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!

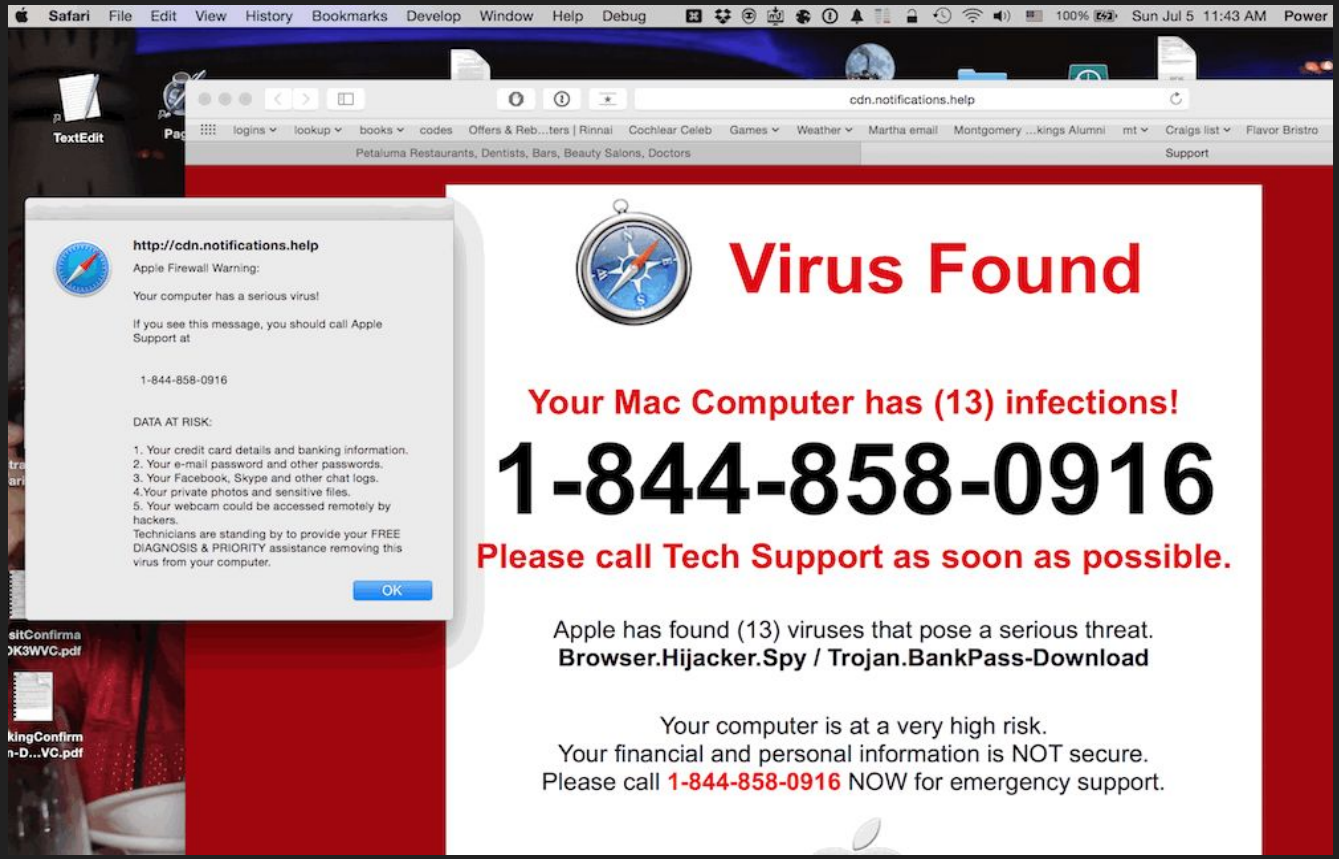
- Backdoor: attacker connects, executes commands on local system
- Botnet: a collection of backdoors controlled by a command and control system (C2 or CnC)
- Downloader: Downloads other malicious code
- Information-stealing: Collects and exfiltrates information; sniffers, keyloggers, hash collectors,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

Malware Classification - Scareware



Profit

Number	Type	Name	Country	City	Phone	Mail	DOB	Price	Select
372845	AMEX		US		Y	N	Y	40$	
528713	MasterCard		US		Y	N	Y	40$	
645450	DISCOVER		US		Y	N	Y	40$	
371527	AMEX		US		Y	N	Y	40$	
646880	DISCOVER		US		Y	N	Y	40$	
651920	DISCOVER		US		Y	N	Y	40$	
645857	DISCOVER		US		Y	N	Y	40$	
371198	AMEX		US		Y	N	Y	40$	
534248	MasterCard		US		Y	Y	Y	40$	
371726	AMEX		US		Y	N	Y	40$	
537161	MasterCard		US		Y	N	Y	40$	
447639	VISA		US		Y	N	Y	40$	
371730	AMEX		US		Y	N	Y	40$	
528730	MasterCard		US		Y	N	Y	40$	
653659	DISCOVER		US		Y	N	Y	40$	
									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