Anaisy Garcia PID: 5734454

Lab 3-1Analyze the malware found in the file Lab03-01.exe using basic dynamic analysis tools.

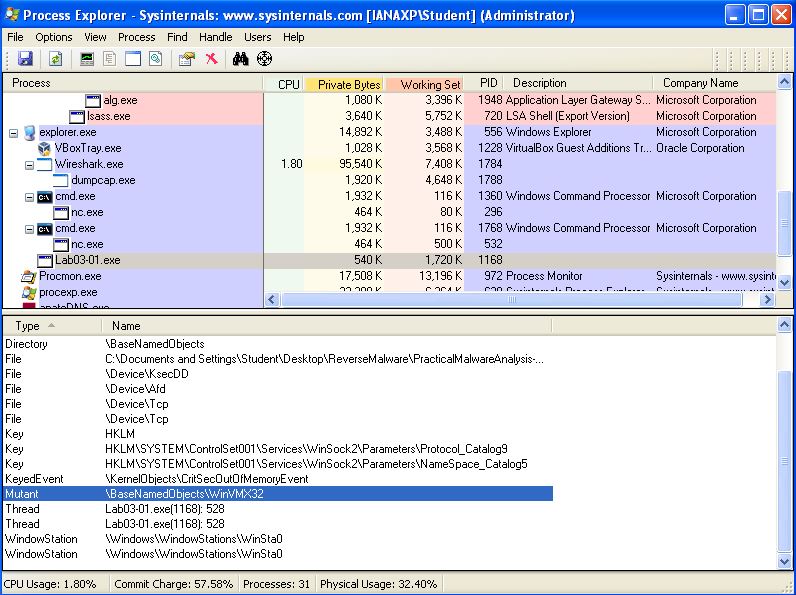
Questions1. What are this malware’s imports and strings?

When put into the PEview program this malware shows that it only has one import “ExitProcess” in the kernel32.dll library. 

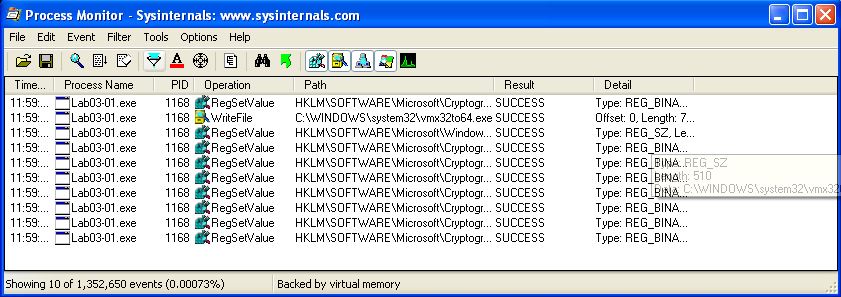
When put into the strings program several strings appear including paths and another .exe file.

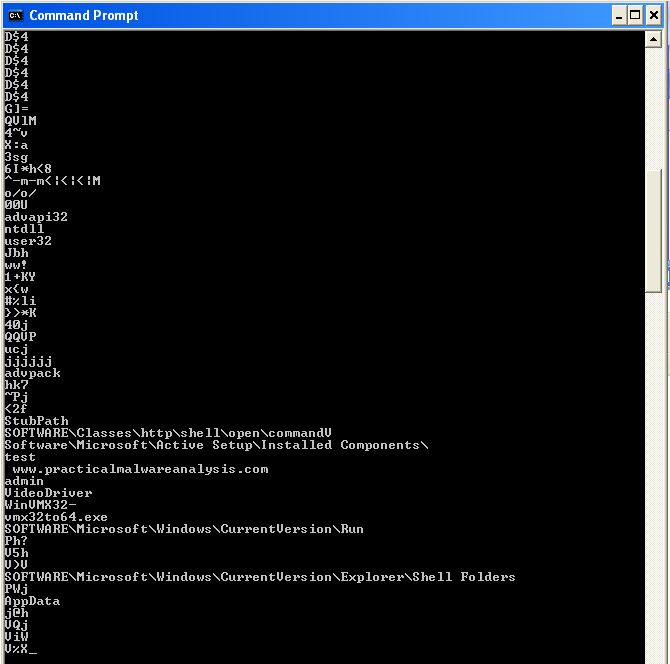
2. What are the malware’s host-based indicators?

Using process explorer, it is found that this program makes a mutant called WinVMX32.

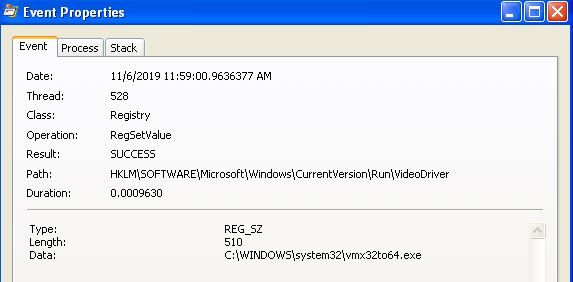


Using process monitor it is found that this malware writes an executable file within C:\WINDOWS\system32\. It is called vmx32to64.exe. Checking this file closer with strings shows the same hash.



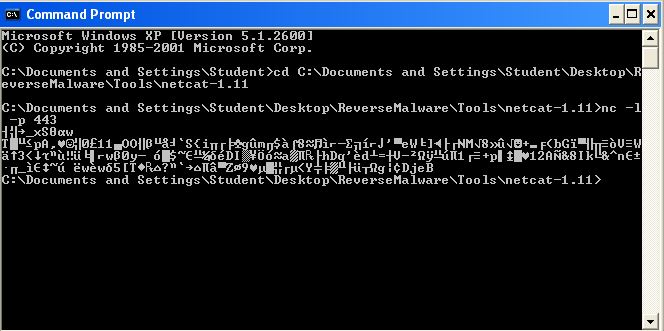


The malware also sets itself up to run on start up. This is seen in a registry process that creates a registry key to path HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver.

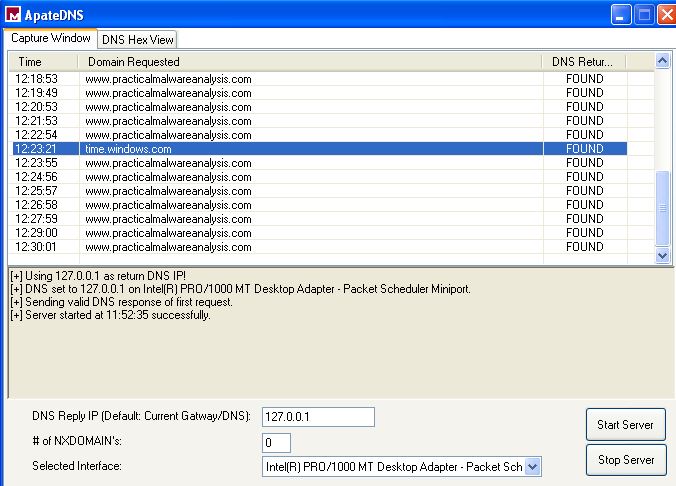


3. Are there any useful network-based signatures for this malware? If so, what are they?

Netcat listed to ports 80 and 443. This malware functioned through port 443. This also just showed a random assortment of strings.



ApateDNS shows us multiple requests for [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com) which were all found.



Wireshark then shows beacon packets consisting of random data after getting to [www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com).