Disclaimer: Scenarios for all of my assignments are *completely fictional*, but may include actual names, locations, and landmarks to add realism.
SCENARIO:

Great work with that CPS Energy Case last week!

HELP!

Your co-worker (Greg) had to leave urgently on a family emergency. Prior to leaving, he was analyzing a critical piece of malware (virus.exe) and said the malware deleted itself during his analysis. Poor Greg failed to make a backup of the malware ahead of time (oops!), so all he has to pass on to you are the results of some static and dynamic analysis he already performed.

Greg zipped his analysis results for you (Greg_Analysis.zip).

It's all up to you! Can you determine the critical details associated with this malware?

Assignment -- Your mission should you choose to accept it:

--Download the Greg_Analysis zip file from Professor Ervin's OneDrive account.
--Also, Install Procmon to load Greg's Procmon analysis.

--To assist you, please reference Prof Ervin's lecture that demonstrates how to use Procmon and it's filter capabilities to narrow down malware operations. Additionally, how to interpret InetSim reporting.

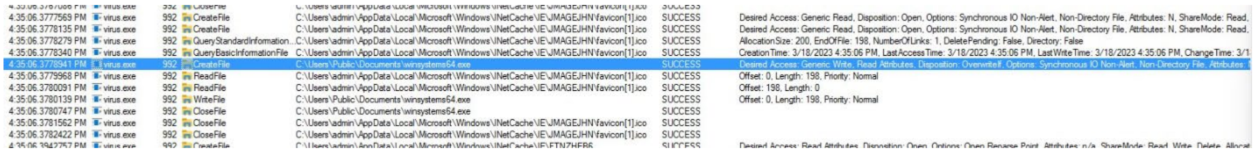
GRADING RUBRIC -- To receive full credit for this assignment, you must answer the following:

1. Use Procmon and Greg's Procmon analysis file (Procmon_log_virus.PML) to determine the file-path and filename where the malware dropper is being stored on the victim system. Submit a screenshot to support your findings.
2. Based on your analysis of Greg's data, what is the URL that is dropping additional malware on the victim system? Law Enforcement needs this to further their investigation! Submit a screenshot to support your findings.

BONUS (10-pts)
An additional 10pts to any student who is able to setup the Win10 Sandbox/Remnux environment, execute the Unknown2.exe malware (as I demonstrate in lecture), send a 'netstat' command to the malware, and submit a screenshot of the base64 output of the command. You may use your own properly-configured sandbox setup or the sandbox VMs I provide (Remnux_Configured.zip and Win10_Sandbox_Configured.zip) in the Week-10 Lecture Folder on OneDrive.
Good Luck!!

1. Used Procmon and Greg's Procmon analysis file (Procmon_log_virus.PML) to determine the file-path and filename where the malware dropper was stored on the victim system.

file-path: `C:\Users\Public\Documents\winsystems64.exe`
filename: `winsystems64.exe`

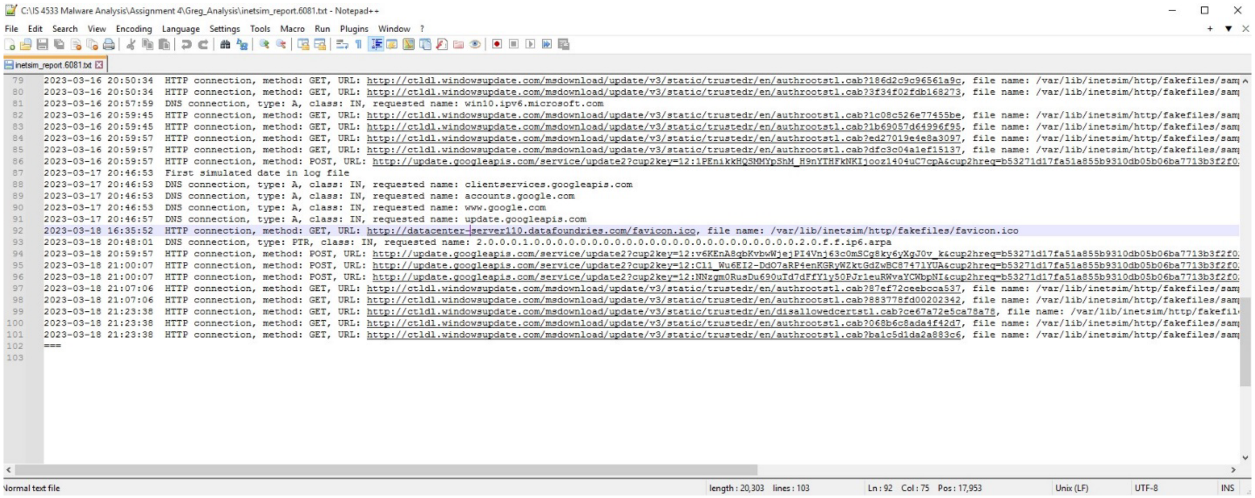


```
4:35:06.3767088 PM  virus.exe  992  CloseFile                    C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS
4:35:06.3777569 PM  virus.exe  992  CreateFile                   C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS  Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read,
4:35:06.3778135 PM  virus.exe  992  CreateFile                   C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS  Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read,
4:35:06.3778279 PM  virus.exe  992  QueryStandardInformation...  C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS  AllocationSize: 200, EndOfFile: 198, NumberOfLinks: 1, DeletePending: False, Directory: False
4:35:06.3778340 PM  virus.exe  992  QueryBasicInformationFile    C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS  CreationTime: 3/18/2023 4:35:06 PM, LastAccessTime: 3/18/2023 4:35:06 PM, LastWriteTime: 3/18/2023 4:35:06 PM, ChangeTime: 3/1
4:35:06.3778941 PM  virus.exe  992  CreateFile                   C:\Users\Public\Documents\winsystems64.exe                                           SUCCESS  Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: 
4:35:06.3779968 PM  virus.exe  992  ReadFile                     C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS  Offset: 0, Length: 198, Priority: Normal
4:35:06.3780091 PM  virus.exe  992  ReadFile                     C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS  Offset: 198, Length: 0
4:35:06.3780139 PM  virus.exe  992  WriteFile                    C:\Users\Public\Documents\winsystems64.exe                                           SUCCESS  Offset: 0, Length: 198, Priority: Normal
4:35:06.3780747 PM  virus.exe  992  CloseFile                    C:\Users\Public\Documents\winsystems64.exe                                           SUCCESS
4:35:06.3781562 PM  virus.exe  992  CloseFile                    C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS
4:35:06.3782422 PM  virus.exe  992  CloseFile                    C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\JMAGEJHN\favicon[1].ico  SUCCESS
4:35:06.3942757 PM  virus.exe  992  CreateFile                   C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\ETNZHFB6                 SUCCESS  Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, Allocat
```

Figure 1: Screen shot captured via Process Monitor

2. Based on my analysis of Greg's data, the URL that was dropping additional malware on the victim system:

URL: `http://datacenter-server110.datafoundries.com/favicon.ico`

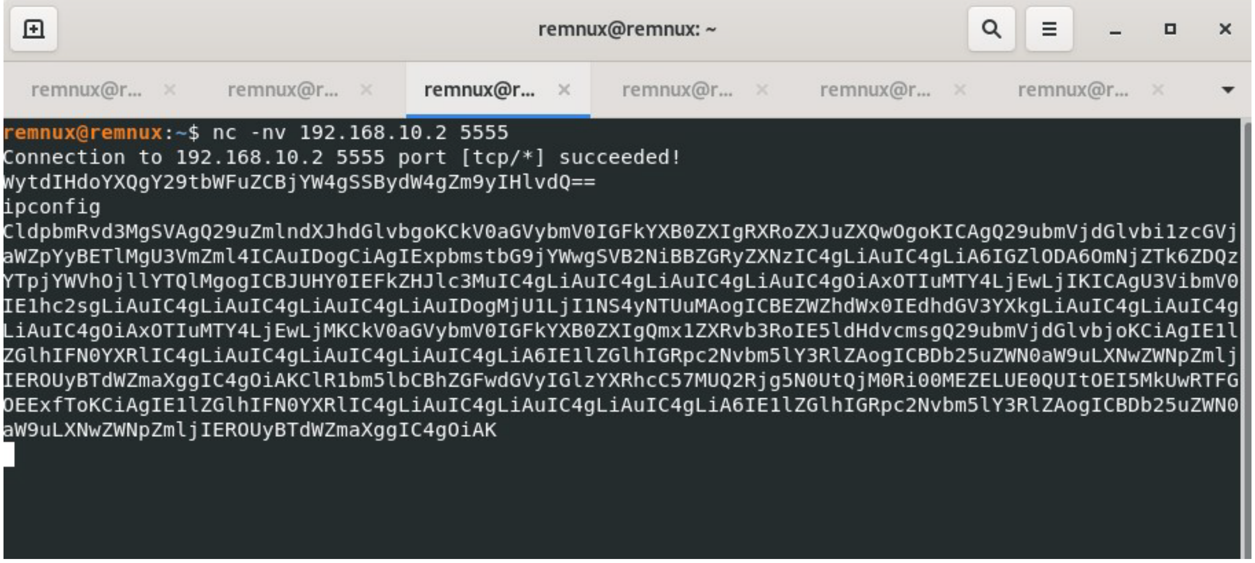


C:\IS 4533 Malware Analysis\Assignment 4\Greg_Analysis\inetsim_report.6081.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
inetsim_report.6081.txt
Normal text file
length : 20,303 lines : 103
Ln : 92 Col : 75 Pos : 17,953
Unix (LF)
UTF-8
INS

```
2023-03-16 20:50:34  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?186d2c9c96561a9c, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-16 20:50:34  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?3f34f02fdb168273, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-16 20:57:59  DNS connection, type: A, class: IN, requested name: win10.ipv6.microsoft.com
2023-03-16 20:59:45  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?1c08c526e77455be, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-16 20:59:45  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?1b69057d64996f95, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-16 20:59:57  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?ed27019e4e8a3097, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-16 20:59:57  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?dfc3c04a1ef15137, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-16 20:59:57  HTTP connection, method: POST, URL: http://update.googleapis.com/service/update2?cup2key=12:1PEnikkHQSMMYpShM_H9nYTHFkNKIjooz1404uC7cpA&cup2hreq=b53271d17fa51a855b9310db05b06ba7713b3f2f0
2023-03-17 20:46:53  First simulated date in log file
2023-03-17 20:46:53  DNS connection, type: A, class: IN, requested name: clientservices.googleapis.com
2023-03-17 20:46:53  DNS connection, type: A, class: IN, requested name: accounts.google.com
2023-03-17 20:46:53  DNS connection, type: A, class: IN, requested name: www.google.com
2023-03-17 20:46:57  DNS connection, type: A, class: IN, requested name: update.googleapis.com
2023-03-18 16:35:52  HTTP connection, method: GET, URL: http://datacenter-server110.datafoundries.com/favicon.ico, file name: /var/lib/inetsim/http/fakefiles/favicon.ico
2023-03-18 20:48:01  DNS connection, type: PTR, class: IN, requested name: 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa
2023-03-18 20:59:57  HTTP connection, method: POST, URL: http://update.googleapis.com/service/update2?cup2key=12:v6KEnA8qbKvbwWjejPI4Vnj63c0mSCg8ky6yXgJ0v_k&cup2hreq=b53271d17fa51a855b9310db05b06ba7713b3f2f0
2023-03-18 21:00:07  HTTP connection, method: POST, URL: http://update.googleapis.com/service/update2?cup2key=12:C11_Wu6EI2-DdO7aRP4enKGRyWZktGdZwBC87471YUA&cup2hreq=b53271d17fa51a855b9310db05b06ba7713b3f2f0
2023-03-18 21:00:07  HTTP connection, method: POST, URL: http://update.googleapis.com/service/update2?cup2key=12:NNzgm0RusDu690uTd7dFfY1y50PJr1euRWvaYCWbpNI&cup2hreq=b53271d17fa51a855b9310db05b06ba7713b3f2f0
2023-03-18 21:07:06  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?87ef72ceebcca537, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-18 21:07:06  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?883778fd00202342, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-18 21:23:38  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ce67a72e5ca78a78, file name: /var/lib/inetsim/http/fakefil
2023-03-18 21:23:38  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?068b6c8ada4f42d7, file name: /var/lib/inetsim/http/fakefiles/sam
2023-03-18 21:23:38  HTTP connection, method: GET, URL: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?ba1c5d1da2a883c6, file name: /var/lib/inetsim/http/fakefiles/sam
===
```

Figure 2: Screen shot captured via Notepad++

BONUS



```
remnux@remnux:~$ nc -nv 192.168.10.2 5555
Connection to 192.168.10.2 5555 port [tcp/*] succeeded!
WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==
ipconfig
CldpbmRvd3MgSVAgQ29uZmlndXJhdGlvbgoKCkV0aGVybmV0IGFkYXB0ZXIgRXRoZXJuZXQwOgoKICAgQ29ubmVjdGlvbi1zcGVj
aWZpYyBETlMgU3VmZml4ICAuIDogCiAgIExpbmstbG9jYWwgSVB2NiBBZGRyZXNzIC4gLiAuIC4gLiA6IGZlODA6OmNjZTk6ZDQz
YTpjYWVhOjllYTQlMgogICBJUHY0IEFkZHJlc3MuIC4gLiAuIC4gLiAuIC4gLiAuIC4gOiAxOTIuMTY4LjEwLjIKICAgU3VibmV0
IE1hc2sgLiAuIC4gLiAuIC4gLiAuIC4gLiAuIDogMjU1LjI1NS4yNTUuMAogICBEZWZhdWx0IEdhdGV3YXkgLiAuIC4gLiAuIC4g
LiAuIC4gOiAxOTIuMTY4LjEwLjMKCkV0aGVybmV0IGFkYXB0ZXIgQmx1ZXRvb3RoIE5ldHdvcmsgQ29ubmVjdGlvbjoKCiAgIE1l
ZGlhIFN0YXRlIC4gLiAuIC4gLiAuIC4gLiAuIC4gLiA6IE1lZGlhIGRpc2Nvbm5lY3RlZAogICBDb25uZWN0aW9uLXNwZWNpZmlj
IEROUyBTdWZmaXggIC4gOiAKClR1bm5lbCBhZGFwdGVyIGlzYXRhcC57MUQ2Rjg5N0UtQjM0Ri00MEZELUE0QUItOEI5MkUwRTFG
OEExfToKCiAgIE1lZGlhIFN0YXRlIC4gLiAuIC4gLiAuIC4gLiAuIC4gLiA6IE1lZGlhIGRpc2Nvbm5lY3RlZAogICBDb25uZWN0
aW9uLXNwZWNpZmljIEROUyBTdWZmaXggIC4gOiAK
```