Song Yang ([sea.yang@rutgers.edu](mailto:sea.yang@rutgers.edu))

Xin Yang ([xin.yang@rutgers.edu](mailto:xin.yang@rutgers.edu))

Zhuohang Li ([zl299@scarletmaik.rutgers.edu](mailto:zl299@scarletmaik.rutgers.edu))

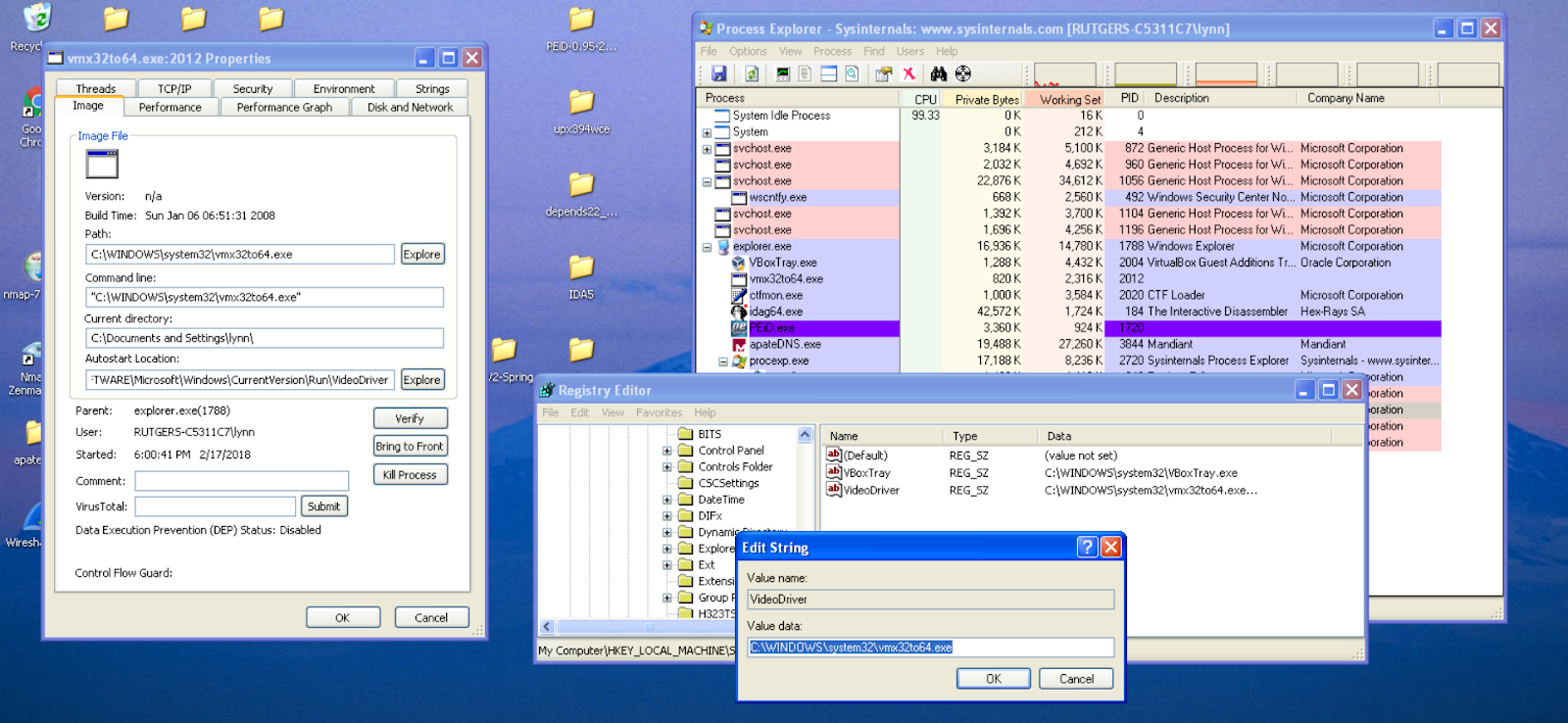
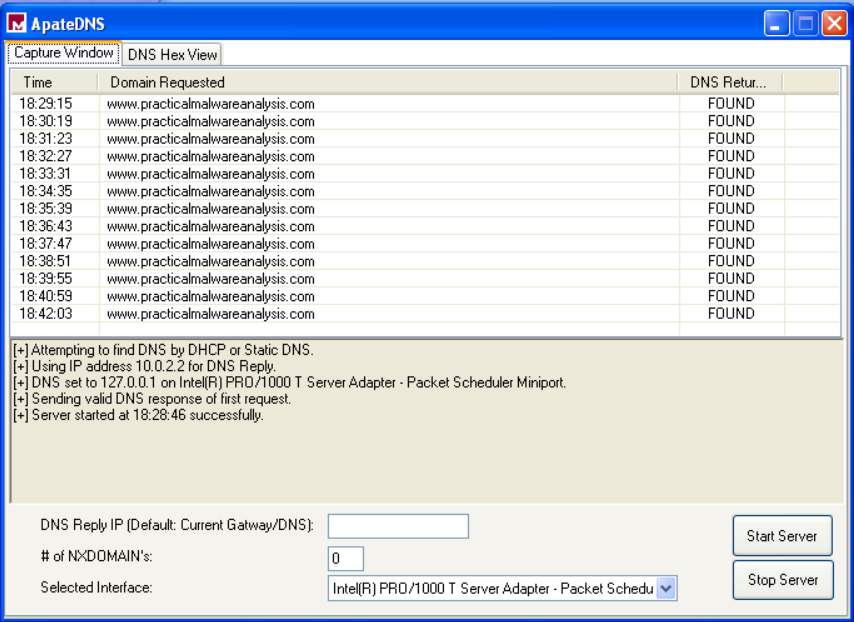
Homework 2

Lab01-01.exe:

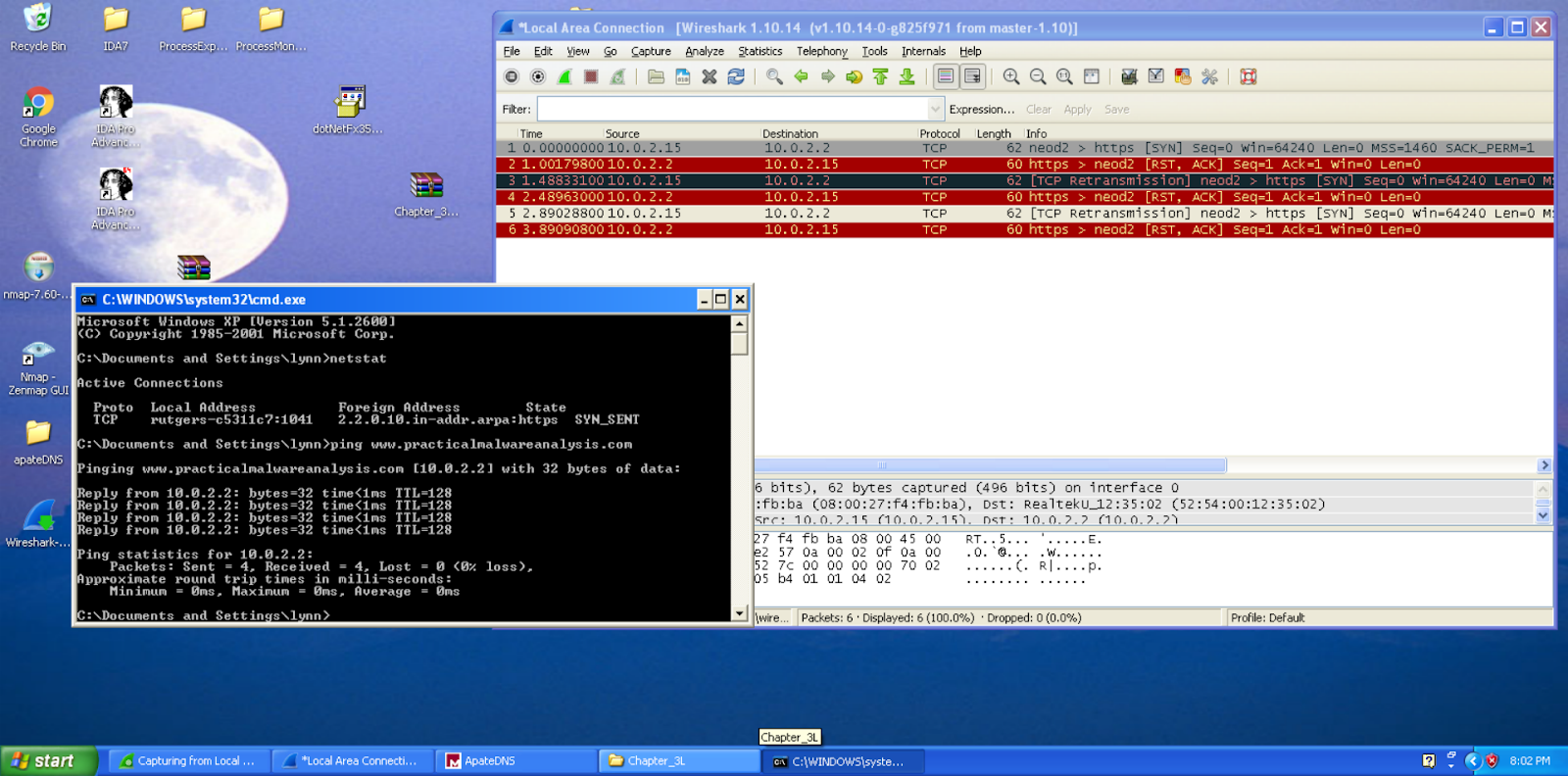
1. I can see both in PEview and Dependency Walker, it has only one import that is ExitProcess imported from kernel32.dll. In strings, apart form exitprocess and kernel32.dll, it also have url [www.practicalmawareanalysis.com](http://www.practicalmawareanalysis.com) , vmx32to64.exe  and two more path that might be used to save or kill.



1. Trying to find host-based indicators. I used ApateDNS. I found that, after running the malware, it sends a request to find DNS of [www.practicalmawareanalysis.com](http://www.practicalmawareanalysis.com) in every 65 seconds. And furthermore, in process monitor, as mentioned in problem 1, i find a string named vmx32to64.exe, the malware open a process in which the file is copied to C:\Windows\System32 and a column is written in regedit which is VideoDriver autostart. The behavior above also explains the path string we found in question 1. Related pictures are shown below.

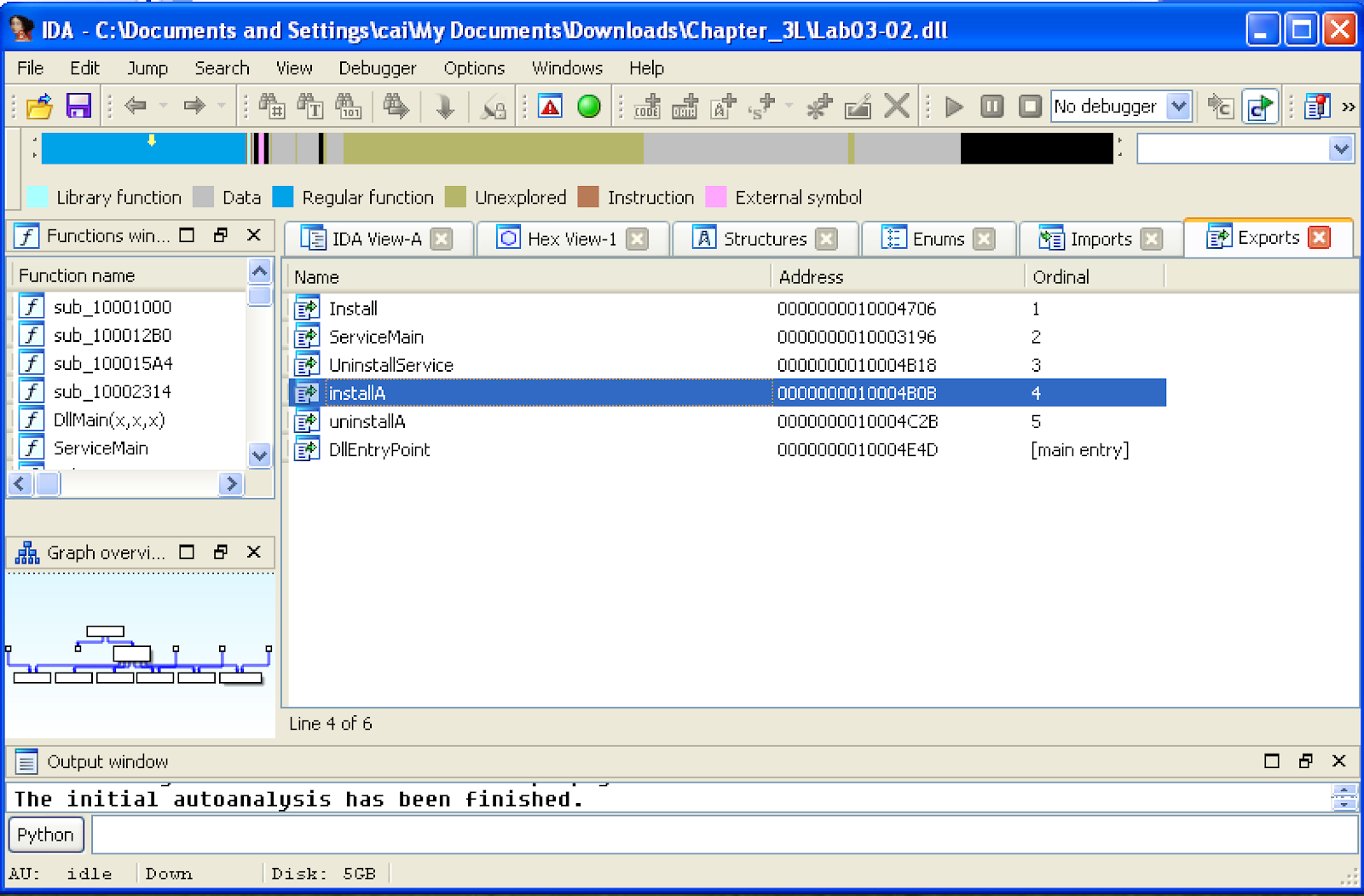


1. The ip of [www.practicalmawareanalysis.com](http://www.practicalmawareanalysis.com) look like 10.0.2.2 as this malware will request this ip once starts, and after it sends request to DNS, i get packages from wireshark. It seems that it is trying to build a tcp link.



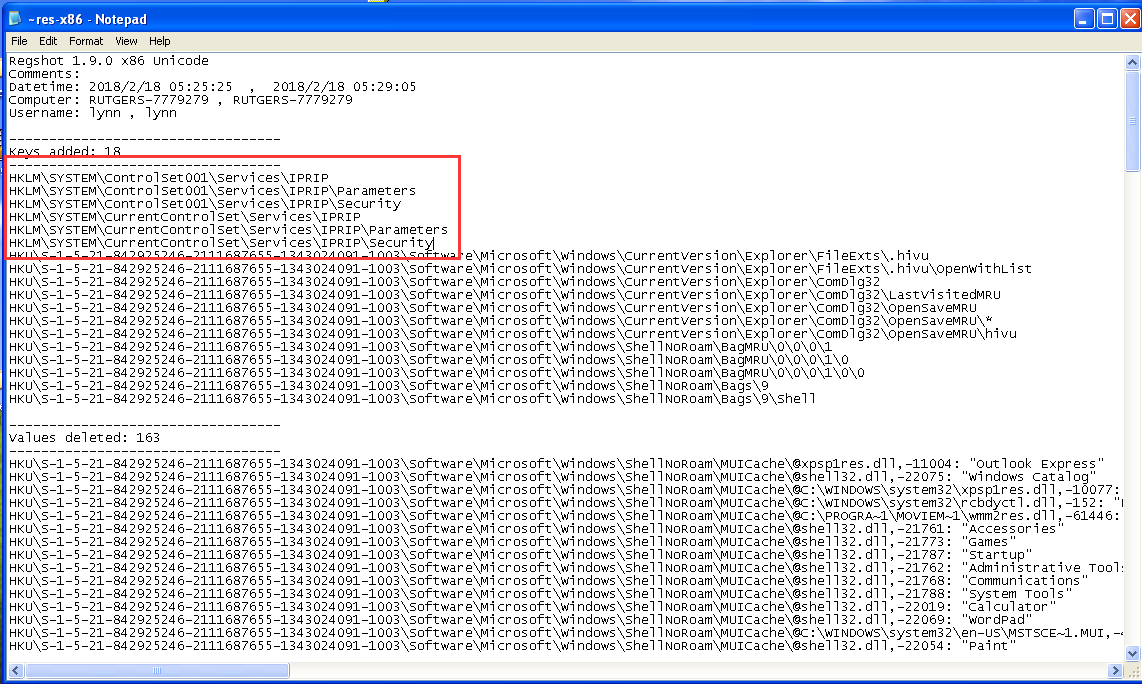
Lab03-02.dll:

1. Open it in IDA pro, check exports.

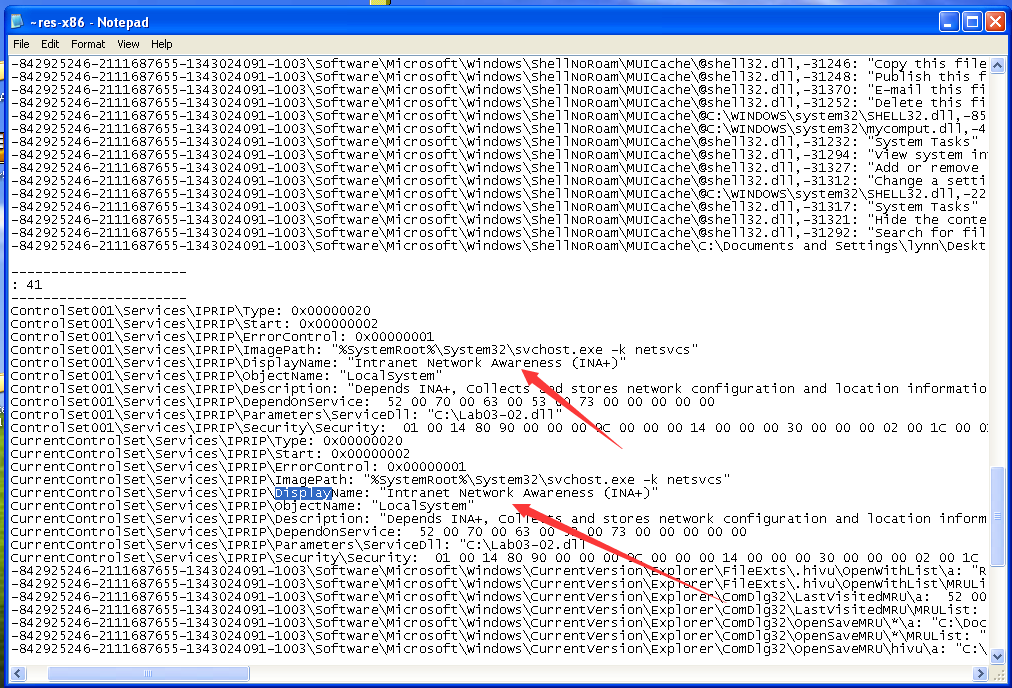


Install it using command rundll32.exe Lab03-02.dll, installA.

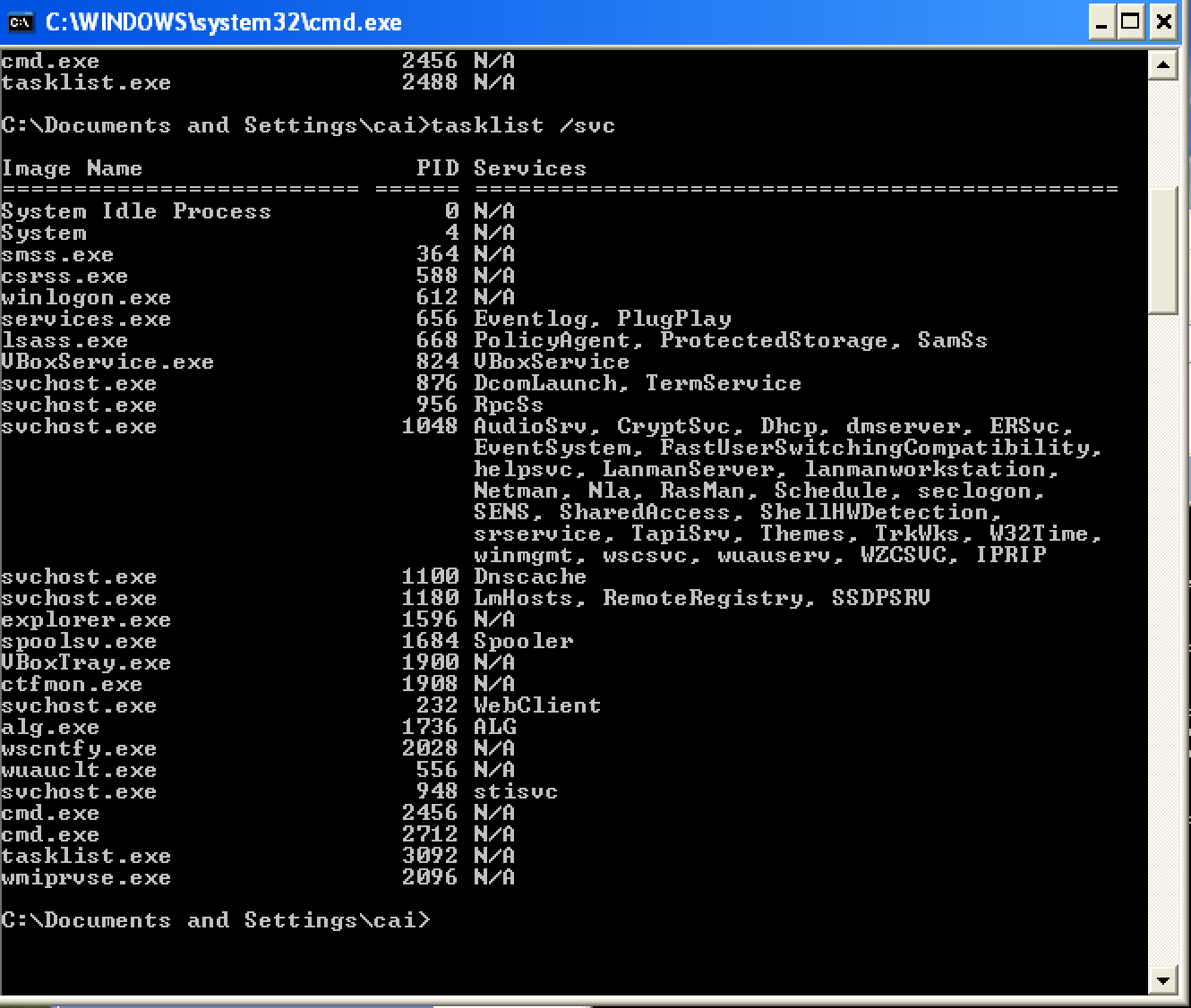
2. As we get from regshot, after running dll file, the changes the did to register is that it add several new keys. They all plugged down below IPRIP service.



It add a new service named IPRIP. So use command: net start IPRIP to start service. And it also said the name of the service should displayed as Intranet Network Awareness (INA+).

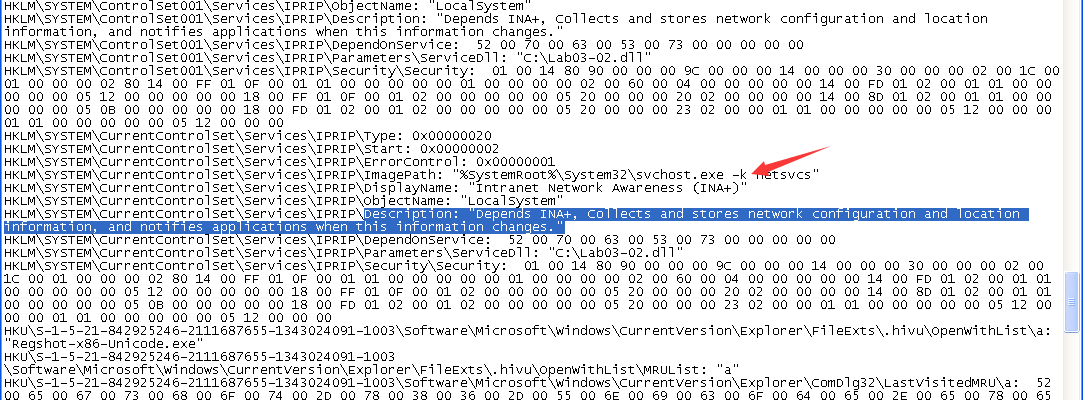


3.Use command tasklist /svc to show all services. From here we can find IPRIP with PID of 1048.

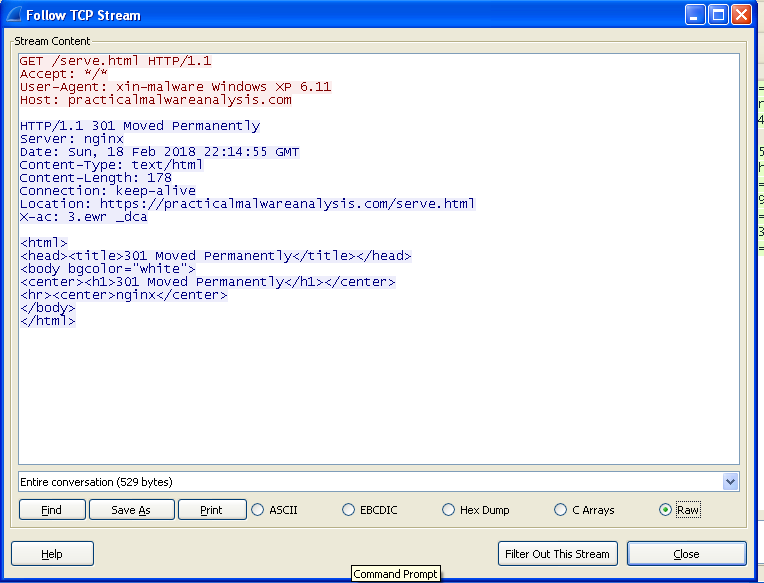


4. As the IPRIP service is started by svchost, we can set a filter to see the PID 1048, this filter contains lots of other processes so it can be hard to distinguish the malware.

5.This malware installs a service named ‘Intranet Network Awareness (INA+)’ to ‘HKLM\SYSTEM\CurrentControlSet\Services\IPRIP’, and it claims it will collect and store network configuration and location information.



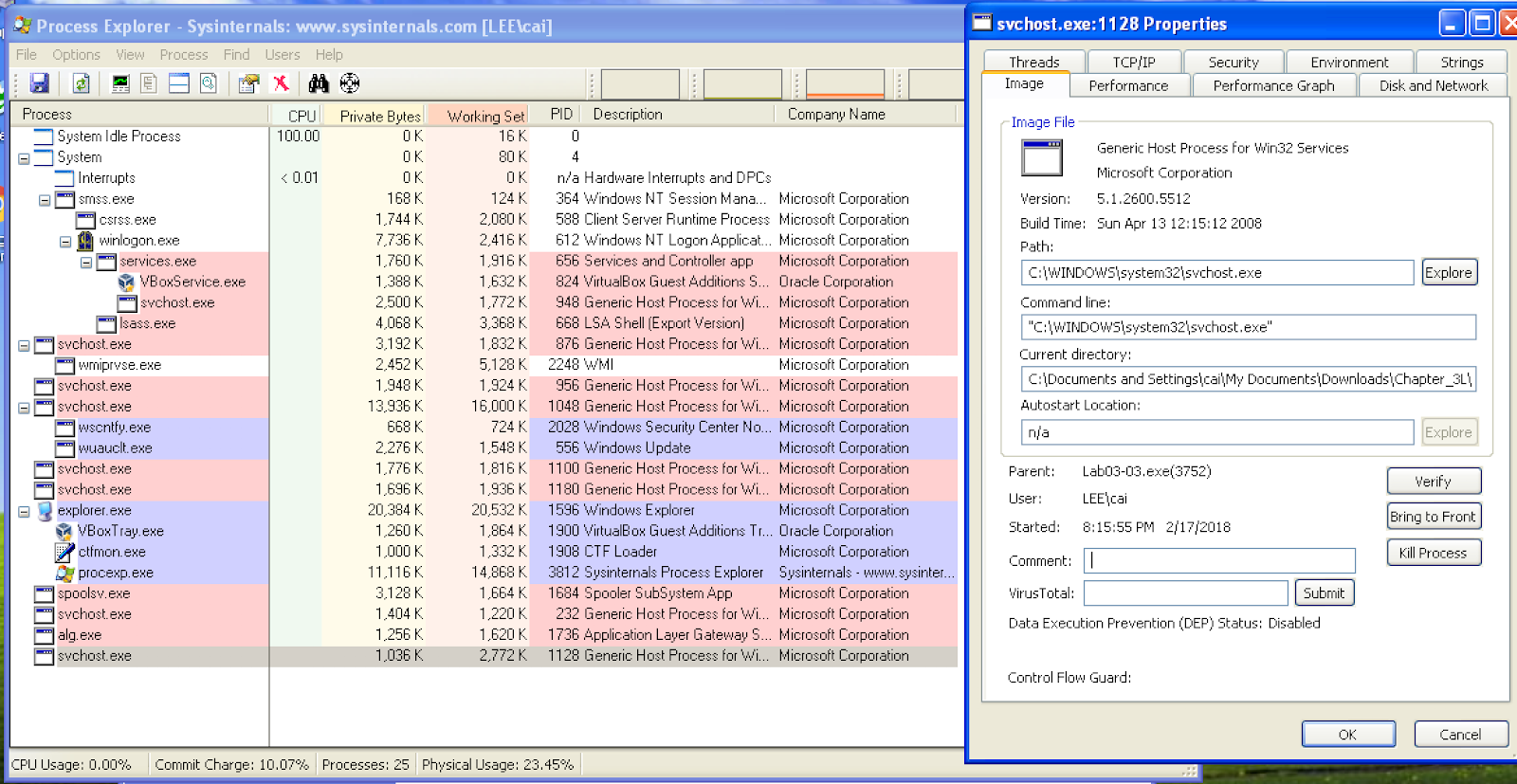
6. By checking the wireshark and apateDNS, nothing shows on apateDNS. But we can find a HTTP GET request and the host is practicalmalwareanalysis.com, also we can find some information about the website which uses a nginx server and the html page is 301 moved permanently. And we can still find this malware trying to find 10.0.2.2 and keeps sending broadcast.



https://lh4.googleusercontent.com/PWUpLt6NidEe7Shg_bA3xPOZ476IHiFavMpXZo0Lvk6oHjfC3ip4fWP4bOWJJ_4Rtsn7pShljFHFLXXOzQDb_z-up0-j0BHb0ym1njTIXHfCcRJZDL6H4eDylBjKKqxzOR7B8Nrs

Lab03-03.exe:

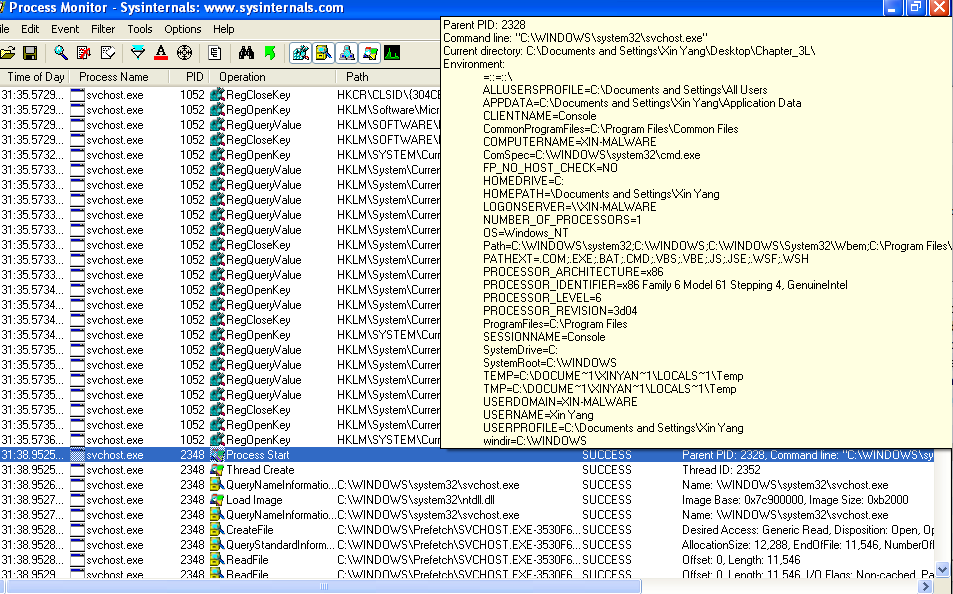
1. It created a new svchost.exe process.

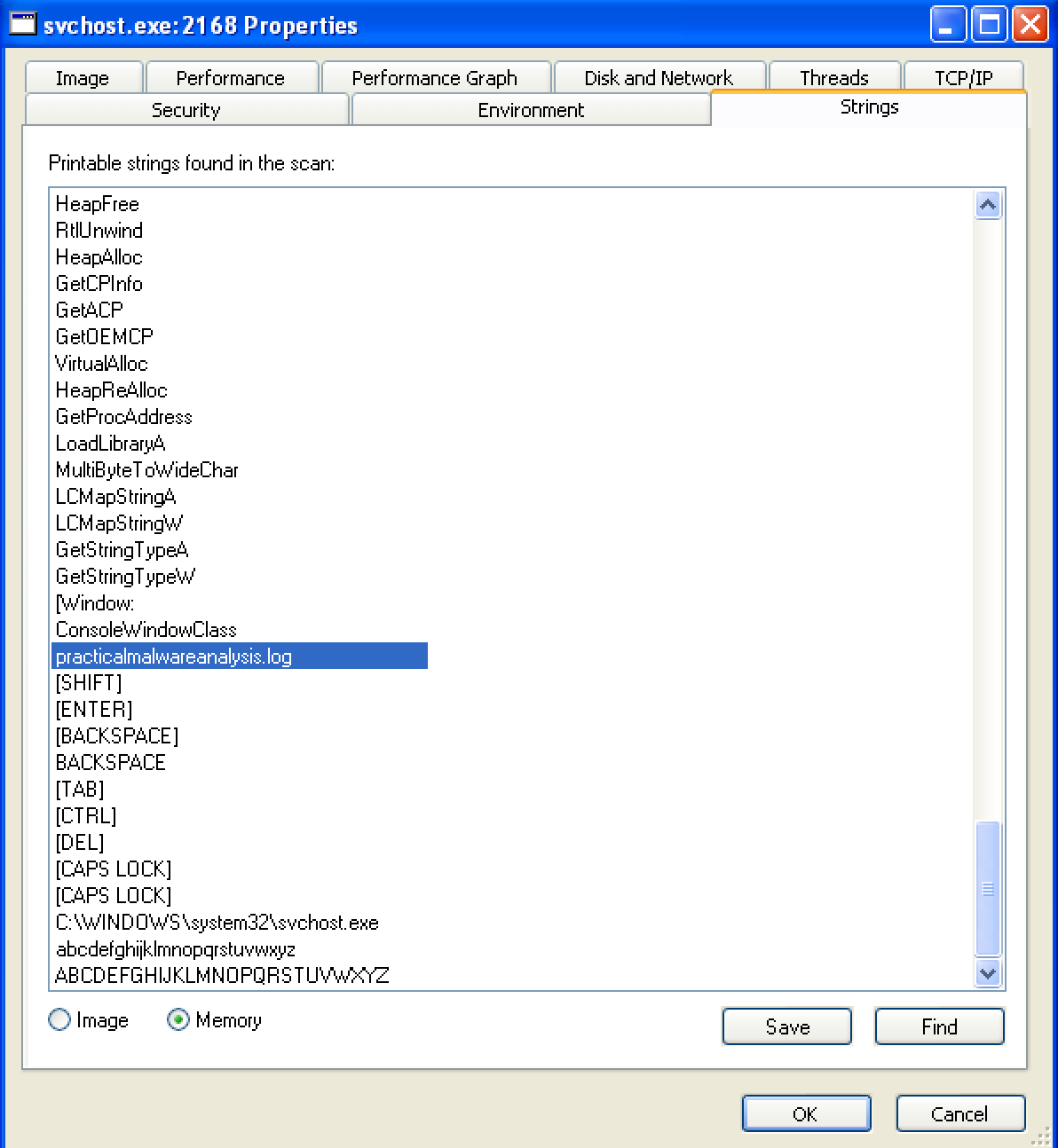


2.From process monitor, we can see it is trying to map and create another svchost.exe process. And the strings in memory refers to a file named ‘practicalmalwareanalysis.log’ , which can’t be a normal system process. Then we filter svchost.exe and we find there’s a new svchost.exe created at the directory of malware, and the parent process is exactly the Lab03-03.exe.

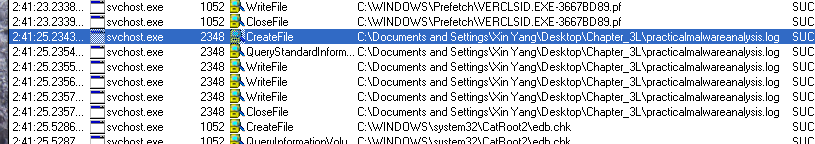
https://lh4.googleusercontent.com/FObYA8BS13lnum1JL4TJXhrsCBHoiOz36s-2-BUWOjN3c07jIGDZ0MpXQ6bqHwpQu1sXGtKMIX-Dg8q8X4vh_Oc_gkBW_dHE7iUQlO4HzwL15ogPrqgEsVNEmLKbxryHEfxX92Y9

https://lh3.googleusercontent.com/2bB9X_3kMpVtXzUDV5-2MC7RbH2Quqr4xl-C8oCBJWOc6RsRULFV321ShQRpqiwx70E0gMg3I5fmqEb9Hpp_3qgwEsVto5JEeredHYL9jZfa61a59YatihPINfYIHOMlUjA8FhWc

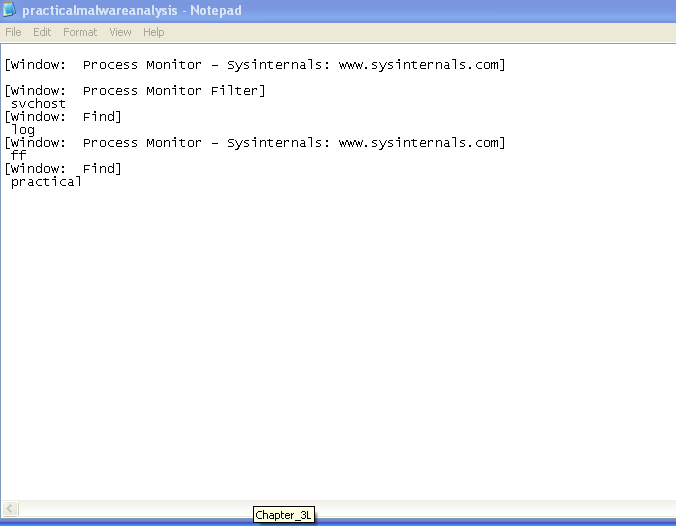




3.From strings we can see there’s a file named ’practicalmalwareanalysis.log’, so we search this filename in process monitor, we can see the fake svchost.exe created this practicalmalwareanalysis.log file in the directory where the malware sits.



4.After open the .log file we found, we conclude this malware is a keylogger. It creates a fake svchost.exe and records the current window and what the user types. In this case this program records my operations in process monitor to find this file.



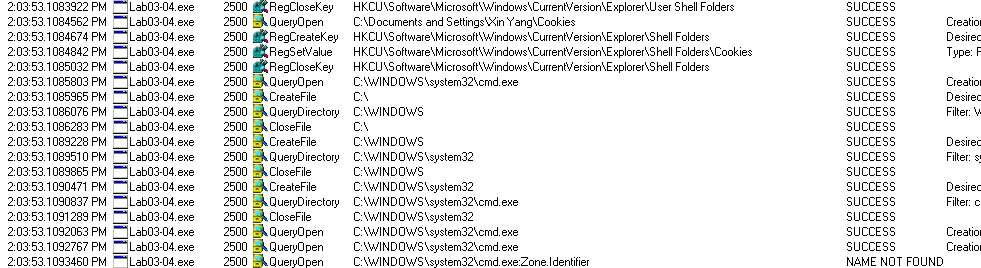
Lab03-04.exe:

1. When you run this file, a command line interface shows up and then disappear, then the Lab03-04.exe file is gone. We can no longer see this process in task manager and it’s not hidden, so we guess it’s likely to be deleted. From Process Monitor, we can see when we run this malware, there’re a bunch of operations to the Registry, and by using regshot, we can see after running this malware, 104 values are added and 14 values are changed. Also we can see from Process Monitor that it’s registering itself to registry and looking for files whose names are related to itself.

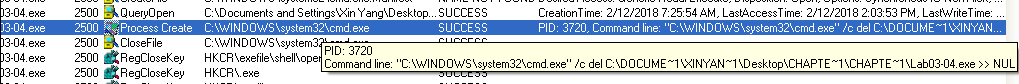
https://lh3.googleusercontent.com/kvtKoP0t4HFarut51spJZFkQVPUcyiV36BVoL53LuAun-1Yd6Gw9OEmvm5w3Wla-tK0mQvCOr4J7UgVzKahhyBA-eLfWx3-n0U0o6LPysuGn2Kg4B-evaWytYl552X9cN9FkTQ-_

https://lh3.googleusercontent.com/WwYsiMhm4n4D3Vt27b2CjL_ilKNZ00xn55kaUYFXClAK88comSa3qicI_MXhJ5fSsuJ6jz4kZspNkQfA3tQOTwA8DBTTxFXdp5PKaKvVpXS4y6VB1q005yUHhv1AytQmDI-Do-mB

Then it looks for the location of cmd.exe try to open windows command line.



At last this malware will delete itself and clean up the mess, but sometimes it won’t work mostly when Process Monitor is turned on and you have to run it several times to see it deletes itself, but when you quit Process Monitor, this would delete itself immediately.



We can’t see this malware call any functions or import any libraries related to network or sockets, but when run strings command, we can however see something related to HTTP and “http://www.practicalmalwareanalysis.com”. We extract this program to different directories and we find that it only deletes the file which are clicked and runned, the other copies are still safe on the disk and not detected by the malware.

1. This malware can delete itself after opened, which can cause a problem for the analysis. We need to pause this malware before it delete itself so we can better analyze and figure out what it really did.
2. Tools like Ollydbg, which can pause the malware and analyze step by step can run this program, also the best way is to use IDA Pro and find out what reasons lead to the branch and prevent it.