Malware Analysis Project

You will receive a PDF that does contain an attack. The attack will deliver and execute another program onto your VM environment. You will need to describe the Windows OS version(s), as well as the Acrobat Reader version(s) that you used for these steps.

It will be your job to use malware analysis methods learned from this class or on your own to document specific characteristics and behaviors of the malware. You will need to employ the methods learned in HW01 and HW02 to collect traffic from the malware. You will also need to provide some yara signatures derived from static analysis, similar to what’s described in HW04.

**PDF Static Analysis**

**PDF File Name:**

**PDF MD5 Hash:**

**PDF SHA-1 Hash:**

**PDF Creation Date:**

**PDF Modification Date:**

**PDF Title:**

**PDF Author:**

**PDF Creator:**

**PDF Producer:**

**Number of named PDF objects:**

**List of PDF object numbers that contain streams:**

**List the object number (or numbers) that contain streams that causes the exploit:**

**Create a yara rule that you can use to identify the object above, using a command like the following: pdf-parser.py -y your-rule.yar attack.pdf**

**If I run the above command, pdf-parser.py should be able to show me the same object(s) that you listed above for the exploit. Include this yara rule in your submission. Name it *username*-pdf.yar (where *username* is your UC user name).**

**PDF Dynamic Analysis**

**You will need to identify at least one version of Acrobat Reader that the PDF will execute with. No need to do an exhaustive search.**

**What system-level effects does the PDF cause Acrobat Reader to take in order to get the backdoor onto the system (writes files to disk, deletes files, etc…)?**

**For instance, the PDF may write one or more files to disk as well as execute one or more subprocesses (including the backdoor). Please list the names of these files as well as the process names.**

**Backdoor Static Analysis**

**The PDF intends to install a backdoor on the system (eventually). This may occur directly from the PDF, or there may be a couple more steps that occur following the PDF to get the backdoor installed. Identify which EXE file installed on the system acts as the backdoor, and analyze it.**

**EXE Filename:**

**EXE Compile Time:**

**EXE Type (.NET or Normal WinAPI executable? 32-bit? 64-bit?):**

**DLL Imports (DLL filename, Symbol name):**

**How does the EXE achieve persistence (Registry Run? Start Menu? Service?):**

Analyze Strings from Malware:

**Do any file names appear to reflect files written during malware execution (hint: you will want to use IDA Free to inspect CreateFileA calls, the data passed to them, and similar). If so, what are these file names (and full paths if present)?**

**Select at least 10 strings from the backdoor that do not occur in the benign set of EXE data I provided. Use these to create a strings-based yara signature that doesn’t generate any hits on the normal windows programs provided. Include the command that you ran to test this.**

**Include the output of running yara with the “-s” option using this yara rule against the backdoor EXE file. Name your yara signature *username*-strings.yar and the output file name should be named *username*-strings.out. This should be similar to what you did in HW04.**

**Backdoor Dynamic Analysis**

**The malware should attempt to communicate to the Internet. Identify the domain name that the malware is attempting to use to communicate to the Internet, as well as the TCP port.**

**You will then need to configure your VM to force the DNS resolution for that domain name to resolve to an IP address that you control within your virtual environment. Utilize some method for capturing the traffic beacon that is sent when the malware successfully connects (you may want to utilize what you learned in the earlier HW01 and HW02, in order to capture the traffic). It is common to do this with two VMs, one of them (such as Remnux) pretending to be the server. However, it is also possible to do this entirely on your windows host, but you would need to install extra software (such as netcat or fakenet).**

**Where was the backdoor installed on the system?**

**Document the HTTP traffic:**

**What is the HTTP path requested?**

**What is the HTTP command/verb being used?**

**What is the User-Agent value being sent (one of the HTTP headers)?**