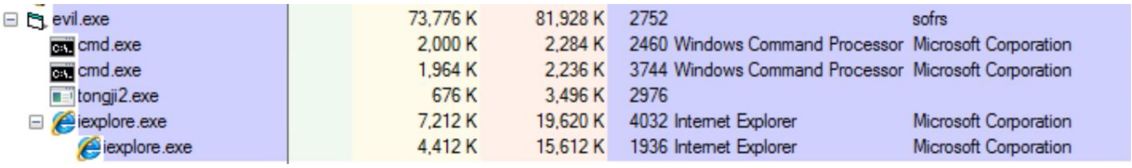
Nicolas Barraclough
10/4/2020
CS373 - Defense Against the Dark Arts

Homework 1 - evil.exe

- The first thing I noticed when I ran “evil.exe” was that FakeNet showed DNS queries being received from the domains: 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa, hisunpharm.com, static.naver.net, timeless888.com, etc. Automatic HTTP GET requests were sent to hisunpharm.com, timeless888.com, as well as some other domains which requested various types of files including one “pao.exe” file.
- Immediately after running evil.exe, a pop-up prompted the setup of Windows Internet Explorer 8 (not sure if this was caused by the malware).
- I tried filtering my Process Monitor to see the actions performed by evil.exe, but a single click inside the window caused it to stop responding. No matter how long I waited, the Process Monitor would not respond.
- I tried opening the command prompt but a window popped up telling me that Microsoft Windows was not responding either. Ending the process removes the desktop completely including the task bar. I’m not sure at the moment if this is the malware at work, or just the poor processing power of the VM.
- In the Process Explorer, I was able to locate the evil.exe process and saw that it was accessing the command prompt, an unknown executable, and Internet Explorer at the domain timeless888.com. (Shown below)



evil.exe		73,776 K	81,928 K	2752		sofrs
cmd.exe		2,000 K	2,284 K	2460	Windows Command Processor	Microsoft Corporation
cmd.exe		1,964 K	2,236 K	3744	Windows Command Processor	Microsoft Corporation
tongji2.exe		676 K	3,496 K	2976		
iexplore.exe		7,212 K	19,620 K	4032	Internet Explorer	Microsoft Corporation
iexplore.exe		4,412 K	15,612 K	1936	Internet Explorer	Microsoft Corporation

- I was able to locate the malware on Anti Spy through the Registry in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run. It was called skunser and its data was an executable in C:\ntldrs\svchest.exe
- In Anti Spy, I was able to locate a couple of the files that were previously mentioned that were obtained via the HTTP GET requests. Located in Temporary Internet Files deep within the C:\Users directory, were the files “favicon[1].htm” and pao[1].exe”. These files are obviously copies. Anti Spy labeled the directory that these files were in as “Hidden”.
  Sharing the same timestamp (which was actually around 6 hours ahead of the time I executed evil.exe) as the two aforementioned files, was “tongji2.exe” located in C:\Program Files. The only file in the directory C:\ntldrs was the actual

malware “svchest.exe”. The other files mentioned in the homework description were not present. Looking at the timestamp column, I was able to see that the ntldrs folder was created along with the previously mentioned files that had a creation time set in the future. The “svchest.exe” had a timestamp of 2014/02/07, so I could conclude that this piece of malware was created in 2014 and is possibly already known.

As for what the malware was intended to do, I could not reach a conclusion. Every so often, the VM would crap out on me and tell me that Microsoft Explorer was not responding. I was unable to access the command prompt after running evil.exe and was very limited on the amount of processing power the VM could use. All I could figure out regarding the intention of the malware was that it created automatically scheduled tasks to run another executable. I found this by sending evil.exe to FileInsight where I was able to see plaintext depicting that the malware attempted to start the Task Scheduler and start the “svchest.exe” file every 30 minutes until the 25 hour.