Practical 1

Antoine Ferguson
2/18/2022
a.ferguson@ufl.edu

Practical 1 - CAP4136

Executive Summary

The malware stores diskcryptor-related files in its resource section and transfers them to C:\DC22. Changes in registry keys indicates that a scheduled task named DefragmentService is created, run, and deleted. Properly executing the malware makes the system reboot however C:\DC22\log_file.txt hints that hard drive encryption is taking place. Upon opening the diskcryptor GUI, about 60GB of the C drive is encrypted and the original password given to the malware is used to decrypt it.

Static Analysis

Using PEStudio to review the malware, the apparent compiled data was April 24 at 6:00:40 UTC (1 am EST).

The malware is run from the command line. It's evident from the command strings discovered by PEStudio, including "cmd /c net use >> c:\dc22\netuse.txt" and 'schtasks /create /tn DefragmentService /TR "cmd.exe /c net use >> c:\dc22\netuse.txt" /sc DAILY'. The imported functions GetCommandLine, ReadConsole, and ShellExecute strengthens my point as these set of functions can read and execute arguments from the command line.

PEStudio revealed over 21,000 strings and 114 import functions from 5 libraries were contained in the malware. This proves the malware isn't obfuscating much of its code since the strings and import libraries were easily analyzed. UPX determined the malware wasn't packed by UPX, which is a common packer used to obfuscate malware's code. From these factors, I don't think the malware is packed.

Some functions suggested privilege escalation, including AdjustTokenPrilvileges, ImpersonateLoggedOnUser, and LookupPrivilegeValue. The SetEnvironmentVariable and GetEnviornmentStrings functions suggest the malware intended on modifying or creating new environment variables on the system. The ShellExecute function suggests the malware intended on running command from the command line.

URL strings frequently referenced were "http://diskcryptor.net", a website that encrypts disk partitions, and "http://ocsp.verisign.com", a certificate signing authority. Other suspicious strings dealing with diskcryptor were "Do you really want to interrupt the encryption\r\nf an iso-file?" and 'Iso-image "%s" successfully encrypted to "%s"' which might indicated the encryption of the Windows iso image. For filepath strings, "%s\drives\%s.sys", "C:\DC22\log_file.txt", "C:\DC22\netpass.txt", and "C:\DC22\Mount.exe", which are mostly likely new files being created by the malware.

Using PEStudio, dlls and executables were found in the .rsrc section of the code. the full list includes: mount.exe, (32 bit and 64bit versions of the following) dcisnt.exe, dccon.exe, dcrypt.exe, dcrypt.sys, dcapi.dll, and netpass.exe. these files made up 91% of the malware code.

Dynamic Analysis

Using the x32dbg debugger, I realized the malware required an additional argument to run. After execution, the computer rebooted. Using fakedns and INetSim, I didn't notice any peculiar network signatures. I mostly saw responses to Microsoft related websites like msftconnecttest.com, teredo.ipv6.microsoft.com, and ctld.windowsupdate.com. However, there were some responses to "sf.symcb.com" and "ocsp.trust-provider.com".

Regarding registry keys, the Defragment service, a service created by the malware, made a new key "HKLM\SYSTEM\ControlSet001\Services\DefragmentService". Some of the subkeys were "Type: 0x10", "Start: 0x02", "DisplayName: 'DefragmentService'", and "ImagePath: 'C:\Users\Malware\Desktop\sample1.exe 12345'". These keys were discovered in RegShot running from the initial start of the malware up to the point where the system rebooted. Another interesting key was "…\HarddiskVolume3\Windows\System32\cme.exe:", as this string was discovered in the malware while debugging with x32dbg.

The malware created the C:\DC22 directory and stored discryptor-related files here; the same files stored in the .rsrc section of the malware. Other files included were the log_file.txt, netpass.txt, and netuse.txt.

The main service started by malware was DefragmentService, which was the command "cmd.exe /c net use >> c:\dc22\netuse.txt". This was confirmed from the registry keys discovered by RegShot and from reviewing the code with x32dbg.

Indicators of Compromise

As I've previously stated, strings about the DefragmentService were discovered. Logs found in DC22\log_file.txt revealed that hard drive encryption has begun. It also lists the argument provided to the malware as a password. When running dcrypt (the diskcryptor GUI) I noticed 60GB of the C drive is encrypted. Using the original password provided to the malware, I'm able to decrypt the drive.