ITSC 303

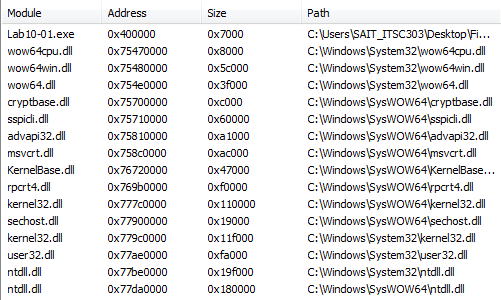
Malware Analysis

Final Project - Weekly Report 6

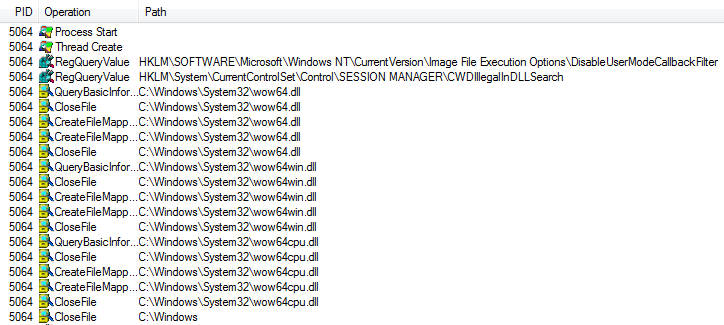
D’Artagnan Boocock & Coleton Sanheim

12/04/2022

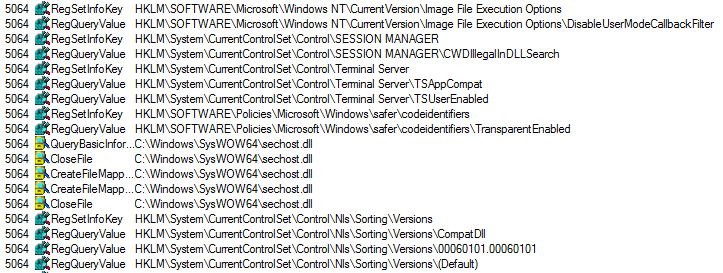
Sample 1:



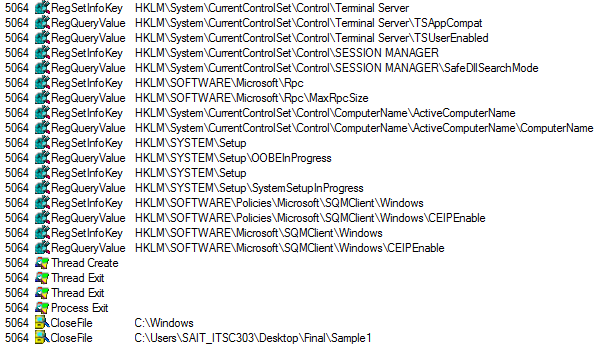
These are the dll’s that are referenced by this sample.



Here we can see the sample is creating a process, looking up registry values, and scanning for data within the system32 directory. It would be safe to assume this is an information stealer of sorts.



Here the sample appears to be editing registry values associated with system security, presumably to either obfuscate itself to prevent detection or to allow itself to escalate privileges so it can access more system data.

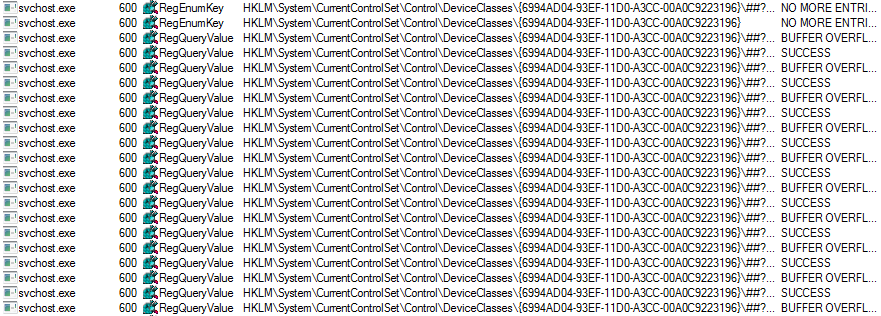


Continued from the previous screenshot, then it closes the malicious process.

Based on the basic dynamic analysis that was performed using procmon, we can assume that this malware appears to try to steal and copy data from the victim.

Sample 2:

For this sample we ran it though adobe acrobat reader, as it was a pdf.

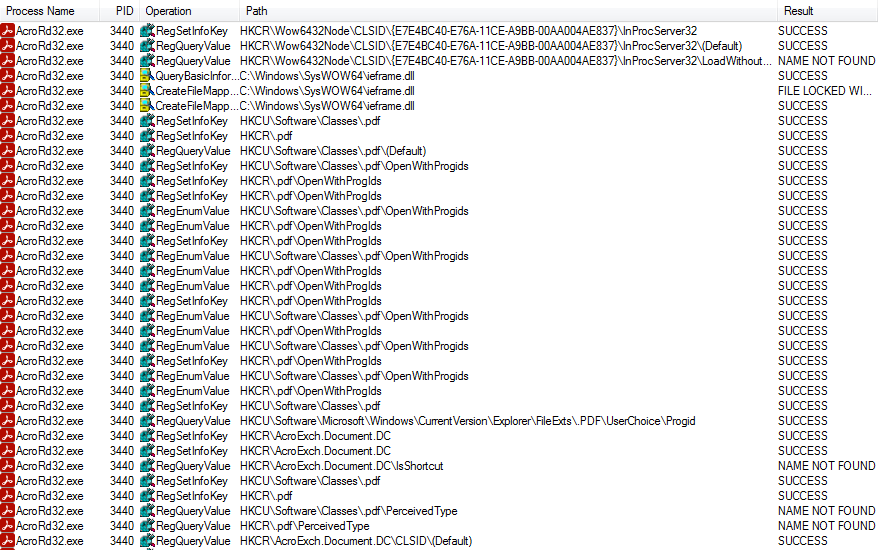


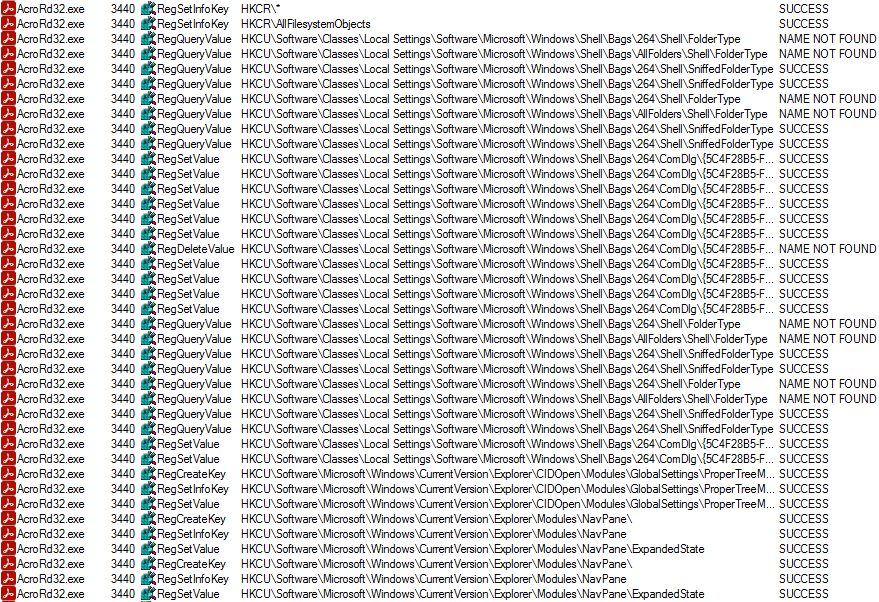
Here we can see it reading a high amount of registry values.

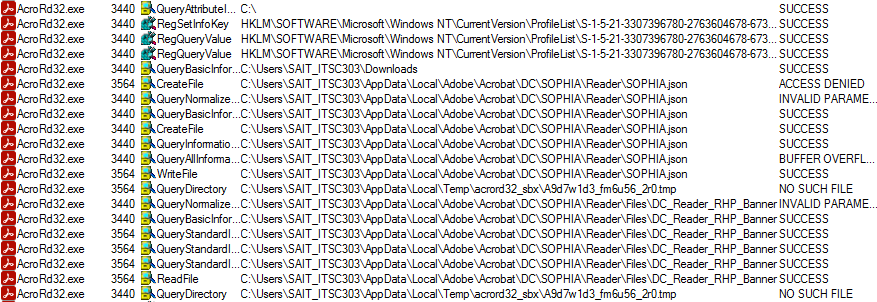


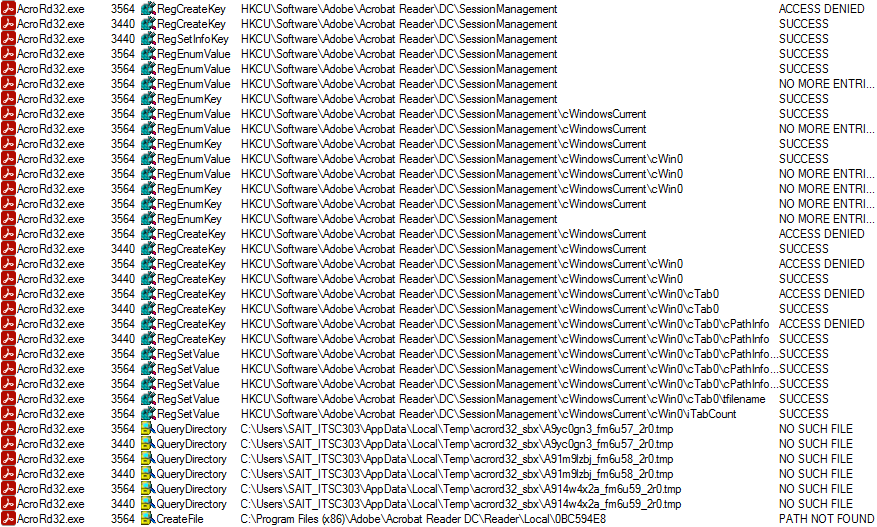
This is an important one to note as it is communicating with something, possibly a command and control server.

Procmon logs









It is unclear what exactly is happening here, there are a LOT of registry notifications but it is not apparent what, if anything, the sample is doing.

Further dynamic analysis will be required to determine this.