INTRO TO ETHICAL HACKING

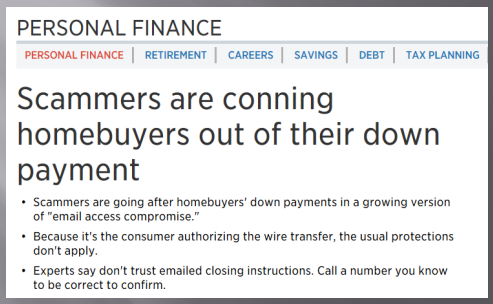
MIS 5211.701

Week 8

Site:
https://community.mis.temple.edu/mis5211sec701fall2020/

1

News



PERSONAL FINANCE

PERSONAL FINANCE | RETIREMENT | CAREERS | SAVINGS | DEBT | TAX PLANNING

Scammers are conning homebuyers out of their down payment

- Scammers are going after homebuyers' down payments in a growing version of "email access compromise."
- Because it's the consumer authorizing the wire transfer, the usual protections don't apply.
- Experts say don't trust emailed closing instructions. Call a number you know to be correct to confirm.

https://www.cnbc.com/2017/10/19/scammers-are-conning-home-buyers-out-of-their-down-payment.html

2

News

- Classic "Reconnasaince"
  - Scammers monitor Realtors or Mortgage companies waiting for "Closing"
  - Shortly before closing the spoof a message to buyer indicating changes to wire transfer instructions
  - Since transfer is initiated by buyer, there is a very limited time period to recover the money

3

SUDO Vunerability

- Already posted to Class Blog
- https://thehackernews.com/2019/10/linux-sudo-run-as-root-flaw.html

4

Tonight's Plan

- Malware

5

Malware

- Code used to perform malicious action

Or

- Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.

6

What it is used for

- Steal personal information
  - Credentials
  - Credit Card Numbers
  - Whole Identities
- Ransom files
- Delete files
- Click fraud
- Use your computer as relay
- Logic bombs

MIS 5211.701 7

7

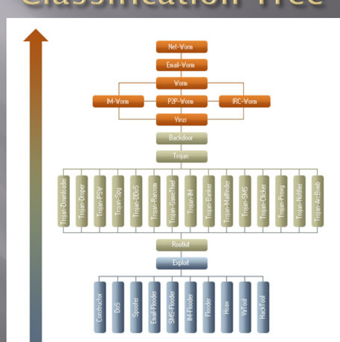
Forms

- Static (My words)
- Polymorphic : uses a polymorphic engine to mutate while keeping the original algorithm intact (packer)
- Metamorphic : Change after each infection

MIS 5211.701 8

8

Kaspersky Malware Classification Tree



Source: http://usa.kaspersky.com/internet-security-center/threats/malware-classifications#.VEcRrXl0vUk

MIS 5211.701 9

9

Some Definitions

- Payload - harmful things the malicious program does, after it has had time to spread.
- Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).
- Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- Logic Bomb - malicious code that activates on an event (e.g., date).
- Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.

10

Shellcode

- You will see the term Shellcode used intermittently throughout the presentation
- Shellcode is defined as a set of instructions injected and then executed by an exploit program – The Shellcoder's Handbook 2nd Edition
- Derived from the original purpose of the software to create a "Shell" at the root level

11

What is a Shell

- First, a shell is not a terminal
  - For the mathematically inclined
  - Shell != Terminal
- What this means
  - Not all terminal commands will work in a shell
  - For instance:
    - Clear for clear screen
    - Turn Echo On or Off
    - CTRL-C
    - CTRL-D
    - Etc…

12

More on Shell

- Terminals include code and protection to interpret user input, and ensure everything works
- A shell is a raw command line to send characters to, and receive characters from a system. That is, raw stdin and stdout. That's it. It cannot interpret or catch control codes or screen commands

13

Technical Types

- User Mode Root Kits
- Kernel Mode Root Kits
- Keyloggers
- Sniffers
- Downloaders
- HTTP C2 Channels

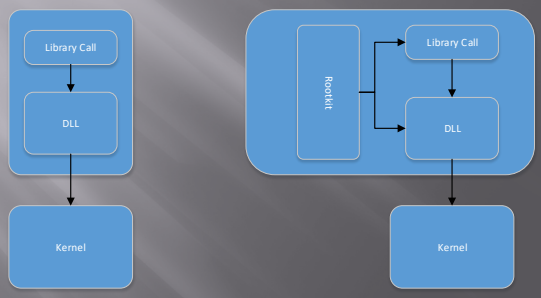
14

User Mode Root Kits

- Purpose
  - Attain access
  - Maintain access
  - Hide access
- Operates in user mode
  - That is, gets injected into one or more individual processes

15

What it Looks Like



16

What is Happening

- Rootkit intercepts data to:
  - Netstat
  - Process Explorer
  - Task Manager
- Therefore, when a user or admin looks at these tools everything looks normal

17

Two Key Infection Steps

- DLL Injection (Dynamic Link Library)
  - Running code within the address space of another process
  - Malware "Injects" itself into a DLL using
    - SetWindowsHookEx
    - CreateRemoteThread/LoadLibrary
  - Note: These are legitimate commands that are used by software for things like patching
- API Hooking (Application Programming Interface)
  - Intercepting function calls, messages, or events passed between software components

18

Notes on Rootkits

- These methods were developed in Windows XP and earlier machines
- Still possible with Vista, 7, and 8 – Just need to work a little harder

19

Kernel Mode Rootkits

- Injected into the Kernel, below the level of process and DLL
- Runs at the highest privilege level for software
- Removal likely requires reinstallation of operating system

20

Keyloggers

- Monitor user key strokes
- Lots of bots, worms, and assorted other malware does this
  - Sends logs to attacker
- Common methods
  - Hook for keyboard events
  - Poll keyboard state with GetAsyncKey()

21

Sniffers

- Similar to tcpdump or windump covered earlier, but now its malicious
- Common method
  - Put interface into promiscuous mode
  - Controller passes all traffic it receives to the CPU
- Other ways
  - Intercept network related calls
  - Intercept higher level functions
    - We'll see this late with Browser proxies
  - Installing BHOs (Browser Helper Objects)

22

Downloaders

- Used by attackers to deliver malware in stages
- Initial malware can be very small, only needs to fetch the next piece of software
  - Easier to obfuscate
  - May escape detection
  - Action is not malicious in and by itself
- Droppers are similar, but embedded the downloaded functionality in their own code

23

Example Commands

- URLDownloadToFile()
  - Download and save file to disk
- ShellExecute()
  - Execute file
- WinExec()
  - Execute file

24

Command and Control Channels

- AKA HTTP C2 Channels
  - Ubiquitous
  - Port 80 almost always open
  - Use port 443 and your coms are encrypted
- Alternatives
  - IRC (Internet Relay Chat)
  - P2P (File Sharing)
  - DNS (Tunnel data over DNS)

25

Approaches

- Reverse shell over HTTP (Port 80)
- Embedded in regular HTTP traffic
  - Disguised like normal user traffic

26

Infection Channels

- MS Office Files
- PDF Files
- Flash
- JavaScript

- Lots more, but these are the ones we will talk about

27

MS Office Files

- Why Office
  - Everybody is using it
  - File freely passed around and not unexpected
  - Parsing binary office format is difficult
  - Robust embedded scripting language (VBA)
  - You can even hook Apple products

Source for Graphic:
http://www.mobilemfx.com/mblog/microsoft_office_coming_for_ipad_as_well_as_a_new_fetchos_version_for_fetchos.html

28

Techniques

- Embedded Shellcode
  - Exploits vulnerability in office software
  - No user interaction required
- Embedded VBA Script
  - Executes on document open
  - May require user to click OK or "Enable Content"

Note about VBA – Term Macro is misleading. Implies it is for basic scripting. Today, VBA is a full fledged language.

29

Adobe PDF

- Why PDF
  - Everybody is using it
  - Files freely passed around and not unexpected
  - PDF Format
    - Proprietary(ish)
      - Used to be proprietary, published by ISO as ISO/IEC 32000-1:2008
    - Feature rich
    - Can include active content
      - JavaScript
      - ActionScript via Flash Objects
  - And finally
    - New vulnerabilities found regularly

30

More Adobe PDF

- High profile attack target
  - http://www.darkreading.com/vulnerabilities---threats/report-sixty-percent-of-users-are-running-unpatched-versions-of-adobe/d/d-id/1136022
  - 6 in 10 installs of Adobe Reader are out of date
- Complex structure
  - Easily obfuscated
  - Need software tools to open and understand
  - Even AV vendors have problems keeping an eye on this

31

Where are the Vulnerabilities

- Parser components
- JavaScript and ActionScript
- Embedded Shellcode executes by exploiting these vulnerabilities

32

Flash

- Ubiquitous on websites
- New vulnerabilities weekly (at least that's how it feels)
- So bad Apple and now Kindle will not allow flash to be installed without jail breaking the devices

33

More Flash

- Uses the SWF file format
- See: http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/devnet/swf/pdf/swf-file-format-spec.pdf
- Supports ActionScript language for scripting, including legacy support for older versions of ActionScript

34

Flash Vulnerabilities

- Client Side
  - Flash Parameter Injection
    - Inject parameters when Flash object is embedded in an HTML page
  - Cross Domain Privilege Escalation
    - Access and modify DOM
  - Cross Site Scripting
    - Access and modify DOM
  - Cross Site Flashing
    - Call another flash object from flash

35

JavaScript

- Just a teaser at this point
- JavaScript is a primary infection path with web site based attacks
  - Used for:
    - Cross Site Scripting (XSS)
    - Cross Site Request Forgery (CSRF)
    - Direct Delivery
      - Downloaders
      - Droppers
      - Keyloggers
      - And anything else you want

36

More JavaScript

- JavaScript based attacks are frequently heavily obfuscated with multiple layers of encryption, obfuscation, encoding, and false flags
- Attackers will "buy" ad space and put up legitimate looking ads on legitimate sites
  - Since adds are rotated, infection is inconsistent and difficult to pin down

37

Testing AV

- During Penetration Tests a tester may be asked to verify that the AV suite is working
- You don't want to actually send malware
- What do you do?

- Answer
  - EICAR
  - http://www.eicar.org/86-0-Intended-use.html

38

EICAR

- EICAR is a Anti-Malware Test File
- Originally developed by Paul Ducklin
- All major AV vendors will flag this file if properly installed and configure
- Tester can simply send the file in via normal channel being tested and then confirm that AV suites correctly identified and blocked file.

39

Odds and Ends

- I'm malware, where do I hide
  - Inside other executables
  - Inside data files
  - In Alternate Data Streams (ADS)
  - On the hard drive, but outside of the file system
  - In BIOS

40

Detection

- Malware in executables and data files can be detected of you know what good is supposed to look like
- Malware also leaves markers in the file system that can be detected
- Commercial tools like Mandiant, FireEye, and others can pick these up
  - Worth noting: FireEye bought Mandiant

41

Alternate Data Stream (ADS)

- Compatibility feature of NTFS
  - Part of file system, but not part of file system
  - Originally created to allow NTFS to handle Apple file attributes that were stored outside of the file structure
  - Creates an "Off Book" location to store data and/or executables that will not be seen via file commands or through GUI folder tools
  - http://www.windowsecurity.com/articles-tutorials/windows_os_security/Alternate_Data_Streams.html

42

Hard Drive

- Not all space on the drive is consumed by the file system
- Vendors sometime use this space to keep configuration information or recovery files
- Attackers can use the space as well
- Caution: While tools exist to read and write to raw space, writing is extremely dangerous as you can render the file system useless.

43

BIOS

- Firmware installed on motherboard that instructs CPU how to turn on
  - What drive to boot from
  - Is there a password to just turn on
- Other hardware has similar Firmware
  - Graphics Cards
  - Network Cards
  - Other specialty boards

44

What is Firmware

- Firmware is rewritable code in a chip or other piece of hardware that retains it's coding even without power
- It only changes when specific external commands are given to update or overwrite

45

Impact of BIOS Malware

- Malware can withstand a complete re-image of the file system
- Replacing the hard drive will not mitigate
- Since it is in place a boot time, before the kernel ever starts, it can re-infect
- Example: Supermicro https://www.bleepingcomputer.com/news/security/firmware-vulnerabilities-disclosed-in-supermicro-server-products/

46

Next Week

- We will be covering
  - OWASP top 10
  - Web Application Hacking
  - Intercepting Proxies
  - URL Editing

47

Questions

?

48