Introduction to Security Malware

Ming Chow (mchow@cs.tufts.edu)

Twitter: @0xmchow

Tufts UNIVERSITY | SCHOOL OF ENGINEERING Computer Science

Learning Objectives

- By the end of this week, you will be able to:
  - Describe types of malware
  - See certain malware behaviors
  - Scan and analyze malware
  - Reverse engineer Android apps to determine if they are malicious

Why Cover Malware In This Course?

- Still extremely relevant
- Still a huge problem
- Still a lot of misunderstandings and misconceptions
- Malware has become more sophisticated
- A logical transition as we have covered topics including networking, static and dynamic analysis, and password cracking which are important in some malware

Disclaimer

- I am not an expert in malware or malware analysis

Definitions

- **Malware** – Malicious software
- Many different types of malware including:
  - Virus
  - Worm
  - Backdoor
  - Trojan Horse
  - Rootkit
  - Ransomware
- **Zombie** – an infected and compromised machine or computing device
- **Botnet** – a network of infected machines; can be used to perform Distributed Denial of Service attacks
- **Bot herder** or **bot master** – attacker(s) who controller a botnet
- **Command and Control (C&C)** – infrastructure (e.g., servers, software) to control malware and botnet

Windows in the Good Old Days vs Unix/Linuxland

- Windowsland: Back in the good-old days, allows third-party applications to run in administrator by default (a.k.a.,root mode)
- Unix/Linuxland: Code will execute only with the permissions that are assigned to you. Therefore, less likely to wreck havok

Virus

- Think of a biological virus: *propagation and piggybacking*
- A malicious piece of executable code
- Propagates by attaching itself to a host file
- A virus can be:
  - An executable (i.e., .exe as seen in e-mail attachment)
  - A script
  - Document containing macros
  - A boot sector of a disk partition
- Note: when propagating, the virus does not have to be an exact copy of itself!
- If you send infected file to someone else and that person executes the file, it will infect the person's system as well
- Viruses do not re-infect already infected files

Anatomy of a Virus

- Wait on trigger event
- Replicate to files and disk
- On trigger event, payload is executed (note: it does not perform propagation)

Worm

- Does not need to attach itself to another file (i.e., self-contained)
- Send copies of itself over a network
- Another difference: a virus infects a machine while a worm infects a network (e.g., consuming bandwidth)
- How does a worm hop from machine to machine on a network? Using remote commands such as `rsh`, password cracking, using socket

Worm Techniques

- Scanning; select random IPv4 addresses
- Send small packets to reduce suspicion
- Connect to vulnerable network services, exploit vulnerability
- Perhaps even open up a shell

Analysis of a Worm: Morris Worm

- Named after Robert Tappan Morris, a Ph.D. student at Cornell, now a professor at MIT
- Brought down the Internet in November 1988
- 99 lines of code
- The idea: connect to another computer, find and use one of several vulnerabilities (buffer overflow in fingerd, password cracking, etc.) to copy itself to that second computer
- Mistake: both the original code and the copy would then repeat these actions in an infinite loop to other computers on the ARPANET
- Sendmail bug: At the time when this worm attack took place, it was possible to send a message to the sendmail program running on a remote machine with the debug mode turned on, and with the name of an executable as the recipient of the message. The sendmail program would then try to execute the named Þle, the code for execution being the contents of the message
- Via rsh and password cracking, when it was able to break into a user account, it would harvest addresses of other remote machines from their '.rhosts' files
- Professor Gene Spafford's analysis: http://spaf.cerias.purdue.edu/tech-reps/823.pdf
- Caused ~$10M - 100M in damages, over 5000 Unix machines affected
- First conviction in the US under the 1986 Computer Fraud and Abuse Act
- Sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.

Analysis of a Worm: Code Red

- July 2001
- Exploited bug in MS IIS to penetrate and spread: MS01-033 https://technet.microsoft.com/library/security/ms01-033
- Probes random IPs for systems running IIS (days 1 - 19 of attack)
- Defaced websites with the statement "Hacked by Chinese!"
- Had trigger time for denial-of-service attack (days 20 - 29 of attack)
- Second wave infected 360,000 servers in 14 hours

Analysis of a Worm: Slammer

- January 2003
- Random scanning worm
- Infected most of the IPv4 Internet in 10 minutes (75,000 hosts infected in one-half hour)
- Reference: http://www.caida.org/publications/papers/2003/sapphire/sapphire.html
- Exploited a buffer overflow bug: only machines running Microsoft SQL 2000 Servers
  - Supports directory service that allows a client to send in a UDP request to quickly find a database
  - MS02-039: https://technet.microsoft.com/library/security/ms02-039

Trojan Horse

- Seemingly useful program that contains code that does harmful things
- Can perform both overt and covert action
- Payload can be anything (e.g., keylogger, spyware)

Backdoor

- Bypasses authentication
- Grants attacker access to remote machine
- Connecting to a remote machine: used netcat or a malware kit (e.g., Mpack)

Backdoor Example: `tini`

- A simple and very small (3kb) backdoor for Windows
- Coded in assembler. It listens at TCP port 7777 and gives anybody who connects a remote Command Prompt.
  - If you have tini.exe, install it on a Windows target machine, double click on it.
  - On attacking machine, connect to Windows target machine say using Netcat: `nc <IP address of Windows target machine> 7777`
- http://ntsecurity.nu/toolbox/tini/ (WARNING: marked as a malicious website)
- VirusTotal details: https://www.virustotal.com/en/file/9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527/analysis/1325191864/
- Will be flagged by most anti-virus software

Rootkit

- Malicious software that *"acquires and maintains privileged access (read: root or administrative access) to the operating system (thus called rootkit) while hiding its presence by subverting normal OS behavior. A rootkit typically has three goals:*
  - *Run: A rootkit wants to be able to run without restriction on a target computer. Most computer systems (including Windows) have mechanisms such as Access Control Lists (ACLs) in place to prevent an application from getting access to protected resources. Rootkits take advantage of vulnerabilities in these mechanisms or use social engineering attacks to get installed so that they have no restrictions on what they are able to do.*
  - *Hide: Specifically, the rootkit does not want an installed security product to detect that it is running and remove it. The best way to prevent this is to appear invisible to all other applications running on the machine.*
  - *Act: A rootkit has specific actions it wants to take (often referred to as its payload). Running and being hidden are all well and good, but a rootkit author wants to get something from the compromised computer, such as stealing passwords or network bandwidth, or installing other malicious software."*
- Source and reference: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/rootkits.pdf

Rootkit (continued)

- Imagine you are running Windows PowerShell –it is not the same Windows PowerShell from Microsoft but a malicious version of PowerShell. How do you know?
- Think cloaking
- Detection can be very difficult
- List of known rootkits: https://www.bleepingcomputer.com/startups/rootkits/
- Defenses:
  - Tool: RootkitRevealer via SysInternals Suite by Microsoft https://technet.microsoft.com/en-us/sysinternals/rootkitrevealer.aspx
  - Secure wipe hard drive and reinstall everything

Ransomware

- The idea: malware that holds or locks your files or computer until you pay up (usually with Bitcoins)
- Rather new (circa 2012)
- Example: WannaCry of May 2017
  - *Background: Server Message Block (SMB) is the transport protocol used by Windows machines for a wide variety of purposes such as file sharing, printer sharing, and access to remote Windows services. SMB operates over TCP ports 139 and 445. In April 2017, Shadow Brokers released an SMB vulnerability named "EternalBlue" (from trove of leaked NSA exploits) which was part of the Microsoft security bulletin MS17-010: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx*
  - *WannaCry takes advantage of this vulnerability to compromise Windows machines, load malware, and propagate to other machines in a network. The attack uses SMB version 1 and TCP port 445 to propagate.*
  - Machines infected with the malware asked for $300 in Bitcoins to unlock contents on computer
  - Source and reference: https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

General Defense Against Malware

- Who do you trust?
- Check checksum of software downloads
- Secure wipe your system every so often
- Scan your system for any suspicious open ports
- Advanced: white-listing, behavior blocking
- Detect for program changes. Examples: Bit9 and Tripwire
- Patch operating system and applications ASAP
- Intrusion detection

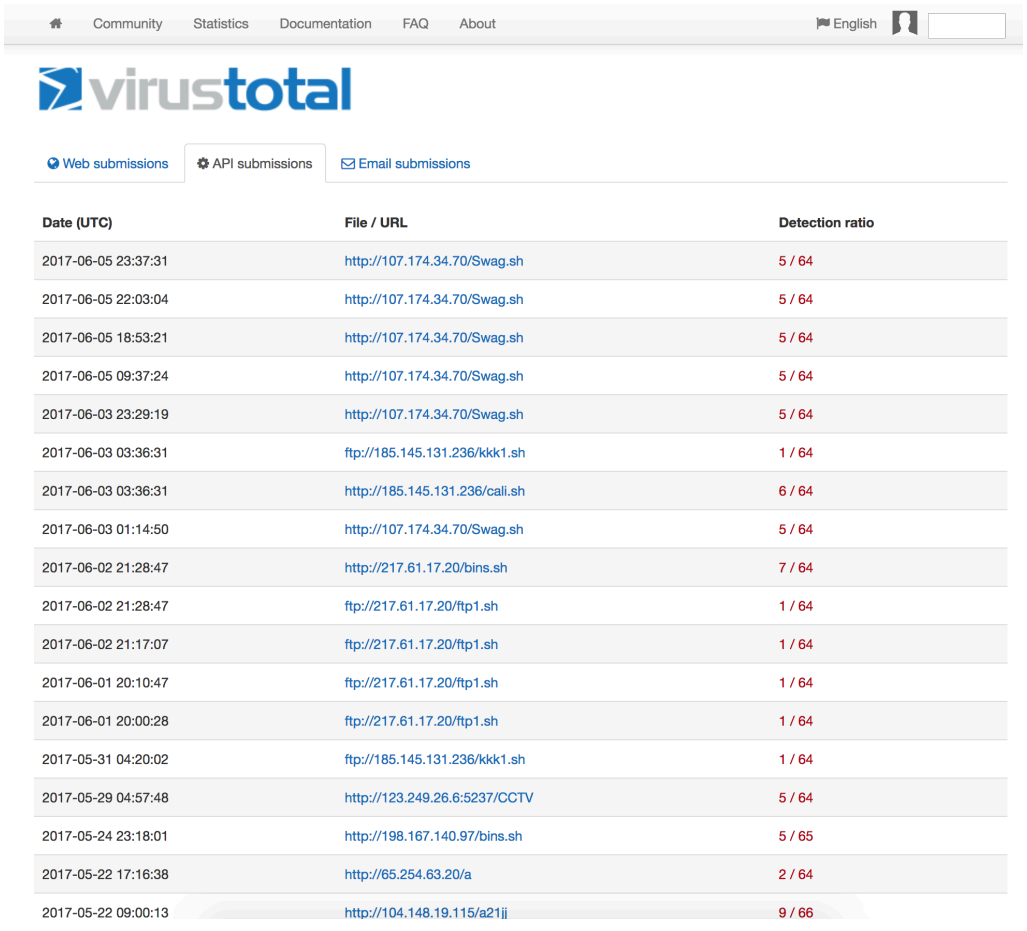
About Anti-Virus Software

- Provide a false sense of security
  - Case-in-point: anti-virus software did not catch WannaCry
- Based on signature scanning; early viruses had characteristic code patterns known as signatures
- Alas, largely reactive; only identifies what is known
- Unfortunately now, viruses are polymorphic, stealthy, and encrypted (decryption and key are somewhere else)
- Worms can prevents an automatic download of the latest virus signatures from the anti-virus software vendors by altering the DNS software on the infected machine

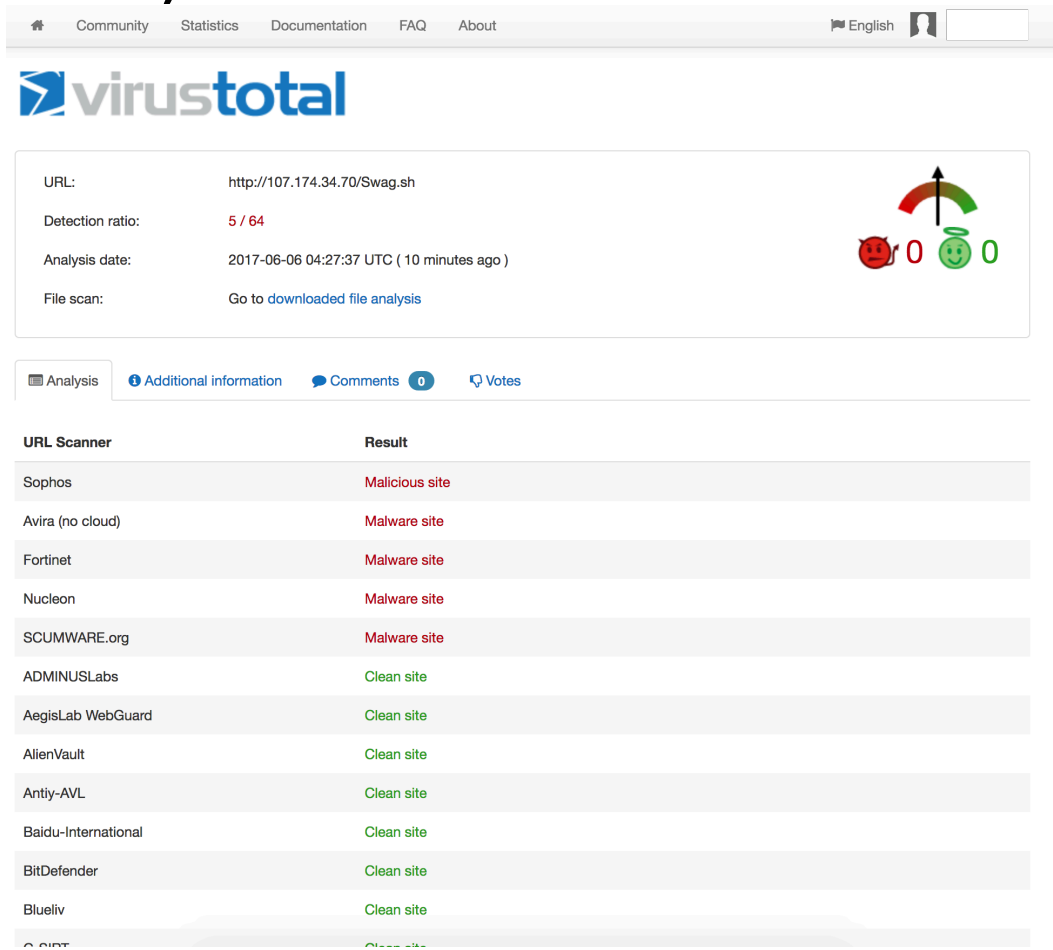
Tool: VirusTotal

- https://www.virustotal.com/
- Free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
- Maximum file size upload: 128MB
- Acquired by Google in September 2012

Tool: VirusTotal (continued)



Date (UTC)	File / URL	Detection ratio
2017-06-05 23:37:31	http://107.174.34.70/Swag.sh	5 / 64
2017-06-05 22:03:04	http://107.174.34.70/Swag.sh	5 / 64
2017-06-05 18:53:21	http://107.174.34.70/Swag.sh	5 / 64
2017-06-05 09:37:24	http://107.174.34.70/Swag.sh	5 / 64
2017-06-03 23:29:19	http://107.174.34.70/Swag.sh	5 / 64
2017-06-03 03:36:31	ftp://185.145.131.236/kkk1.sh	1 / 64
2017-06-03 03:36:31	http://185.145.131.236/cali.sh	6 / 64
2017-06-03 01:14:50	http://107.174.34.70/Swag.sh	5 / 64
2017-06-02 21:28:47	http://217.61.17.20/bins.sh	7 / 64
2017-06-02 21:28:47	ftp://217.61.17.20/ftp1.sh	1 / 64
2017-06-02 21:17:07	ftp://217.61.17.20/ftp1.sh	1 / 64
2017-06-01 20:10:47	ftp://217.61.17.20/ftp1.sh	1 / 64
2017-06-01 20:00:28	ftp://217.61.17.20/ftp1.sh	1 / 64
2017-05-31 04:20:02	ftp://185.145.131.236/kkk1.sh	1 / 64
2017-05-29 04:57:48	http://123.249.26.6:5237/CCTV	5 / 64
2017-05-24 23:18:01	http://198.167.140.97/bins.sh	5 / 65
2017-05-22 17:16:38	http://65.254.63.20/a	2 / 64
2017-05-22 09:00:13	http://104.148.19.115/a21jj	9 / 66



URL Scanner	Result
Sophos	Malicious site
Avira (no cloud)	Malware site
Fortinet	Malware site
Nucleon	Malware site
SCUMWARE.org	Malware site
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Baidu-International	Clean site
BitDefender	Clean site
Blueliv	Clean site

Where to Download Malware Samples

- Open Malware: http://openmalware.org/
- Contagio: https://contagiodump.blogspot.com/
- MalwareBlacklist: http://www.malwareblacklist.com/showMDL.php
- theZoo: https://github.com/ytisf/theZoo
- More sites to download malware samples at https://zeltser.com/malware-sample-sources/
- Why do this?
  - Research and learning purposes
  - To understand techniques used by malware writers, attackers (old and new)
  - To understand perhaps who the malware writers and attackers are
  - To build new tools and defenses

To Ponder

- Can you really get rid of a virus or worm now using anti-virus?
- If your system is infected with malware, can you even restore your system to "normal"?
- Do the general defenses listed previously even work?