**Cyber Forensics and IOT Security**

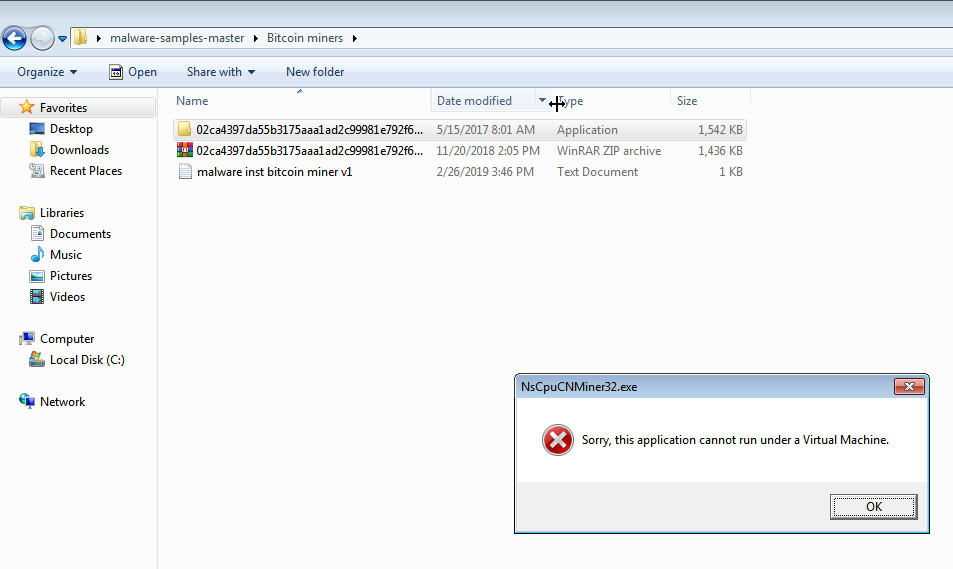
**Assignment 1**

**(MTech PESU 2018-2020)**

|  |  |
| --- | --- |
| **USN** | **NAME** |
| **PES1201802353** | **ROOPESH R** |
| **PES1201802600** | **SADAQATH HUSSAIN** |
| **PES1201802455** | **RAJAT P RAYADURG** |

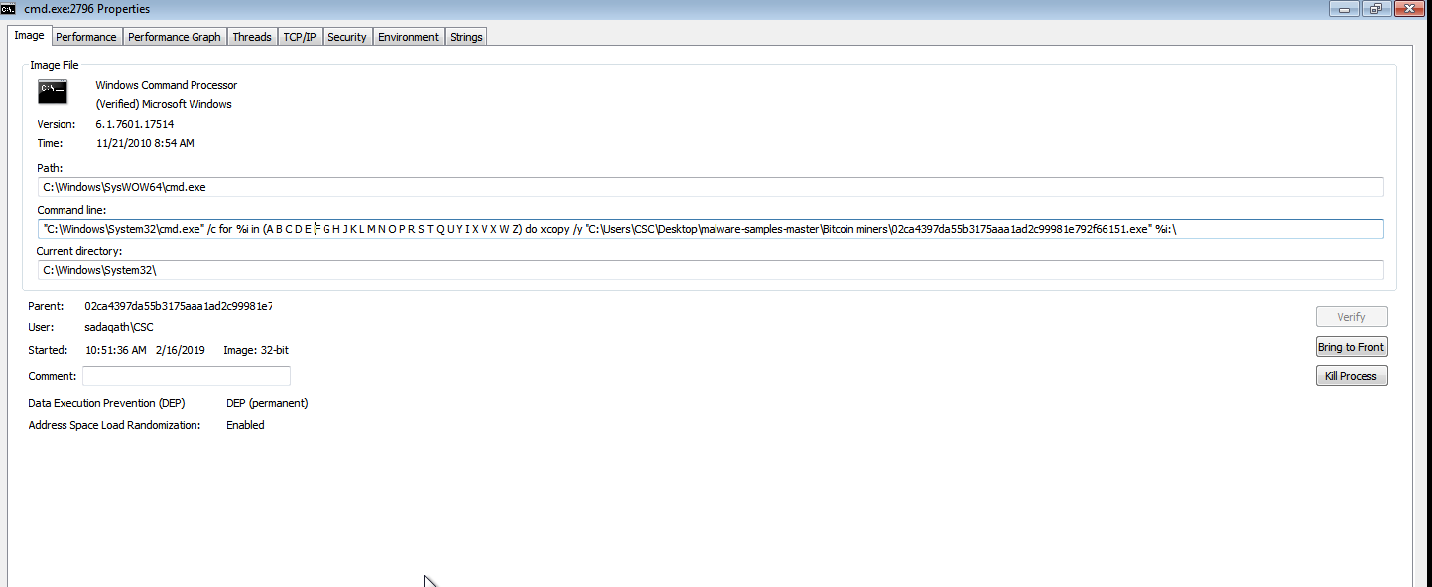
**A. BITCOIN MINER (**02ca4397da55b3175aaa1ad2c99981e792f66151.exe {pseudo random name}**)**

1. The bitcoin miner which has the title **NsCpuCNMiner32.exe**, says that it cannot execute on a VM, but it does execute itself as checked in the process explorer.



A1 The bitcoin miner claims it cannot run on VM

2. The malware ran a **cmd.exe** ,which executes a command line argument to run the **xcopy** application to spawn more **cmd.exe**s which in turn copied the malware.

1. 

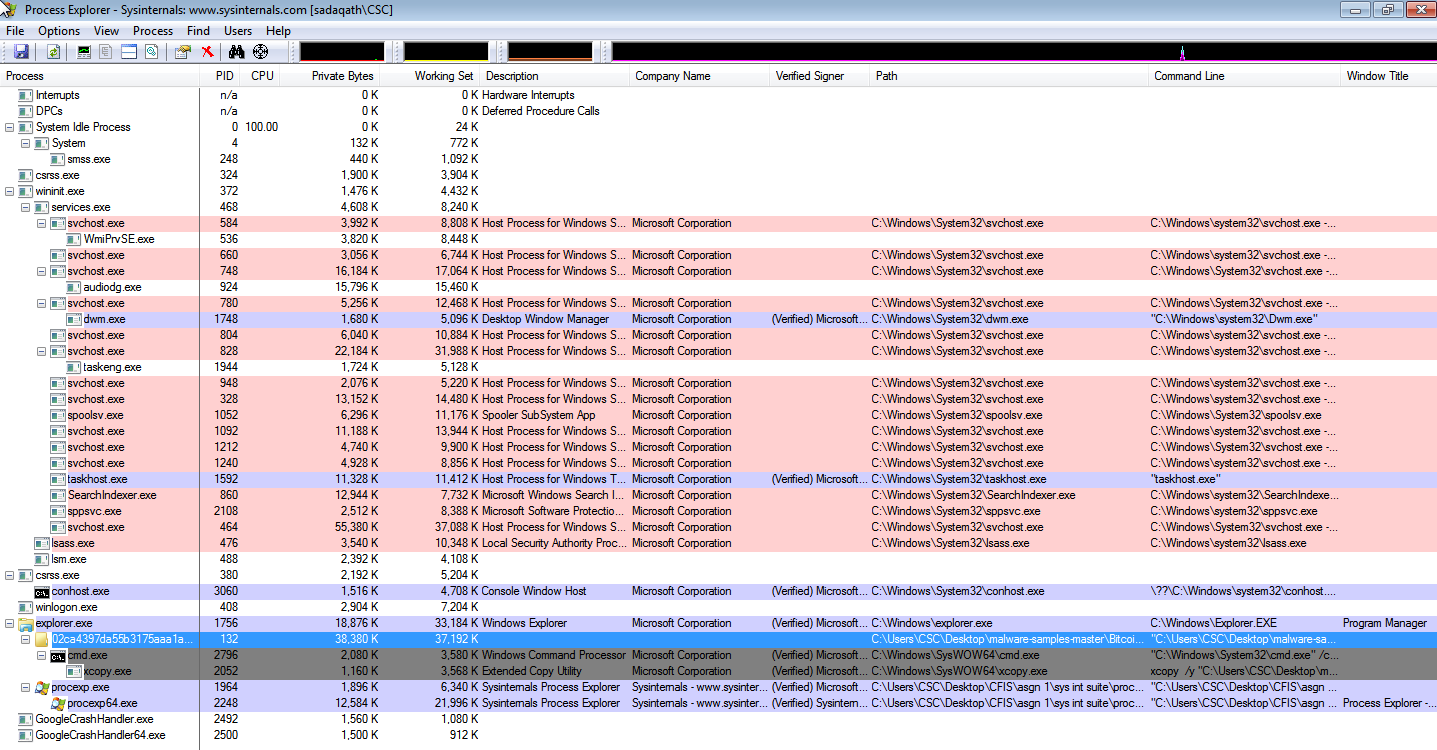
A2 Properties of the cmd.exe generated by the bitcoin miner.

**"C:\Windows\System32\cmd.exe" /c for %i in (A B C D E F G H J K L M N O P R S T Q U Y I X V X W Z)**

**do xcopy /y "C:\Users\CSC\Desktop\malware-samples-master\Bitcoin miners\02ca4397da55b3175aaa1ad2c99981e792f66151.exe" %i:\**

The block of text shown above is the **command line** argument **run by the cmd.exe** which instructs the **xcopy** app to copy the bitcoin malware on all available logical drives on the system(**from A: to Z:)**

1. The malware kept copying itself even upon deletion, so it was considered best to suspend all the process, and then kill them one after the other.

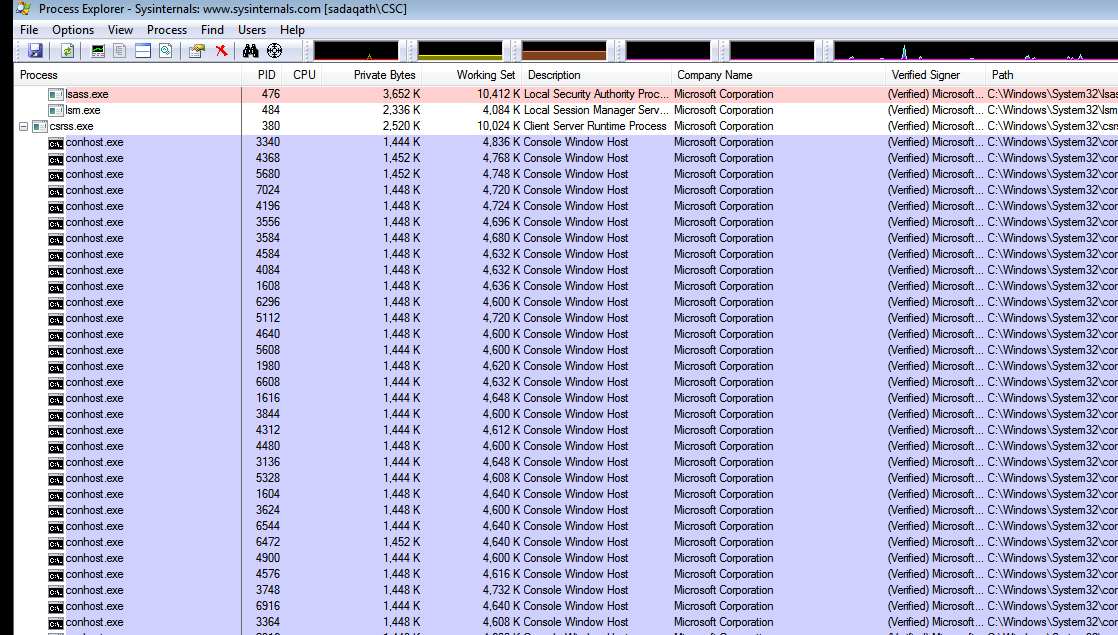


A.3 The bitcoin miner creates a child process cmd.exe with the command line arguments

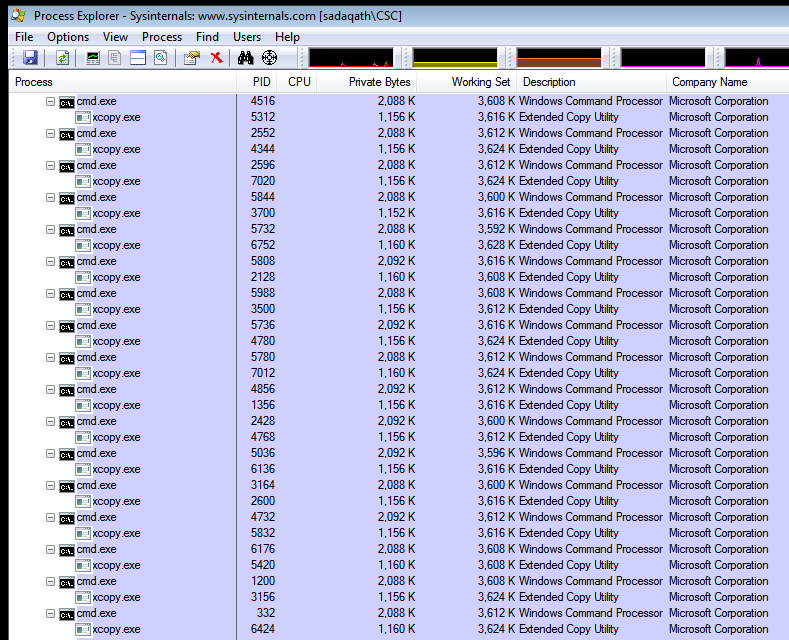
Required to create xopy application which is used in turn to copy the malware again.

Cmd.exe is created by the bitcoin miner named 02ca4397da55b3175aaa1ad2c99981e792f66151.exe , as you can see from the screenshot, the highlighted processes.

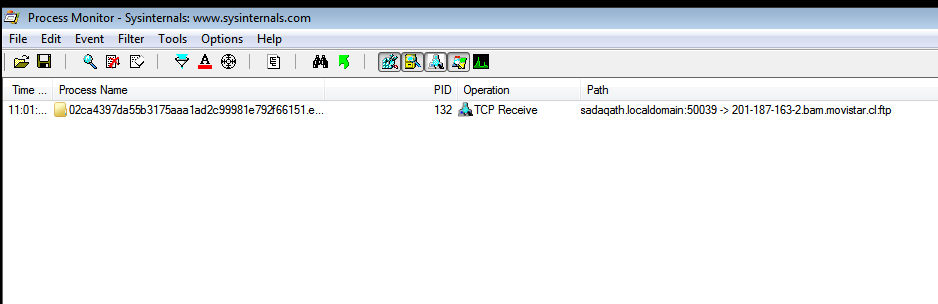
1. The cmd.exe was generated by conhost.exe.



A.4 As you can see from the screenshot above that conhost.exe, there are several instances of it being created.

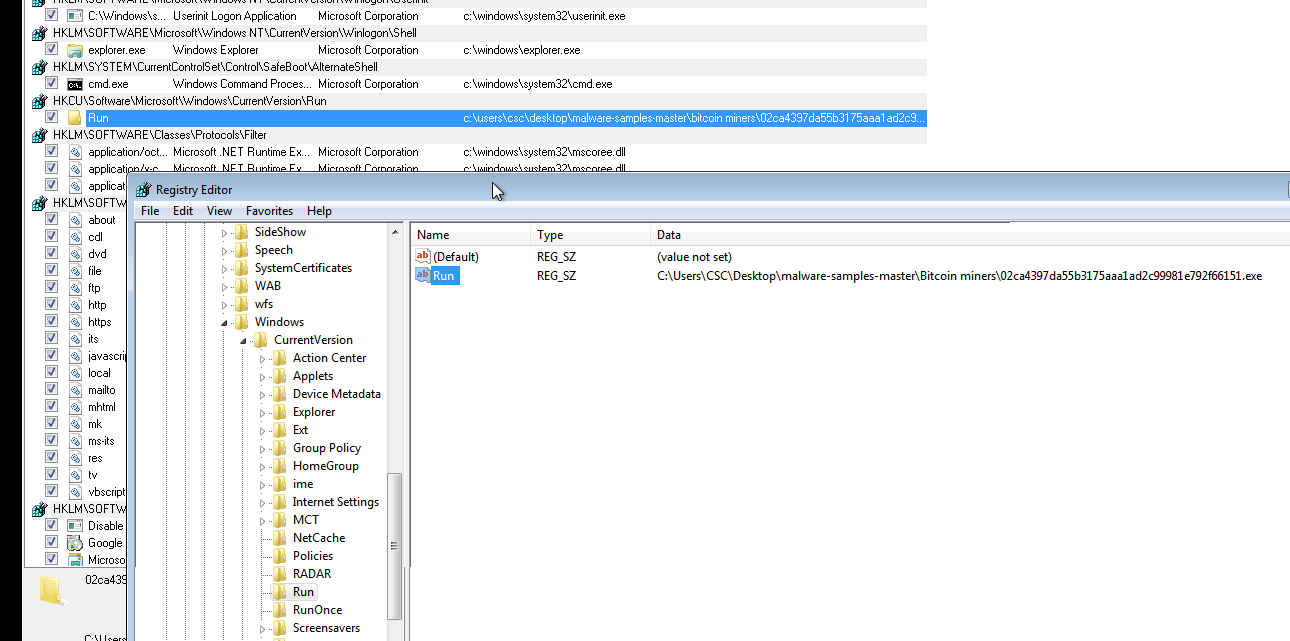


A.5 **xcopy** being generated continually by cmd.exe



The malware also made requests from local port 50039 to the server with ip 201.187.163.2

1. Run the process monitor, and make sure boottime logging is done. By doing so, we can intercept any processes that are automatically invoked once the system boots up.
2. For these boot logs, use the name of the malware as the search term.
3. Now go line by line and check when the process, is run from the registry using run key or runonce key (in this case it’s in **run** key)
4. Now you can edit the registery key using autoruns in administrator mode.



A.6. As you can see from the above screenshot, the run key contains the name of the bitcoin miner’s location as value, which indicates that this malware gets executed every time the system is booted.

9. And then uncheck the run key for the malware. This solves the problem as it is not executed automatically anymore.

**B) SdBot (**28247211d1eb08370aa363f08821a653.exe {pseudorandom name}**)**

1. SdBot is run, and checked in process explorer
2. It creates a **Windows** batch file with a pseudo random name, followed by a .bat extension (indicating that it’s a batch file that is created)

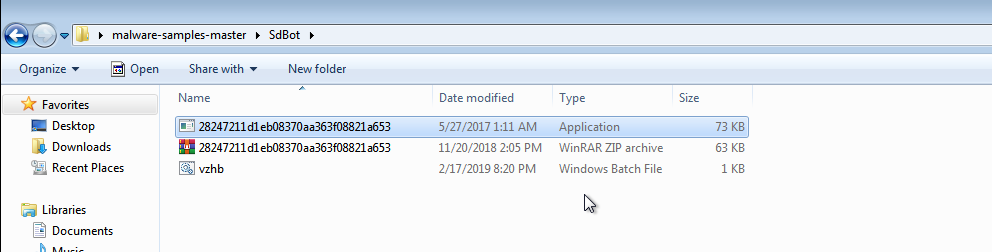


Fig B.1 Suspicious batch file created

1. It spawns a **cmd.exe** and then using this cmd it invokes the windows batch file(suspicious file) as seen from the process’s command line

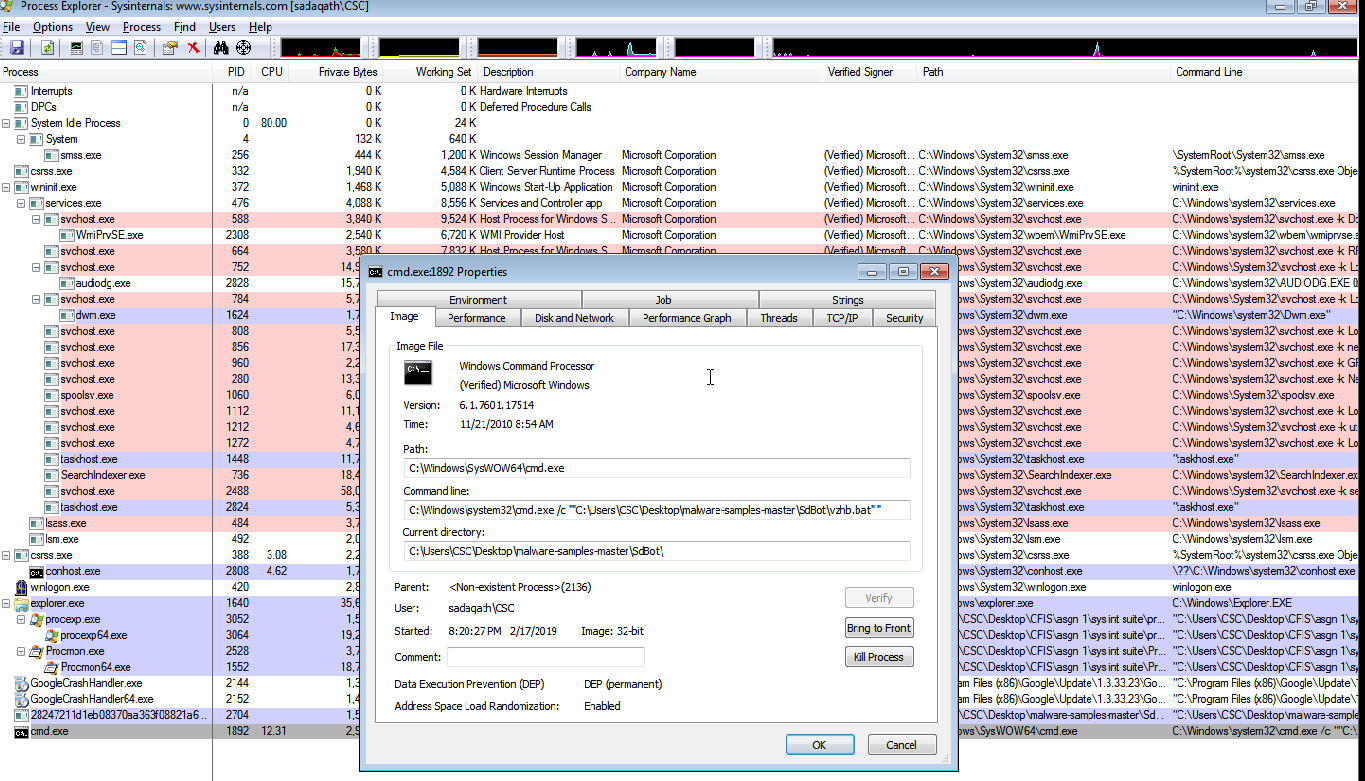


Fig B.2 cmd\_spawn1 cmdline

1. At times the malware deletex itself from the source folder trying to erase all evidence of its existence. (This is seen especially when your try to restart the process using process explorer). The process kills itself and removes itself from the disk.

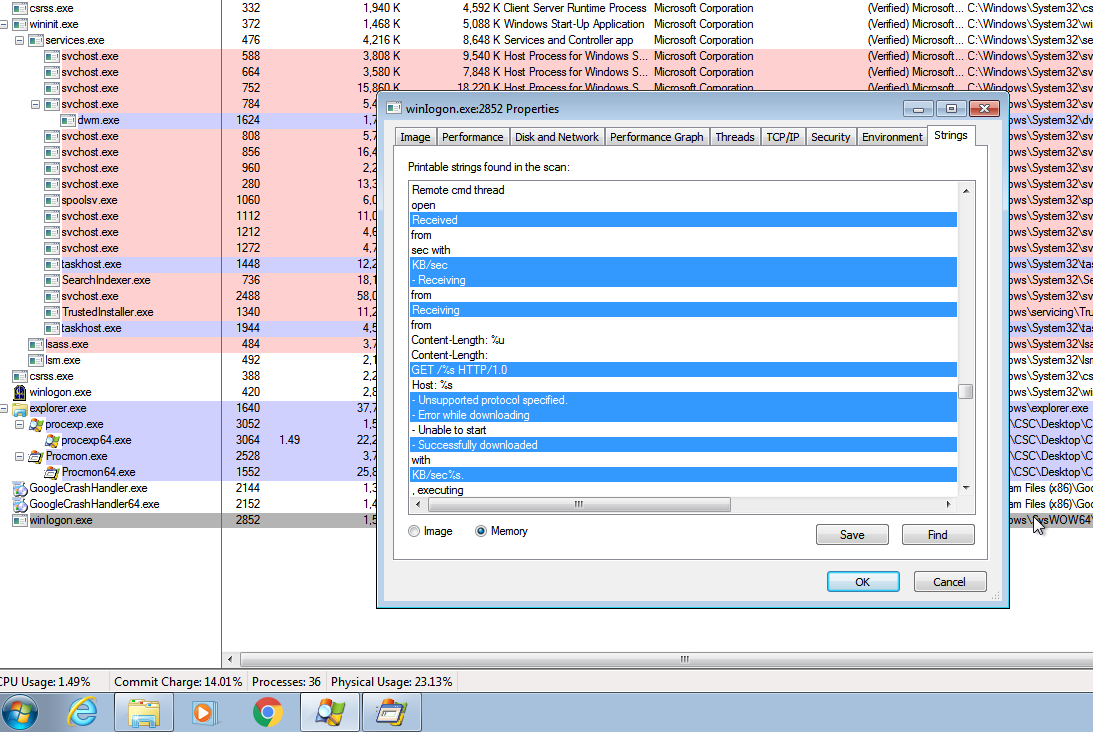
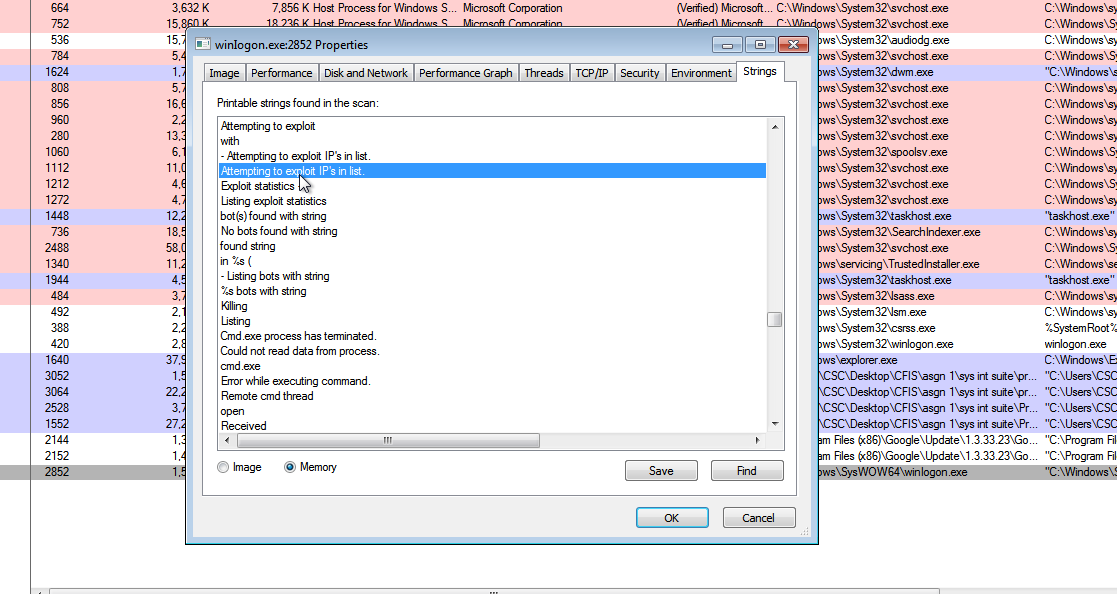


Fig B.3 string properties in memory of winlogon.exe spawned by SdBot, after killing itself , mostly interacting with botnets

**Observations from the above screen shot:**

1. The above application doesn’t have a logo, moreover, it doesn’t have a verified signature even though it has a seemingly trustworthy name like winlogon.exe (which sounds like Microsoft Windows application).
2. It has some strings like receiving, Successfully downloaded, GET, HTTP, KB/s. All this indicates that it can be a backdoor malware being controlled remotely/ or it is a malware that downloads other malwares from the internet.
3. Once you restart the malware, it kills itself sometimes and start winlogon.exe, which has no description, company name and also no verified signature.



B.4 Some more strings observed in winlogon.exe

**Some more observations from the strings present in winlogon.exe**

1. The string in the above screenshot “**Attempting to exploit IPs in list**” makes a very clear statement that, this malware is attempting to interact with bots connected to the internet.
2. Another clue for the statement made above is the presence of the string “**bots with the string**”

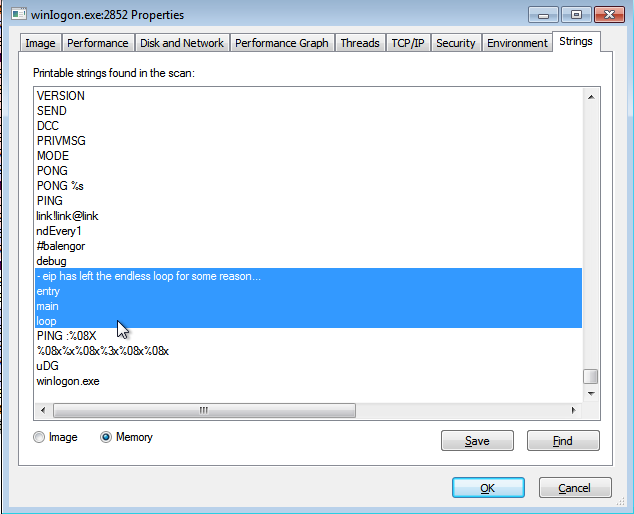


Fig B.5 string properties in memory of winlogon exe spawned by SdBot,tell tale signs that it could be a virus

1. The above screenshot, shows the presence of the 3 main keywords of virus, **entry, main & loop**