

Info 499

Practical Malware Analysis
Lecture 0

Introduction - Instructor

Introduction - Course Mechanics

What is Malware?

- Malicious software; causes detriment to a user, computer, or network
- Viruses, Worms, Trojans, Spyware, Adware, Scareware, Ransomware, Rootkits, Exploit Kits, Potentially Unwanted Applications, etc.
- Made by anyone: criminals, nation states, hacktivists, college kids

1. Steal assets
2. ...
3. Profit

What is Malware Analysis?

- Responding to an intrusion
- Determine what and how of an incident - who, when, why is usually for Digital Forensic Investigators
- Determine infection vector, persistence, exfiltration, and anti-forensics mechanisms employed by malware
- Develop host- and network-based signatures to assist with remediation and prevention

Malware Analysis Techniques

Compiled source code is not human-readable

- Basic static analysis
 - Examine executable without viewing instructions
 - Confirm maliciousness, determine basic functionality
 - Straightforward, quick, ineffective against sophisticated malware, misses a lot
- Basic dynamic analysis
 - Run the executable and observe behaviors and artifacts
 - Provides enough information to form some signatures
 - Straightforward, can still miss a lot
 - Requires a sandbox

Malware Analysis Techniques

- Advanced static analysis
 - Reverse engineer the executable by loading it into a disassembler and looking at instructions
 - Tells exactly what the program does
 - Requires specialized knowledge of disassembly, code constructs, and OS concepts
- Advanced dynamic analysis
 - Use a debugger while running the executable to step through the functionality
 - Can assist greatly with making sense of code during static analysis

Malware Classification

Knowing what you're looking for can help you find it!

- Backdoor: attacker connects, executes commands on local system
- Botnet: a collection of backdoors controlled by a command and control system (C2 or CnC)
- Downloader: Downloads other malicious code
- Information-stealing: Collects and exfiltrates information; sniffers, keyloggers, hash collectors, etc.

Malware Classification

- Launcher: uses non-traditional techniques to launch other programs
- Rootkit: conceals existence of malicious code
- Scareware: social engineering through fear
- Spam-sender: generates revenue for the attacker by sending spam as part of their spam-sending service
- Worm/Virus: Malware that replicates itself through user interaction (virus) or self-replication (worm) to infect other computers

Malware Classification - Ransomware

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



OK

Malware Classification - Scareware

The image is a screenshot of a Mac desktop. In the background, a Safari browser window is open to the URL `cdn.notifications.help`. The browser's address bar and menu bar are visible. The menu bar includes 'Safari', 'File', 'Edit', 'View', 'History', 'Bookmarks', 'Develop', 'Window', 'Help', and 'Debug'. The address bar shows the URL `cdn.notifications.help`. Below the address bar, there are several tabs or bookmarks, including 'logins', 'lookup', 'books', 'codes', 'Offers & Reb...', 'Rinnai', 'Cochlear Celeb', 'Games', 'Weather', 'Martha email', 'Montgomery ...kings Alumni', 'mt', 'Craigs list', and 'Flavor Bristo'. The main content area of the browser shows a red banner with the text 'Petaluma Restaurants, Dentists, Bars, Beauty Salons, Doctors' and a 'Support' link.

In the foreground, a fake 'Virus Found' alert is displayed. The alert has a red border and a white background. At the top, there is a compass icon and the text 'Virus Found' in large red letters. Below this, the text reads: 'Your Mac Computer has (13) infections!' followed by the phone number '1-844-858-0916' in large black letters. Below the phone number, it says 'Please call Tech Support as soon as possible.' At the bottom, it states: 'Apple has found (13) viruses that pose a serious threat. Browser.Hijacker.Spy / Trojan.BankPass-Download'. Below this, it says: 'Your computer is at a very high risk. Your financial and personal information is NOT secure. Please call 1-844-858-0916 NOW for emergency support.'

On the left side of the alert, there is a small window titled 'http://cdn.notifications.help' with a compass icon. It contains the text: 'Apple Firewall Warning: Your computer has a serious virus! If you see this message, you should call Apple Support at 1-844-858-0916. DATA AT RISK: 1. Your credit card details and banking information. 2. Your e-mail password and other passwords. 3. Your Facebook, Skype and other chat logs. 4. Your private photos and sensitive files. 5. Your webcam could be accessed remotely by hackers. Technicians are standing by to provide your FREE DIAGNOSIS & PRIORITY assistance removing this virus from your computer.' There is an 'OK' button at the bottom of this window.

Profit

Number	Type	Name	Country	City	Phone	Mail	DOB	Price	Select
372845		Charles F D	US	LA 90025	Y	N	Y	40\$	<input type="checkbox"/>
528713		Christopher B	US	Chicago IL 60606	Y	N	Y	40\$	<input type="checkbox"/>
645450		D WJ Rudy	US	MO 63106	Y	N	Y	40\$	<input type="checkbox"/>
371527		D Stevens	US	CA 90088	Y	N	Y	40\$	<input type="checkbox"/>
646880		Doris Darling	US	LA 90025	Y	N	Y	40\$	<input type="checkbox"/>
651920		Dora J	US	MO 63106	Y	N	Y	40\$	<input type="checkbox"/>
645857		D Roegner	US	MO 63106	Y	N	Y	40\$	<input type="checkbox"/>
371198		F Weininger	US	Phoenix AZ 85008	Y	N	Y	40\$	<input type="checkbox"/>
534248		Gordon M	US	Phoenix AZ 85008	Y	Y	Y	40\$	<input type="checkbox"/>
371726		Gary B	US	MO 63106	Y	N	Y	40\$	<input type="checkbox"/>
537161		Holly A	US	Chicago IL 60606	Y	N	Y	40\$	<input type="checkbox"/>
447639		John B	US	CA 90025	Y	N	Y	40\$	<input type="checkbox"/>
371730		J Roegner	US	Phoenix AZ 85008	Y	N	Y	40\$	<input type="checkbox"/>
528730		J Worling	US	CA 90088	Y	N	Y	40\$	<input type="checkbox"/>
653659		J W Rudy	US	MO 63106	Y	N	Y	40\$	<input type="checkbox"/>
									<input type="button" value="Buy"/>

Malware Classification

Malware may span categories

Can also be classified as mass (commodity) or targeted

- Mass
 - Shotgun approach
 - Most common, least sophisticated, easy to detect
- Targeted
 - Tailored to a specific organization
 - Rare, sophisticated, difficult to detect

General Rules

- Malware is complicated, focus on key parts and overviews - don't get stuck in the weeds
- Try different tools and approaches
- As we get better, so do they; security is a game of cat and mouse
- Malware analysis is an art, not a science