists
  - What it does
  - What kinds of systems it targets

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

How Malware Spreads

Worm

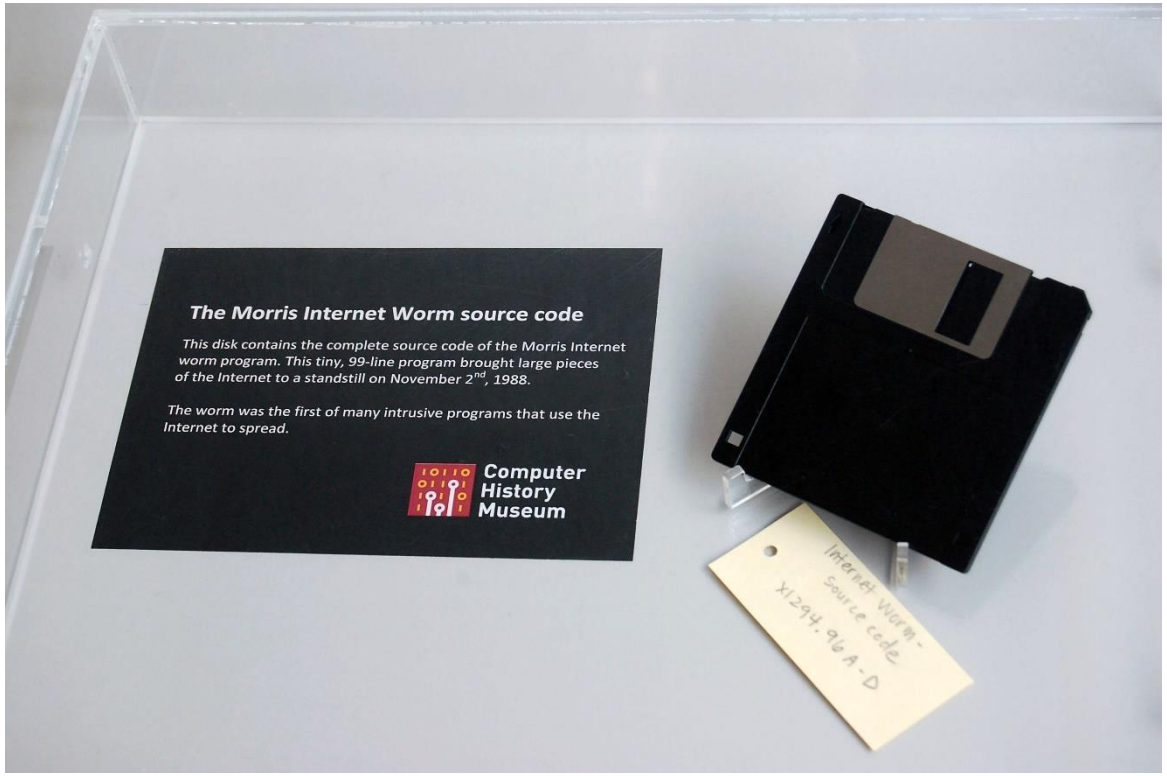
- Standalone program
- Replicates itself and spreads automatically
  - Attempt to infect as many computers as possible
- Normally spread via a network
  - Consumes bandwidth; dangerous even if “harmless”
- Usually exploits a vulnerability to do so
  - Or captured authorization credentials

Worm Example: Conficker

- Exploits the MS08-067 vulnerability (an overflow vulnerability!)
  - Vulnerability was patched before the worm came out
- Still propagating a decade later
  - Mostly on unpatched legacy systems
- Estimated 9 to 15 million computers infected since 2008
- The authors of the worm still have not been identified

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 lead it to re-infect machines, with 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 everything*** 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.

What Malware 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

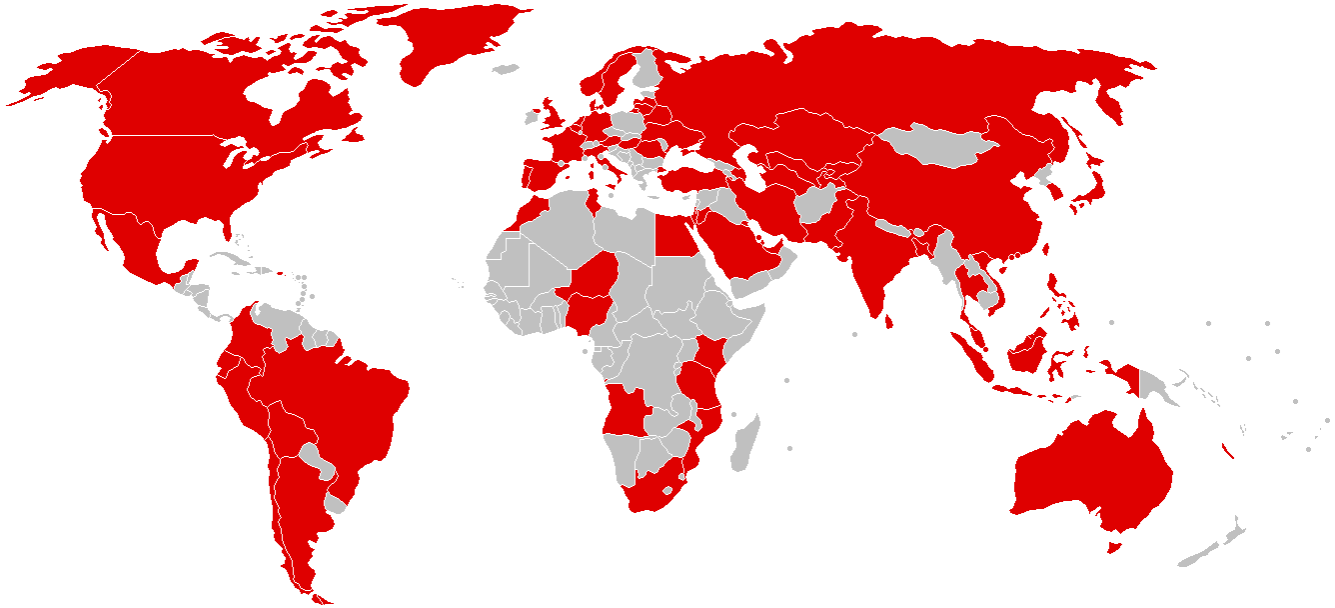
Information taken from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans

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 (not a Trojan)
- Uses a leaked NSA-developed exploit to propagate
  - Exploit called “EternalBlue,” leaked by the Shadow Brokers
  - 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)

Cryptojacking (Cryptocurrency Miners)

- Silently mines cryptocurrency for cybercriminals
- Uses the victim's computer without their knowledge
  - Only sign of infection is slow performance/lagging
- Current cybercriminal favorite as of late 2017
  - Much stealthier and does not require the victim to do anything

- 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 (Trapdoor)

- Secret entry point into a program
  - Legitimate tool for debugging and testing (“maintenance hook”)
  - Used to circumvent long setups or authentication procedures

- Can also allow a bad actor to remotely access a computer that has been infected, and bypass the authentication

Remote Access Tool/Trojan (RAT)

- "Backdoor on steroids"
- Gives actor remote access to, and a high level of control over, the infected computer

- 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

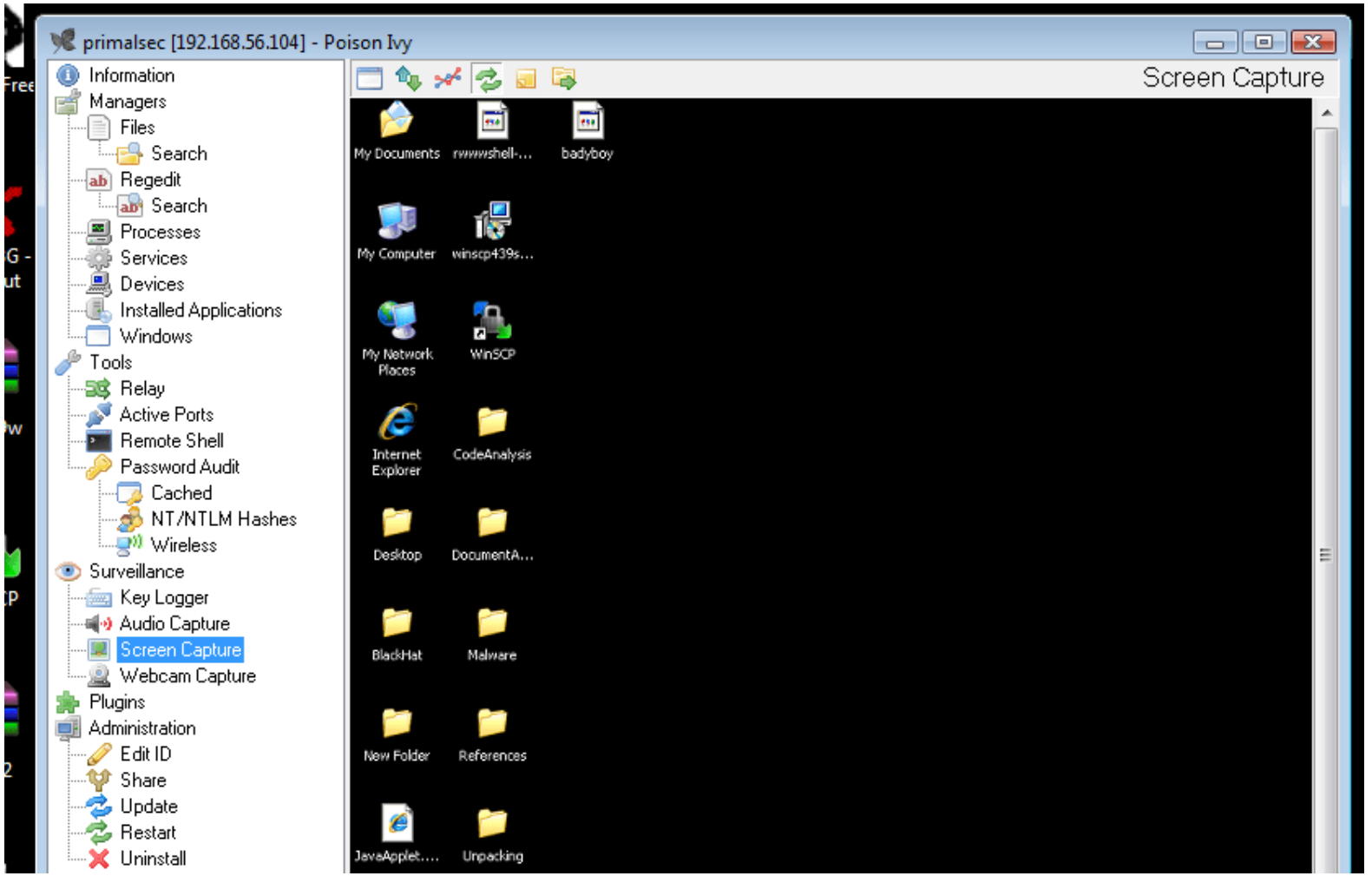


Image from http://www.primalsecurity.net/poison-ivy-remote-access-tool-rat/

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 the actor has fine control of a machine
- 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
  - (Or spyware in general)
  - Dumping and extracting from password hashes

Rootkit

- Set of programs that maintains covert access to that system
  - Normally with administrator (root) privileges
  - 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

Wiper

- Wipes the hard drive of the infected system

- 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

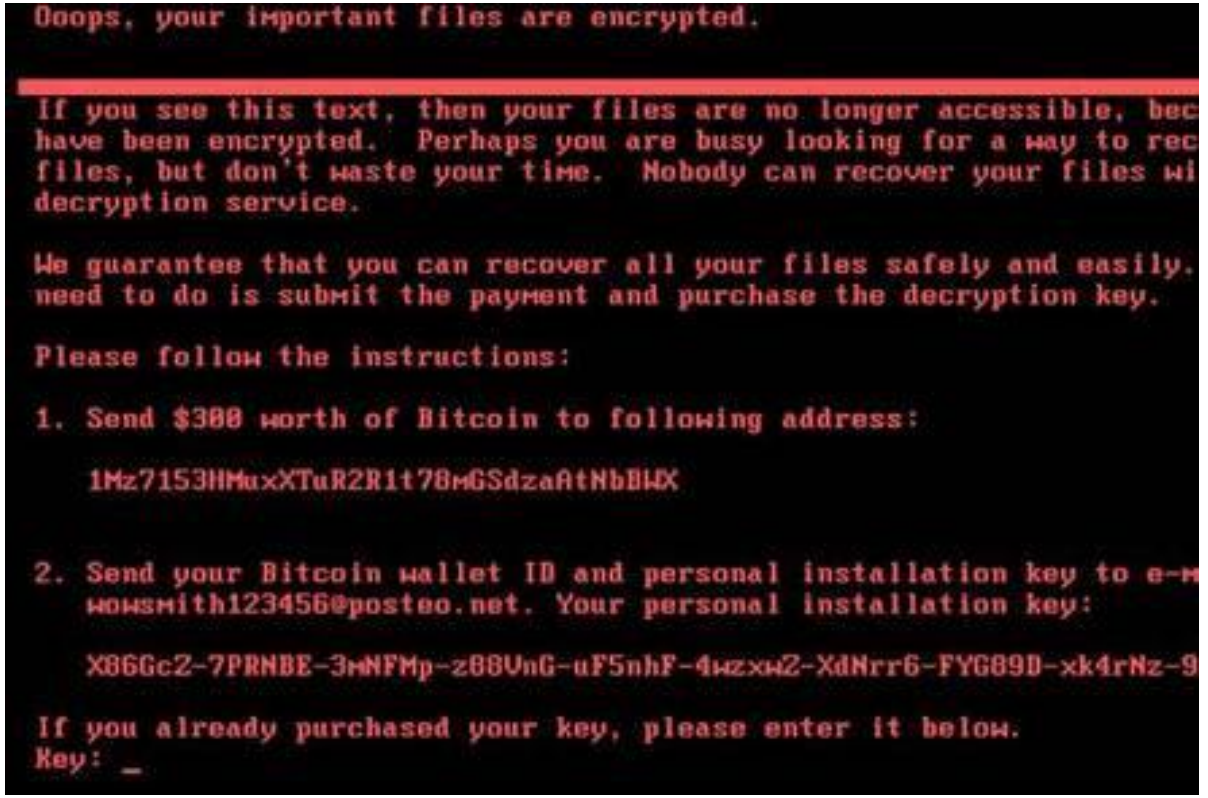


Image from https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

What Systems Malware 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

Announcements

- Schedule is now up on the course website
  - First midterm pushed back to Tuesday, October 9th
  - General topics laid out for rest of semester
- Assignments page also up to date
  - All assignments have release and due dates
- Lab 1 and Paper 1 are due at midnight on Wednesday, September 26th

Image Sources

- Morris worm disk (adapted from):
  - https://www.flickr.com/photos/intelfreepress/10483246033
- Trojan horse:
  - https://commons.wikimedia.org/wiki/File:Trojan_Horse_by_A_Yakovlev_1911.jpg
- WannaCry screenshot:
  - https://en.wikipedia.org/wiki/File:Wana_Decrypt0r_screenshot.png