CMSC 426
Principles of Computer Security

Lecture 08

Malware Categories and Lifecycle

Last Class We Covered

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

- Malware categories
  - How it spreads
  - *Worm, File infector (virus), Trojan*

Any Questions from Last Time?

Today's Topics

- Malware categories
    - How it spreads
        - *Covered last time*
    - What it does
    - What kinds of systems it targets

- Malware lifecycles

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

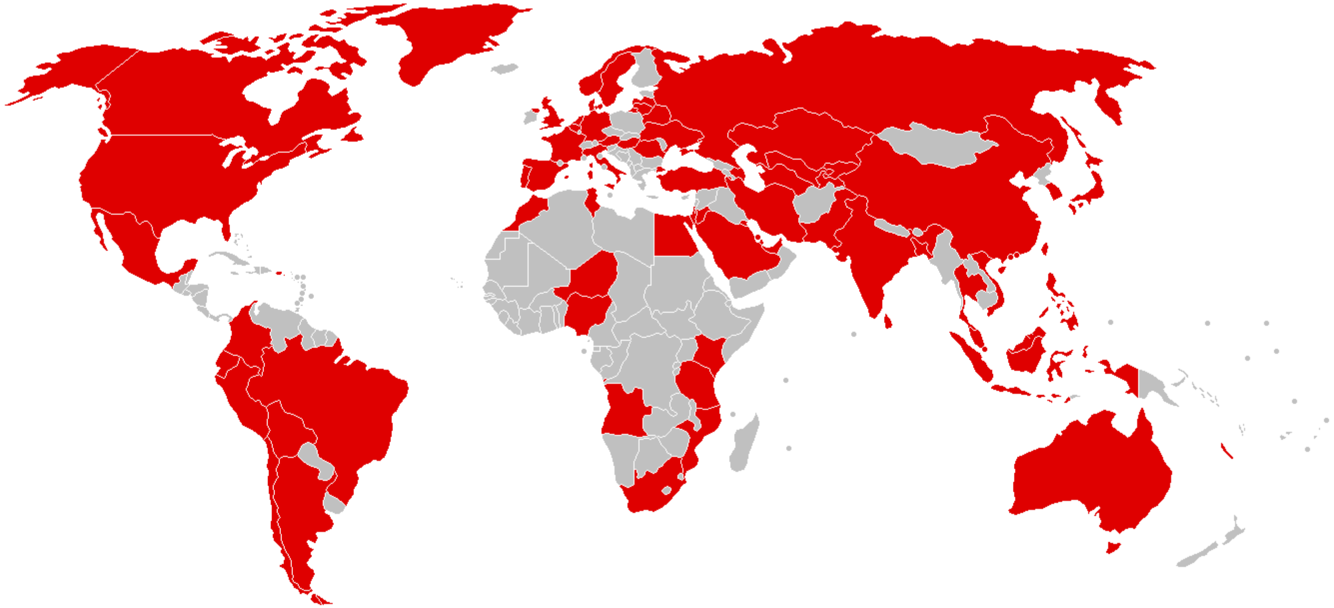
Information taken from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans

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

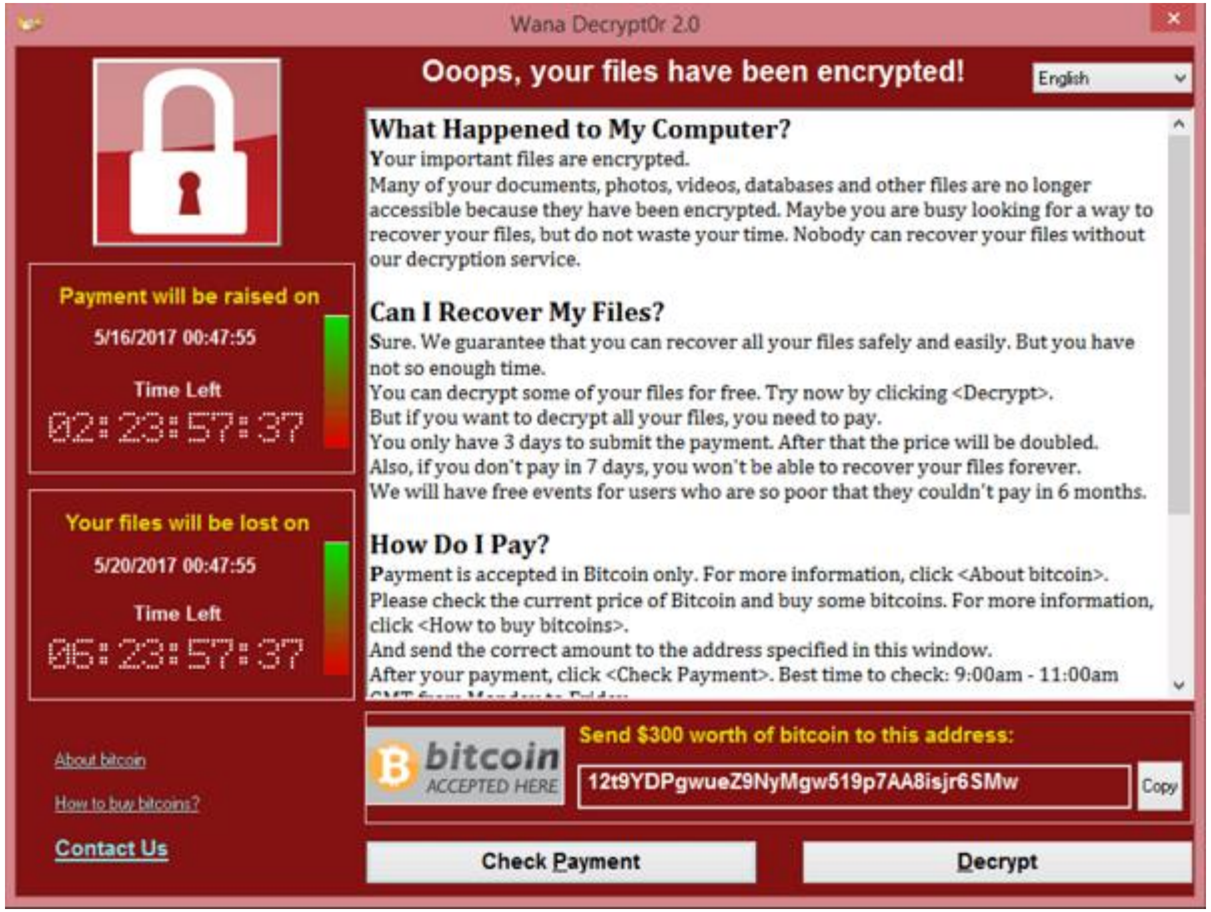


- WannaCry was released worldwide in May 2017
  - Caused billions of dollars in losses and damages

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)



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

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

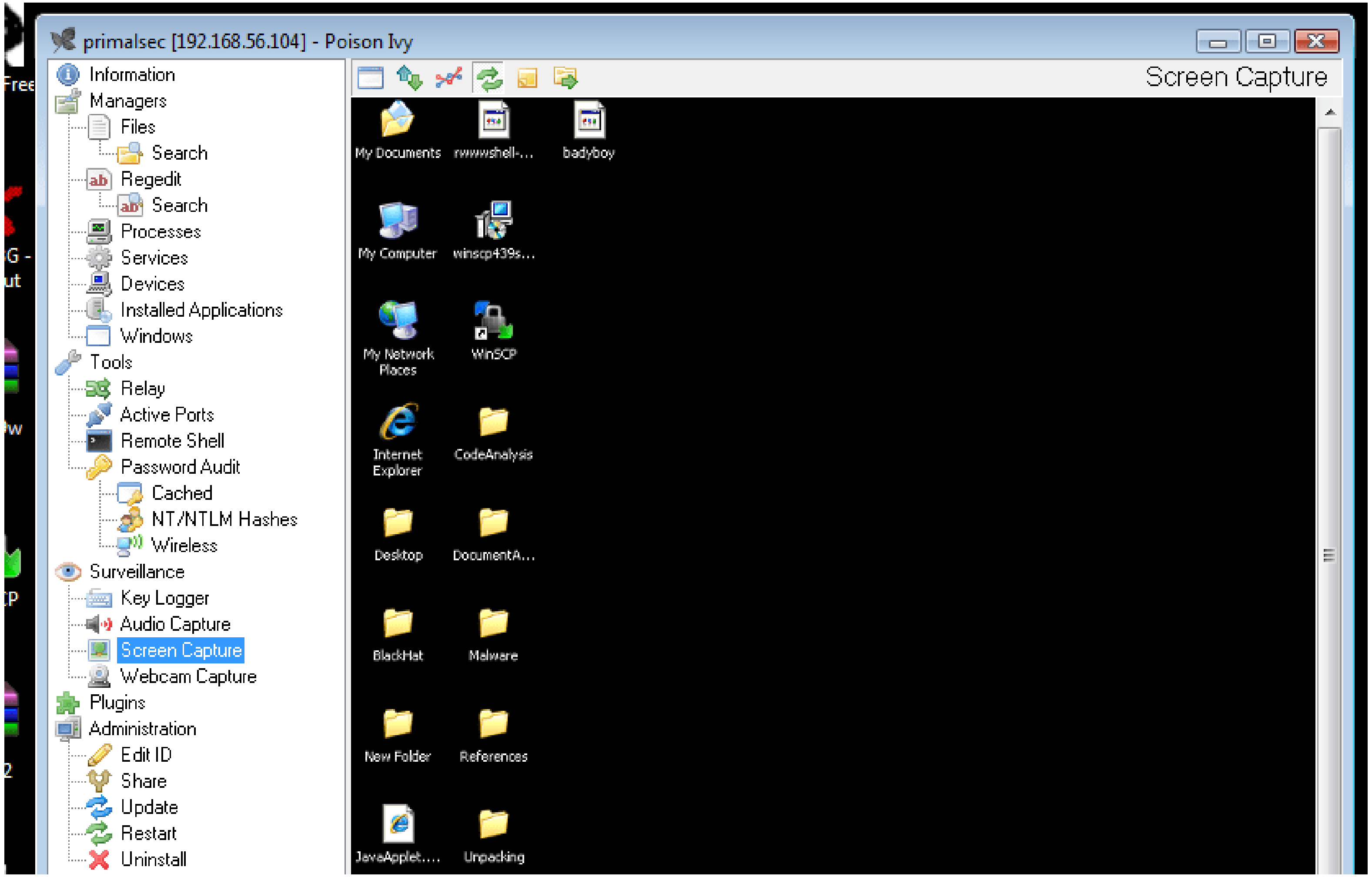


Image from http://www.primalsecurity.net/poison-ivy-remote-access-tool-rat/

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

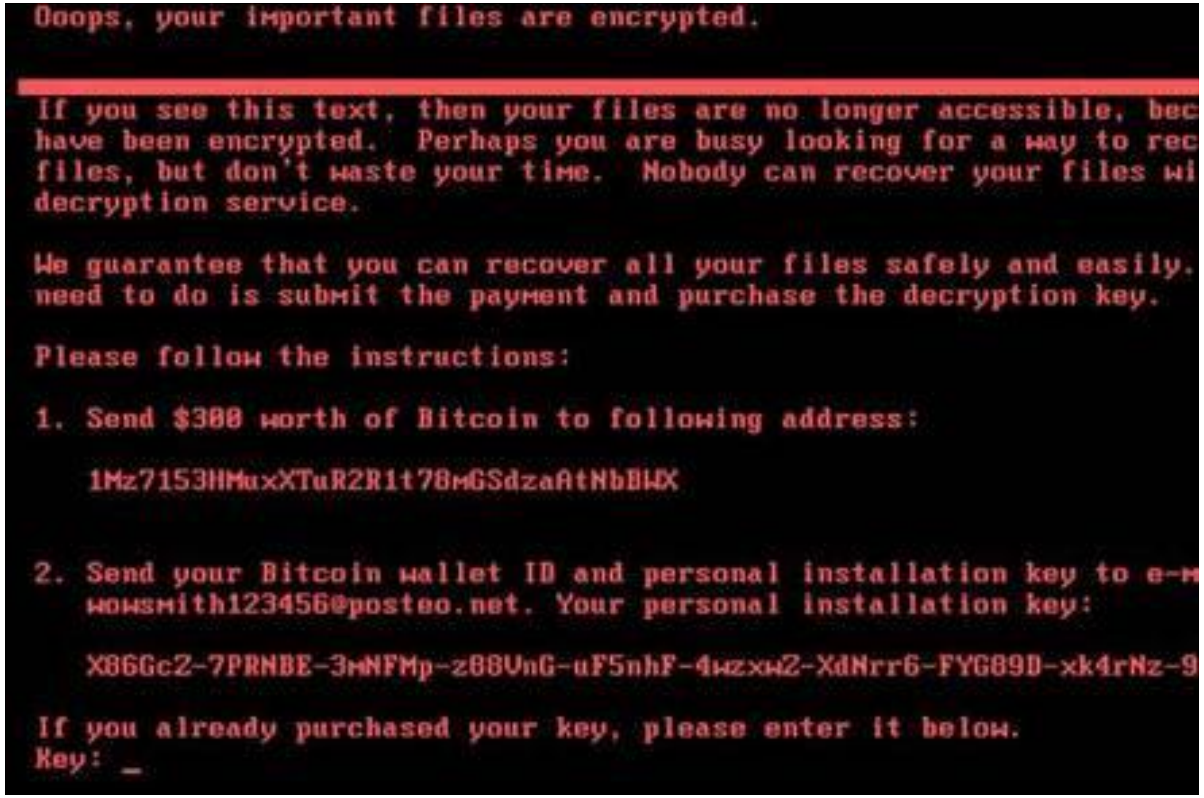
- Wipes the hard drive of the infected system

- 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 <u>the</u> costliest cyberattack to date

- Attributed to the Sandworm APT group, which is Russian state-sponsored



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, bec
have been encrypted.  Perhaps you are busy looking for a way to rec
files, but don't waste your time.  Nobody can recover your files wi
decryption service.

We guarantee that you can recover all your files safely and easily.
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-m
   wowsmith123456@posteo.net. Your personal installation key:

   X86Gc2-7PRNBE-3mNFMp-z88VnG-uF5nhF-4wzxw2-XdNrr6-FYG89D-xk4rNz-9

If you already purchased your key, please enter it below.
Key: _
```

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

Malware Lifecycle

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 last time
  - 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

- The parts of the malware that actually do the “cool stuff”

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

Missing Command & Control

- Not every malware has a C&C stage
  - Depends on malware’s actions and end goal

- Ransomware
  - Victim communicates “directly” with the actor
- Wiper
  - No communication necessary

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