Arthur Liou

CS373

**Lab 1 Writeup**

Prompt:

* Please submit a write-up detailing what you looked at, how you looked at it, what you found, and what conclusions you've come to. Be detailed.

I’ve added the link to VM instructions and steps below. My write up will be after the steps

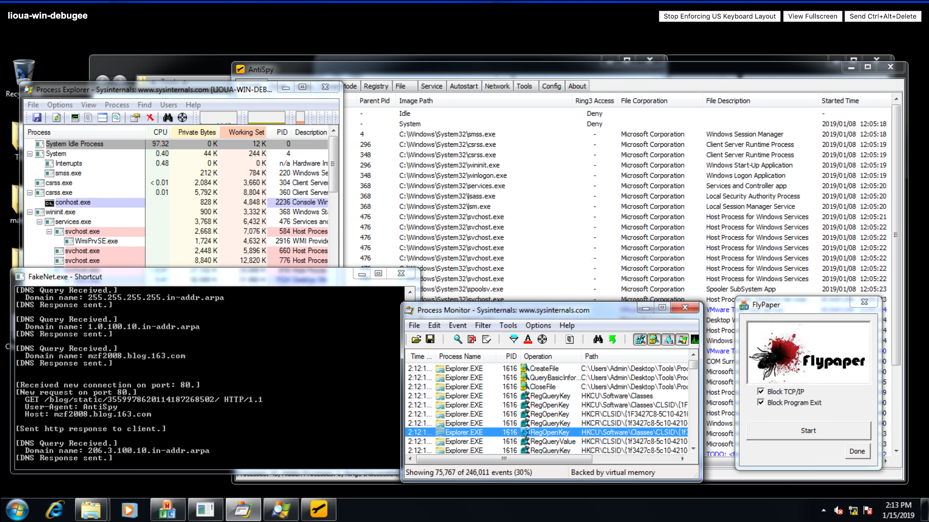
VM Instructions: <https://oregonstate.instructure.com/courses/1712159/pages/vm-instructions?module_item_id=18495782>

Steps: Everything below should be on the VM unless stated otherwise.

1. Go to (Desktop\malware\malwarebasics\Class1\Lab2\Replication\Sample1\0012b0384774e51acd053c0f6b1dd112)
2. Rename this file to evil.exe
3. Startup the following tools from your tools folder on the Desktop:
   * Flypaper (and click start)
   * Fakenet
   * Process Monitor
   * Process Explorer
   * Antispy
4. BE SURE YOU HAVE TAKEN A SNAPSHOT BEFORE THE FOLLOWING STEP
5. Run the malware ‘Evil.exe’ – note the time your executing it since you can use this timestamp for events in the tools and system-tools of Windows
6. Watch the tools in action, what are you observations in the tools for Evil.exe, what registry keys, files, scheduled tasks etc.
   * Process Monitor, stop the monitoring of the events and look for evil.exe, and examine what happens
   * Investigate process activity with the tools
   * You should find items like below and investigate them:
     + C:\WINDOWS\system32\drivers\etc\hosts /t /g everyone:F
     + cmd /c attrib -r -a -s -h C:\WINDOWS\system32\drivers\etc\hosts
     + cmd /c ""C:\ntldrs\funbots.bat" "
     + "C:\Program Files\Internet Explorer\IEXPLORE.EXE" <http://timeless888.com/tong.htm>
7. Look at the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\skunser = C:\ntldrs\svchest.exe CreateFile:
8. Look at the output from the tools with regards to network activity.
9. Investigate the file-locations you should have found with the tools used:
   * C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\KLTT2YG3\pao[1].exe
   * C:\Program Files\tongji2.exe
   * C:\ntldrs\svchest.exe
   * C:\ntldrs\Isinter.gif
   * C:\ntldrs\funbots.bat
   * C:\ntldrs\system.yf
10. Process Explorer: By selecting a process with a right-mouse-click you can look into the properties and will find details about the process running – like a strings-dump.
11. Use Windows build in tools and commands to look at the infection. Think about:
    * Windows Search
    * Taskscheduler
    * Command-prompt using commands like: AT, use the ‘attrib’ command on the malware folder created etc.

**Write Up**

Step 4



* What I looked at: I ran an “evil.exe” malware program.
* How you looked at it: I followed the steps above and tracked the processes through the 5 tools listed above.
* What you found: My observations included, in addition to observing the processes listed in 6 and 9 above, I would see popups, such as for setting up Internet Explorer, windows menu popping up, “Windows Explorer is not responding” error (which might be normal since CPU usage did hit 95%+ and often 100%, leading to slow processing), and some other popups which indicated. In Process Explorer, I saw that evil.exe opened up the command terminal, it’s own program of iexplore.exe, and a rundll32.exe
  + When looking at the processes in Process Monitor, looking for the 4 commands below, I could see these run being run via cmd.exe (see Additional Screenshots below)
    - C:\WINDOWS\system32\drivers\etc\hosts /t /g everyone:F
    - cmd /c attrib -r -a -s -h C:\WINDOWS\system32\drivers\etc\hosts
    - cmd /c ""C:\ntldrs\funbots.bat" "
    - "C:\Program Files\Internet Explorer\IEXPLORE.EXE" <http://timeless888.com/tong.htm>
  + In FakeNet, I found multiple calls to ports with “Windows Media Center PC”, it looks like it was trying to get exe files, gif, txt. It looks like it was trying to maintain a connection “Keep-Alive” and also had a host: www.download.windowsupdate.com” and hisunpharm.com, and also downloading a authrootst1.cab
  + I also went to the evil.exe Properties in Process Explorer, went to the Strings tab, and found a plethora of printable strings.. A lot of gifs, some cmds to drivers/hosts, a “WHAT A FFFING DAY”, a lot of gibberish strings, then a “Task Scheduler” and a whole bunch of the “interactive svchest.exe at every 30 minute interval, includes some execution files, close and creation of registration keys, file downloads, etc. I inspected some of the other sub-exe executions, but thought the “overview” exe would be best to write down and analyze.
    - Student Note to Instructor: I thought opening this up was the most useful part of this lab.
  + Also: Cscls.exe – control ACLs Progress, Attribute utility (attrib.exe), longji2.exe
* What conclusions you've come to: The malware looked like a spam program. It utilized the command terminal, added / altered registry keys and other .exe hosts. Opened a query windows to a specific location to find an exe (the rundll32.exe), which had a target of dsquery.dll. It seemed to open connections and download files (gifs, txt, exe, see Step 9) from multiple URLs. It seemed to schedule an exe to run each half hour and would do a bunch of “random” things (see strings above). It looked like it would rewrite, delete, and create registry keys to prevent the user from being able to block and / or remdy the situation.

Also I found a post / question in Piazza regarding the tools which I found useful as I am a beginner in all the tools. I’ve copied them here for future reference.

* FakeNet emulates the network environment and trick the malware into thinking it is connected to the Internet.
* Process Explorer allows you to view running processes and drill down/explore into those process details.
* ProcMon shows real-time file system, Registry and process/thread activity.
* Antispy allows you to spot malware.
* Flypaper loads as a device driver and blocks all attempts to exit a process, end a thread, or delete memory. All components used by the malware will remain resident in the process list, and will remain present in physical memory.

Additional Screenshots

