CSec15233
Malicious Software Analysis

Malware Analysis Primer

Qasem Abu Al-Haija

Introduction

Consider the following Scenario

- The phone rings, and the networking guys tell you that you've been hacked and that your customer's sensitive information has been stolen from your network.
  - You begin your investigation by checking your logs to identify the hosts involved.
  - You scan the hosts with antivirus software to find the malicious program and catch a lucky break when it detects a trojan horse named **TROJ.snapAK**.
  - You delete the file in an attempt to clean things up, and you use network capture to create an intrusion detection system (IDS) signature to ensure no other machines are infected.
  - Then you patch the hole that you think the attackers used to break in to ensure that it doesn't happen again.

Consider the following Scenario

- Then, several days later, the networking guys are back, telling you that sensitive data is being stolen from your network.
  - It seems like the same attack, but you have no idea what to do.
  - Clearly, your IDS signature failed because more machines are infected, and your antivirus software isn't providing enough protection to isolate the threat.

- Now upper management demands an explanation of what happened, and all you can tell them about the malware is that it was **TROJ.snapAK**.
  - You don't have the answers to the most important questions, and you're looking kind of lame.

Consider the following Scenario

- You don't have the answers to the most important questions, and you're looking kind of lame.
  - How do you determine exactly what TROJ.snapAK does so you can eliminate the threat?
  - How do you write a more effective network signature?
  - How can you find out if any other machines are infected with this malware?
  - How can you ensure you've deleted the entire malware package and not just one part of it?
  - How can you answer management's questions about what the malicious program does?

Consider the following Scenario

- All you can do is tell your boss that you need to hire expensive outside consultants because you can't protect your network.
  - That's not the best way to keep your job secure.
  - But fortunately, you were smart enough to study the practical malware analysis course.
  - The skills covered in this course teach you how to answer such questions and protect your network from malware.

What is Malware?

- Any software that does something that causes detriment to the user, computer, or networks.
  - Such as viruses, trojan horses, worms, rootkits, scareware, and spyware.
  - Malicious software (malware) plays a part in most computer intrusion and security incidents.

- While malware appears in many forms, common techniques are used to analyze malware.
  - Your choice of which technique to employ will depend on your goals.

What is Malware Analysis?

- Malware analysis is the art of dissecting malware to understand: (1) how it works, (2) how to identify it, and (3) how to defeat or eliminate it.
  - You don't need to be an uber-hacker to perform malware analysis.
  - With millions of malicious programs in the wild and more encountered every day, malware analysis is critical for anyone who responds to computer security incidents.
  - With a shortage of malware analysis professionals, skilled malware analyst is in serious demand.

What is Malware Analysis?

- That said, this is not a course on how to find malware.
  - Our focus is on how to analyze malware once it has been found.
- We focus on malware found on Windows OS: the most common OS in use today.
  - But the skills you learn will serve you well when analyzing malware on any operating system.
  - We focus on executables since they are the most common and the most difficult files that you'll encounter.

Types of Malware

Types of Malware

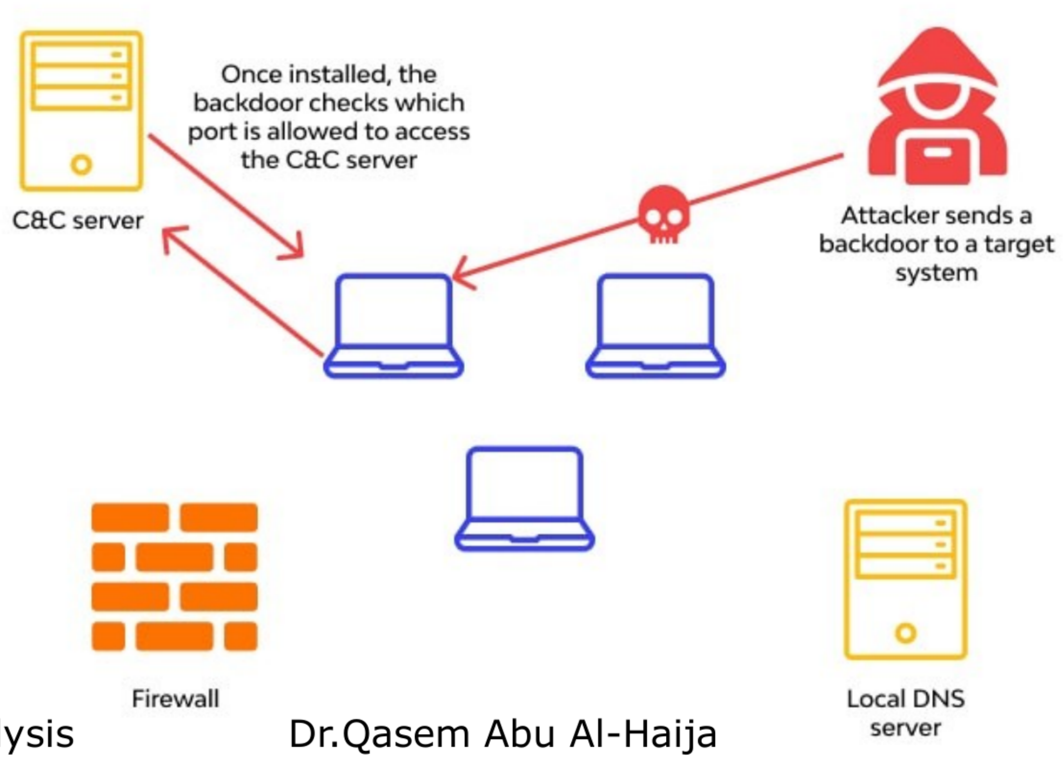
- When performing MA, you can often speed up your analysis by guessing what the malware is trying to do.

- Of course, to make better guesses, you need to know the kinds of things that malware usually does.

- To that end, here are the categories that most malware falls into the following types.

Types of Malware

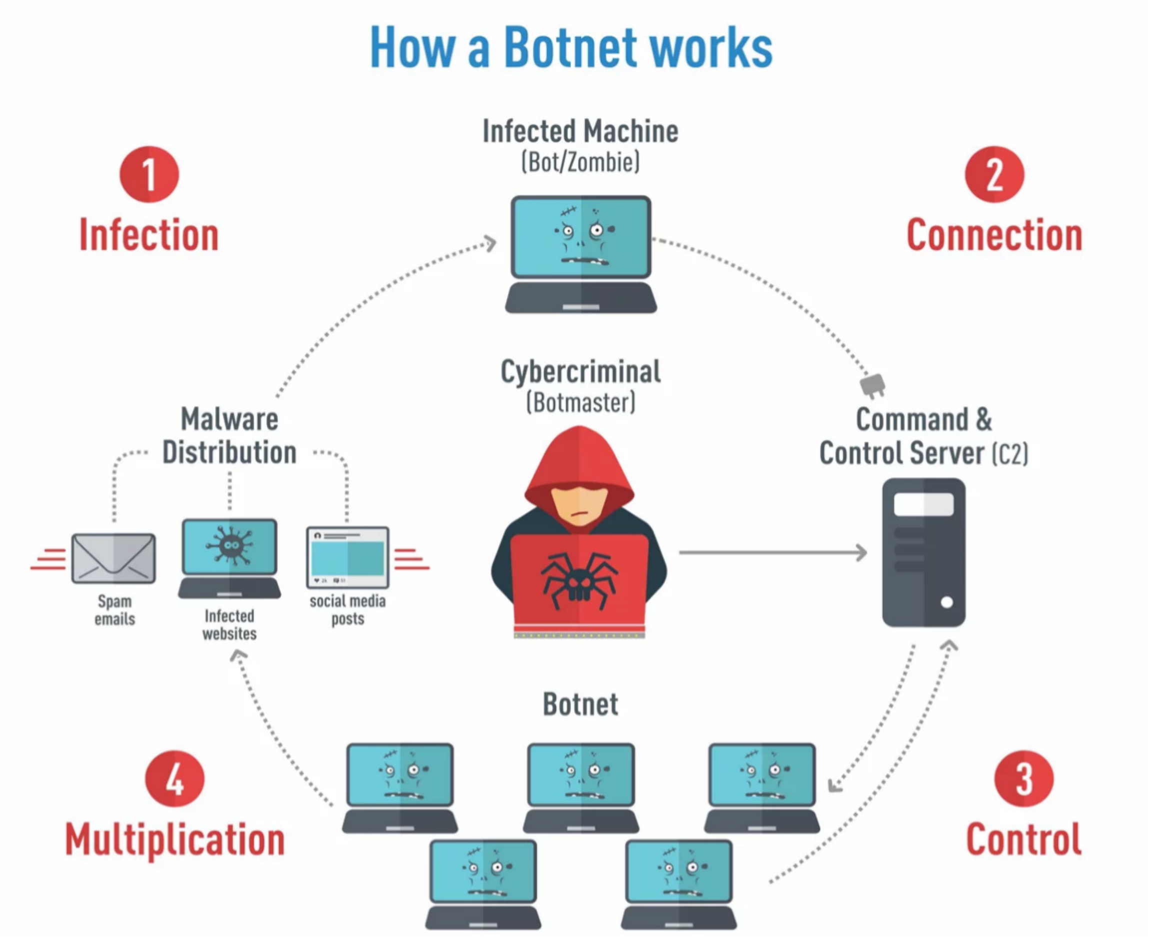
- Backdoor
  - Malicious code that installs itself onto a computer allows the attacker access to control the system
  - Backdoors usually let the attacker connect to the computer with little or no authentication and execute commands on the local system.



C&C server
Once installed, the backdoor checks which port is allowed to access the C&C server
Attacker sends a backdoor to a target system
Firewall
Local DNS server

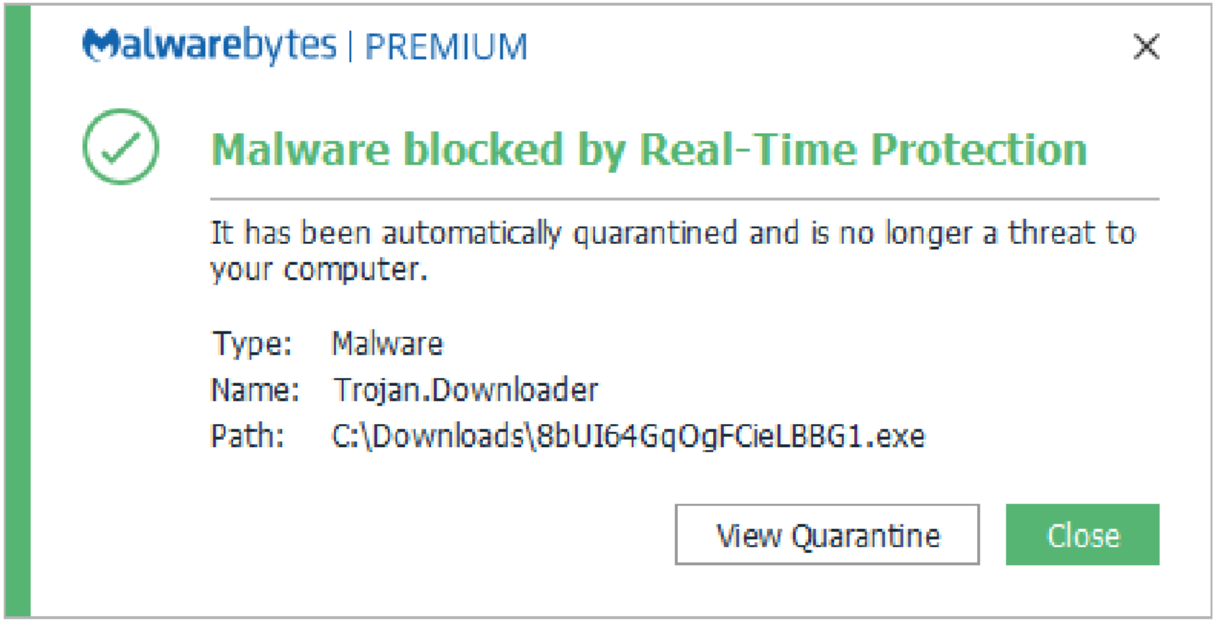
Types of Malware

- Botnet
  - Similar to a backdoor in that it allows the attacker access to the system,
  - But all infected computers receive instructions from the same C&C server



Types of Malware

- Downloader
  - Malicious code that exists only to download other malicious code
  - Used when the attacker first gains access
  - The downloader program will download and install additional malicious code.
  - It needs to connect to the internet to download the files.



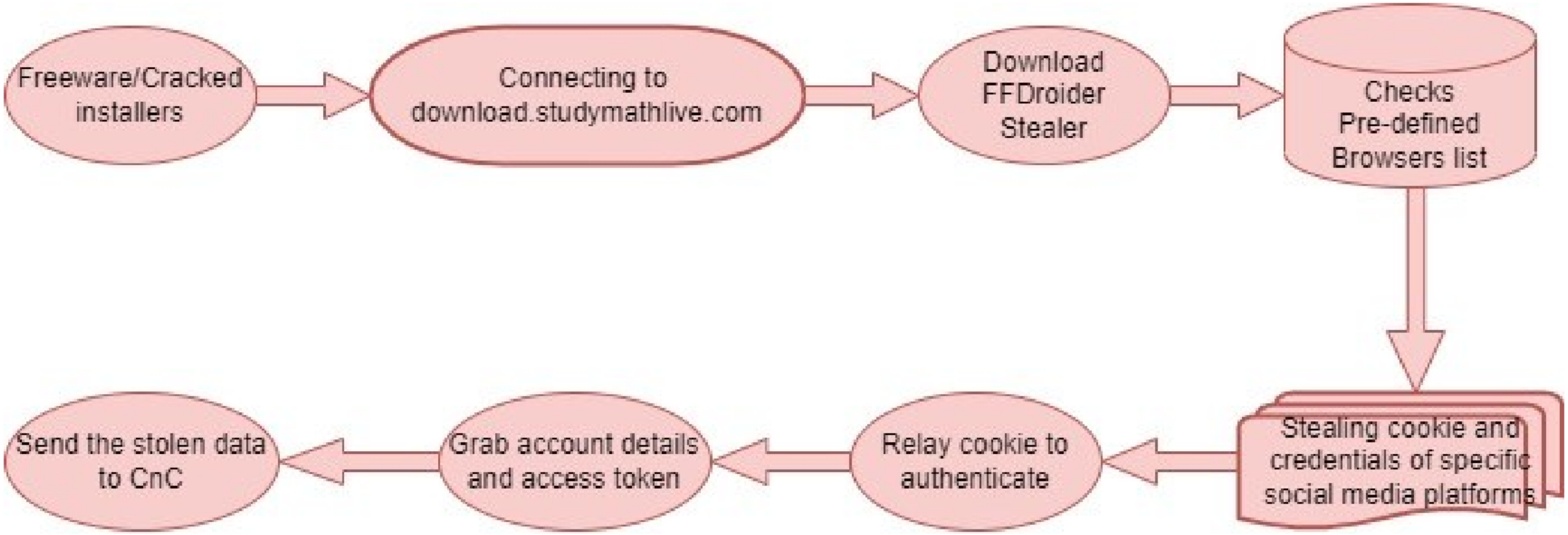
Malware blocked by Real-Time Protection

It has been automatically quarantined and is no longer a threat to your computer.

Type: Malware
Name: Trojan.Downloader
Path: C:\Downloads\8bUI64GqOgFCieLBBG1.exe

Types of Malware

- Information-stealing malware
  - Malware collects information from a victim's computer and usually sends it to the attacker.
  - Examples include sniffers, keyloggers, and password hash grabbers.
  - This malware is typically used to gain access to online accounts such as email or online banking.

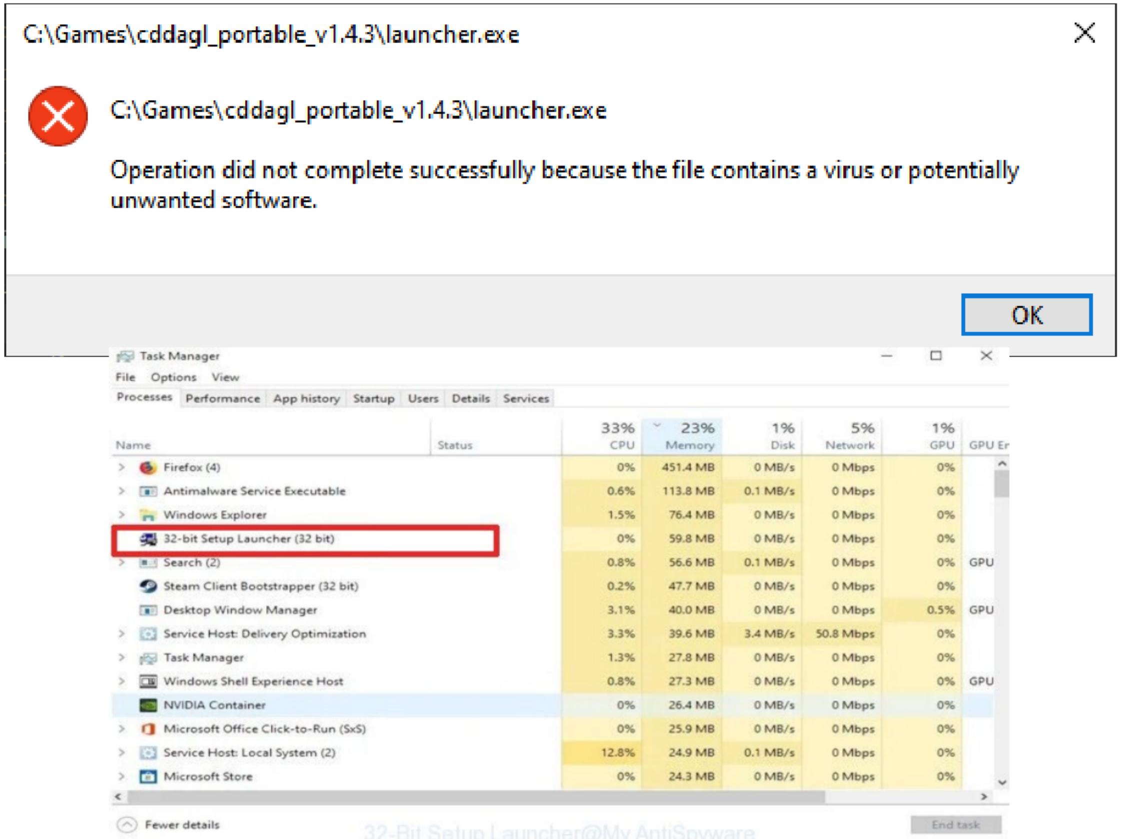

Freeware/Cracked installers
Connecting to download.studymathlive.com
Download FFDroider Stealer
Checks Pre-defined Browsers list
Stealing cookie and credentials of specific social media platforms
Relay cookie to authenticate
Grab account details and access token
Send the stolen data to CnC

Example: FFDroider, a new information-stealing malware disguised as the Telegram app

Check this: https://securityaffairs.co/wordpress/130094/cyber-crime/ffdroider-info-stealer.html.

Types of Malware

- **Launcher**
  - Malicious program used to launch other malicious programs
  - Usually, launchers use nontraditional techniques to launch other malicious programs in order to ensure stealth or greater access to a system.



C:\Games\cddagl_portable_v1.4.3\launcher.exe

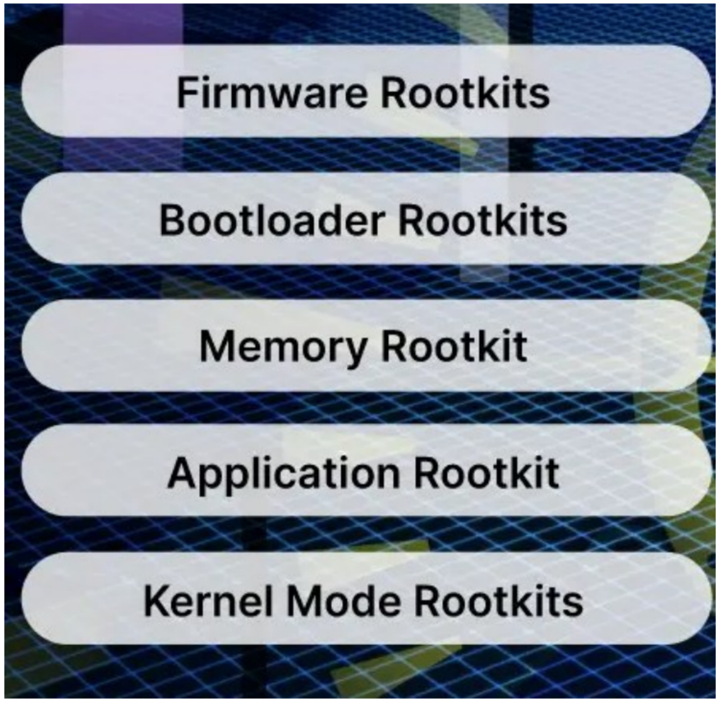
C:\Games\cddagl_portable_v1.4.3\launcher.exe

Operation did not complete successfully because the file contains a virus or potentially unwanted software.

Name	Status	33% CPU	23% Memory	1% Disk	5% Network	1% GPU	GPU Er
Firefox (4)		0%	451.4 MB	0 MB/s	0 Mbps	0%	
Antimalware Service Executable		0.6%	113.8 MB	0.1 MB/s	0 Mbps	0%	
Windows Explorer		1.5%	76.4 MB	0 MB/s	0 Mbps	0%	
32-bit Setup Launcher (32 bit)		0%	59.8 MB	0 MB/s	0 Mbps	0%	
Search (2)		0.8%	56.6 MB	0.1 MB/s	0 Mbps	0%	GPU
Steam Client Bootstrapper (32 bit)		0.2%	47.7 MB	0 MB/s	0 Mbps	0%	
Desktop Window Manager		3.1%	40.0 MB	0 MB/s	0 Mbps	0.5%	GPU
Service Host: Delivery Optimization		3.3%	39.6 MB	3.4 MB/s	50.8 Mbps	0%	
Task Manager		1.3%	27.8 MB	0 MB/s	0 Mbps	0%	
Windows Shell Experience Host		0.8%	27.3 MB	0 MB/s	0 Mbps	0%	GPU
NVIDIA Container		0%	26.4 MB	0 MB/s	0 Mbps	0%	
Microsoft Office Click-to-Run (SxS)		0%	25.9 MB	0 MB/s	0 Mbps	0%	
Service Host: Local System (2)		12.8%	24.9 MB	0.1 MB/s	0 Mbps	0%	
Microsoft Store		0%	24.3 MB	0 MB/s	0 Mbps	0%	

Types of Malware

- Rootkit
  - Malware that conceals the existence of other code
  - Usually paired with other malware, especially the backdoor
    - Allow remote access to the attacker and make the code difficult for the victim to detect.
    - Remotely access your computer, manipulate it, and steal data.
  - Potential consequences of a rootkit include Concealed malware, Information theft, File deletion, Eavesdropping, File execution, and Remote access.



Firmware Rootkits

Bootloader Rootkits

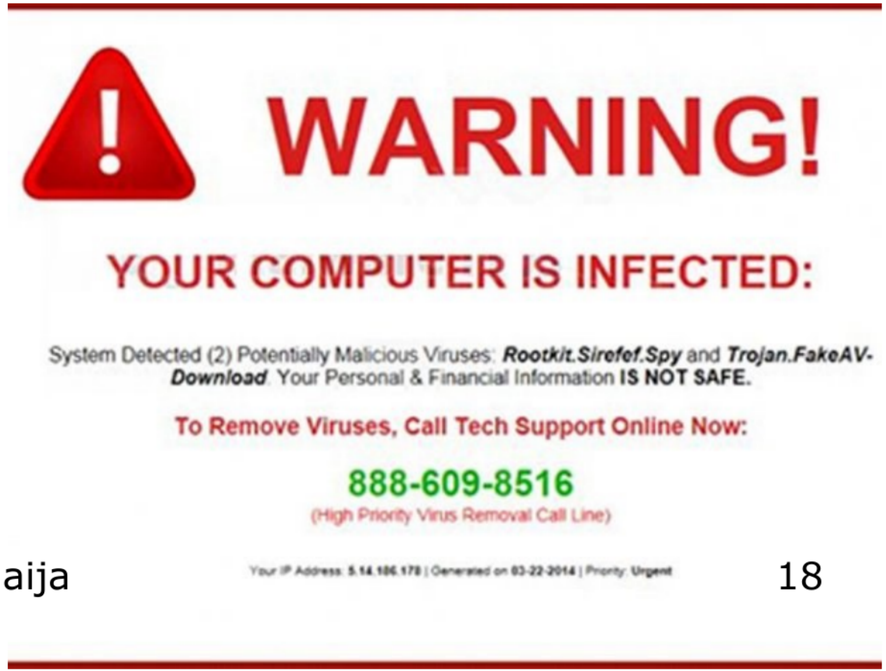
Memory Rootkit

Application Rootkit

Kernel Mode Rootkits

Types of Malware

- Scareware
  - Designed to Frightens users into buying something
  - It usually has a user interface that makes it look like an antivirus or another security program.
  - It informs users that there is malicious code on their system and that the only way to get rid of it is to buy their “software,” when the software it’s selling does nothing more than remove the scareware.



WARNING!

YOUR COMPUTER IS INFECTED:

System Detected (2) Potentially Malicious Viruses: ***Rootkit.Sirefef.Spy*** and ***Trojan.FakeAV-Download***. Your Personal & Financial Information **IS NOT SAFE.**

To Remove Viruses, Call Tech Support Online Now:

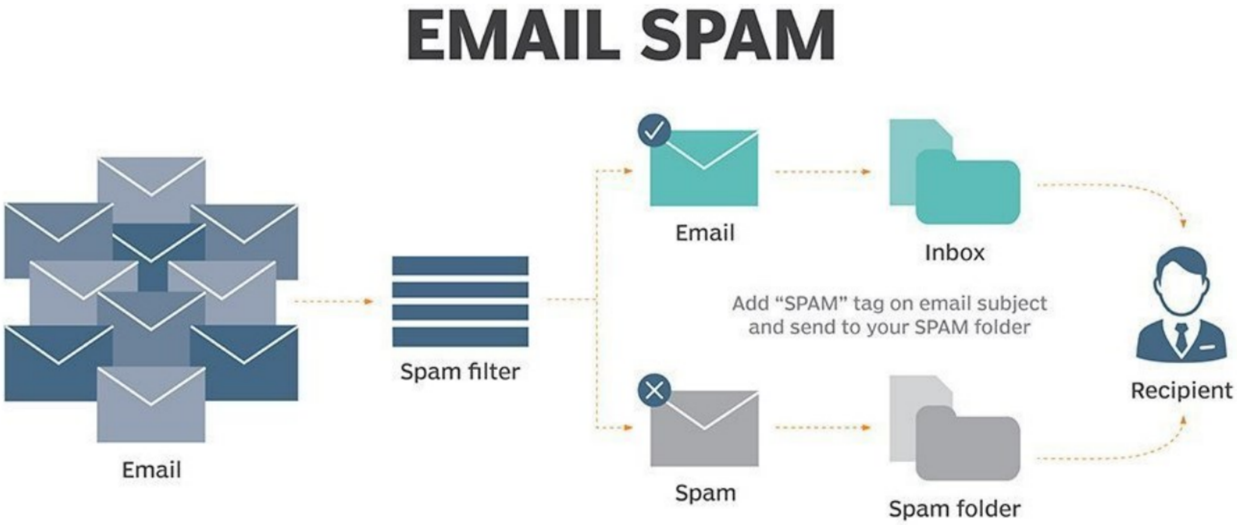
888-609-8516

(High Priority Virus Removal Call Line)

Your IP Address: 5.14.186.178 | Generated on 03-22-2014 | Priority: Urgent

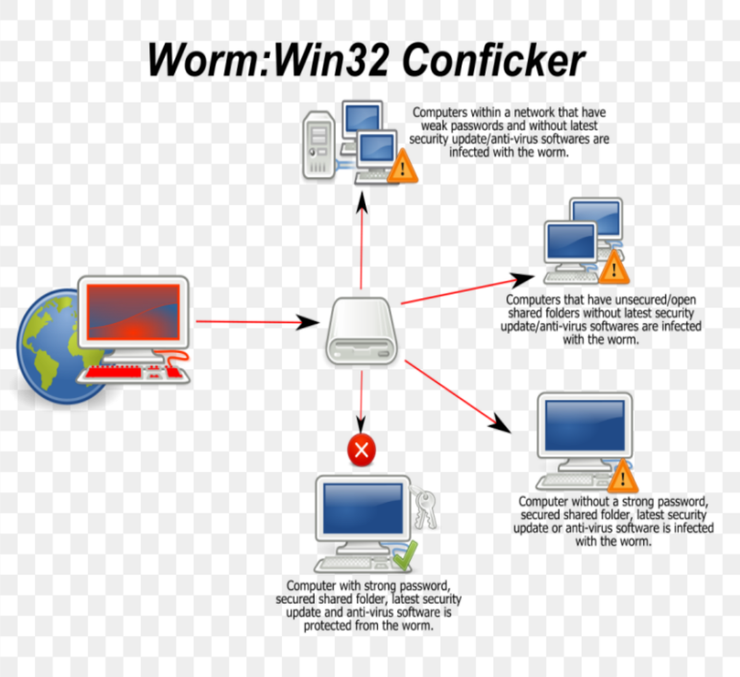
Types of Malware

- Spam-sending malware
  - Malware that infects a user's machine and then uses that machine to send spam (Attacker rents machine to spammers).
  - This malware generates income

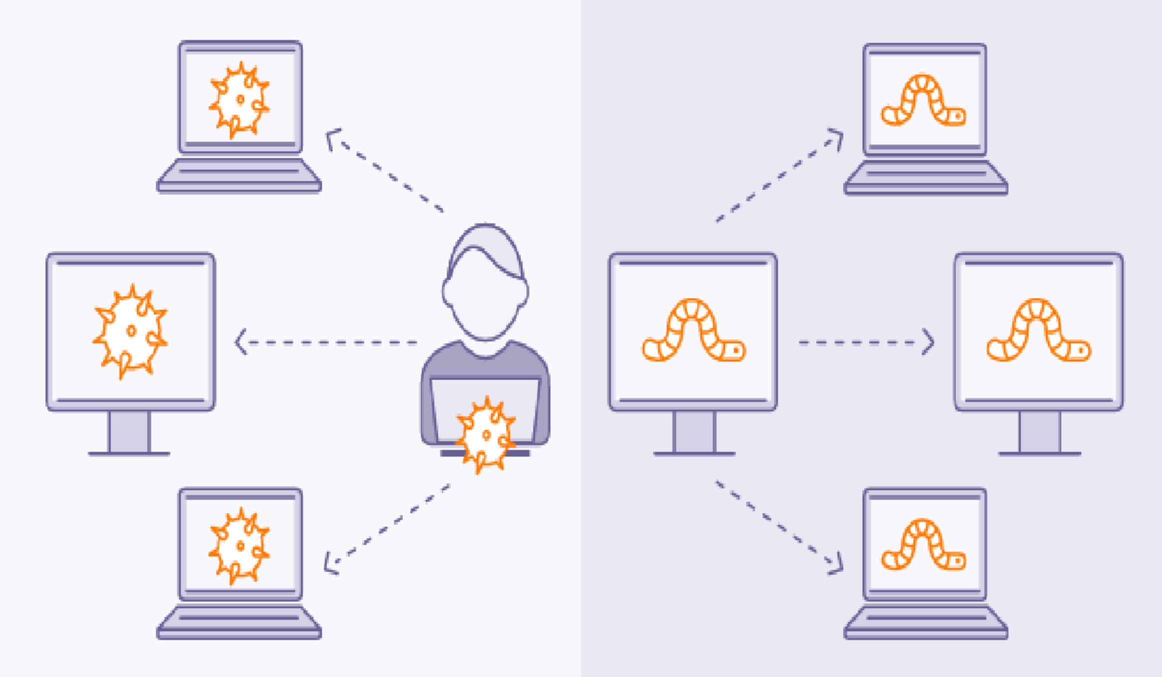

EMAIL SPAM
Email
Spam filter
Email
Inbox
Add "SPAM" tag on email subject and send to your SPAM folder
Recipient
Spam
Spam folder

Types of Malware

- Worms or viruses
  - Malicious code that can copy itself and infect additional computers

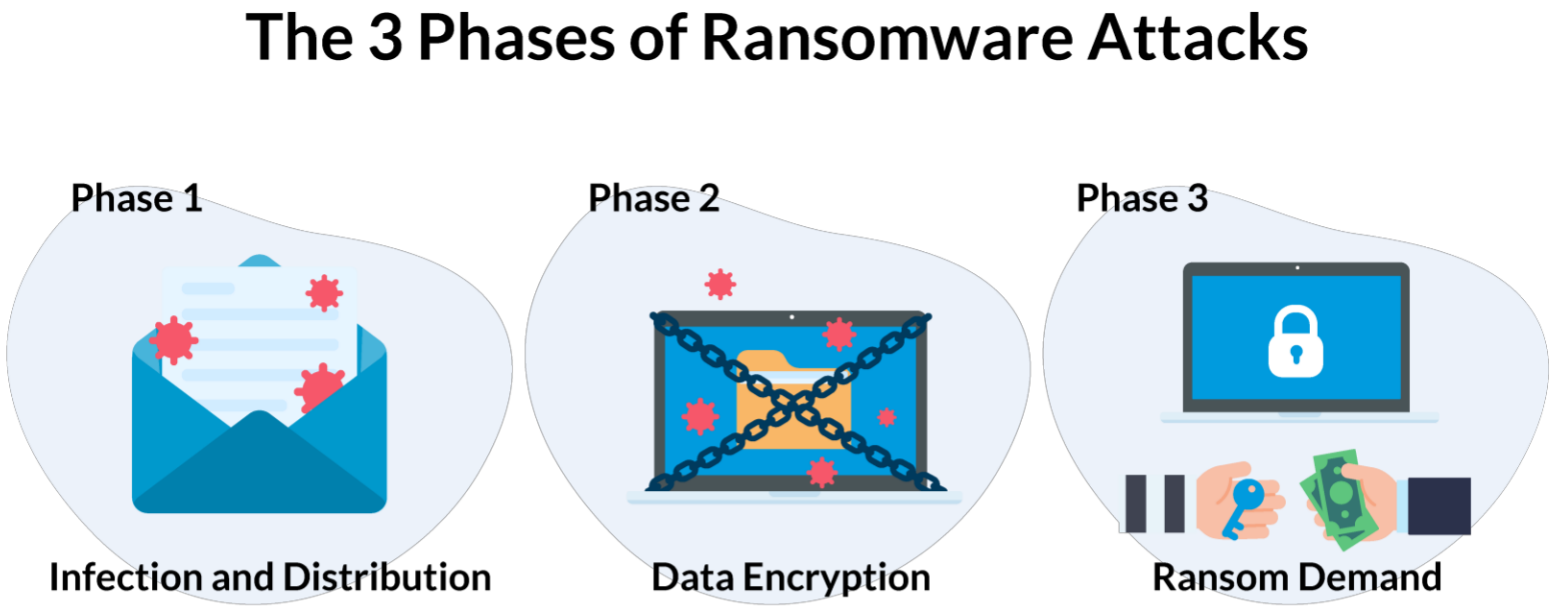


Worm:Win32 Conficker
Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.
Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.
Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.
Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.



Types of Malware

- Ransomware
  - Encrypts files, demands a ransom in Bitcoin



The 3 Phases of Ransomware Attacks

Phase 1

Infection and Distribution

Phase 2

Data Encryption

Phase 3

Ransom Demand

Types of Malware

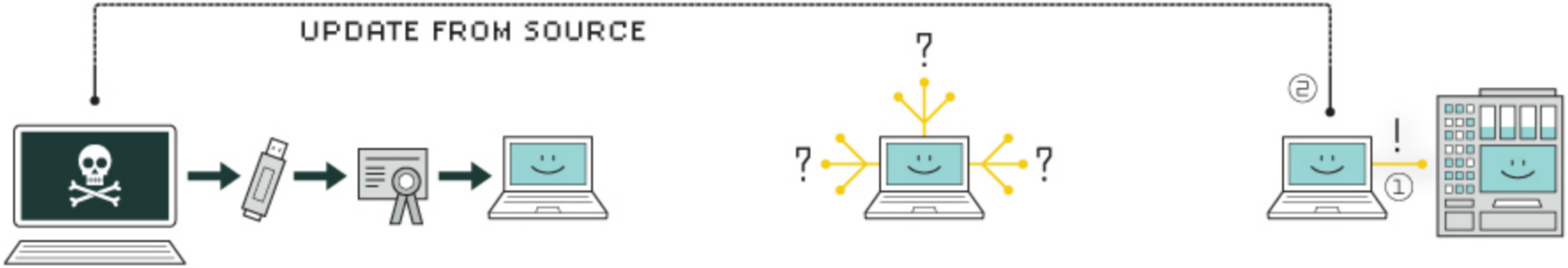
- Hybrid
  - Malware often spans multiple categories.
  - For example, a program might have a keylogger that collects passwords and a worm component that sends spam.
- Don’t get too caught up in classifying malware according to its functionality.
- Malware can also be classified based on whether the attacker’s objective is mass or targeted.
  - **Mass Malware.**
  - **Targeted Malware.**

Mass vs. Targeted Malware

- Mass malware (Shotgun Approach)
  - Intended to infect as many machines as possible
  - It's the most common type. Example: scareware
  - it's less sophisticated and easier to detect and defend against because security software targets it.

- Targeted malware (Tailored Approach)
  - Tailored to a specific target, such as Backdoors.
  - Its is a bigger threat to networks than mass malware.
    - Because it is not widespread, your security products probably won't protect you from it.
  - Very difficult to detect, prevent, and remove
  - It's very sophisticated, Requires advanced analysis techniques.
  - Ex: Stuxnet

HOW STUXNET WORKED



1. infection

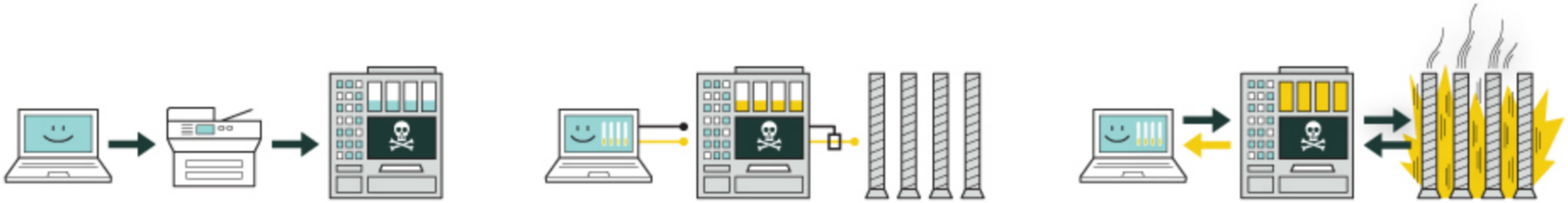
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Main Sources for these slides

- *Michael Sikorski and Andrew Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software"; ISBN-10: 1593272901.*

- *Xinwen Fu, “Introduction to Malware Analysis,” University of Central Florida*

- *Sam Bowne, “Practical Malware Analysis,” City College San Francisco*

- *Abhijit Mohanta and Anoop Saldanha, “Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware,” ISBN: 1484261925.*

Thank you