**INSTRUCTIONS**

In Lecture 1, we discussed setting up the Flare VM for your malware analysis environment. To do this, follow the lecture examples.

Once this is set up, open LECTURE1.BIN, change the .bin to .exe and follow the examples from the lectures. Once your analysis is complete, you can run the software in your VM.

Answer the following questions:

* Upload the file to [http://www.VirusTotal.com/](http://www.virustotal.com/). Does the file match any existing antivirus signatures?

Using the tools we discussed today, answer the below.

* When was this file compiled?
* Are there any indications that this file is packed or obfuscated?
  + If so, what are the indicators?
* Do any imports hint at what this malware does?
  + If so, which imports are they?
* Are there other files or host-based indicators you could look for on infected systems?
* \****ONLY IN THE VM\****  Run the file and record your observations.
  + Take a screenshot showing "The Thing."
  + Have you seen this application before? Where have you seen it, or what was it like when you first observed it? If this is your first time, what do you think?
  + What network-based indicators could be used to find this malware on infected machines?
  + What would you guess is the purpose of this file?
  + What challenges did you face with this setup and running this in your VM?
  + What was the more exciting part once you ran the file?
* Now, how often would you be able to run this VM?
* What is one question that you would like to ask the author?
* Go to another post and answer as if you were the author. Come back here and provide a link to your response.

**WRITEUP**

The compilation timestamp is 2054-07-03 at 03:59:10 UTC. The odd timestamp is confirmed in VirusTotal as an evasion technique and the file matched an existing antivirus signature for the Trojanxd malware.

PEiD shows that there was nothing found for file packing and VirusTotal doesn’t seem to indicate that the malware is packed based off of the behavior. No indicators of obfuscation were detected. A .exe file extension wasn’t appended to the normal file extension and a packer was not used to camouflage the program’s true intentions.

Some .dll imports called by this program are concerning. The Dependencies program detected imports of kernel32, user32, gdi32, and ntdll. They hint that this piece of malware has the capability to access and modify the core OS functions (kernel32 and ntdll) in order to manipulate the user interface in some fashion (user32/gdi32).

Other host-based indicators to look for on infected systems vary greatly and depend on the type of malware one is searching for. One could search for Remote Access Trojans, backdoors, or a bot infection through a network traffic and CPU/RAM usage analysis. Other types of malware that are hidden can also be intuitively sensed by the user if their computer deviates too far from baseline performance. Log file inspections would provide a great indicator of a malware infection. They could assist in determining the vector of such an attack so far as they are retained for a sufficient period of time. An additional location for malware to hide would be in the registry. Most likely, a piece of malware would be embedded in a file that a user downloaded from an untrusted website.

This is my first time viewing this malware. I’m very fortunate I don’t have epilepsy because it could cause someone with that condition to have a seizure. But after the lightshow was over, I thought the screen melt was kind of cool. I don’t believe that there would be any network-based IoCs with this malware as the general purpose of it is to just be a nuisance for the host machine. Most likely, the developer of this malware did it “for the lulz” due to the name being “Trojanxd” where XD is an emoticon of someone laughing hard.

The most exciting part of detonating this malware was knowing that my VM could easily be restored to the desired state and that my PC was unaffected.

The most difficult part of setting up the VM was configuring Windows appropriately to ensure that FlareVM installed correctly. Most annoying was disabling OneDrive and editing the registry to ensure that the local desktop was displayed and not the OneDrive desktop. Next, ensuring that the Group Policy for Windows Defender was appropriately set was an interesting exercise and the first time that I have tinkered with the GP editor. Lastly, since the free VMWare Workstation 16 doesn’t have a snapshot tool incorporated into it, I decided to buy a software license for VMWare Pro. My time and monetary investment in establishing this VM is indicative of my intention to run it often, whether it be professionally or recreationally.

**Question for the malware author:** If this program ended up killing someone due to them suffering an epileptic seizure, would you think that going to prison for manslaughter is justified?

Resources:

<https://github.com/mandiant/flare-vm>

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

The password to your VM is "Passw0rd!"

Your user name should not have a space in it **AT ALL**

<https://www.fireeye.com/services/freeware/flare-vm.html#:~:text=FLARE%20VM%20is%20a%20freely,%2C%20forensicators%2C%20and%20penetration%20testers.>