Lab 1

Lab_01-1.malware

- This was compiled on 5/14/2009, 13:12:41PM
- List a few imports or sets of imports and describe how the malware might use them
  - TerminateThread and TerminateProcess might be used for terminating itself in case it detects that the user is trying to detect it while it's running.
  - CreateProcessA might be used in process hollowing.
  - WriteFile can be used for writing to the child process created by CreateProcessA, additionally, it can be used to write to the socket that lets the program communicate with the ip address 60.248.52.95:443.
- What are a few strings that stick out to you and why?
  - http://www.ueopen.com/test.html - I figure this could be used to check if the computer is connected to the internet
  - 60.248.52.95:443 - The malware probably uses this ip address to phone home, given that the check for the previous string succeeded
  - "cmd.exe" indicates that it's probably running some commands and "/c del" is probably what it uses to delete itself
- What happens when you run this malware? Is it what you expected and why?
  - It deletes itself. It makes sense because they have `cmd.exe /c del`, but I wasn't expecting it to delete itself, but rather just some temporary files
- Name a procmon filter and why you used it.
  - I used "Process Name is Lab_01-1.exe, Include" to only see events from the malware executable itself.
- Are there any host-based signatures? (Files, registry keys, processes or services, etc).
  - Yes, there's cmd.exe, WS2_32.dll, urlmon,dll, KERNEL32.dll, USER32.dll, SHELL32.dll, and MSVCRT.dll
- Are there any network based signatures?
  - Yes, there's `http://www.ueopen.com/test.html` and `60.248.52.95.443`
- Is there anything that impeded your analysis?
  - Yes, the file kept deleting itself, which made it harder to run multiple times because I'd have to restart my virtual machine and restore the snapshot from before I ran it.

- What do you think is the purpose of this malware?
  - I think this malware is supposed to send information from the machine it's running on to a server.

Lab_01-2.malware

- What is the md5sum? What of interest does VirusTotal report?
  - The md5sum is 02658bc9801f98dfdf167accf57f6a36. It tires to send an HTTP request to an IP address, it writes to the user's cookies, it opens a bunch of `\DEVICE` files, it deletes a setup file, and it reads and writes to various internet setting related registry keys.
- List a few imports or sets of imports and describe how the malware might use them.
  - KERNEL32.dll, which it probably uses to read and write to the registry keys and cookies
  - MSVCRT.dll, uses for C++ stdlib functions.
  - WININET.dll is probably used to send information back to an IP address
- What are a few strings that stick out to you and why?
  - `69.25.50.10`, which is probably the server that it's sending information back to
  - `cmd /c`, which it uses to execute shell commands
  - "Begin Download", "Downloadfiles", "Begin Upload", and "Uploadfiles" indicate that it's probably an interactive program used to download/upload files.
  - The "Microsoft Corporation" related strings and "svchost.exe" help disguise it
- What happens when you run this malware?
  - Nothing visible happens, but it opens and writes to a bunch of files and registry keys, like I expected. I wasn't able to find any instances of it connecting to the internet though, which confused me.
- Name a procmon filter and why you used it.
  - I used Detail contains "Network" to try and find any network
- Are there any host-based signatures?
  - KERNEL32.dll, wuacult.exe, svchost.exe, WININET.dll, MSVCRT.dll
- Are there any network based signatures?
  - 69.25.50.10
- Is there anything that impeded your analysis?
  - I'm having trouble getting it to connect to the IP to analyze the network traffic.
- What do you think is the purpose of this malware?
  - I think the malware is a thing that intercepts web traffic and sends it to a server.

Lab_01-3.malware

- Are there any indicators that this malware is packed? What are they? What is it packed with?
  - Yes, it has UPX in its signature, it has high entropy, and it uses VirtualAlloc
- Are you able to unpack it? Why or why not?
  - Not with UPX because it was modified after packing, but I was able to do it manually with x32dbg.
- What are a few strings that stick out to you and why?
  - "Mozilla/4.0" and "http://%s//5s/" right after, which are probably used to send an HTTP request
  - "ld.exe", I'm not super sure what this is for, but I suppose it's probably used to check the linker for some reason
  - "Program:" and "GetLastActivePopup" being very close to each other leads me to believe that it's a program with a GUI
- What happens when you run this malware? Is it what you expected and why?
  - It brings up a black window. I expected that it would bring up a window, but I thought it would have buttons and text and stuff, instead of just being black
- Are there any host-based signatures?
  - Yes, WININET.dll, WS2_32.dll, ld.exe, KERNEL32.dll
- Are there any network based signatures?
  - I couldn't find any in the executable, but Virustotal says there's a few practicalmalwareanalysis.com
- What do you think is the purpose of this malware?
  - I'm not sure