CSF 434/534: Advanced Network and System Security

Week 01 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

An Overview of Malware

An Overview of Malware

Malware

- Malicious software - These can be very bad
- Gather information - Keystrokes
- Participate in a group - Controlled over a network
- Show you advertising - Big money
- Viruses and worms
  - Encrypt your data
  - Ruin your day

An Overview of Malware

Malware types and methods

- Viruses
- Crypto-malware, Ransomware
- Worms
- Trojan Horse
- Rootkit
- Keylogger
- Adware/Spyware
- Botnet

An Overview of Malware

How you get malware?

- These all work together
  - A worm takes advantage of a vulnerability
  - Installs malware that includes a remote access backdoor
  - Bot may be installed later
- Your computer must run a program
  - Email link
  - Don't click links
  - Web page pop-up
  - Drive-by download
  - Worm
- Your computer is vulnerable
  - Operating system
  - Keep your OS updated!
  - Application
  - The Adobe Flash vulnerability of the moment

Viruses and Worms

An Overview of Malware

Virus

- Malware that can reproduce itself
  - It doesn't need you to click anything
  - It needs you to execute a program
- Reproduces through file systems or the network
  - Just running a program can spread a virus
- May or may not cause problems
  - Some viruses are invisible, some are annoying
- Anti-virus is very common
  - Thousands of new viruses every week
  - Is your signature file updated?

An Overview of Malware

Types of Viruses

- Program viruses - It's part of the application
- Boot sector viruses - Who needs an OS?
- Script viruses - Operating system and browser-based
- Macro viruses - Common in Microsoft Office

An Overview of Malware

Worms

- Malware that self-replicates
  - Doesn't need you to do anything
  - Uses the network as a transmission medium
  - Self-propagates and spreads quickly
- Worms are pretty bad things
  - Can take over many systems very quickly
- Firewalls and IDS/IPS can mitigate many worm infestations
  - Doesn't help much once the worm gets inside

Ransomware and Crypto-Malware

Ransomware and Crypto-Malware

Your data is valuable

- Personal data
  - Family pictures and videos
  - Important documents
- Organization data
  - Planning documents
  - Employee personally identifiable information (PII)
  - Financial information
  - Company private data
- How much is it worth?
  - There's a number

Ransomware and Crypto-Malware

Ransomware

- The bad guys want your money
  - They'll take your computer in the meantime
- Probably a fake ransom
  - Locks your computer "by the police"
- The ransom may be avoided
  - A security professional may be able to remove these kinds of malware

Ransomware and Crypto-Malware

Crypto-malware

- New generation of ransomware
  - Your data is unavailable until you provide cash
- Malware encrypts your data files
  - Pictures, documents, music, movies, etc.
  - Your OS remains available
  - They want you running, but not working
- You must pay the bad guys to obtain the decryption key
  - Untraceable payment system
  - An unfortunate use of public-key cryptography

Ransomware and Crypto-Malware

Ransomware

- Denies access to a computer system or data until a ransom is paid

Crypto-malware

- Encrypts programs and files on the computer in order to extort money from the user

Ransomware and Crypto-Malware

Protecting against ransomware

- Always have a backup - an offline backup, ideally
- Keep your operating system up to date
  - Patch those vulnerabilities
- Keep your applications up to date
  - Security patches
- Keep your anti-virus/anti-malware signatures up to date
  - New attacks every hour
- Keep everything up to date.

Trojans and RATs

Trojans and RATs

Trojan horse

- Used by the Greeks to capture Troy from the Trojans
  - A digital wooden horse
- Software that pretends to be something else
  - So it can conquer your computer
  - Doesn't really care much about replicating
- Circumvents your existing security
  - Anti-virus may catch it when it runs
- The better Trojans are built to avoid and disable AV
- Once it's inside it has free reign
  - And it may open the gates for other programs

Trojans and RATs

Backdoors

- Why go through normal authentication methods?
  - Just walk in the back door
- Often placed on your computer through malware
  - Some malware software can take advantage of backdoors created by other malware
- Some software includes a backdoor
  - Old Linux kernel included a backdoor
  - Bad software can have a backdoor as part of the app

Trojans and RATs

Remote Access Trojans (RATs)

- Remote Administration Tool
  - The ultimate backdoor
  - Administrative control of a device
- Malware installs the server/service/host
  - Bad guys connect with the client software
- Control a device
  - Key logging, screen recording/screenshots, copy files
- Embed more malware

Rootkits

Rootkits

Rootkits

- Originally a Unix technique
  - The “root” in rootkit
- Modifies core system files
  - Part of the kernel
- Can be invisible to the operating system
  - Won’t see it in Task Manager
- Also invisible to traditional anti-virus utilities
  - If you can’t see it, you can’t stop it

Rootkits

Kernel drivers

- Zeus/Zbot malware
  - Famous for cleaning out bank accounts
- Now combined with Necurs rootkit
  - Necurs is a kernel-level driver
- Necurs makes sure you can’t delete Zbot
  - Access denied
- Trying to stop the Windows process?
  - Error terminating process: Access denied

Rootkits

Finding and Removing rootkits

- Look for the unusual
  - Anti-malware scans
- Use a remover specific to the rootkit
  - Usually built after the rootkit is discovered
- Secure boot with UEFI
  - Security in the BIOS

Keyloggers

Keyloggers

Keyloggers

- Your keystrokes contain valuable information
  - Web site login URLs, passwords, email messages
- Save all of your input
  - Send it to the bad guys
- Circumvents encryption protections
  - Your keystrokes are in the clear
- Other data logging
  - Clipboard logging, screen logging, instant messaging, search engine queries

Keyloggers

Preventing Keyloggers

- Usually installed with malware
  - Use anti-virus/anti-malware
  - Keep your signatures updated
- Block unauthorized communication
  - Block the exfiltration attempt
  - Firewall rules / monitoring
- Run a keylogging scanner
  - Checks for keylogging activity

Adware and Spyware

Adware and Spyware

Adware

- Your computer is one big advertisement
  - Pop-ups with pop-ups
- May cause performance issues
  - Especially over the network
- Installed accidentally
  - May be included with other software installations
- Be careful of software that claims to remove adware
  - Especially if you learned about it from a pop-up

Adware and Spyware

Spyware

- Malware that spies on you
  - Advertising, identity theft, affiliate fraud
- Can trick you into installing
  - Peer to peer, fake security software
- Browser monitoring - Capture surfing habits
- Keyloggers
  - Capture every keystroke, send it back to the mother ship

Adware and Spyware

Why is there so much adware and spyware?

- Money - Your eyeballs are incredibly valuable
- Money - Your computer time and bandwidth is incredibly valuable
- Money - Your bank account is incredibly valuable

Adware and Spyware

Protecting against adware/spyware

- Maintain your anti-virus / anti-malware
  - Always have the latest signatures
- Always know what you're installing
  - And watch your options during the installation
- Where's your backup?
  - You might need it someday
  - Cleaning adware isn't easy
- Run some scans
  - Malwarebytes

Bots and Botnets

Bots and Botnets

Botnets

- Robot networks
  - Skynet is self-aware
- Once your machine is infected, it becomes a bot
  - You may not even know
- How does it get on your computer?
  - Trojan Horse (I just saw a funny video of you! Click here.) You run a program or click an ad you THOUGHT was legit, but...
  - OS or application vulnerability
- A day in the life of a bot
  - Sit around. Check in with the mother ship. Wait for instructions.

Bots and Botnets

Botnets (cont.)

- A group of bots working together
  - Nothing good can come from this
- Distributed Denial of service (DDoS)
  - The power of many
- Botnets are for sale
  - Rent time from the bad guys
  - Not a long-term business proposition

Bots and Botnets

Stopping the Bots

- Prevent the initial infection
  - OS and application patches
  - Anti-virus/anti-malware and updated signatures
- Identify an existing infection
  - On-demand scans
  - Network monitoring
- Prevent command and control (C&C)
  - Block at the firewall
  - Identify at the workstation with a host-based firewall or host-based IPS

Logic Bombs

Logic Bombs

Logic Bomb

- Waits for a predefined event
  - Often left by someone with grudge
- Time bomb - Time or date
- User event - Logic bomb
- Difficult to identify
  - Difficult to recover if it goes off

Logic Bombs

Real world logic bombs

- March 19, 2013, South Korea
  - Email with malicious attachment sent to South Korean organizations
  - Posed as a bank email
  - Trojan installs malware
- March 20, 2013, 2 p.m. local time
  - Malware logic-bomb activates
  - Storage and master boot record deleted, system reboots
- Boot device not found.
  - Please install an operating system on your hard disk.

Logic Bombs

Preventing a logic bomb

- Difficult to recognize
  - Each is unique - No predefined signatures
- Process and procedures
  - Formal change control
- Electronic monitoring
  - Alert on changes
  - Host-based intrusion detection, Tripwire, etc.
- Constant auditing
  - An administrator can circumvent existing systems

Phishing

Phishing

Phishing

- Social engineering with a touch of spoofing

Check the URL

- Usually there's something not quite right
  - Spelling, fonts, graphics
- Vishing is done over the phone
  - Fake security checks or bank updates

Phishing

Spearfishing

- Phishing with inside information
  - Makes the attack more believable
  - Spearphishing the CEO is "whaling"
- April 2011 - Epsilon
  - Less than 3,000 email addresses attacked
  - 100% of email operations staff
  - Downloaded anti-virus disabler, keylogger, and remote admin tool
- April 2011 - Oak Ridge National Laboratory
  - Email from the "Human Resources Department"
  - 530 employees targeted, 57 clicked, 2 were infected
  - Data downloaded, servers infected with malware

Tailgating and Impersonation

Tailgating and Impersonation

Tailgating

- Use someone else to gain access to a building
  - Not an accident
- Johnny Long / No Tech Hacking
  - Blend in with clothing
  - 3rd-party with a legitimate reason
  - Temporarily take up smoking
  - I still prefer bringing doughnuts
- Once inside, there's little to stop you
  - Most security stops at the border

Tailgating and Impersonation

Watching for tailgating

- Policy for visitors
  - You should be able to identify anyone
- One scan, one person
  - A matter of policy or mechanically required
- Mantrap / Airlock
  - You don't have a choice
- Don't be afraid to ask
  - Who are you and why are you here?

Tailgating and Impersonation

Impersonation

- Pretend to be someone you aren't
  - Halloween for the fraudsters
- Use some of those details you got from the dumpster
  - You can trust me, I'm with your help desk
- Attack the victim as someone higher in rank
  - Office of the Vice President for Scamming
- Throw tons of technical details around
  - Catastrophic feedback due to the depolarization of the differential magnetometer
- Be a buddy
  - How about those Cubs?

Tailgating and Impersonation

Protect against Impersonation

- Never volunteer information
  - My password is 12345
- Don't disclose personal details
  - The bad guys are tricky
- Always verify before revealing info
  - Call back, verify through 3rd parties
- Verification should be encouraged
  - Especially if your organization owns valuable information

CSF 434/534: Advanced Network and System Security

Week 01 - Review

"If you spend more on coffee than on IT security, you will be hacked."

– Richard Clarke

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes