# 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 rawsize 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.

3 X 8 8				
c:\users\maiware\desktop\sample1\sample1.exe	property	value	detail	
and indicators (109)	compiler-stamp	0x571C6108	Sun Apr 24 06:00:40 2016   UTC	
	size-of-optional-header	0x00E0	224 bytes	de la
dos-header (64 bytes)	signature	0x00004550	PEOD	
→ dos-stub (168 bytes) → rich-header (checksum)	machine	0x014C	Intel	
m P file-header (Apr.2016)	sections	0x0005	5	
	pointer-symbol-table	0x00000000	0x0000000	
directories (6)	number-of-symbols	Dx00000000	0x0000000	
> sections (files)	processor-32bit	0x00000100	true	
	system-image	0x00000000	false	
functions (112)	executable	0x0000002	true	
🕞 exports (n/a)	dynamic-link-library	0x00000000	false	
tis-callbacks (n/a)	debug-stripped	0x0000000	false	
🕞 .NET (n/a)	line-stripped-from-file	0x00000000	false	
	local-symbols-stripped-from-file	0x0000000	false	
abc strings (size)	relocation-stripped	0x0000000	false	
- Tr debug (Apr.2016)	large-address-aware	0x00000000	false	
	uniprocessor	0x00000000	false	
(1.) version (n/a)	bytes-of-machine-words-reversed-Low	0x00000000	false	
🔄 🖸 overlay (n/a)	bytes-of-machine-words-reversed-Hi	0x00000000	false	
	media-run-from-swap	0x00000000	false	
	network-run-from-swap	0x0000000	false	

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.

e settings about				
c:\users\malware\desktop\sample1\sample1.exe	property	value	detail	
indicators (109)		Dx0003	console	
	subsystem	0x0003	PE	
> dos-header (64 bytes)	magic file-checksum	0x0000000	0x0024DD40 (expected)	
dos-stub (168 bytes)		0x00000000	section: text	
> rich-header (checksum)	entry-point base-of-code	0x00008217	section:.text	
> file-header (Apr.2016)	base-of-code			
> optional-header (console)		0x0001F000	section:.rdata	
📆 directories (6)	size-of-code	0x0001E000	122880 bytes	
> sections (files)	size-of-initialized-data	0x00231600	2299392 bytes	
	size-of-uninitialized-data	Gx00000000	0 bytes	
	size-of-image	0x00252000	2433024 bytes	
🕞 exports (n/a)	size-of-headers	0×00000400	1024 bytes	
tis-callbacks (n/a)	size-of-stack-reserve	0x00100000	1048576 bytes	
🕞 .NET (n/a)	size-of-stack-commit	6x00001000	4096 bytes	
	size-of-heap-reserve	0x00100000	1048576 bytes	
abc strings (size)	size-of-heap-commit	0x00001000	4096 bytes	
	section-alignment	0x00001000	4096 bytes	
🗐 manifest (administrator)	file-alignment	0x00000200	512 bytes	
💶 version (n/a)	directories-number	0x0000010	16	
i overlay (n/a)	LoaderFlags	0x0000000	0x00000000	
	Win32VersionValue	0x0000000	0x00000000	
	image-base	0x00400000	0x00400000	
	linker-version	11.0	11.0	
	os-version	5.1	5.1	
	image-version	0.0	0.0	
	subsystem-version	5.1	5.1	
,	address-space-layout-randomization (ASLR)	0x0040	true	

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.

settings about							
c:\users\malware\desktop\sample1.exe	property	value	value	value	value	value	
indicators (109)	name	.text	rdata	.data	rsrc	reloc	
- Virustotal (error)	md5	CBBCA559CCA09EF0DD9B4	98CD5B6FEE8B38884F51B86	07C402FC32F18247C378308	DF321AA5F0C50DF1BC43DC	862DF70B511B357EEED3E43	
<ul> <li>b dos-header (64 bytes)</li> </ul>	entropy	6.637	4.718	3.630	6.410	1.869	
dos-stub (168 bytes)	file-ratio (99.96%)	5.09 %	1.61 %	0.30 %	91,29 %	1.67 %	
ich-header (checksum)	raw-address	0x00000400	0x0001E400	0x00027C00	0x00029800	0x00243C00	
> file-header (Apr.2016)	raw-size (2414080 bytes)	0x0001E000 (122880 bytes)	0x00009800 (38912 bytes)	0x00001C00 (7168 bytes)	0x0021A400 (2204672 bytes)	0x00009E00 (40448 bytes)	
optional-header (console)	virtual-address	0x00401000	0x0041F000	0x00429000	0x0042D000	0x00648000	
📑 directories (6)		0x0001DE6D (122477 bytes)	0x000096DC (38620 bytes)	0x00003C00 (15360 bytes)	0x0021A308 (2204424 bytes)	0x00009C72 (40050 bytes)	
	entry-point	0x00008217	-	-	enough des (aconter bytes)	-	
functions (112)	characterístics	0x60000020	0x40000040	0xC0000040	0x40000040	0x42000040	
	writable			×			
	executable	x		17			
	shareable	2					
a resources (executable) *	discardable					×	
-abc strings (size)	initialized-data		x		÷	*	
debug (Apr.2016)	uninitialized-data					-	
manifest (administrator)	unreadable						
u version (n/a)	self-modifying						
- 🕒 overlay (n/a)	virtualized						
	file				executable, offset: 0x0008F0		
	file				executable, offset: 0x0003FF		
	file				executable, offset: 0x0007D5		
	file				executable, offset: 0x000562		
	file		-		executable, offset: 0x00029D		
	file				executable, offset: 0x000250		
	file				executable, offset: 0x000822		
	file				executable, offset: 0x0017A0		
	file				executable, offset: 0x0017A0		
	Ine				executable, onset: 0x00177A		

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.

IV II R				ĺ
Image: State	property md5 sha1 sha256 first-bytes-hex first-bytes-text file-size entropy imphash <b>3</b> ignature tooling entry-point file-type cpu subsystem compiler-stamp debugger-stamp import-stamp exports-stamp version-stamp	value           2CD9Ex3ECE0898CAAF7CB8513E2350101           2CS8565A8A37CA0407088AA7E82A1828A00A021C           5180132559738034AA0A1666081A2755398C157098E8660F979EDE10ADED           40 55 49 00 00 00 00 00 00 00 00 00 00 00 00 00		

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.

XII					
c:\users\malware\desktop\sample1.exe ze (bytes)	file-offset	blacklist (383)	hint (572)	group (22)	value (21804)
dal indicators (79)	0x00024FB8	×	×		C:\DC22
Virustotal (error)	0x000250A8	×	file		C:\DC22\netpass.exe /stab C:\DC22\netpass.txt
dos-header (64 bytes)	0x00024C18	×	file		C:\DC22\log file.txt
dos-stub (168 bytes)	0x00236A60	×	file		C:\DC22\log file.txt
rich-header (checksum)	0x00024FC0	x	file		C:\DC22\netpass.txt
▷ file-header (Apr.2016)	0x00236C5C	×	file		C:\DC22\netpass.txt
<ul> <li>optional-header (console)</li> <li>directories (6)</li> </ul>	0x00236CB0	×	file		C:\DC22\netuse.bt
sections (files)	0x000254B4	×	file		C:\DC22\Mount.exe
libraries (5)	0x00085E9C	×			boot from first partition with appropriate password
imports (112)	0x0017F9DC	×			boot from first partition with appropriate password
C exports (n/a)	0x00085F2E	×			boot from unknown partition, id %0.8x
A exceptions (n/a)	0x0017FA6E	×	2		boot from unknown partition, id %0.8x
-o tis-callbacks (n/a)	0x000200A0	×		execution	WaitForThreadpoolTimerCallbacks
∲ relocations (3612)	0x00051EC4	×		execution	PsSetCreateProcessNotifyRoutine
resources (executable)	0x000F0198	×		execution	WaitForThreadpoolTimerCallbacks
abc strings (size)	0x00149214	×		execution	PsSetCreateProcessNotifyRoutine
🗘 debug (path)	0x001E3248	x		execution	WaitForThreadpoolTimerCallbacks
manifest (administrator)	0x0022E3E8	×		execution	WaitForThreadpoolTimerCallbacks
1.0 version (n/a)	0x00024C84	×		storage	Wow64DisableWow64EsRedirection
certificate (n/a)	0x00051B50	×		execution	PsSetLoadImageNotifyRoutine
🕒 overlay (n/a)	0x00148E48	×		execution	PsSetLoadImageNotifyRoutine
Б	0x000274C9	×		services	StartServiceCtrlDispatcher
5	0x0008BBC7	×		console	FillConsoleOutputCharacter
5	0x0008BBE4	×		console	GetConsoleScreenBufferInfo
5	0x00185DAF	×		console	FillConsoleOutputCharacter
5	0x00185DCC	×		console	GetConsoleScreenBufferInfo
5	0x0006918B	×			Boot from active partition
5	0x00085A6F	×			boot from active partition
5	0x0016250B	×			Boot from active partition
5	0x0017F593	×			boot from active partition
5	0x00051C80	×		synchronization	InterlockedPushEntrySList

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.

settings about			
	md5 sha1 sha2 sha2 sha2 sha2 without-overlay sha256 without-overlay sha256-without-overlay first-bytes-hex file-size size-without-overlay entropy imphash size-without-overlay entropy imphash size-without-overlay entropy imphash size-without-overlay entropy imphash size-without-overlay entropy imphash size-without-overlay entropy imphash size-without-overlay entropy entropy size-size exputs-stamp exports-stamp version-stamp	value           3CD9EA3ECEDB9CAAF7CBB513E2350101           5C5865A8A37CA0407888AA7E82A1E28A00A021C           5180132559753045AADA16668081A275E5399C15790BE866EDF979EDE10ADED           n/a           b365           DBF007948060169227EB869F7DA98258           Microsoft Visual C4= 8           E8 07 94 00 00 E9 76 FE FF FF CC	
	version-stamp certificate-stamp	n/a n/a	

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

**<u>kernel32.dll</u>**: 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.

c:\users\malware\desktop\sa	name (112)	group (13)	type (1)	ordinal (0)	blacklist (28)	anti-debug (0)	undocumented (0)	deprecated (4)	library (5)
-Jul indicators (79)	ChangeServiceConfig2W	services	implicit	-	x	-	-		advapi32.dll
>> virustotal (error)	StartServiceCtrlDispatche	services	implicit		×				advapi32.dll
dos-header (64 bytes)	CreateServiceW	services	implicit		x				advapi32.dll
dos-stub (168 bytes)	RevertToSelf	security	implicit		x				advapi32.dll
<ul> <li>rich-header (checksum)</li> <li>file-header (Apr.2016)</li> </ul>	ImpersonateLoggedOnU	security	implicit		×				advapi32.dll
<ul> <li>p file-neader (Apr.2010)</li> <li>p optional-header (console</li> </ul>	LookupPrivilegeValueW	security	implicit		x				advapi32.dll
- directories (6)	LogonUserW	security	implicit		×				advapi32.dll
sections (files)	OpenProcessToken	security	implicit		x				advapi32.dll
libraries (5)	AdjustTokenPrivileges	security	implicit		×				advapi32.dll
imports (112)	CreateProcessAsUserW	execution	implicit		×				advapi32.dll
exports (n/a)	GetNativeSystemInfo	system-information	implicit		×				kernel32.dll
<pre> f exceptions (n/a) </pre>	CreateProcessA	execution	implicit		×				kernel32.dll
⊷o tis-callbacks (n/a)	GetExitCodeProcess	execution	implicit		x				kernel32.dll
ŷ relocations (3612)	SetEnvironmentVariableA	execution	implicit		×				kernel32.dll
resources (executable)	TerminateProcess	execution	implicit		x				kernel32.dll
abc strings (size)	GetCurrentThreadId	execution	implicit		×				kernel32.dll
🛱 debug (path)	GetCurrentProcessId	execution	implicit		×				kernel32.dll
manifest (administrator)	GetEnvironmentStringsW	execution	implicit		×				kernel32.dll
LA version (n/a)	RaiseException	exception-handling	implicit		×				kernel32.dll
certificate (n/a)	GetModuleFileNameW	dynamic-library	implicit		×				kernel32.dll
🗋 overlay (n/a)	GetModuleFileNameA	dynamic-library	implicit		×				kernel32.dll
	GetModuleHandleExW	dynamic-library	implicit		x				kernel32.dll
	OutputDebugStringW	diagnostic	implicit		x				kernel32.dll
	GetConsoleWindow	console	implicit		×				kernel32.dll
	ReadConsoleW	console	implicit		x				kernel32.dll
	ShellExecuteW	execution	implicit		×				shell32.dll
	ShellExecuteA	execution	implicit		x				shell32.dll
	ExitWindowsEx	administration	implicit		×				user32.dll
	RegisterServiceCtrlHandl	services	implicit						advapi32.dll
	SetServiceStatus	services	implicit						advapi32.dll
· · · · · · · · · · · · · · · · · · ·	OpenSCManagerW	services	implicit						advani32.dll

**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

e settings about						
c:\users\malware\desktop\sample1.exe	property	value	value	value	value	value
Jul indicators (79)	name	.text	.rdata	.data	itste	.reloc
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	md5	CBBCA559CCA09EF0DD9B4	98CD5B6FEE8B38884F51B86	07C402FC32F18247C378308	DF321AA5F0C50DF1BC43DC	862DF70B511B357EEED3E43
> dos-header (64 bytes)	entropy	6.637	4.718	3.630	6.410	1.869
dos-stub (168 bytes)	file-ratio (99.96%)	5.09 %	1.61 %	0.30 %	91.29 %	1.67 %
rich-header (checksum) file-header (Apr.2016)	raw-address	0x00000400	0x0001E400	0x00027C00	0x00029800	0x00243C00
P file-header (Apr.2016) P optional-header (console)	raw-size (2414080 bytes)	0x0001E000 (122880 bytes)	0x00009800 (38912 bytes)	0x00001C00 (7168 bytes)	0x0021A400 (2204672 bytes)	0x00009E00 (40448 bytes)
directories (6)	virtual-address	0x00401000	0x0041F000	0x00429000	0x0042D000	0x00648000
sections (files)	virtual-size (2420931 bytes)	0x0001DE6D (122477 bytes)	0x000096DC (38620 bytes)	0x00003C00 (15360 bytes)	0x0021A308 (2204424 bytes)	0x00009C72 (40050 bytes)
libraries (5)	entry-point	0x00008217	-	-	-	-
imports (112)	characteristics	0x60000020	0x40000040	0xC0000040	0x40000040	0x42000040
	writable			x		•
	executable	x				
tis-callbacks (n/a)	shareable					
→  ŷ relocations (3612)	discardable					×
resources (executable)	initialized-data		×	x	×	x
abc strings (size)	uninitialized-data					
	unreadable					
manifest (administrator)	self-modifying					
	virtualized					
Crificate (n/a)	file	executable, offset: 0x000074			executable, offset: 0x0008F0	
l 🗋 overlay (n/a)	file	n/a			executable, offset: 0x0007FF	
	file	n/a			executable. offset: 0x0007D5	
	file	n/a			executable, offset: 0x000562	
	file	n/a			executable, offset: 0x00029D	
	file	n/a			executable, offset: 0x000BE2	
	file	n/a			executable, offset: 0x001889	
	file	n/a			executable, offset: 0x0017A0	
	file	n/a			executable, offset: 0x00177A	
	file	n/a			executable, offset: 0x0014BF	
	file	n/a			executable, offset: 0x001188	
	file	n/a			executable, offset: 0x001BC5	
	file	n/a			executable. offset: 0x0020D1	

### 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.

le settings about							
1日 × 自 🥊							
c:\users\malware\desktop\sample1.exe	type (14)	name	file-offset (14)	signature (2)	non-standard	size (2203064 byt	file-ratio (91.2
	manifest	1	0x00243980	manifest	2	392	0.02 %
->> virustotal (error)	64DCAPI.DLL	110	0x00188980	executable	×	211968	8.78 %
dos-header (64 bytes)	64DCCON.EXE	109	0x0017A058	executable	×	59688	2.47 %
rich-header (checksum)	64DCINST.EXE	108	0x00177A58	executable	x	9728	0.40 %
<ul> <li>P file-header (Checksum)</li> <li>P file-header (Apr.2016)</li> </ul>	64DCRYPT.EXE	107	0x0014BF30	executable	×	178984	7.41 %
	64DCRYPT.SYS	106	0x00118868	executable	×	210632	8.72 %
	64NETPASS.EXE	113	0x001BC580	executable	×	330752	13.70 %
sections (files)	32DCAPLDLL	105	0x0008F068	executable	×	193024	7.99 %
	32DCCON.EXE	104	0x0007FF40	executable	×	61736	2.56 %
imports (112)	32DCINST.EXE	103	0x0007D540	executable	×	10752	0.45 %
exports (n/a)	32DCRYPT.EXE	102	0x00056218	executable	x	160552	6.65 %
	32DCRYPT.SYS	101	0x00029D50	executable	×	181448	7.51 %
	32NETPASS.EXE	112	0x000BE268	executable	×	370176	15.33 %
— ŷ relocations (3612) — isources (executable)	MOUNT.EXE	111	0x0020D180	executable	x	223232	9.24 %
-abc strings (size)							
- III version (n/a) - III certificate (n/a)							
overlay (n/a)	4						

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.

```
You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (w88990
1665@yandex.com) YOURID: 123139_
```

### 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.

remnux@remnux:~\$ fakedns
fakedns[INF0]: dom.query. 60 IN A 192.168.245.133
<pre>fakedns[INF0]: Response: g.live.com -&gt; 192.168.245.133</pre>
<pre>fakedns[INF0]: Response: ctldl.windowsupdate.com -&gt; 192.168.245.133</pre>
fakedns[INF0]: Response: edge.microsoft.com -> 192.168.245.133
<pre>fakedns[INF0]: Response: teredo.ipv6.microsoft.com -&gt; 192.168.245.133</pre>
fakedns[INF0]: Response: settings-win.data.microsoft.com -> 192.168.245.133
fakedns[INFO]: Response: slscr.update.microsoft.com -> 192.168.245.133
<pre>fakedns[INF0]: Response: umwatson.events.data.microsoft.com -&gt; 192.168.245.133</pre>
<pre>fakedns[INF0]: Response: msedge.api.cdp.microsoft.com -&gt; 192.168.245.133</pre>
fakedns[INF0]: Response: config.edge.skype.com -> 192.168.245.133
fakedns[INF0]: Response: ctldl.windowsupdate.com -> 192.168.245.133
fakedns[INFO]: Response: g.live.com -> 192.168.245.133
fakedns[INFO]: Response: www.msftncsi.com -> 192.168.245.133
fakedns[INF0]: Response: teredo.ipv6.microsoft.com -> 192.168.245.133
<pre>fakedns[INF0]: Response: slscr.update.microsoft.com -&gt; 192.168.245.133</pre>
<pre>fakedns[INF0]: Response: fe3cr.delivery.mp.microsoft.com -&gt; 192.168.245.133</pre>
<pre>fakedns[INF0]: Response: fe3cr.delivery.mp.microsoft.com -&gt; 192.168.245.133</pre>
<pre>fakedns[INF0]: Response: ctldl.windowsupdate.com -&gt; 192.168.245.133</pre>
<pre>fakedns[INF0]: Response: config.edge.skype.com -&gt; 192.168.245.133</pre>

Figure 11: fakedns

ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> aptur	a Analuma Statistics Tal	onhonu Mirola	es Tools Hale							
🚺 🔳 🖉 🕑 📘 🛅	🕺 🙆 🔍 🔄 🖄	· K & 📃		1						
tcp.dstport == 443								$\times$	1.	•]•
Source	Destination	▼ Protocol	Length Info						E	Ξ
27397 192.168.245.129	192.168.245.133	TCP	60 60071	→ 443 [RS	T, ACK]	Seq=296 Ack=1556	Win=0 Len=0			=
40610 192.168.245.129	192.168.245.133	TCP	66 60073	→ 443 [SY	N] Seq=0	Win=64240 Len=0	MSS=1460 WS=25	6 SACK_		=
78076 192.168.245.129	192.168.245.133	TCP	60 60073	→ 443 [AC	K] Seq=1	Ack=1 Win=21022	72 Len=0			=
35561 192.168.245.129	192.168.245.133	TLSv1.2	252 Client	t Hello						=
6976 192.168.245.129	192.168.245.133	TLSv1.2	147 Client	t Key Exch	ange, Ch	ange Cipher Spec	, Encrypted Han	dshake	=	=
30819 192.168.245.129	192.168.245.133	TCP	60 60073	→ 443 [AC	K] Seq=2	92 Ack=1525 Win=	2102272 Len=0			=
95378 192.168.245.129	192.168.245.133	TCP	60 60073	→ 443 [FI	N, ACK]	Seq=292 Ack=1525	Win=2102272 Le	n=0	=	=
155 14 100 100 015 100	400 400 045 400	TOP	CO. CO070	140 [D0	T 10K1	Company Aslanters	Lines Lanes			-
Frame 5979: 147 bytes	on wire (1176 hite)	147 butos o	anturod (117	6 hitc) or	intorfa	co onc22 id 0				

Fransmission Control Protocol, Src Port: 60073, Dst Port: 443, Seq: 199, Ack: 1299, Len: 93

Transport Layer Security
 TLSV1.2 Record Layer: Handshake Protocol: Client Key Exchange
 TLSV1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 TLSV1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

### 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 HKLM HKLM HKLM	\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{1D036814-2F0A-482F-9E3B-0F6A01546B1A} \SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{8209350-6593-47604-4312-8B52-5B488BB8457B} \SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{E42D9350-6593-477A-A5C0-BEA017F0987B} \SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{FEDF738E-80F4-4709-AEBA-294A9E602E43} \SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{FEDF738E-80F4-4709-AEBA-294A9E602E43} \SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\19abea5c-4f2a-480d-bda5-474dc88c3482 \SOFTWARE\Microsoft\Windows\Media Player NSS\3.0\Events\{67E402D-3400-4309-9400-8E209869B596}
HKU\ HKU\ HKU\ HKU\ HKU\	<pre>\\SYSTEM\Setup\SetupapiLogStatus \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Ex: \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Ex: \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports' \S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\VirtualStore\WACHINE\SOFTWARE\VirtualStore\WACHINE\SOFTWARE\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\VirtualStore\Virtua</pre>
HKU\ HKU\ HKU\ HKU\ HKU\	<pre>S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\Windows\Current (S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decouple (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\Wirdows\CurrentVersion\G (S-1-5-21-1715238675-2618861422-3236400253-1004_Classes\virtualStore\MACHINE\SOFTWARE\Microsoft\Wirdows\CurrentVersion\G</pre>

#### **Figure 13: Keys Deleted Short FilePaths**

:2038038230}

ersion/Internet Settings\5.0\Cache\Extensible Cache\MSHistO12022011720220124 ersion/Internet Settings\5.0\Cache\Extensible Cache\MSHistO12022013120220201 uE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{10036814-2F0A-482F-9E3B-0F6A01546B1A} uE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{9980C3E4-7604-4312-BB52-5B488BBB4578} uE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{FEDF738E-B0F4-4709-AEBA-294A9EE02E43} uE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\19abea5c-4f2a-480d-bda5-474dc88c3482 uE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{FDF738E-B0F4-4709-AEBA-294A9EE02E43} uE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{10036814-2F0A-482F-9E3B-0F6A01546B1A} uE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{10036814-2F0A-482F-9E3B-0F6A01546B1A} uE\Microsoft\WBEM\Transports\Decoupled\Client\{10036814-2F0A-482F-9E3B-0F6A01546B1A} uE\Microsoft\WBEM\Transports\Decoupled\Client\{10036814-2F0A-482F-9E3B-0F6A01546B1A} uE\Microsoft\WBEM\Transports\Decoupled\Client\{50573477A-A5C0-BEA017F0957B} uE\Microsoft\WBEM\Transports\Decoupled\Client\{FDF738E-B0F4-4709-AEBA-294A9EE02E43} uE\Microsoft\WBEM\Transports\Decoupled\Client\{FDF738E-B0F4-4709-AEBA-294A9E02E43} uE\Microsoft\WIndows\CurrentVersion\Group Policy\ServiceInstances\19abea5c-4f2a-480d-bda5-474dc88c3482 uE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\19abea5c-4f2a-480d-bda5-474dc88c3482 uE\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\Decoup]ed\Client\{36A0146E-82DD-4176-AFDC-994499AFFB1A}
HKLM/SOFTWARE/Microsoft/WBEM/Transports/Decoupled/Client/{7982872-6388-42AC-944D-BAA366547F92}
HKLM/SOFTWARE/Microsoft/WBEM/Transports/Decoupled/Client/{7CDDED66-ADC9-4022-BC58-9F3E3DC8F584}
HKLM/SOFTWARE/Hicrosoft/WBEM/Transports/Decoupled/Client/{A6EE273-CB15-4180-91F7-4E919E331BB5}
HKLM/SOFTWARE/VICrosoft/Windows/current/version/Group Policy/ServiceInstances/fa85664e-d4f7-40b4-8760-ba80a29caa96
HKLM/SOFTWARE/WICrosoft/Windows/current/version/Windows/budate/Reporting/RebotWatch
HKLM/SOFTWARE/Wicrosoft/Windows/Media Player NSS/3.0/Events/468BF1C7-460A-4207-93DF-A40163BLC7CB}
HKLM/SOFTWARE/Weware, Inc. \Mware Tools\Muppradetejper\ddapters\00:50:56:87:85:14
HKLM/SYSTEM/ControlSet001/service/se
HKLM/SYSTEM/ControlSet001/Services/dcrypt/config
HKLM/SYSTEM/ControlSet001/services/dcrypt/linstances
HKLM/SYSTEM/controlSet001/services/dcrypt/Instances/dcrypt
hkLM/SysteM/controlSet001/serviceS/dc/ypt/thotaiteS/dc/ypt
HKLM/SYSTEM/controlSet001/services/beframentService
HKLM/SYSTEM/controlSet002/services/dcrvpt
HKLM/SYSTEM/ControlSet002/services/dcrypt/config
HKLM/SYSTEM/ControlSet002/services/dcrypt/linstances
HKLM/SPSTEM/ControlSet002/services/dcrypt/Instances/dcrypt
HKLM/SYSTEM/controlSet002/services/beframentService
HKLM\SYSTEM\CurrentControlSet\services\dcrvpt
HKLM\SYSTEM\CurrentControlSet\services\dcrypt\config
HKLM\SYSTEM\CurrentControlSet\services\dcrvpt\Instances
HKLM\SYSTEM\CurrentControlSet\services\dcrypt\Instances\dcrypt
HKLM\SYSTEM\CurrentControlSet\services\dcrvpt\Enum
HKLM\SYSTEM\CurrentControlSet\services\DefragmentService
HKU\S-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv
HKU\5-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\windows\currentversion\Explorer\FileExts\.hiv
HKU\5-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\windows\CurrentVersion\Explorer\FileExts\.hiv\OpenwithList
HKU\5-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{c7864612-cc06-11e2-8faa-806e6f6e6963}
HKU\5-1-5-21-1715238675-2618861422-3236400253-1004\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\M5Hist012022013120220207
HKU\5-1-5-21-1715238675-2618861422-3236400253-1004\Software\Microsoft\windows\currentVersion\Internet Settings\5.0\cache\Extensible Cache\MSHist012022021320220214
HKU\5-1-5-21-1715238675-2618861422-3236400253-1004\Software\classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\1
HKU\5-1-5-21-1715238675-2618861422-3236400253-1004\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\5-1-5-21-1715238675-2618861422-3236400253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\2
HKU\5-1-5-21-1715238675-2618861422-3236400253-1004\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

rypt\Enum
ifragmentService 19233-1004/Software/Microsoft\windows\currentversion\Explorer\compla32\openSavePidlMRU\hiv
10233-1004 Software Wicrosoft Windows Current version Explorer (Child Figure Raver a mixed in V 10233-1004 Software Wicrosoft (Windows Current version) Explorer (FileExts), hiv
0253-1004/Software/wicrosoft/windows/Currentversion/Explorer/FileExts/.hiv/openwithList
10253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{c7864612-cc06-11e2-8faa-806e6f6e6963}
10253-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.hiv
10253-1004\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012022013120220207
10253-1004/Software/Microsoft/windows/CurrentVersion/Internet_Settings/5.0/Cache/Extensible_Cache/MSHist012022021320220214
10253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\1
0253-1004\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\10\10
)0233-1004/Software/classes/Local SettingS/Software/Wicrosoft/Windows/Shell/BagWRU/10/1/0/0 )0233-1004/Software/classes/Local SettingS/Software/Wicrosoft/Windows/Shell/BagWRU/10/2
10233-1004/Software/classes/Local Settings/Software/wicrosoft/windows/Shell/Bags/61
10233-1004/Software/classes/Local setting/Software/Wicrosoft/windows/Shell/BagS/01
10233-1004\Software\classes\Local Settings\Software\vircosoft\windows\shell\Baqs\61\complq\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
)0253-1004\Software\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\61\Shell
10253-1004\Software\classes\Local Settings\Software\Microsoft\windows\Shell\Bags\62
10253-1004\Software\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\62\ComDlg
10253-1004\software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\62\ComDIg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
10253-1004/software/classes/Local settings/Software/wicrosoft/windows/shell/Bags/62/shell
10233-1004/Software\Classes\virtualStore\MACHINE\SofTWARE\Vircosoft\WBEN\Transports\Decoupled\Client\{36A0146E-82DD-4176-AFDC-994499AFFB1A} 10233-1004/Software\Classes\virtualStore\MACHINE\SofTWARE\Vircosoft\WBEN\Transports\Decoupled\Client\{796287E2E-638E-43AC-940+BA36547F92}
10233-1004/Software/Classes/Virtualstore/MACHIE/SOFTWARE/Microsoft/WBEM/Transports/Decoupled/Cirent//7920728-0580-4724C-9440-6AA306347P32}
10253-1004\Software\Classes\virtualStore\MARLHE\SofTwARE\Microsoft\WBEM\TransportS\Decoupled\Client\A6EE2273-CB15-4180-91F7-4E919E331BB5
10253-1004\Software\classes\virtualStore\MACHINE\SOFTWARE\Microsoft\windows\CurrentVersion\Group Policy\ServiceInstances\fa85664e-d4f7-40b4-8760-ba80a29caa96
10253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\windows\CurrentVersion\windowsUpdate\Reporting\Rebootwatch
10253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\windows Media Player NSS\3.0\Events\{468BF1C7 <sup>-4</sup> 60A-4207-93DF-A40163B1C7CB}
10253-1004\Software\Classes\VirtualStore\MACHINE\SOFTWARE\VMware, Inc.\VMware Tools\VMUpgradeHelper\Adapters\00:50:56:87:85:14
10233-1004_Classes\Local Settings\Software/Wircosoft\Windows\Shell\BagMRW110\1 10233-1004_Classes\Local Settings\Software/Wircosoft\Windows\Shell\BagMRW110\10
10233-1004_classes/Local Settings/Software/wircrosoft/windows/Shell/Badmku/L0/L/0/ 10233-1004_classes/Local Settings/Software/wircrosoft/windows/Shell/Badmku/L0/L/0/
10253-100_Classes(Local Setting(Software)Wicrosoft/Window(Shell)BadWRU(10/2
0253-1004_Classes\ucal Settings\Software\Vircosoft\Virdows\Shell\Bags\61
10253-1004_Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\61\ComDlg
<pre>10253-1004_Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\61\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}</pre>
10253-1004_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\61\Shell
10253-1004_Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\62
)0233-1004_Classes\Local settings\Software\Wircosoft\Windows\Shell\Bagis{2}ComDlg 10233-1004_Classes\Local settings\Software\Wircosoft\Windows\Shell\Bagis{2}ComDlg
10233-1004_Classes/Local settings/Software/Microsoft/Windows/Shell/Bags/62/Shell
10253-1004_Classe/VirtualStore(MACHINE/SOFTWARE/Microsoft/WBEM/Transports/Decoupled/Client/{36A0146E-82DD-4176-AFDC-994499AFB1A}
10253-1004_Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{79B28F2E-63E8-42AC-944D-BAA36B547F92}
10253-1004_classes/virtualstore/MACHINE/SOFTWARE/Microsoft/wBEM/Transports/Decoupled/client/{7CD0ED66-ADC9-4022-BC5B-9F3E3DC8F584}
10253-1004_classes\virtualStore\MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Client\{A6EE2273-CB15-4180-91F7-4E919E331BB5}
10253-1004_Classes\Virtualstore\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\fa85664e-d4f7-40b4-8760-ba80a29caa96
10253-1004_Classes/Virtualstore/MACHINE/SOFTWARE/Microsoft/Windows/Currentversion/WindowsUpdate/Reporting/RebootWatch
10233-1004_Classes\virtualstore\MACHINE\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Events\{468BF1C7 <sup>24</sup> 60A-4207-930F-A40I63B1C7CB} 10233-1004_Classes\virtualstore\MACHINE\SOFTWARE\Microsoft\Windows Tools\MUpgradeHelper\Addreslerers\005\556:87:85:14
Income to a set of the contraction of the contract of the contraction

Figure 16: Keys Added long filepaths

.

m

Files added:27 C: ProgramData\Microsoft\RAC\Temp\sqlE4C2.tmp C: Users\All Users\Microsoft\RAC\Temp\sqlE531.tmp C: Users\All Users\Microsoft\RAC\Temp\sqlE531.tmp C: Users\All Users\Microsoft\RAC\Temp\sqlE531.tmp C: Users\malware\AppData\Local\Wicrosoft\Windows\History\History.IE5\MSHist012022013120220207\index.dat C: Users\malware\AppData\Local\Wicrosoft\Windows\History\History.IE5\MSHist01202201320220214\index.dat C: Users\malware\AppData\Local\Temp\-res.txt C: Users\malware\AppData\Local\Temp\-res.txt C: Users\malware\AppData\Roaming\Wicrosoft\Windows\Recent\firstshot.hiv.lnk C: Users\malware\Desktop\firstshot.hiv C: Users\malware\Desktop\firstshot.hiv C: Windows\System32\drivers\drivers\drivers\drivers\secondshot.hiv. C: Windows\System32\drivers\drivers\drivers\secondshot.hiv C: Windows\System32\drivers\drivers\drivers\bedc078b-4dc4-4de4-84b0-8b97e4866e1d C: Windows\System32\Wicrosoft\Protect\S-1-5-18\User\c66606e-6560-4894-9643-37d2996327b7 C: SdcSys\$ C: DC22\dcinst.exe C: DC22\netpass.exe C: DC22\netpass.exe C: DC22\netpass.exe C: DC22\netpass.exe

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\maiware\AppData\Loca'\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\1b4dd67f29cb19	ticDestinations-ms
C:\Users\malware\Desktop\Dynamic Analysis\Packages\RegShot\language.ini	
C:\Users\ma]ware\Desktop\Dynamic Analysis\Packaĝes\ReĝShot\regŝhot.ini	
C:\Upers\malware\NTUSER.DAT C:\Upers\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\7B296FBO-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\{127D0AD-4FF2-11D1-8608-00C04Fc295EE}\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\S939f588-fdf8-4bc9-b81-4aad19f5639	
C:\windows\5ystem32\LogFiles\5cm\5b184694-64c3-4633-94c5-945b3fa561d6	
C:\windows\System32\LogFiles\Scm\9b75c702-ea13-406a-badb-6c588ee4375b	
C:\windows\System32\LogFiles\Scm\alcfa52f-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\5ystem32\cogFiles\5cm\debae53-2809-4f75-85ef-427d364b9b2c	
C:\windows\System32\LogFiles\Scm\f1369a11-e983-4458-b390-712efalcba44	
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	
Figure 18: Files Modified short paths	

#### g

C:\Windows\System32\wbem\Repository\MAPPING1.MAP
C:\windows\\$ystem32\wbem\Repositor\MAPPING2.MAP
C:\windows\\$ystem32\wben\Reportor\00BJECTS.DATA
C (\windows\\$ystem32\winevtLogs\Application.evtx
C:\windows\system32\winevtLogs\mirrosoft-Windows-BranchCache5MB%40perational.evtx
C:\windows\system32\winevt\Logs\microsoft+Windows-bianciachesmbooperational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%40perational.evtx
C:/windows/System32/winevt/Logs/Microsoft-Windows-GroupPolicy%40perational.evtx
C#\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%40perational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders API Service.evtx
C:\windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%40perational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-OfflineFiles%40perational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%40perational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Detector%40perational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%40perational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Service%40perational.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%40perational.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%40perational.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\lasks\schebde.int

#### 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.

Image: synchost exe       < 0.01       8,280 K       9,416 K       1192 Host Process for Windows S Microsoft Corporation Microsoft Corporation         Image: synchost exe       5,548 K       10,036 K       1304 Spooler Sub System App Microsoft Corporation         Image: synchost exe       8,820 K       10,360 K       1340 Host Process for Windows S Microsoft Corporation         Image: synchost exe       1,200 K       5,088 K       1440         Image: synchost exe       0.72       976 K       3,388 K       3268         Image: synchost exe       0.72       976 K       3,388 K       3268         Image: synchost exe       0.72       976 K       13,200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: synchost exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: synchost exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: synchese       0.01       1,336 K       4,148 K       3636 Microsoft Windows Search P Microsoft Corporation         Image: synchese       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Image: synchese       0.03       2,440 K       6,120 K       2172 Microsoft	Image: synchost exe       < 0.01       8,280 K       9,416 K       1192 Host Process for Windows S Microsoft Corporation Microsoft Corporation Synchost exe         Image: synchost exe       5,548 K       10,036 K       1304 Spooler SubSystem App Microsoft Corporation Microsoft Corporation         Image: synchost exe       8,820 K       10,360 K       1340 Host Process for Windows S Microsoft Corporation         Image: synchost exe       1,200 K       5,088 K       1440         Image: synchost exe       0.72       976 K       3,388 K       3268         Image: synchost exe       0.72       976 K       3,388 K       1536 Host Process for Windows T Microsoft Corporation         Image: synchost exe       0.72       976 K       3,388 K       1536 Host Process for Windows T Microsoft Corporation         Image: synchost exe       0.72       976 K       3,388 K       1536 Host Process for Windows T Microsoft Corporation         Image: synchost exe       0.04       8,352 K       13,200 K       2032 VMware Tools Core Service       VMware. Inc.         Image: synchost exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: synchese       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Image: synchexe		XA	W Law				Δ
Image: spoolsv.exe       5,548 K       10,036 K       1304 Spooler Sub System App       Microsoft Corporation         Image: sychost.exe       8,820 K       10,360 K       1340 Host Process for Windows S Microsoft Corporation         Image: sychost.exe       1,200 K       5,088 K       1440         Image: sychost.exe       0.72       9.76 K       3,388 K       3268         Image: sychost.exe       0.72       9.76 K       13,200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: sychost.exe       0.16       16,708 K       9.540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: sychost.exe       0.16       16,708 K       9.540 K       1400 Microsoft Windows Search P Microsoft Corporation         Image: sychost.exe       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Image: sychost.exe       0.03       2,440 K       6,120 K <th>Spoolsv.exe       5,548 K       10,036 K       1304 Spooler SubSystem App       Microsoft Corporation         Svchost.exe       8.820 K       10,360 K       1340 Host Process for Windows S       Microsoft Corporation         sample1 exe       1,200 K       5,088 K       1440         dccon.exe       0.72       976 K       3,388 K       3268         taskhost.exe       2,412 K       5,816 K       1536 Host Process for Windows T       Microsoft Corporation         wntoolsd.exe       0.04       8,352 K       13,200 K       2032 V/Mware Tools Core Service       V/Wware, Inc.         SearchIndexer.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search L       Microsoft Corporation         SearchIndexer.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search P       Microsoft Corporation         SearchFilterHost.exe       932 K       3,400 K       3660       Microsoft Corporation         SearchFilterHost.exe       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Microsoft Corporation       2,440 K       6,120 K       2172 Microsoft Distributed Transa       Microsoft Corporation         spspsvc.exe       2,092 K       7,460 K       2788 Microsoft Software Protec</th> <th>Process</th> <th>CPU</th> <th>Private Bytes</th> <th>Working Set</th> <th>PID Description</th> <th>Company Name</th> <th></th>	Spoolsv.exe       5,548 K       10,036 K       1304 Spooler SubSystem App       Microsoft Corporation         Svchost.exe       8.820 K       10,360 K       1340 Host Process for Windows S       Microsoft Corporation         sample1 exe       1,200 K       5,088 K       1440         dccon.exe       0.72       976 K       3,388 K       3268         taskhost.exe       2,412 K       5,816 K       1536 Host Process for Windows T       Microsoft Corporation         wntoolsd.exe       0.04       8,352 K       13,200 K       2032 V/Mware Tools Core Service       V/Wware, Inc.         SearchIndexer.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search L       Microsoft Corporation         SearchIndexer.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search P       Microsoft Corporation         SearchFilterHost.exe       932 K       3,400 K       3660       Microsoft Corporation         SearchFilterHost.exe       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Microsoft Corporation       2,440 K       6,120 K       2172 Microsoft Distributed Transa       Microsoft Corporation         spspsvc.exe       2,092 K       7,460 K       2788 Microsoft Software Protec	Process	CPU	Private Bytes	Working Set	PID Description	Company Name	
Image: Synchost exe       8,820 K       10,360 K       1340 Host Process for Windows S Microsoft Corporation         Image: Sample Lexe       1,200 K       5,088 K       1440         Image: Conserve       0.72       976 K       3,388 K       3268         Image: Conserve       0.74       8,357 K       13,200 K       2032 V/Mware Tools Core Service       VMware, Inc.         Image: Conserve       0.16       16,708 K       9,504 K       1400 Microsoft Windows Search I       Microsoft Corporation         Image: Search Indexer exe       0.16       16,708 K       9,504 K       3660       Microsoft Corporation         Image: Search FilterHost exe       932 K       3,400 K       3660       Microsoft Corporation         Image: Microsoft Corporation       932 K       3,400 K       2172 Microsoft Distributed Transa       Microsoft Corporation         Image: Microsoft Corporation       2,440 K       6,120 K       2172 Microsoft Softwa	Image: Synchost exe       8.820 K       10.360 K       1340 Host Process for Windows S Microsoft Corporation         Image: Sample Lexe       1.200 K       5,088 K       1440         Image: Conserve       0.72       976 K       3,388 K       3268         Image: Conserve       2.412 K       5,816 K       1526       Microsoft Corporation         Image: Conserve       0.04       8,325 K       13,200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: SearchIndexer.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: SearchProtocolHost.e       <0.01	svchost.exe	< 0.01	8,280 K	9,416 K	1192 Host Process for Windows S.	. Microsoft Corporation	
Image: Sample 1.exe       1,200 K       5,088 K       1440         Image: Sample 1.exe       0.72       976 K       3,388 K       3268         Image: Sample 1.exe       0.72       976 K       3,388 K       3268         Image: Sample 1.exe       0.72       976 K       3,388 K       3268         Image: Sample 1.exe       0.48       5.816 K       1536 Host Process for Windows T Microsoft Corporation         Image: Sample 1.exe       0.04       8,352 K       13,200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: Sample 1.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: Sample 1.exe       0.01       1,336 K       4,148 K       3636 Microsoft Windows Search P Microsoft Corporation         Image: Sample 1.exe       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Image: Sample 1.exe       0.03       2,440 K       6,120 K       2172 Microsoft Distributed Transa Microsoft Corporation         Image: spsvc.exe       2,022 K       7,460 K       2788 Microsoft Software Protectio Microsoft Corporation	Image: Sample 1.exe       1.200 K       5,088 K       1440         Image: Sample 1.exe       0.72       976 K       3,388 K       3268         Image: Sample 1.exe       0.72       976 K       3,388 K       3268         Image: Sample 1.exe       0.72       976 K       3,388 K       3268         Image: Sample 1.exe       0.04       8,352 K       13,200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: Sample 1.exe       0.04       8,352 K       13,200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: Sample 1.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search 1       Microsoft Corporation         Image: Sample 1.exe       0.01       1,336 K       4,148 K       3636 Microsoft Windows Search P       Microsoft Corporation         Image: Sample 1.exe       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Image: Sample 1.exe       0.03       2,440 K       6,120 K       2172 Microsoft Distributed Transa       Microsoft Corporation         Image: Sample 2.exe       0.03       2,440 K       6,120 K       2788 Microsoft Software Protectio       Microsoft Corporation         Image: spsyc.exe       2,022 K       7,460 K	spoolsv.exe		5,548 K	10,036 K	1304 Spooler SubSystem App	Microsoft Corporation	
Indexent exe       0.72       976 K       3,388 K       3268         Intersect exe       2,412 K       5,816 K       1536 Host Process for Windows T Microsoft Corporation         Intersect exe       0.04       8,352 K       13,200 K       2022 VMware Tools Core Service       VMware, Inc.         Intersect exe       0.04       8,352 K       13,200 K       2022 VMware Tools Core Service       VMware, Inc.         Intersect exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I Microsoft Corporation         Intersect exe       0.01       1,336 K       4,148 K       3636 Microsoft Windows Search P Microsoft Corporation         Intersect exe       932 K       3,400 K       3660       Microsoft Corporation         Intersect exe       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Intersect exe       0.03       2,440 K       6,120 K       2172 Microsoft Distributed Transa Microsoft Corporation         Intersect exe       2,040 K       6,40 K       2788 Microsoft Software Protectio Microsoft Corporation	Indexent       0.72       976 K       3,388 K       3268         Intersection       2,412 K       5,816 K       1536 Host Process for Windows T Microsoft Corporation         Intersection       0.04       8,352 K       13,200 K       2032 VMware Tools Core Service       VMware, Inc.         Intersection       0.04       8,352 K       13,200 K       2032 VMware Tools Core Service       VMware, Inc.         Intersection       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I       Microsoft Corporation         Intersection       0.01       1,336 K       4,148 K       3636 Microsoft Windows Search P       Microsoft Corporation         Intersection       932 K       3,400 K       3660       676 COM Surrogate       Microsoft Corporation         Intersection       0.02       3,068 K       8,576 K       676 COM Surrogate       Microsoft Corporation         Intersection       0.03       2,440 K       6,120 K       2172 Microsoft Distributed Transa       Microsoft Corporation         Intersection       2,998 vc.exe       2,068 K       6,120 K       2788 Microsoft Software Protectio       Microsoft Corporation	svchost.exe		8,820 K	10,360 K	1340 Host Process for Windows S.	. Microsoft Corporation	
Itaskhost.exe       2.412 K       5.816 K       1536 Host Process for Windows T Microsoft Corporation         Image: SearchIndexer.exe       0.04       8.352 K       13.200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: SearchIndexer.exe       0.16       16.708 K       9.540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: SearchFiterHost.exe       0.16       16.708 K       9.540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: SearchFiterHost.exe       0.16       16.708 K       9.540 K       3636 Microsoft Windows Search P Microsoft Corporation         Image: SearchFiterHost.exe       0.02       3.068 K       8.576 K       676 COM Surrogate       Microsoft Corporation         Image: SearchFiterHost.exe       0.03       2.440 K       6.120 K       2172 Microsoft Distributed Transa Microsoft Corporation         Image: SearchFiterHost.exe       0.03       2.440 K       6.120 K       2172 Microsoft Distributed Transa Microsoft Corporation         Image: SearchFiterHost.exe       0.03       2.440 K       6.120 K       2172 Microsoft Software Protectio Microsoft Corporation         Image: SearchFiterHost.exe       0.03       2.440 K       6.120 K       2788 Microsoft Software Protectio Microsoft Corporation	Itaskhost.exe       2.412 K       5.816 K       1536 Host Process for Windows T Microsoft Corporation         Image: Windows exe       0.04       8.352 K       13.200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: Windows exe       0.16       16.708 K       9.540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: Windows exe       0.16       16.708 K       9.540 K       1400 Microsoft Windows Search P Microsoft Corporation         Image: Windows exe       0.01       1.336 K       4.148 K       3636 Microsoft Windows Search P Microsoft Corporation         Image: Windows exe       0.02       3.068 K       8.576 K       676 COM Surrogate       Microsoft Corporation         Image: Windows exe       0.03       2.440 K       6.120 K       2172 Microsoft Distributed Transa Microsoft Corporation         Image: Windows exe       0.03       2.440 K       6.120 K       2788 Microsoft Software Protectio Microsoft Corporation         Image: Windows exe       2.092 K       7.460 K       2788 Microsoft Software Protectio Microsoft Corporation	🖃 💼 sample 1.exe	-	1,200 K	5,088 K	1440		
Image: Without State       0.04       8.352 K       13.200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: SearchIndexer.exe       0.16       16.708 K       9.540 K       1400 Microsoft Windows Search I       Microsoft Corporation         Image: SearchIndexer.exe       0.16       16.708 K       9.540 K       1400 Microsoft Windows Search I       Microsoft Corporation         Image: Search ProtocolHost.e       932 K       3.400 K       3660       Microsoft Corporation         Image: Search FilterHost.exe       0.02       3.068 K       8.576 K       676 COM Surrogate       Microsoft Corporation         Image: matc.exe       0.03       2.440 K       6.120 K       2172 Microsoft Distributed Transa       Microsoft Corporation         Image: spsysc.exe       2.092 K       7.460 K       2788 Microsoft Software Protectio       Microsoft Corporation	Image: Without Service       0.04       8.352 K       13.200 K       2032 VMware Tools Core Service       VMware, Inc.         Image: SearchIndexer.exe       0.16       16.708 K       9.540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: SearchIndexer.exe       0.16       16.708 K       9.540 K       1400 Microsoft Windows Search I Microsoft Corporation         Image: SearchIndexer.exe       0.01       1.336 K       4.148 K       3636 Microsoft Windows Search P Microsoft Corporation         Image: SearchIndexer.exe       0.02       3.068 K       8.576 K       676 COM Surrogate       Microsoft Corporation         Image: Mitcle.exe       0.03       2.440 K       6.120 K       2172 Microsoft Distributed Transa Microsoft Corporation         Image: spsysc.exe       2.092 K       7.460 K       2788 Microsoft Software Protectio Microsoft Corporation	dccon.exe	0.72	100 million (100 m	3,388 K	3268		
SearchIndexer.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I Microsoft Corporation         SearchProtocolHost.e       < 0.01	SearchIndexer.exe       0.16       16,708 K       9,540 K       1400 Microsoft Windows Search I Microsoft Corporation         SearchProtocolHost.e       < 0.01							
Image: Search ProtocolHost.e       < 0.01	Search ProtocolHost.e         < 0.01         1.336 K         4.148 K         3636 Microsoft Windows Search P Microsoft Corporation           Search FilterHost.exe         932 K         3.400 K         3660         Microsoft Corporation           Image: Microsoft Corporation         932 K         3.400 K         3660         Microsoft Corporation           Image: Microsoft Corporation         932 K         3.68 K         8.576 K         676 COM Surrogate         Microsoft Corporation           Image: Microsoft Corporation         2.440 K         6.120 K         2172 Microsoft Distributed Transa Microsoft Corporation           Image: Spsyc.exe         2.024 K         7.460 K         2788 Microsoft Software Protectio Microsoft Corporation							
Search FilterHost.exe         932 K         3,400 K         3660           Idlihost.exe         0.02         3,068 K         8,576 K         676 COM Surrogate         Microsoft Corporation           Image: Spread with the search of t	Search FilterHost.exe         932 K         3,400 K         3660           Idlinost.exe         0.02         3,068 K         8,576 K         676 COM Surrogate         Microsoft Corporation           Image: Spread with the search of t	SearchIndexer.exe	0.16	16,708 K	9,540 K	1400 Microsoft Windows Search I	Microsoft Corporation	
Oldhost.exe     O.02     O.03     O.03     O.03     O.03     O.04     O.03     O.04     O.05	OL2     O	hanned in the second se	< 0.01			3636 Microsoft Windows Search P.	Microsoft Corporation	
Image: Construction         0.03         2.440 K         6.120 K         2172 Microsoft Distributed Transa Microsoft Corporation           Image: Sppsyc.exe         2.092 K         7.460 K         2788 Microsoft Software Protectio Microsoft Corporation	Image: Construction of the system         0.03         2.440 K         6.120 K         2172 Microsoft Distributed Transa Microsoft Corporation           Image: Sppsyc.exe         2.092 K         7.460 K         2788 Microsoft Software Protectio Microsoft Corporation	SearchFilterHost.exe		932 K				
sppsvc.exe 2,092 K 7,460 K 2788 Microsoft Software Protectio Microsoft Corporation	sppsvc.exe     2.092 K     7.460 K     2788 Microsoft Software Protectio Microsoft Corporation			2 000 1/	8 576 K	676 COM Sumonate	Microsoft Corporation	
				10000	0.2200000000000000000000000000000000000			
Name Name	Name Name	ansdtc.exe		2,440 K	6,120 K	2172 Microsoft Distributed Transa	Microsoft Corporation	
		spsvc.exe		2,440 K	6,120 K	2172 Microsoft Distributed Transa	Microsoft Corporation	
		sppsvc.exe		2,440 K	6,120 K	2172 Microsoft Distributed Transa	Microsoft Corporation	
		sppsvc.exe		2,440 K	6,120 K	2172 Microsoft Distributed Transa	Microsoft Corporation	
		msdtc.exe		2,440 K	6,120 K	2172 Microsoft Distributed Transa	Microsoft Corporation	

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.