Malware Reverse Engineering Report Practical 1

By: Gary Jones
Jonegn1@ufl.edu
CAP4136 Practical 1: Reverse Malware Engineering

Executive summary

Project overview

The goal of Practical 1 is to dissect the functionality of sample1.exe using static and dynamic analysis.

Summary of findings

Sample1.exe is evidently malware as confirmed through various analytical methods and witnessed by the successful execution of the program on the virtual machine. The functionality of the program is to serve as an encryptor for the recipient's entire computer system thus locking the user out of their machine until the correct password is input – which may be provided from a malicious third party.

Several methodologies were utilized to determine the presence of obfuscation. These methods include looking at the number of strings present, identifying any discrepancies between the raw-size of the file and the virtual-size of the file, taking note of the entropy, and looking at the signature value. These methods failed to return identifiers expected for obfuscated or packed malware leading to the conclusion that the malware is not obfuscated.

From the 112 functions imported by the executable we see there are 28 blacklisted from 4 out of 5 libraries. The 4 libraries involved with the blacklisted functions are advapi32.dll, kernel32.dll, user32.dll, and shell32.dll. Of the library not associated with any blacklisted functions is shlwapi.dll. The functionality of the blacklisted functions includes involvement with security, the console, system-information, dynamic-libraries, administration, execution, and exception-handling.

Utilizing regshot there were significant registry and file system changes made to the windows system after executing the malware. While there is significant noise being generated by the windows system there were commonalities between running the malware multiple times. Malware activity includes deletion of 21 keys, adding 62 to 72 keys, and deleting 22 Values. Changes to the filesystem includes adding 19 to 27 files, modifying 72 to 86 files, adding 3 folders, and deleting 2 folders.

Several programs were utilized to analyze network activity include fakedns, wireshark, and inetsim. However, there were no signatures that would indicate network activity by the malware.

The malware did illustrate IPS signatures including I.P. addresses to websites. In all there were over 21000 strings identified with several hundred considered blacklisted with numerous hints being listed as well. Within these strings are messages which spell out "You are Hacked !!!!", "DiskCryptor driver ver %d detected", and "http://diskcryptor.net/index/php/DiskCryptor". In addition, the top blacklisted values match the signature of the Mamba Ransomware. This may provide possible insight into some functionality of sample1.exe as there appears to be similarities between the two.

Technical report

Introduction

The malware under analysis was inspected using a variety of static and dynamic software tools including Wireshark, fakdns, inetsim, procmon, regshot, and process explorer. Combined, these tools were used to illustrate the interaction and modifications performed by sample1.exe when executed. These tools were used to address a variety of asked questions as expanded upon below.

Findings: Static Analysis

1. Identify the apparent compilation date of the program.

The compilation date of a program can be a good indicator for malfeasance. This parameter is modifiable, so dishonest representations are possible. Two examples of possible malfeasance include having the compilation date set to some point in the future or ridiculously in the past. However, in the case of this program, when analyzed in pestudio we see that the listed compilation date is **24APR2016**. This finding does not raise any issues.

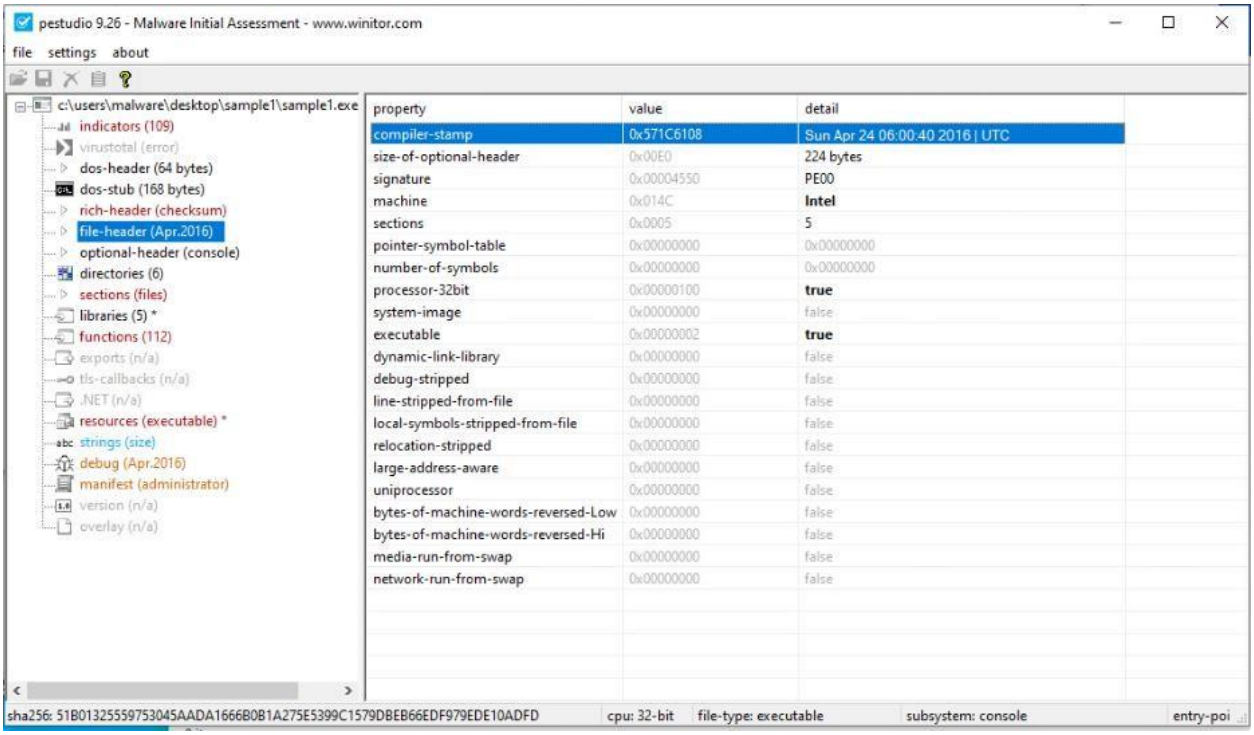

Figure 1: Compilation Date of 24APR2016 Sample1.exe from pestudio

2. Identify whether the program is a Windows GUI or command-line program.

Identifying whether a program is a Windows GUI or command-line program is useful to help understand how it can be activated. In the case of this program, when viewed in pestudio, we can see that the subsystem is listed as console thus informing us that it is a command-line program.

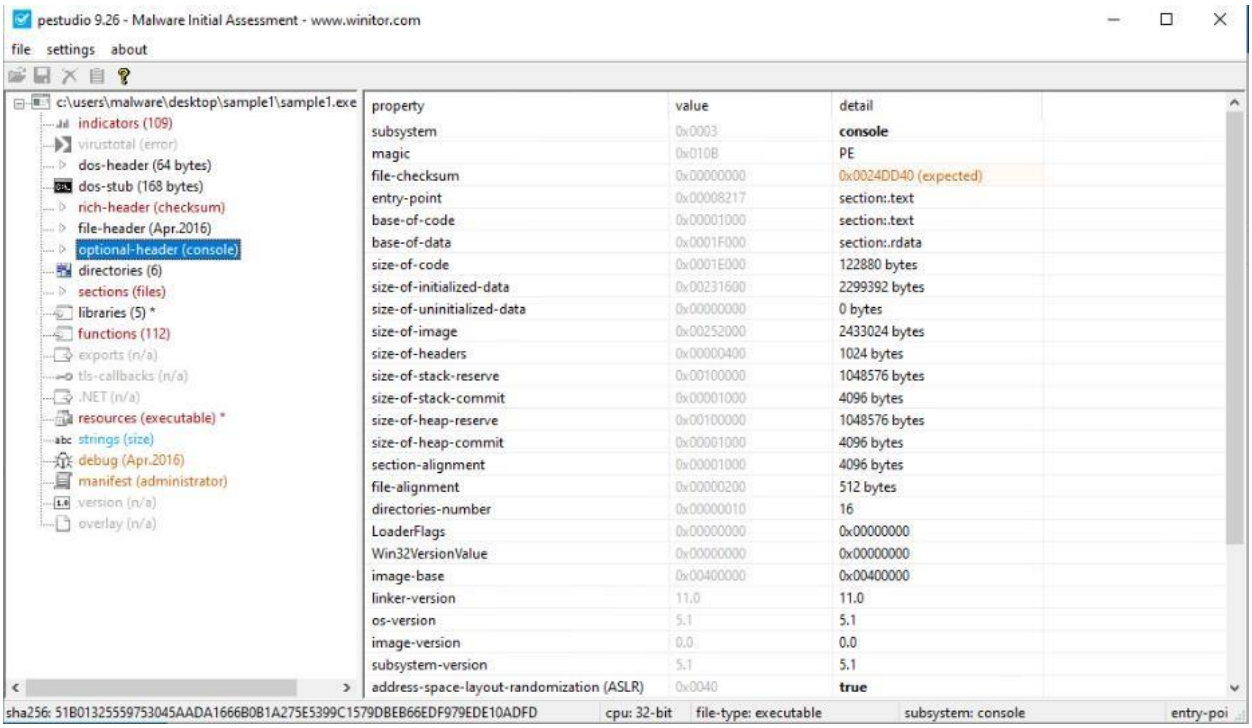

Figure 2: Command-Line Program

3. Is the program packed? Use multiple indicators, explaining the significance of each

When determining the packing or obfuscation status of a program there are a multitude of indicators which can be used. When analyzing sample1.exe several such indicators were utilized. The first of these indicators was the comparison of the raw-size of the file, and the virtual-size of the file. This indicator is useful because it can identify if a program is taking up significantly more space in memory than on the disk. An example of this scenario would occur if the virtual-size was much larger than the raw-size. However, when looking at sample1.exe we see the raw-size of the file at 2414080 bytes and the virtual-size of the file at 2420931 bytes. As these indicators are comparable in size this is not an indication of obfuscation or packing of the program.

When the file size of the raw and virtual space are compared by sections of the code, as shown below, we see a similar trend with the .text, .rdata, .rsrc, and .reloc values. However, we do see a significan difference in the .data value with the raw-size at 7168 bytes and the virtual-size at 15360 bytes. However, this discrepancy is common in windows programs when it comes to the .data file sizes. For this reason, looking into the specific sections of the code does not yield a positive indicator of obfuscation or packing.

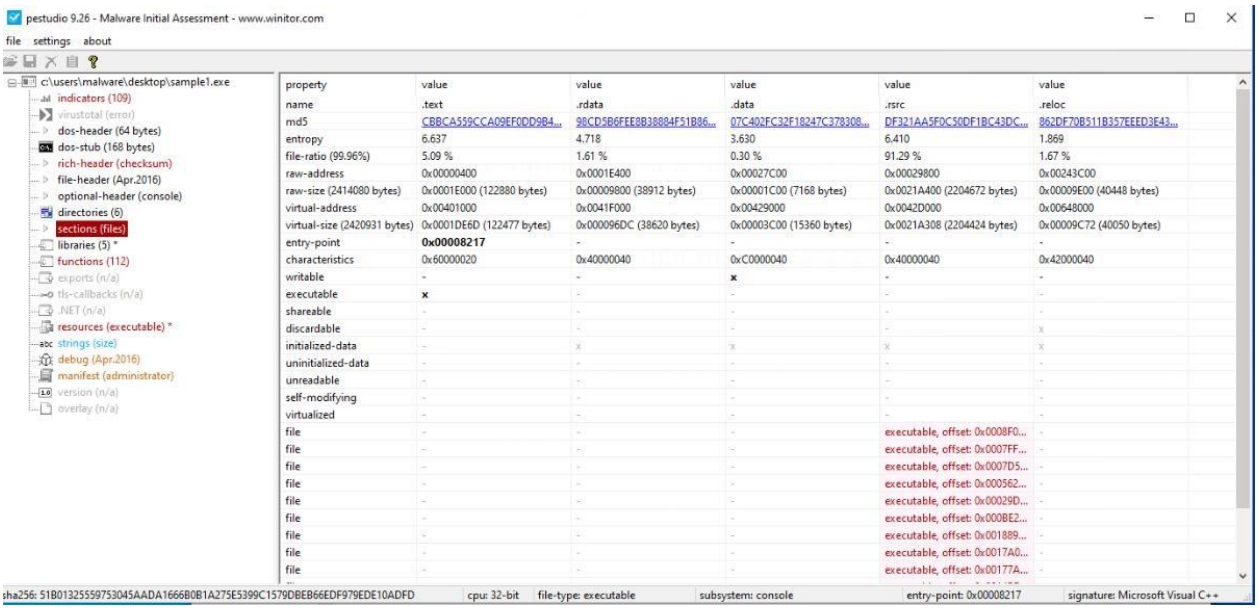

Figure 3: raw-size vs virtual-size of files and sections

Another useful indicator that illuminates if a program is packed or obfuscated is the entropy of the file. Entropy is a measure of data randomness within a file. This randomness correlates to packed and obfuscated files because it indicates hidden data and suspicious scripts. Within PE studio we can see that the listed entropy is 6.365. This value is under 7 which is a common bar used to establish potential obfuscation and packing. As such the level of entropy identified by pestudio does not indicate that sample1.exe is packed or obfuscated.

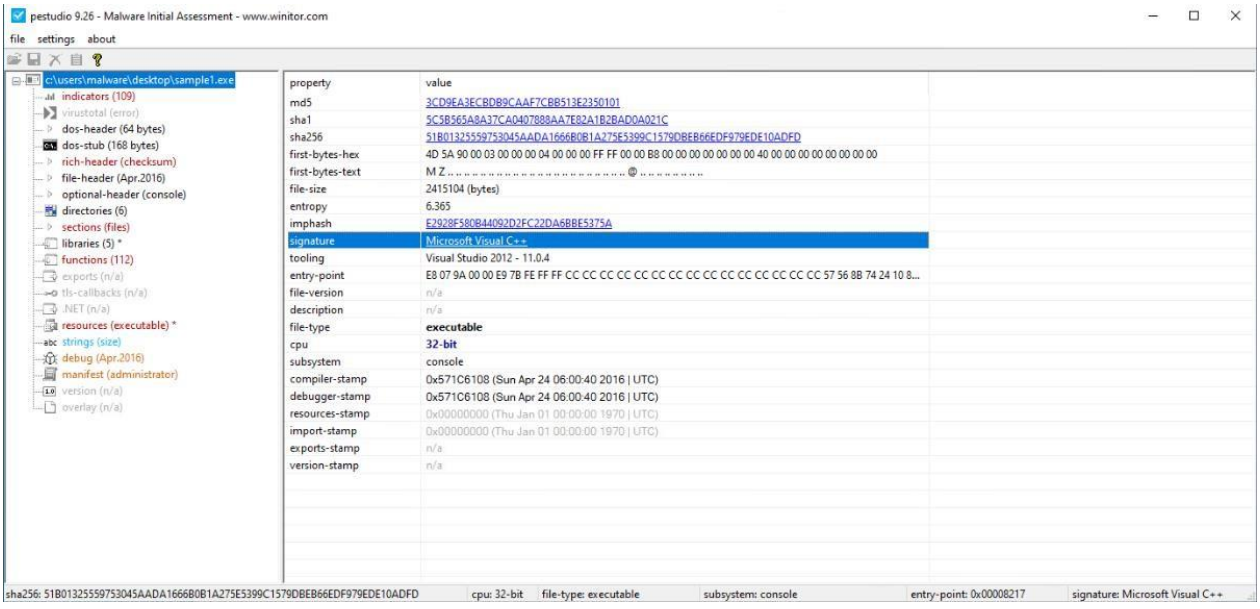

Figure 4: Sample1.exe Entropy

A third, and excellent, indicator to tell if a program is packed or obfuscated is looking at the number of strings identified in the program. An unpacked and non-obfuscated program is liable to have a significant number of strings identified. Looking at the program pestudio registers 21804 strings. The amount of strings identified is a good indication that sample1.exe is not packed or obfuscated.

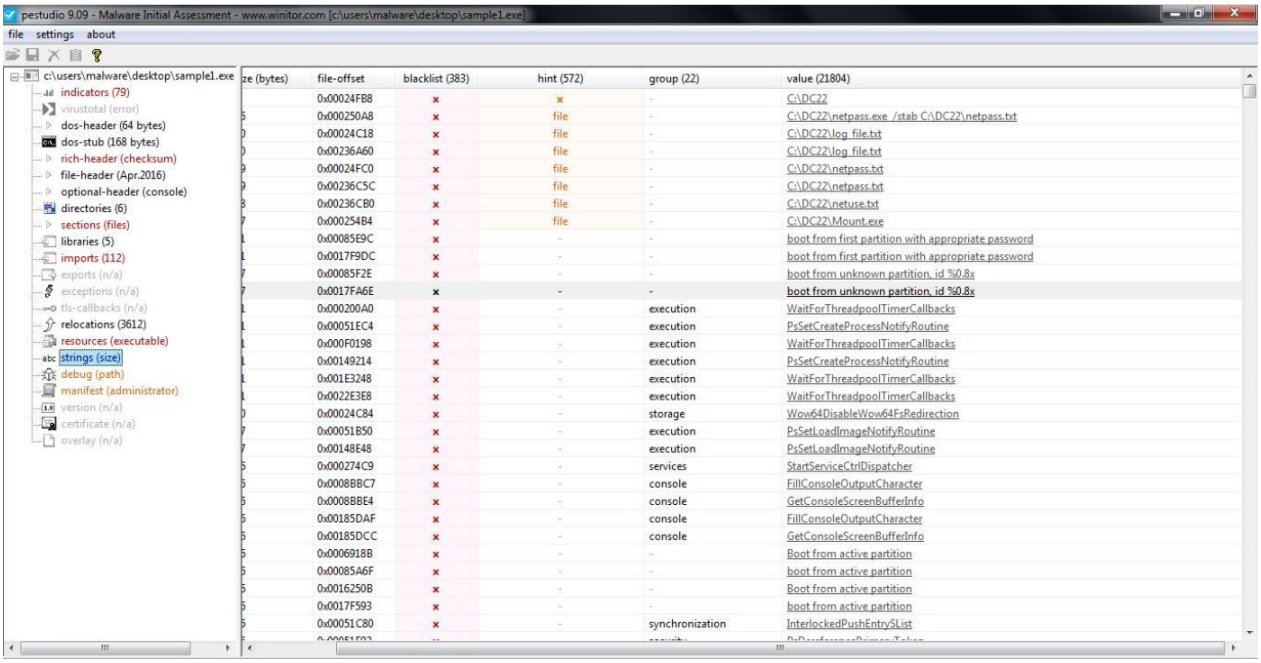

Figure 5: Number of Strings in Sample1.exe

The last indicator used to determine if sample1.exe was packed or obfuscated was the signature provided by pestudio. If the program was packed then the packer could show up in the signature which could be used to identify how to unlock the file. However, the only signature listed is Microsoft Visual C++ 8. For this reason, the signature of the file does not indicate sample1.exe is packed or obfuscated.

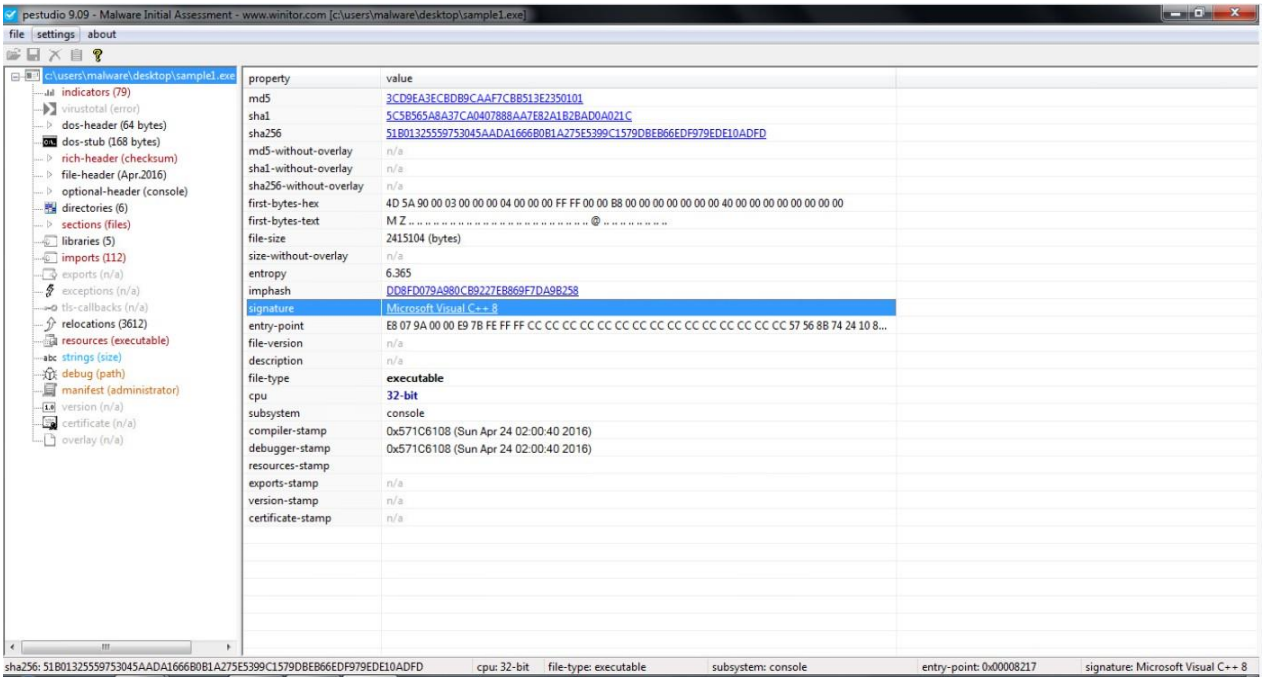

Figure 6: Signature of Sample1.exe

Based on the analysis described above sample1.exe is not packed as the utilized indicators do not point in that direction.

4. Identify any suspicious functions imported by the program

There are 112 functions imported by the sample1.exe file with 28 of those being blacklisted by pestudio. All of these blacklisted functions are associated with 4 libraries with a total of 5 libraries being imported. See below for a general breakdown of all imported libraries associated with blacklisted functions:

dvapi32.dll: This library is part of the advanced API service library and gives access to the kernel. It is responsible for the registry, controlling windows services, managing user accounts, and restarting and shutting down the system

kernel32.dll: This library is a kernel module and a dynamic link library. It carries out functions like memory management, input/output operations, and interrupts.

user32.dll: This library creates and manipulates the graphic user interface or GUI.

shell32.dll: This library is used to open web pages and files.

The identified libraries can be used to give a general idea of the categories the 28 blacklisted functions operate within. As a further breakdown, we can see pestudio identifying the blacklisted functions as impacting security (6 functions), services (3 functions), system-information (1 function), execution (10 functions), exception-handling (1 function), dynamic-library (3 functions), diagnostic (1 function), console (2 functions), and administration (1 function).

From the above description we can see that the malware is implementing code that can impact a wide host of functionality on the host computer. This impact ranges from security, to the creation

of new processes, and forced rebooting after the malware implements its code. The exact functionality of each blacklisted function can be viewed on the docs.microsoft website.

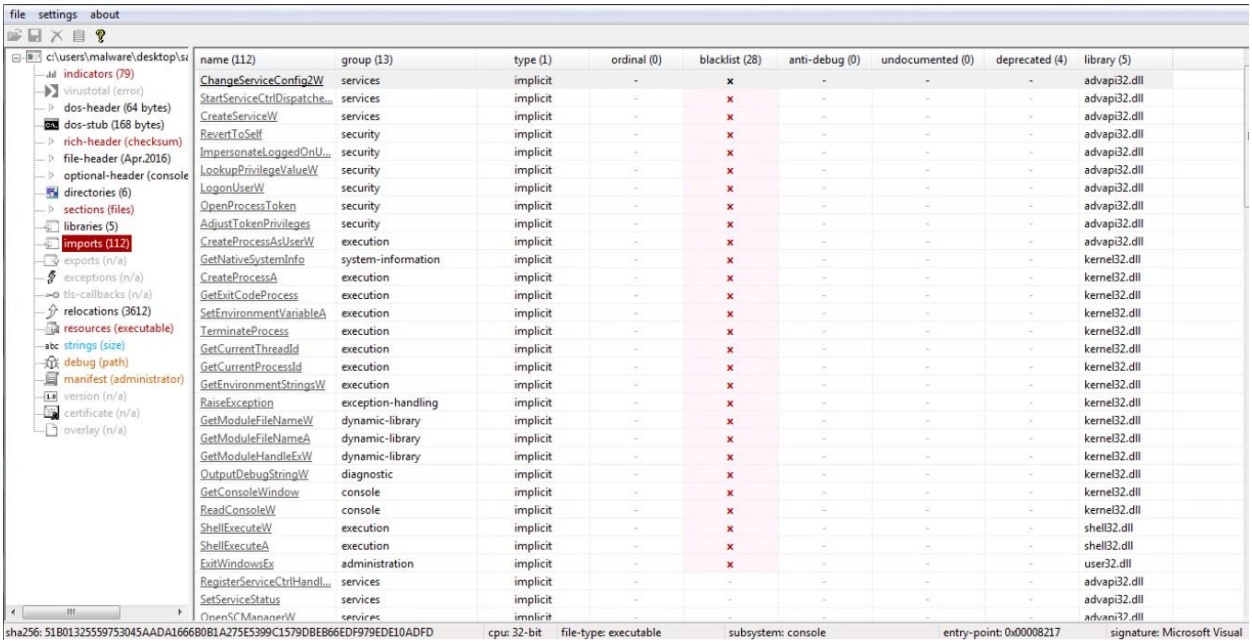

Figure 7: Suspicious Imported Functions

5. Identify any suspicious or relevant strings (IP addresses, urls, process names, file names, etc.).

Sample1.exe is a program with 21804 strings identified, 383 of which are blacklisted. These strings identify files, reference websites and have ominous messages associated with them. As there are far too many to discuss individually the following are a series of strings that stood out.

1. You are Hacked !!! Your H.D.D. Encrypted . Contact Us For Decryption Key (w889901665@yandex.com) YOURID: 123139".
2. "1.1.846.118"
3. "http://diskcryptor.net/index/php/DiskCryptor"
4. "DiskCryptor driver ver %d detected"
5. "This device cannot be decrypted because 'Deny access to unencrypted HDD's' option enabled."

The most clear-cut string that illustrates malicious intent are those with the phrase **(1)**. This string is self-evident in its intent as it declares that the host has become a victim of an encryption software. This is not the only suspicious string identified as, we can continue the narrative with the identified string values in **(2)** and **(3)**. These two strings, when searched on the internet, result in the user being directed to an encryption software called DiskCryptor. The DiskCryptor software is able to encrypt a user's filesystem and its incorporation into this malware indicates that DiskCryptor is being used for malicious intent. Progressing forward with the next identified string we find **(4)**. We can surmise at this point that this is being used as verification that

DiskCryptor has been installed and this is confirmation of that installation. Lastly, we also have: **(5)** which is again self-evident in its purpose.

With the aforementioned strings identified we can put together a cohesive understanding of what is going on with this malware and its association with DiskCryptor. We can see that the malware identifies a specific website and software tool. We can also see a message that looks for confirmation that the software was downloaded. Following this we see that there exists a message telling the user that their system is encrypted as well as another string that explains why a system cannot be decrypted. Individually these strings are suspicious; however, together they tell of a malicious intent.

6. Identify the program section(s) and possible contents

There are 5 sections in sample1.exe:

1. .text
2. .rdata
3. .data
4. .rsrc
5. .reloc

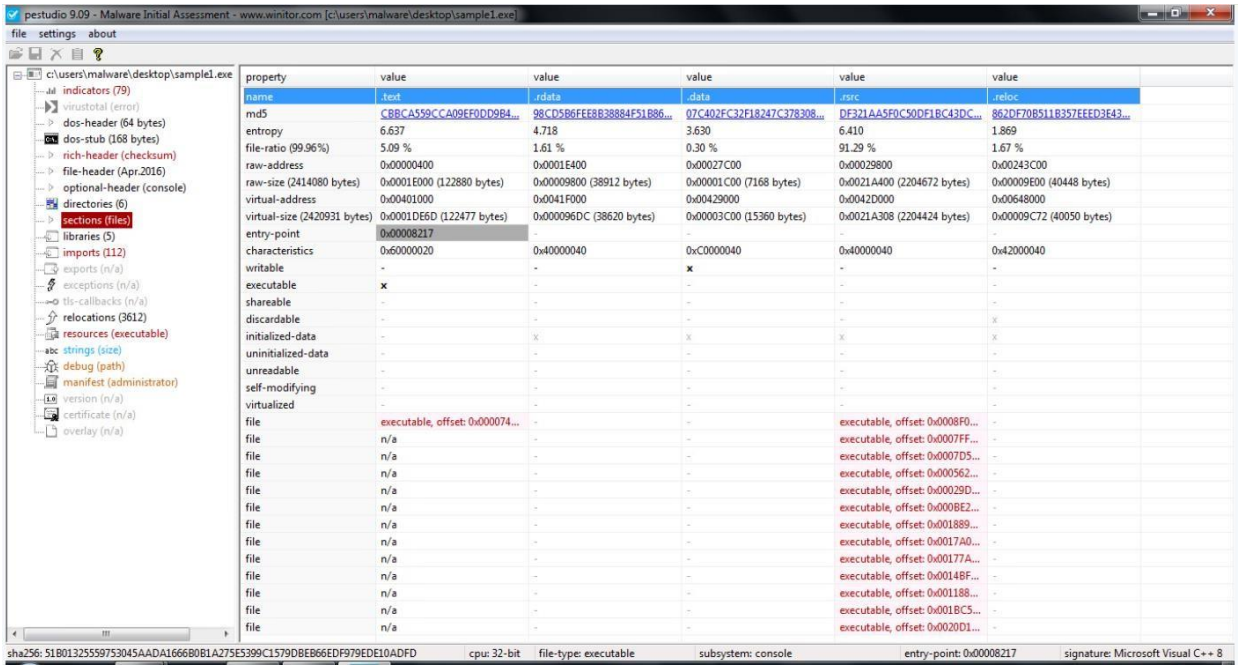

Figure 8: Sample1.exe sections

Looking at the resources used by sample1.exe we can see several executables used. These executables share a similar signature to another malware program called Mamba Ransomware and is responsible for encrypting victims filesystems and requiring bitcoin to unlock. Of special

note is MOUNT.EXE and netpass.exe. Looking at Figure 16 we can see that these files were added after malware execution in the folder DC22. MOUNT.EXE is able to be used to search for mounted drives like external hard drives and USB sticks – which means that if they were installed at the time of execution they could be impacted as well. As for netpass.exe this is an executable that aims to steal the usernames and passwords of the infected host.

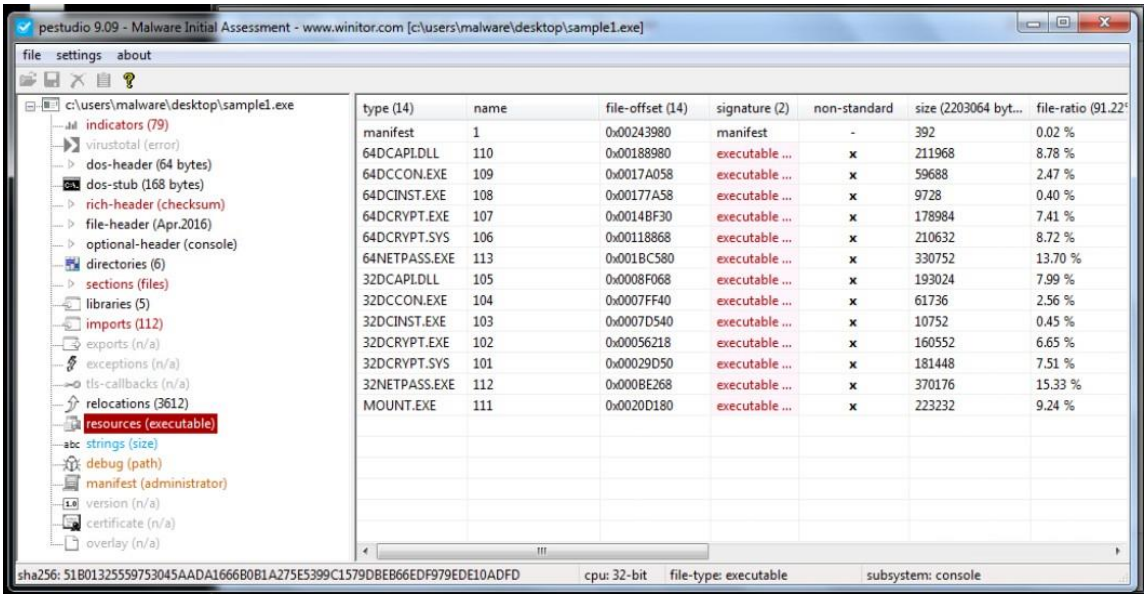

Figure 9: Resources

Findings: Dynamic Analysis

1. Interesting behaviours that occur after the malware has executed.

After successful execution of sample1.exe the observed behavior included a forced reboot of the Microsoft Windows computer whereupon relogging into the system the user is able to use Windows as normal. However, upon additional restart the user becomes unable to use the Windows system and is presented with a Message indicating that they have been hacked. The exact message matches a string that was identified as suspicious in the static analysis.

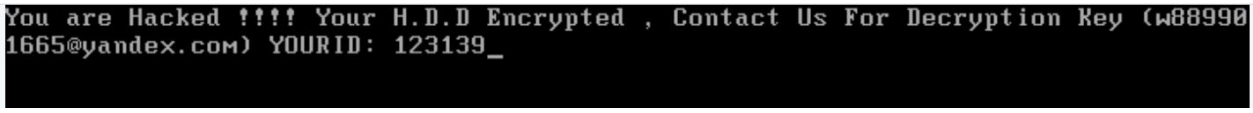

Figure 10: Hacked Message Upon Restart

2. Machines and services the malware attempts to identify or contact by IP or domain/host name.

During the dynamic analysis, several services were used to determine network activity including fakedns, wireshark, and inetsim. However, through the use of these applications there was no indication of network activity from the software. Instead the results identified by the applications

appear to be noise generated through the Windows software itself. This noise is possibly being generated through the applications attempts to update. However, the identified hits occur without sample1.exe execution and as such do not indicate that there is network activity by the malware.

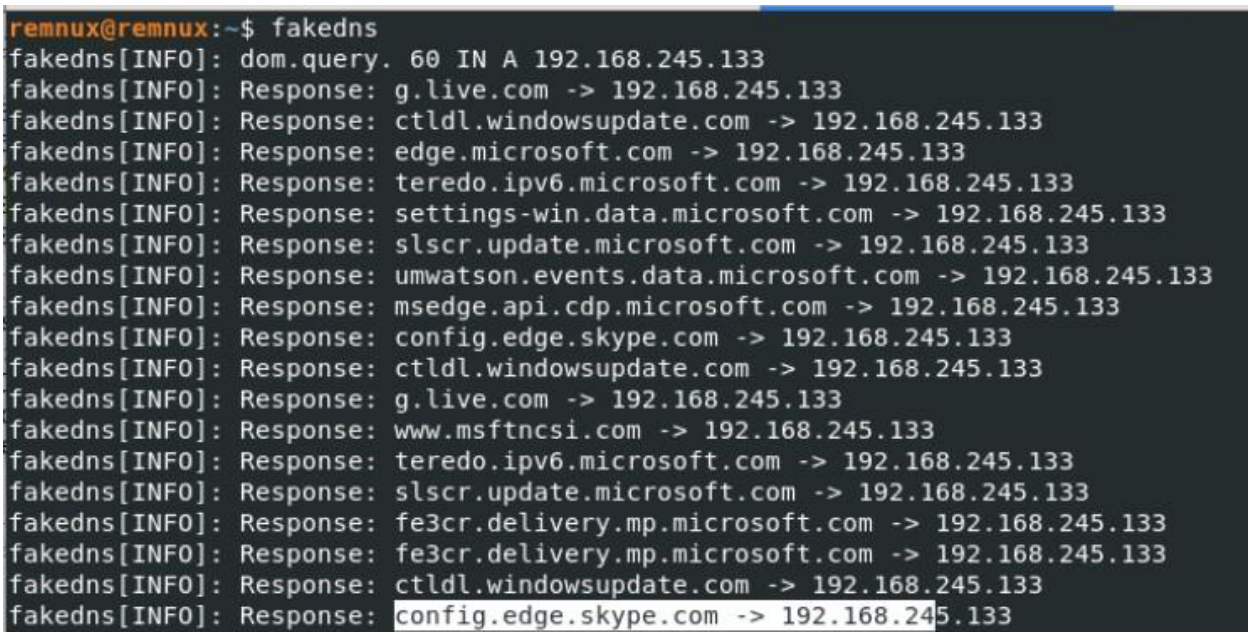

Figure 11: fakedns

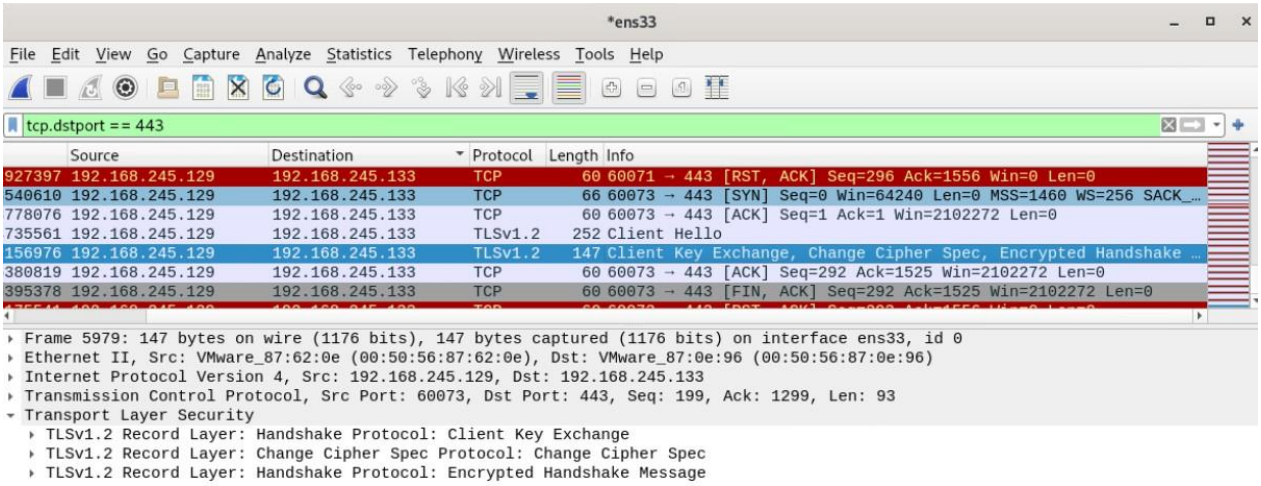

Figure 12: Wireshark

3. Registry Keys created/modified by the malware. / Files created/modified by the malware. Regshot is a useful tool that was used to compare the Windows system status before and after execution of the malware. When run several times there were some parameters that changed and others that remained the same. The difference for those parameters that changed are likely a result of the generated noise from Windows.

When run it was identified that 21 keys were deleted, while 62 to 72 keys were added. Among the added keys we see that they are for the dcrypt and DefragmentService drivers as they map to those created paths. In addition, the filesystem had 19 to 27 files added and 72 to 86 files modified.

```
----------------------------------
Keys deleted:21
----------------------------------
HKLM\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{1D036814-2F0A-482F-9E3B-0F6A01546B1A}
HKLM\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{998DC3E4-7604-4312-BB52-5B488BBB457B}
HKLM\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{EA2D9350-6593-477A-A5C0-BEA017FD9B7B}
HKLM\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{FEDF738E-B0F4-4709-AEBA-294A9EE02E43}
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\19abea5c-4f2a-480d-bda5-474dc88c3482
HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Events\{67E402DD-340D-4309-9400-8E209B69B596}
HKLM\SYSTEM\Setup\SetupapiLogStatus
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Ex
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Ex
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows\Current
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows Media P
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\G
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows Media Player NSS
```

Figure 13: Keys Deleted Short FilePaths

```
:209B69B596}

ersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012022011720220124
ersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012022013120220201
E\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{1D036814-2F0A-482F-9E3B-0F6A01546B1A}
E\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{998DC3E4-7604-4312-BB52-5B488BBB457B}
E\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{EA2D9350-6593-477A-A5C0-BEA017FD9B7B}
E\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{FEDF738E-B0F4-4709-AEBA-294A9EE02E43}
E\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\19abea5c-4f2a-480d-bda5-474dc88c3482
E\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Events\{67E402DD-340D-4309-9400-8E209B69B596}
E\Microsoft\WBEM\Transports\Decoupled\Client\{1D036814-2F0A-482F-9E3B-0F6A01546B1A}
E\Microsoft\WBEM\Transports\Decoupled\Client\{998DC3E4-7604-4312-BB52-5B488BBB457B}
E\Microsoft\WBEM\Transports\Decoupled\Client\{EA2D9350-6593-477A-A5C0-BEA017FD9B7B}
E\Microsoft\WBEM\Transports\Decoupled\Client\{FEDF738E-B0F4-4709-AEBA-294A9EE02E43}
E\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\19abea5c-4f2a-480d-bda5-474dc88c3482
E\Microsoft\Windows Media Player NSS\3.0\Events\{67E402DD-340D-4309-9400-8E209B69B596}
```

Figure 14: Keys Deleted Long FilePaths

```
Keys added:72
----------------------------------
HKLM\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{36A0146E-82DD-4176-AFDC-994499AFFB1A}
HKLM\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{79B28F2E-63E8-42AC-944D-BAA36B547F92}
HKLM\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{7CD0ED66-ADC9-4022-BC5B-9F3E3DC8F584}
HKLM\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{A6EE2273-CB15-4180-91F7-4E919E331BB5}
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\fa85664e-d4f7-40b4-8760-ba80a29caa96
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Reporting\RebootWatch
HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Events\{468BF1C7-460A-4207-93DF-A40163B1C7CB}
HKLM\SOFTWARE\VMware, Inc.\VMware Tools\VMUpgradeHelper\Adapters\00:50:56:87:85:14
HKLM\SYSTEM\ControlSet001\services\dcrypt
HKLM\SYSTEM\ControlSet001\services\dcrypt\config
HKLM\SYSTEM\ControlSet001\services\dcrypt\Instances
HKLM\SYSTEM\ControlSet001\services\dcrypt\Instances\dcrypt
HKLM\SYSTEM\ControlSet001\services\dcrypt\Enum
HKLM\SYSTEM\ControlSet001\services\DefragmentService
HKLM\SYSTEM\ControlSet002\services\dcrypt
HKLM\SYSTEM\ControlSet002\services\dcrypt\config
HKLM\SYSTEM\ControlSet002\services\dcrypt\Instances
HKLM\SYSTEM\ControlSet002\services\dcrypt\Instances\dcrypt
HKLM\SYSTEM\ControlSet002\services\DefragmentService
HKLM\SYSTEM\CurrentControlSet\services\dcrypt
HKLM\SYSTEM\CurrentControlSet\services\dcrypt\config
HKLM\SYSTEM\CurrentControlSet\services\dcrypt\Instances
HKLM\SYSTEM\CurrentControlSet\services\dcrypt\Instances\dcrypt
HKLM\SYSTEM\CurrentControlSet\services\dcrypt\Enum
HKLM\SYSTEM\CurrentControlSet\services\DefragmentService
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv\OpenWithList
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{c7864612-cc06-11e2-8faa-806e6f6e6963}
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.hiv
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012022013120220207
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012022021320220214
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\1
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\1\0
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\1\0\0
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\2
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\61
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\61\ComDlg
```

Figure 15: Keys Added short filepaths

Figure 16: Keys Added long filepaths

Figure 17: Files added

```
------------------------------------
Files [attributes?] modified:72
------------------------------------
C:\Boot\BCD
C:\Boot\BCD.LOG
C:\pagefile.sys
C:\Users\malware\AppData\Local\IconCache.db
C:\Users\malware\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\malware\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\malware\AppData\Local\Microsoft\Windows\UsrClass.dat
C:\Users\malware\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
C:\Users\malware\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\malware\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
C:\Users\malware\Desktop\Dynamic Analysis\Packages\RegShot\language.ini
C:\Users\malware\Desktop\Dynamic Analysis\Packages\RegShot\regshot.ini
C:\Users\malware\NTUSER.DAT
C:\Users\malware\ntuser.dat.LOG1
C:\Windows\bootstat.dat
C:\Windows\debug\PASSWD.LOG
C:\Windows\inf\WmiApRpl\0009\WmiApRpl.ini
C:\Windows\inf\WmiApRpl\WmiApRpl.h
C:\Windows\setupact.log
C:\Windows\SoftwareDistribution\DataStore\DataStore.edb
C:\Windows\SoftwareDistribution\DataStore\Logs\edb.chk
C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log
C:\Windows\SoftwareDistribution\DataStore\Logs\tmp.edb
C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
C:\Windows\System32\catroot2\edb.chk
C:\Windows\System32\catroot2\edb.log
C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb
C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
C:\Windows\System32\LogFiles\Scm\0d9b5d92-3a22-486d-a887-3aa21597cf27
C:\Windows\System32\LogFiles\Scm\59a9f588-fdf8-4bc9-b810-4aade19f5639
C:\Windows\System32\LogFiles\Scm\5b184694-64c3-4633-94c5-945b3fa561d6
C:\Windows\System32\LogFiles\Scm\9b75c702-ea13-406a-badb-6c588ee4375b
C:\Windows\System32\LogFiles\Scm\a1cfa52f-06f2-418d-addb-cd6456d66f43
C:\Windows\System32\LogFiles\Scm\a316e645-1c56-45a6-bd6a-7dca79778090
C:\Windows\System32\LogFiles\Scm\a6394592-54ce-4e93-8d64-1a068f462632
C:\Windows\System32\LogFiles\Scm\bba67ad0-4ba0-4b44-827b-ff419b70c057
C:\Windows\System32\LogFiles\Scm\de8bae53-2809-4f75-85ef-427d364b9b2c
C:\Windows\System32\LogFiles\Scm\f1369a11-e983-4458-b390-712efa1cba44
C:\Windows\System32\Microsoft\Protect\S-1-5-18\User\Preferred
C:\Windows\System32\perfc009.dat
C:\Windows\System32\perfh009.dat
C:\Windows\System32\PerfStringBackup.INI
C:\Windows\System32\wbem\Performance\WmiApRpl.h
C:\Windows\System32\wbem\Performance\WmiApRpl.ini
C:\Windows\System32\wbem\Repository\INDEX.BTR
C:\Windows\System32\wbem\Repository\MAPPING1.MAP
C:\Windows\System32\wbem\Repository\MAPPING2.MAP
```

Figure 18: Files Modified short paths

```
C:\Windows\System32\wbem\Repository\MAPPING1.MAP
C:\Windows\System32\wbem\Repository\MAPPING2.MAP
C:\Windows\System32\wbem\Repository\OBJECTS.DATA
C:\Windows\System32\winevt\Logs\Application.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-BranchCacheSMB%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders API Service.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-OfflineFiles%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Service%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4Operational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4WHC.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-WindowsBackup%4ActionCenter.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
C:\Windows\System32\winevt\Logs\Security.evtx
C:\Windows\System32\winevt\Logs\System.evtx
C:\Windows\Tasks\SA.DAT
C:\Windows\Tasks\SCHEDLGU.TXT
C:\Windows\WindowsUpdate.log
```

Figure 19: Files Modified long paths

4. Services or processes started by the malware.

After the malware was executed and the forced reboot was complete process explorer showcased a process being executed by sample1.exe which is dccon.exe. Upon investigation and looking up the nature of this executable it was found that this is the executable of the Disk Cryptor software. In other words, it is after the force reboot occurs that the malware implements the Disk Cryptor service to encode the users filesystem.

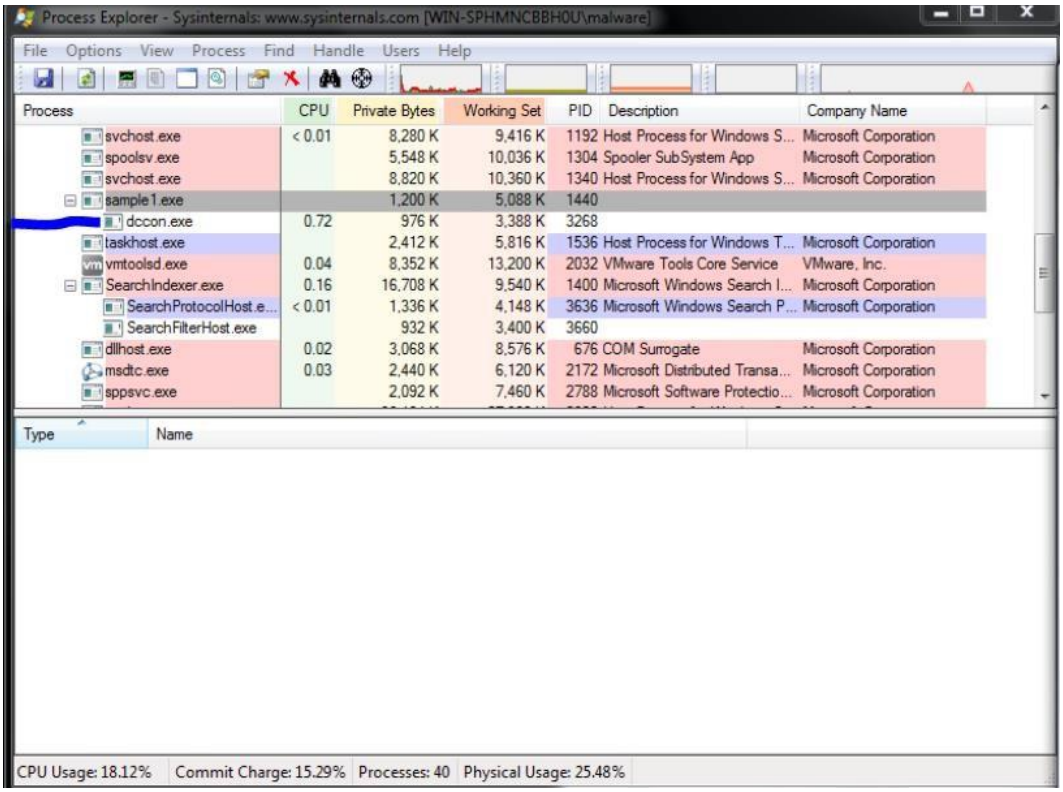

Figure 20: Execution of dccon.exe

Indicators of Compromise

The biggest indicator of compromise for this system is the use of DiskCryptor in the sample1.exe. While this software is not malicious by nature it is being co-opted for this purpose. The reason this is an indicator of compromise is that this service is being used in a manner which is not advertised to the user. Beyond this, we can also see a signature of DC22 folder being related to other malicious programs online – such the Mamba ransomware. More apparent however, is the forced reboot that the program implements as this is not a standard practice for software to engage with as it strips the authoritative access away from the owner. There are other indicators, as described within this report. However, the indicators discussed within this section are black flags in a sea of red flags.