

SecurityScorecard Expands from Security Ratings to Supply Chain Detection and Response

[Learn More](#)



[Close](#) X

Resources ▶ A Deep Dive Into ALPHV/BlackCat Ransomware



RESEARCH

# A Deep Dive Into ALPHV/BlackCat Ransomware

Share



## Executive summary

ALPHV/BlackCat is the first widely known ransomware written in Rust. The malware must run with an access token consisting of a 32-byte value (-access-token parameter), and other parameters can be specified. The ransomware comes with an encrypted configuration that contains a list of services/processes to be stopped, a list of whitelisted directories/files/file extensions, and a list of stolen credentials from the victim environment. It deletes all Volume Shadow Copies, performs privilege escalation using the CMSTPLUA COM interface, and enables “remote to local” and “remote to remote” symbolic links on the victim’s machine.

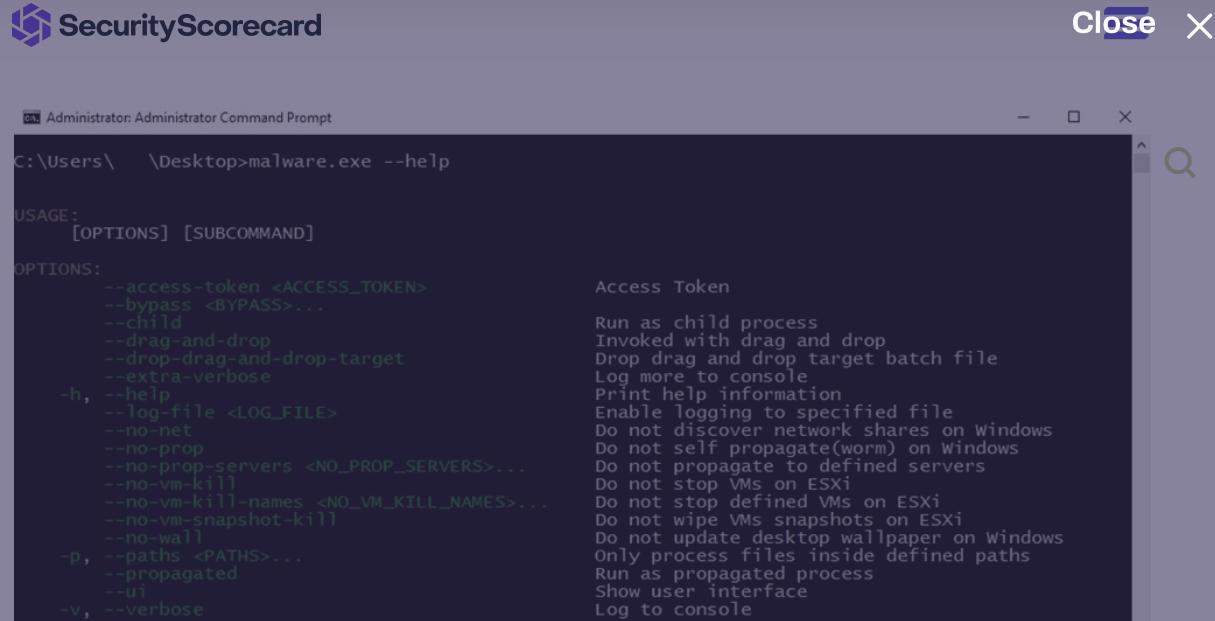
### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Use necessary  
cookies only

Allow selection

Allow all cookies



The screenshot shows a Windows Command Prompt window titled "Administrator: Administrator Command Prompt". The command entered is "C:\Users\...\Desktop>malware.exe --help". The output displays the usage information and a detailed list of options. A tooltip is visible over the "--access-token" option, providing its definition: "Run as child process Invoked with drag and drop Drop drag and drop target batch file Log more to console Print help information Enable logging to specified file Do not discover network shares on Windows Do not self propagate(worm) on Windows Do not propagate to defined servers Do not stop VMs on ESXi Do not stop defined VMs on ESXi Do not wipe VMs snapshots on ESXi Do not update desktop wallpaper on Windows Only process files inside defined paths Run as propagated process Show user interface Log to console".

```
C:\Users\...\Desktop>malware.exe --help

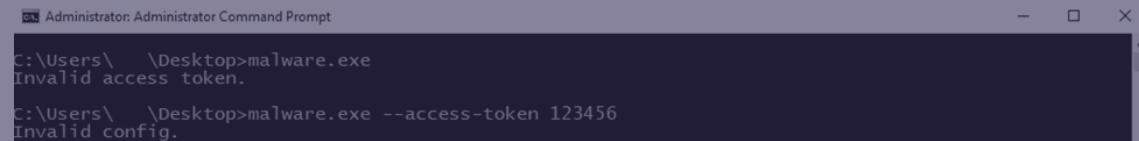
USAGE:
[OPTIONS] [SUBCOMMAND]

OPTIONS:
--access-token <ACCESS_TOKEN>
--bypass <BYPASS>...
--child
--drag-and-drop
--drop-drag-and-drop-target
--extra-verbose
-h, --help
--log-file <LOG_FILE>
--no-net
--no-prop
--no-prop-servers <NO_PROP_SERVERS>...
--no-vm-kill
--no-vm-kill-names <NO_VM_KILL_NAMES>...
--no-vm-snapshot-kill
--no-wall
-p, --paths <PATHS>...
--propagated
--ui
-v, --verbose

Access Token
Run as child process
Invoked with drag and drop
Drop drag and drop target batch file
Log more to console
Print help information
Enable logging to specified file
Do not discover network shares on Windows
Do not self propagate(worm) on Windows
Do not propagate to defined servers
Do not stop VMs on ESXi
Do not stop defined VMs on ESXi
Do not wipe VMs snapshots on ESXi
Do not update desktop wallpaper on Windows
Only process files inside defined paths
Run as propagated process
Show user interface
Log to console
```

Figure 1

Whether the ransomware is running with no parameters or with an invalid access token, an error message is displayed:



The screenshot shows two lines of a Windows Command Prompt window. The first line is "C:\Users\...\Desktop>malware.exe" followed by the error message "Invalid access token.". The second line is "C:\Users\...\Desktop>malware.exe --access-token 123456" followed by the error message "Invalid config.".

```
C:\Users\...\Desktop>malware.exe
Invalid access token.

C:\Users\...\Desktop>malware.exe --access-token 123456
Invalid config.
```

Figure 2

By performing the dynamic analysis, we've found that the access token must be a 32-byte value that is not unique.

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 4

The executable retrieves the command-line string for the process using the GetCommandLineW function:

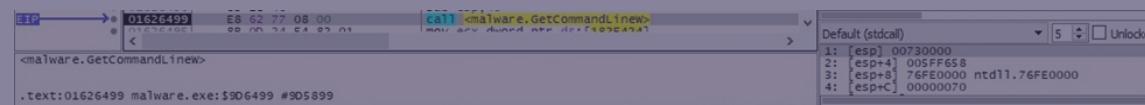
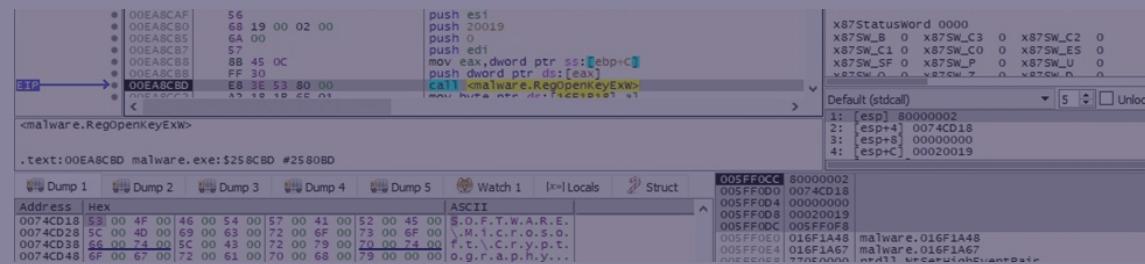


Figure 5

BlackCat opens the "SOFTWARE\Microsoft\Cryptography" registry key by calling the RegOpenKeyExW routine (0x80000002 = HKEY\_LOCAL\_MACHINE, 0x20019 = KEY\_READ):



#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

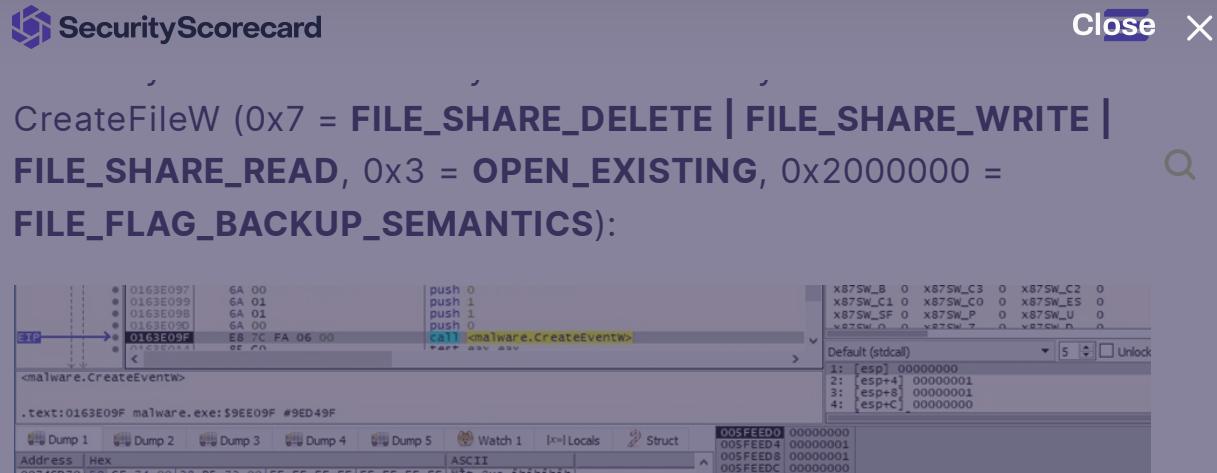


Figure 8

The executable generates 16 random bytes by calling the BCryptGenRandom API (0x2 = BCRYPT\_USE\_SYSTEM\_PREFERRED\_RNG):

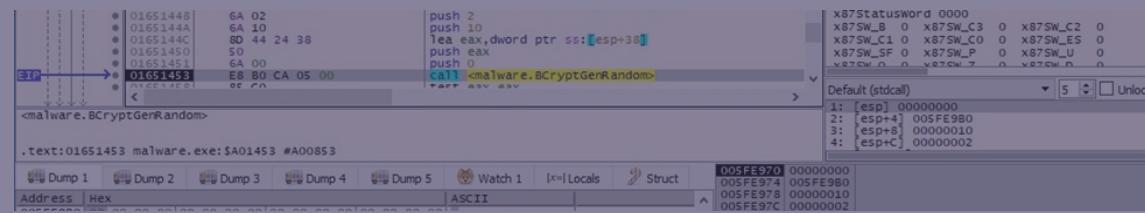


Figure 9

A named pipe whose name contains the current process ID and random bytes generated above is created using

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

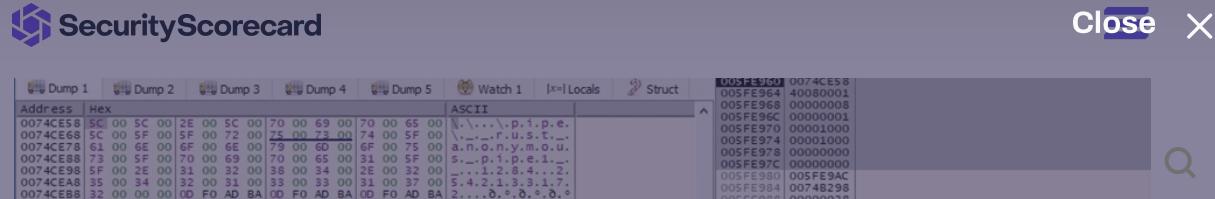


Figure 10

The process opens the named pipe for writing using the CreateFileW routine (0x40000000 = **GENERIC\_WRITE**, 0x3 = **OPEN\_EXISTING**):

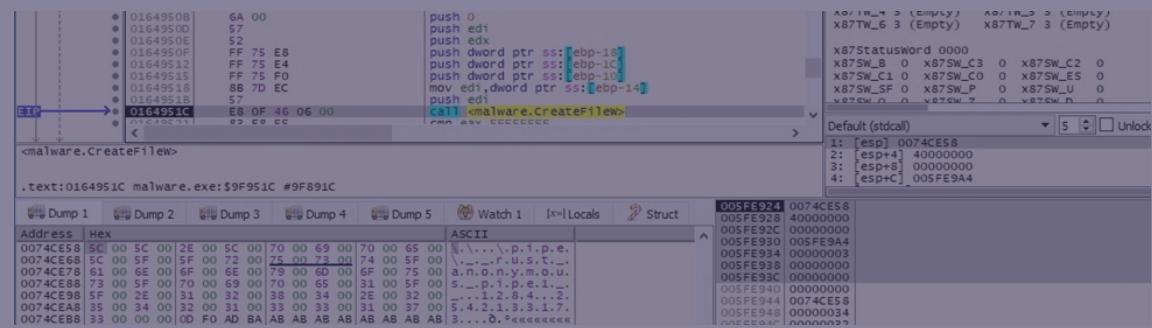


Figure 11

The ransomware creates a read and a write named pipe, respectively.

The wmic process is used to extract the UUID (0x08000400 = **CREATE\_NO\_WINDOW** | **CREATE\_UNICODE\_ENVIRONMENT**):

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

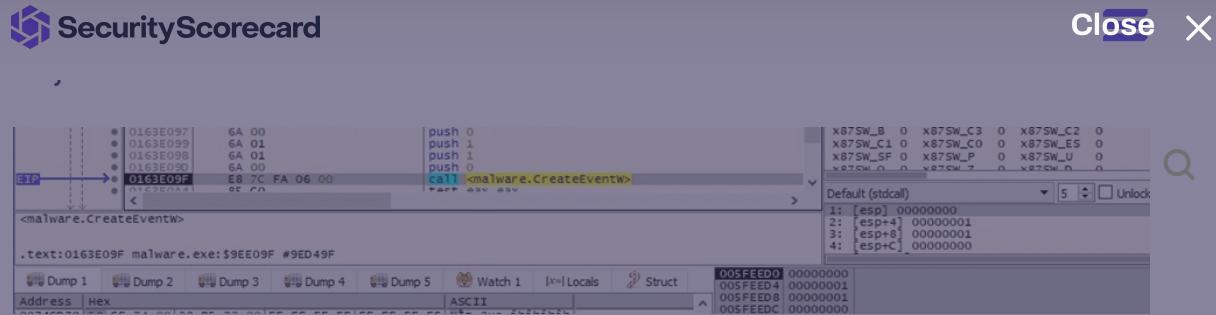


Figure 13

The binary waits until the event objects are in the signaled state by calling WaitForMultipleObjects:

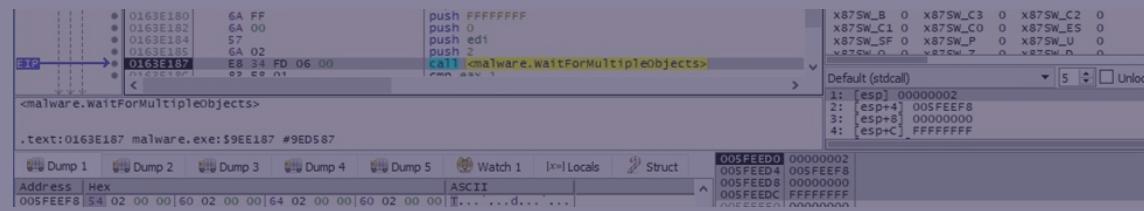
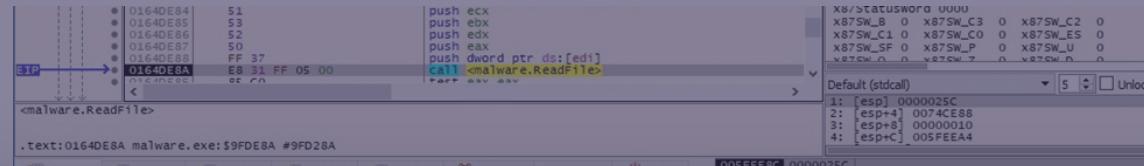


Figure 14

The output of the above process is read from the named pipe using the ReadFile routine:



This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

The screenshot shows a hex editor interface with two panes. The left pane displays memory addresses from 005FF4BC to 005FF4CC, their corresponding hex values, and ASCII text. The right pane shows memory addresses from 005FF3C8 to 005FF3D0, their hex values, and ASCII text. The ASCII text includes parts of the ransom note and instructions for recovering files.

Figure 16

The content of the ransom note and the text that will appear on the Desktop Wallpaper are decrypted by the ransomware:

Address	Hex	ASCII
0074CF48	3E 20 57 68 61 74 20 68 61 70 70 65 6E 65 64	>> What happened
0074CF58	3F 0A 0A 49 6D 70 6F 72 74 61 6E 74 20 66 69 6C	?..Important fil
0074CF68	65 73 20 6F 6E 20 79 6F 75 72 20 6E 65 74 77 6F	es on your netwo
0074CF78	72 6B 20 77 61 73 20 45 4E 43 52 59 50 54 45 44	rk was ENCRYPTED
0074CF88	20 61 6E 64 20 6E 6F 77 20 74 68 65 79 20 68 61	and now they ha
0074CF98	76 65 20 22 75 68 77 75 76 7A 75 22 20 65 78 74	ve "uhwuvzu" ext
0074CFA8	65 6E 73 69 6F 6E 2E 0A 49 6E 20 6F 72 64 65 72	ension..In order
0074CFB8	20 74 6F 20 72 65 63 6F 76 65 72 20 79 6F 75 72	to recover your
0074FCFC8	20 66 69 6C 65 73 20 79 6F 75 20 6E 65 65 64 20	files you need
0074CFD8	74 6F 20 66 6F 6C 6C 6F 77 20 69 6E 73 74 72 75	to follow instru
0074CFE8	63 74 69 6F 6E 73 20 62 65 6C 6F 77 2E 0A 0A 3E	ctions below...>
0074CFF8	3E 20 53 65 6E 73 69 74 69 76 65 20 44 61 74 61	> Sensitive Data
0074D008	0A 0A 53 65 6E 73 69 74 69 76 65 20 64 61 74 61	..Sensitive data
0074D018	20 6F 6E 20 79 6F 75 72 20 6E 65 74 77 6F 72 6B	on your network
0074D028	20 77 61 73 20 44 4F 57 4E 4C 4F 41 44 45 44 2E	was DOWNLOADED.
0074D038	0A 49 66 20 79 6F 75 20 44 4F 4E 27 54 20 57 41	.If you DON'T WA
0074D048	4E 54 20 79 6F 75 72 20 73 65 6E 73 69 74 69 76	NT your sensitiv
0074D058	65 20 64 61 74 61 20 74 6F 20 62 65 20 50 55 42	e data to be PUB
0074D068	4C 49 53 48 45 44 20 79 6F 75 20 68 61 76 65 20	LISHED you have

Figure 17

Address	Hex	ASCII
0074AA98	49 6D 70 6F 72 74 61 6E 74 20 66 69 6C 65 73 20	Important files
0074AAA8	6F 6E 20 79 6F 75 72 20 6E 65 74 77 6F 72 6B 20	on your network
0074AAB8	77 61 73 20 44 4F 57 4E 4C 4F 41 44 45 44 20 61	was DOWNLOADED a
0074AAC8	6E 64 20 45 4E 43 52 59 50 54 45 44 2E 0A 53 65	nd ENCRYPTED..Se
0074AAD8	65 20 22 52 45 43 4F 56 45 52 2D 75 68 77 75 76	e "RECOVER-uhwuv
0074AAE8	7A 75 2D 15 19 16 15 53 35 71 72 71 33 30 66 69	zhu FILES.TEX" fi

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 20

The process opens the access token associated with the current process (0x80000000 = **GENERIC\_READ**):

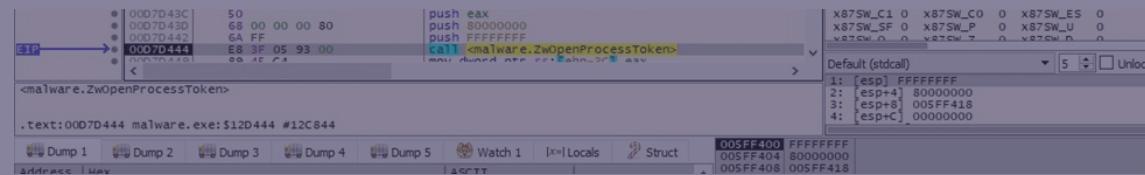
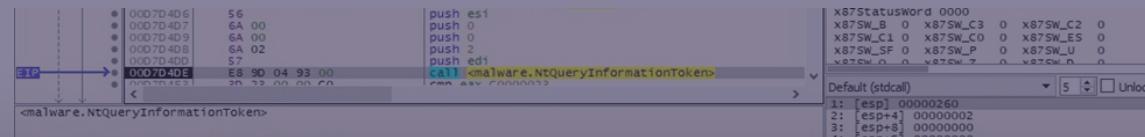


Figure 21

BlackCat extracts a TOKEN\_GROUPS structure containing the group accounts associated with the above token using the NtQueryInformationToken function (0x2 = **TokenGroups**):



#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 23

The malicious binary retrieves a pointer to a PEB structure using the ZwQueryInformationProcess routine (0x0 = ProcessBasicInformation):

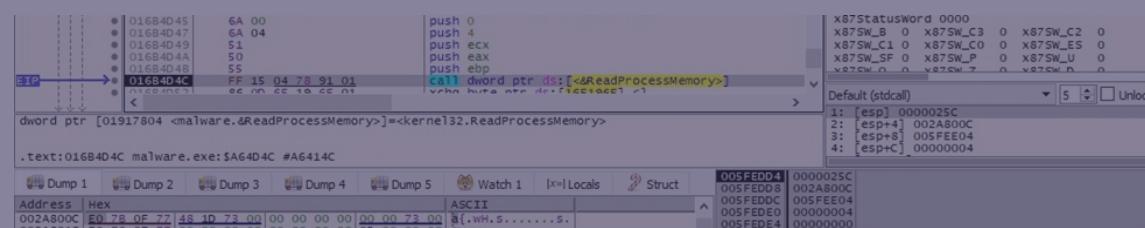
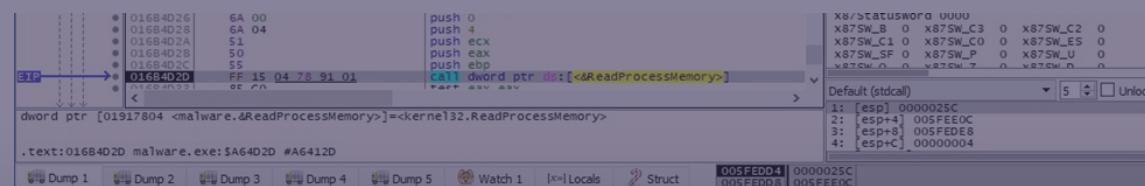


Figure 24

The executable retrieves a pointer to a PEB\_LDR\_DATA structure containing information about the loaded modules in the process and then to the head of a doubly linked list that contains the loaded modules:



#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

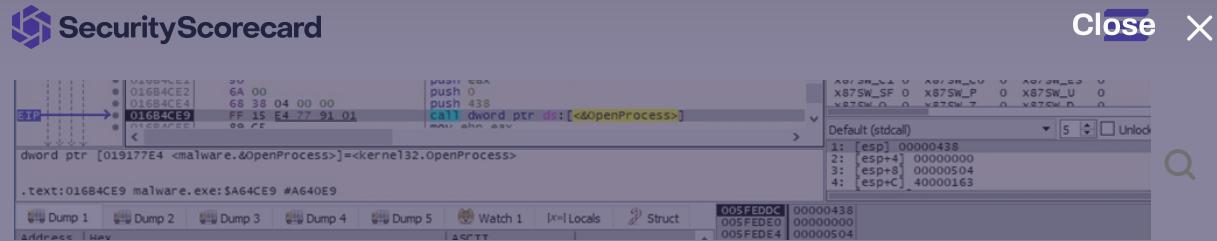


Figure 27

## Privilege escalation via UAC bypass using CMSTPLUA COM interface

The ransomware initializes the COM library for use by the current thread via a call to CoInitializeEx (0x2 = COINIT\_APARTMENTTHREADED):

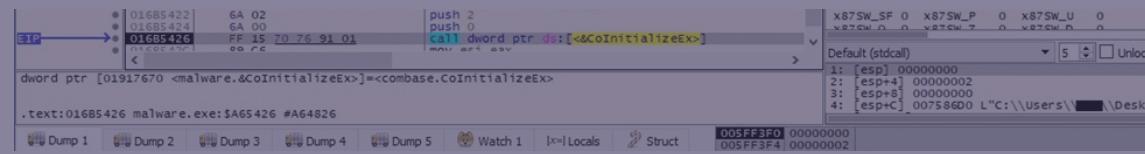


Figure 28

BlackCat ransomware uses the auto-elevated CMSTPLUA interface **{3E5FC7F9-9A51-4367-9063-A120244FBEC7}** in order to escalate privileges:

### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

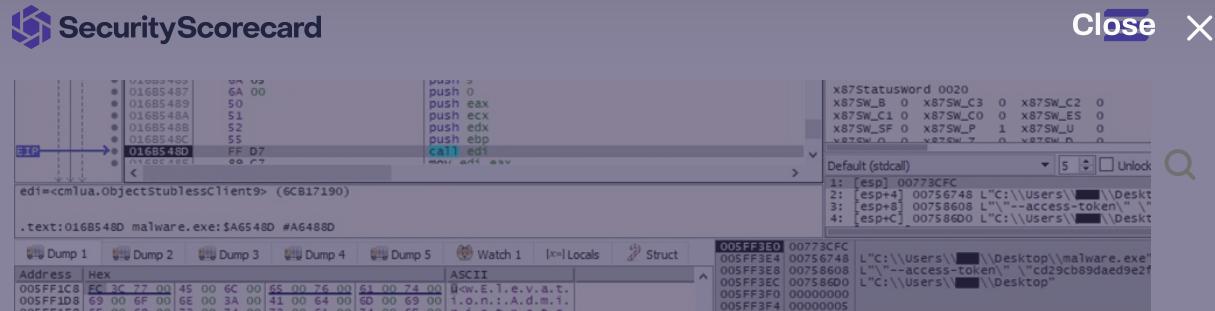


Figure 30

The `LookupPrivilegeValueW` routine is utilized to retrieve the locally unique identifier that represents the following privileges:

- `SeIncreaseQuotaPrivilege` `SeSecurityPrivilege`  
`SeTakeOwnershipPrivilege`
- `SeLoadDriverPrivilege` `SeSystemProfilePrivilege`  
`SeSystemtimePrivilege`
- `SeProfileSingleProcessPrivilege` `SeIncreaseBasePriorityPrivilege`
- `SeCreatePagefilePrivilege` `SeBackupPrivilege` `SeRestorePrivilege`
- `SeShutdownPrivilege` `SeDebugPrivilege`  
`SeSystemEnvironmentPrivilege`
- `SeChangeNotifyPrivilege` `SeRemoteShutdownPrivilege`  
`SeUndockPrivilege`
- `SeManageVolumePrivilege` `SeChangeObjectPrivilege`

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Close X



Figure 31

All the above privileges are enabled in the access token using AdjustTokenPrivileges:

The screenshot shows the assembly view of the malware's code. The instruction at address 0007E313 is a call to the Windows API function `malware.AdjustTokenPrivileges`. The assembly code includes pushes for parameters like the access token and privilege values. The debugger interface shows registers, memory dump tabs, and a watch window.

Figure 32

The binary creates the following processes that enable “remote to local” and “remote to remote” symbolic links on the local machine:

The screenshot shows the assembly view of the malware's code. The instruction at address 01650980 is a call to the Windows API function `malware.CreateProcessW`. The assembly code includes pushes for parameters like the command line and process creation flags. The debugger interface shows registers, memory dump tabs, and a watch window.

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 34  
The malware tries to stop the Internet Information service (IIS) using IISReset.exe:

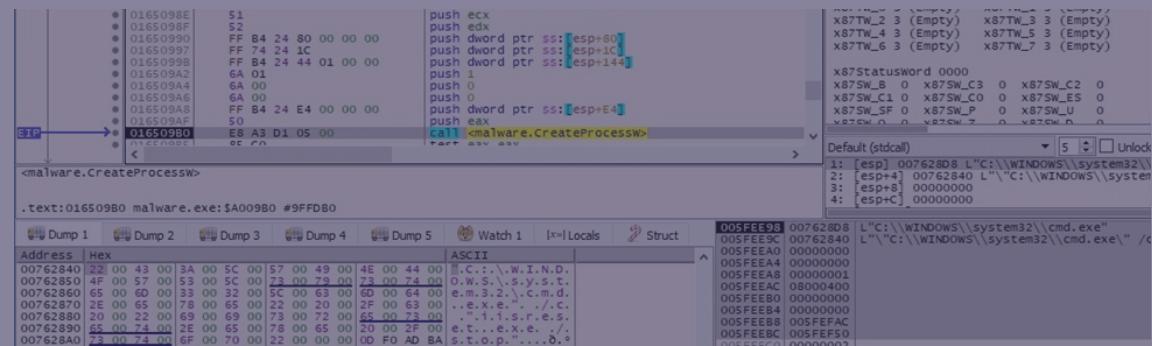
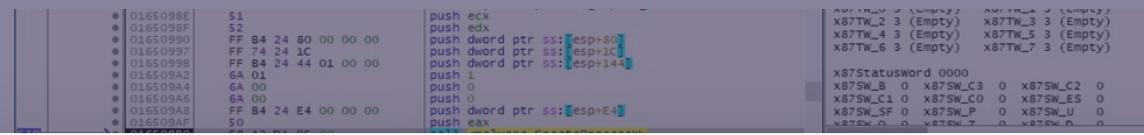
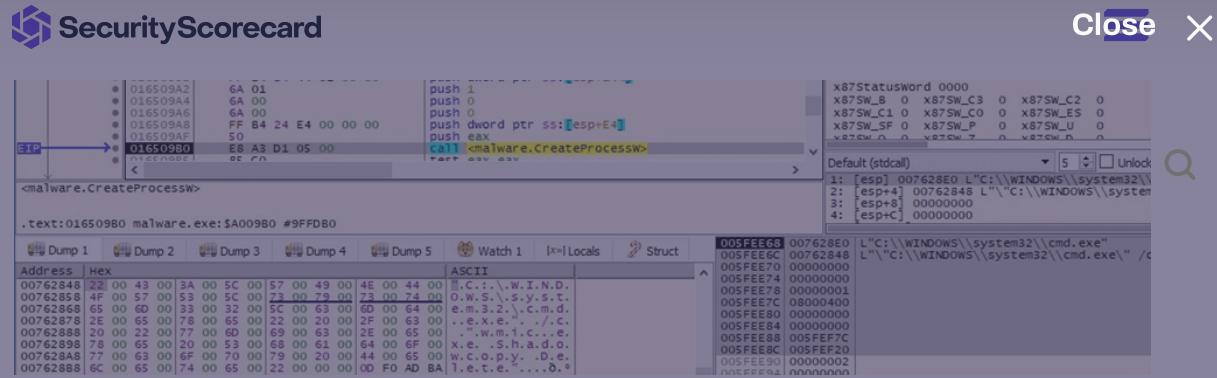


Figure 35  
The ransomware deletes all volume shadow copies using the vssadmin.exe utility:



#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



The screenshot shows the SecurityScorecard debugger interface. The assembly pane displays the following code:

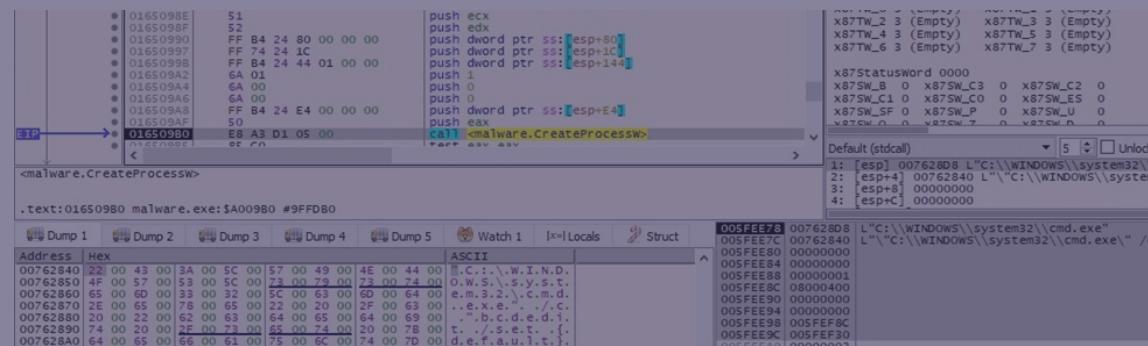
```
push 1
push 0
push 0
push 0
push dword ptr ss:[esp+E4]
push eax
call malware.createProcessW
```

The memory dump pane shows the command being sent to the malware process:

```
L"C:\Windows\system32\cmd.exe" /c
```

Figure 37

Interestingly, the malware runs the following command that is incomplete and returns an error:



The screenshot shows the SecurityScorecard debugger interface. The assembly pane displays the following code:

```
push ecx
push edx
push dword ptr ss:[esp+80]
push dword ptr ss:[esp+IC]
push dword ptr ss:[esp+144]
push 0
push 0
push 0
push eax
call malware.createProcessW
```

The memory dump pane shows the command being sent to the malware process:

```
L"C:\Windows\system32\cmd.exe" /c
```

Figure 38

Address	Hex	ASCII
00762860	54 68 65 20 73 65 74 20 63 6F 6D 6D 61 6E 64 20	The set command

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 40

The ransomware tries to clear all event logs, however, the command is incorrect and returns an error, as highlighted below:

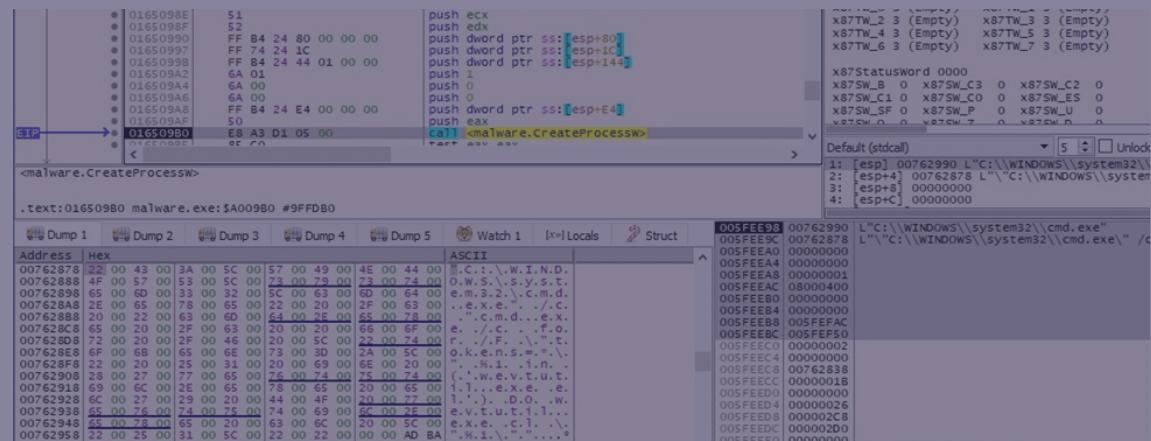


Figure 41

Address	Hex	ASCII
007628B8	15 37 D0 18 DB 28 00 18 5C 22 74 6F 6B 65 6E 73	.7D.0(..\"tokens
007628C8	3D 2A 5C 22 20 77 61 73 20 75 6E 65 78 70 65 63	="\\" was unexpect
007628D8	74 65 64 20 61 74 20 74 68 69 73 20 74 69 6D 65	ed at this time
007628E8	2E 0D 0A BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA	...".\0.\0.\0.\0.\0.

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

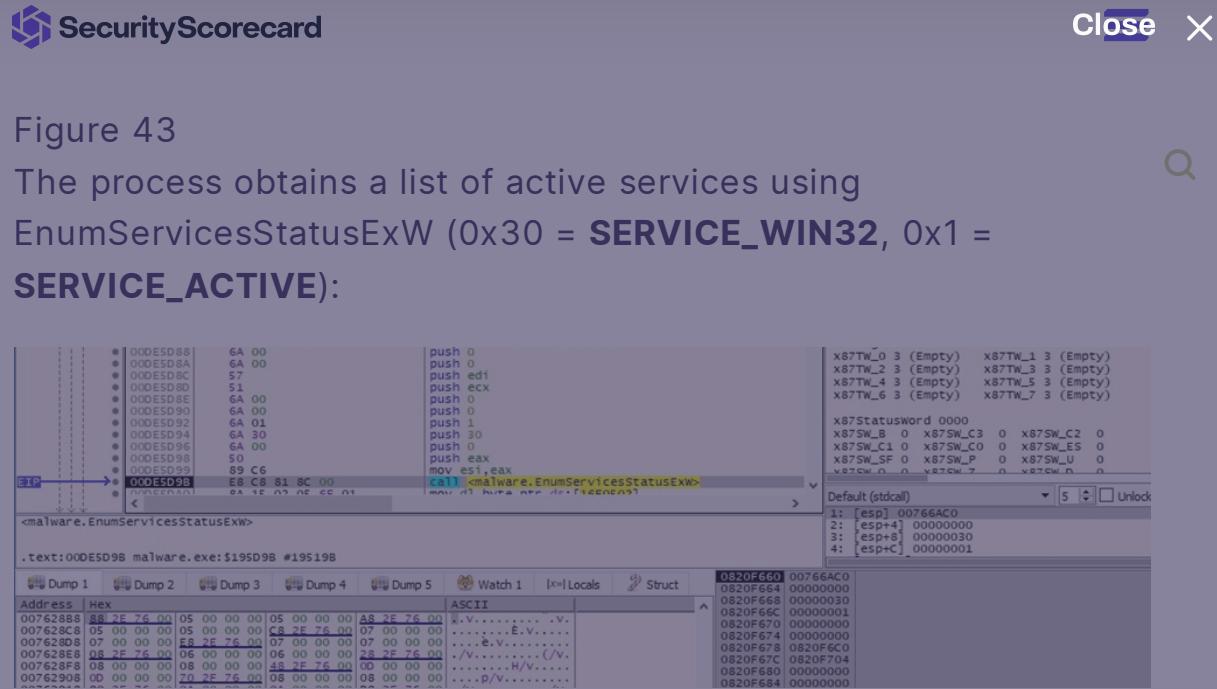
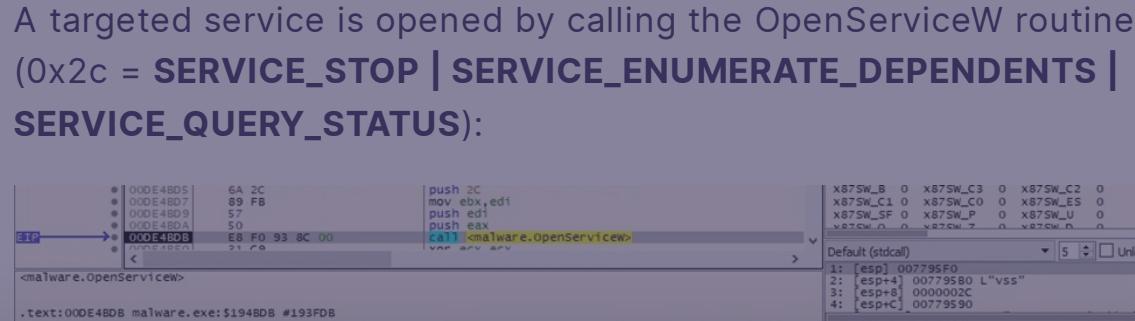


Figure 43  
The process obtains a list of active services using `EnumServicesStatusExW` (0x30 = **SERVICE\_WIN32**, 0x1 = **SERVICE\_ACTIVE**):



#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

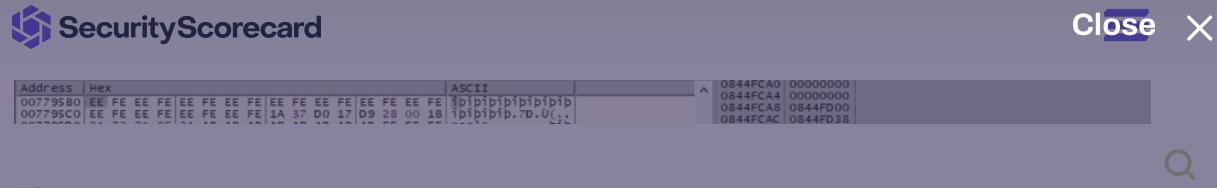


Figure 46

BlackCat stops the targeted service using the ControlService function (0x1 = **SERVICE\_CONTROL\_STOP**):

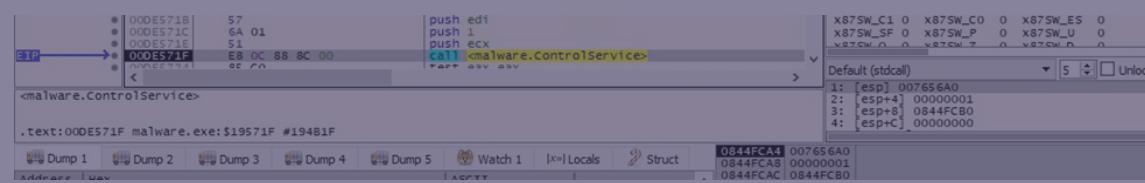


Figure 47

## Killing targeted processes

The executable takes a snapshot of all processes and threads in the system (0xF = **TH32CS\_SNAPALL**):

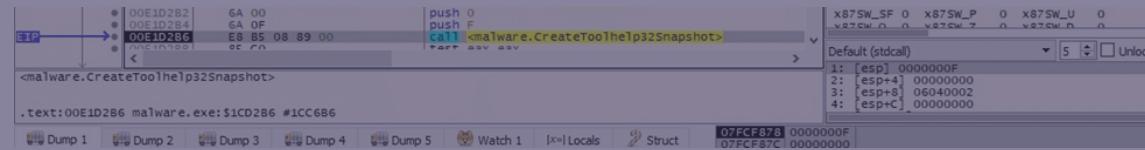


Figure 48

The processes are enumerated using the Process32FirstW and Process32NextW APIs:

### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 50

The malware targets the list of processes from the kill\_processes element in the BlackCat configuration.

It opens a targeted process using OpenProcess (0x1 = PROCESS\_TERMINATE):

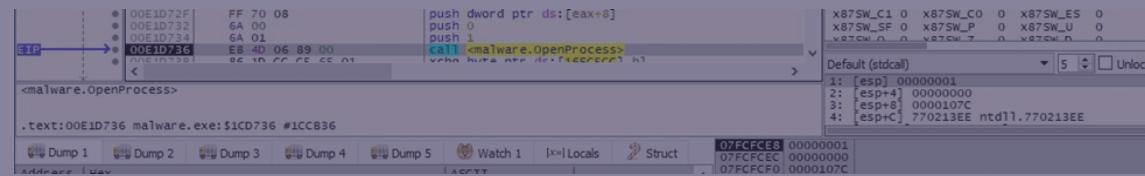


Figure 51

The ransomware terminates the targeted process by calling the TerminateProcess API:

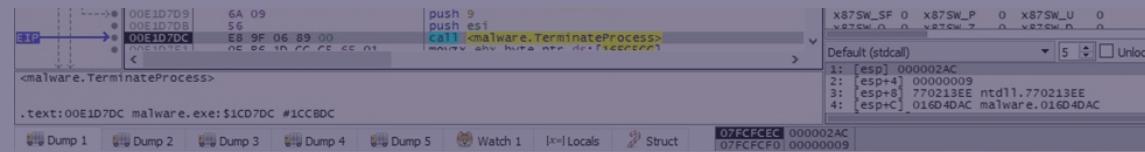


Figure 52

The binary spawns multiple child processes by adding the “-child” parameter to the command line (see figure 53). The new processes run in the security context of credentials that were specified in the credentials entry from the BlackCat configuration.

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

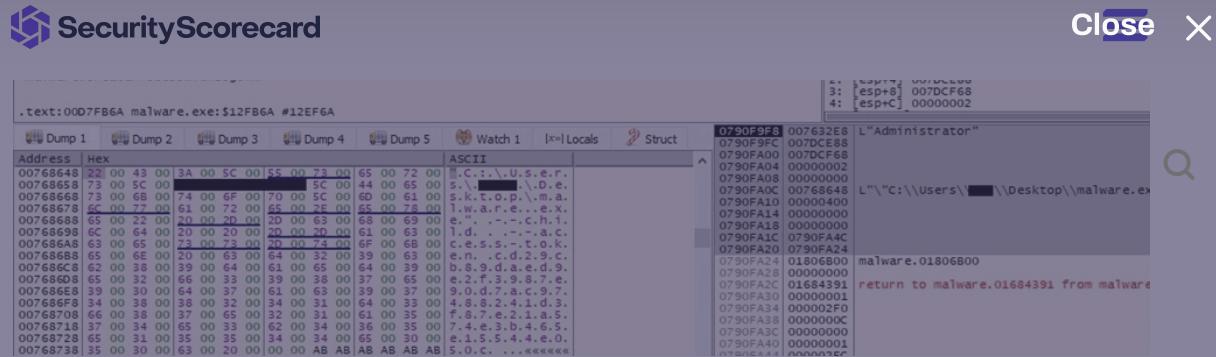


Figure 53

The number of network requests the Server Service can make is set to the maximum by modifying "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxMpxC Registry value:

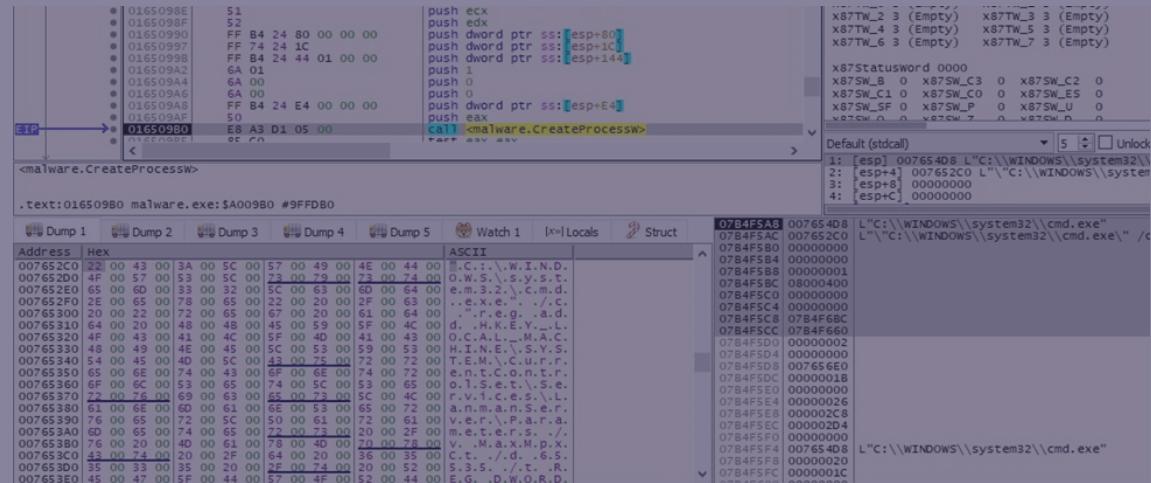


Figure 54

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 55

The net use command is utilized to connect to the local computer using different credentials stored in the BlackCat configuration:

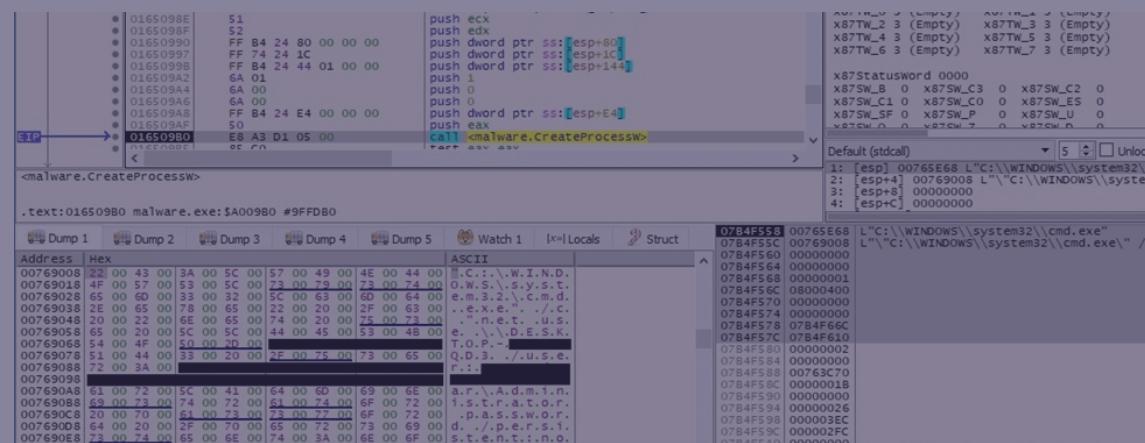
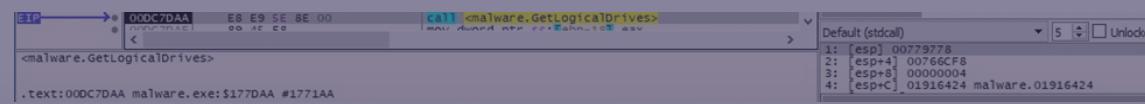


Figure 56

The malware retrieves the currently available disk drives by calling the GetLogicalDrives routine:



### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

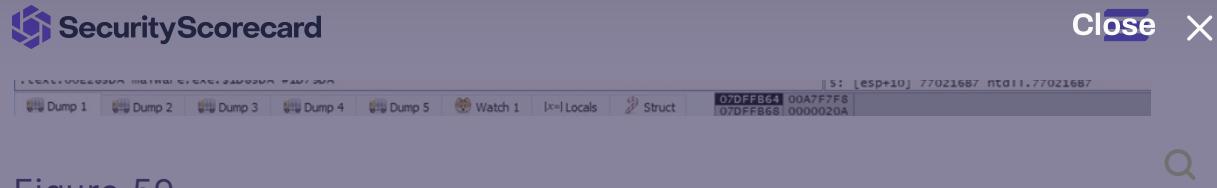


Figure 59

The list of drive letters and mounted folder paths for the above volume is extracted by the malware:

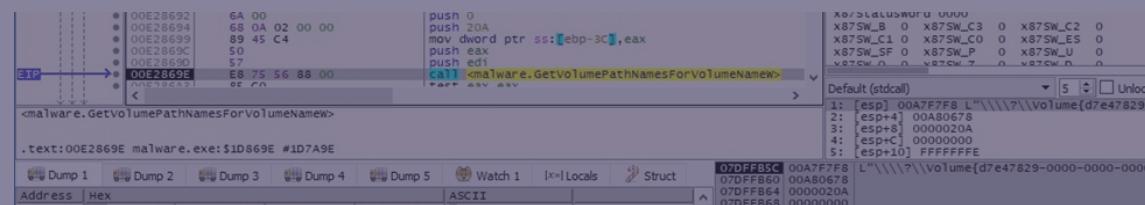


Figure 60

The volume's enumeration continues by calling the FindNextVolumeW function:

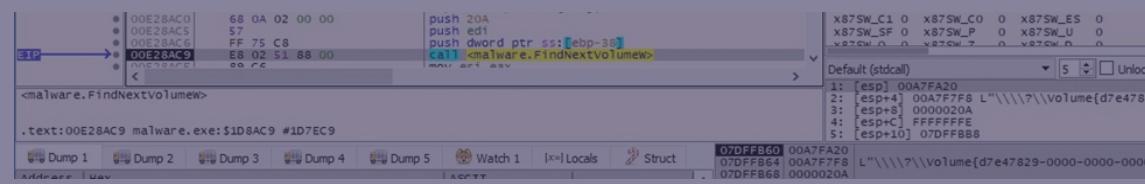
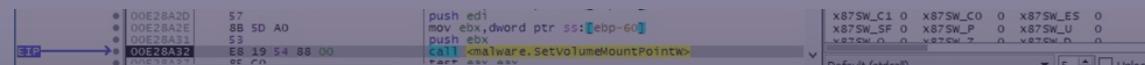


Figure 61

All unmounted volumes are mounted via a function call to SetVolumeMountPointW:



#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

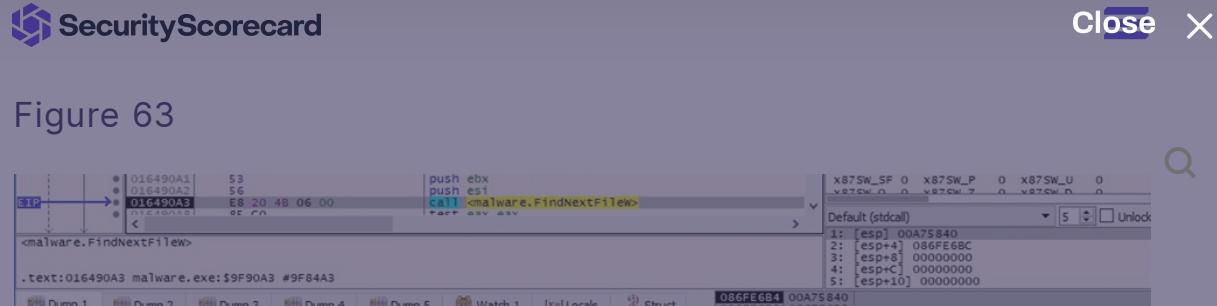


Figure 63

Figure 64

The BlackCat configuration is stored in JSON form and is decrypted at runtime. It contains:

- the extension appended to the encrypted files
- RSA public key that is used to encrypt the AES encryption key
- ransom note name and content
- stolen credentials specific to the victim's environment
- encryption cipher: AES
- list of services and processes to be killed
- list of folders, files, and extensions to be skipped
- boolean values that indicate network discovery, lateral movement, setting the Desktop Wallpaper, killing VMware ESXi virtual machines, removing VMware ESXi virtual machine snapshots, and deleting VMware ESXi virtual machine configurations.

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

The screenshot shows the assembly code for the `CreateFileW` API call. The assembly code includes instructions like `push 0`, `push edi`, `push edx`, `push dword ptr ss:[ebp-18]`, `push dword ptr ss:[ebp-1C]`, `push dword ptr ss:[ebp-10]`, `mov edi,dword ptr ss:[ebp-14]`, and `push edi`. The `call malware.CreateFileW` instruction is highlighted. Below the assembly, the raw dump of the memory shows the ransom note text: `\n.\n?\\C:\\U.S.e.r.s.\\D.e.s.k.t.o.p.\n\\S.a.m.p.l.e.N.o.t.e\n\\RECOV`. The right pane shows the stack dump with various memory locations and their values.

Figure 66

The ransom note is created in every traversed directory  
( $0x40000000 = \text{GENERIC\_WRITE}$ ,  $0x7 = \text{FILE\_SHARE\_DELETE} | \text{FILE\_SHARE\_WRITE} | \text{FILE\_SHARE\_READ}$ ,  $0x2 = \text{CREATE\_ALWAYS}$ ):

This screenshot is similar to Figure 66, showing the assembly code for the `CreateFileW` API call and the resulting ransom note text in memory dump 1. The text is identical to the one in Figure 66: `\n.\n?\\C:\\U.S.e.r.s.\\D.e.s.k.t.o.p.\n\\S.a.m.p.l.e.N.o.t.e\n\\RECOV`. The right pane shows the stack dump with memory locations and values.

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 69

The file's extension is changed using the MoveFileExW function.

The renamed file is opened using CreateFileW (0x7 = FILE\_SHARE\_DELETE | FILE\_SHARE\_WRITE | FILE\_SHARE\_READ, 0x3 = OPEN\_EXISTING, 0x02000000 = FILE\_FLAG\_BACKUP\_SEMANTICS):

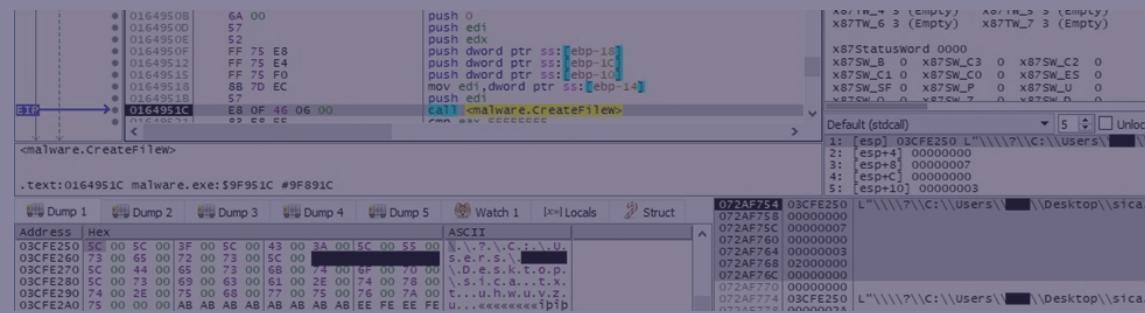


Figure 70

Interestingly, BlackCat creates intermediary files called "checkpoints-<encrypted file name>" during the encryption

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

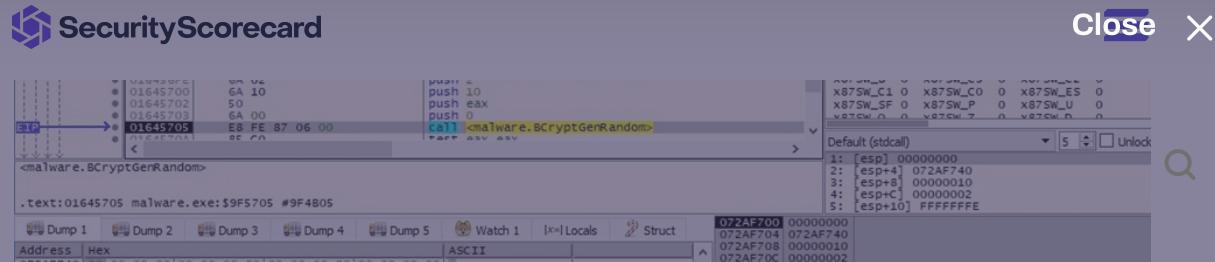


Figure 72

The ransomware moves the file pointer to the beginning of the file by calling the SetFilePointerEx API (0x0 = FILE\_BEGIN):

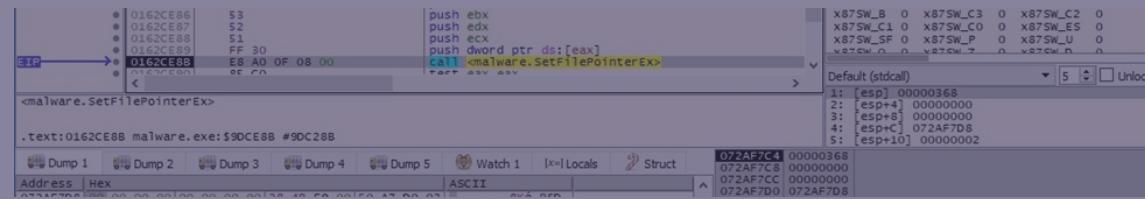


Figure 73

The process reads 4 bytes from the beginning of the file using ReadFile:

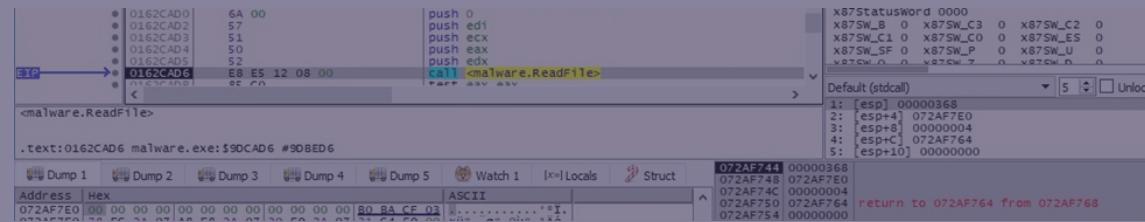


Figure 74

This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 75

The binary generates 0x50 (80) random bytes that are used to border the JSON form. The resulting buffer has a size of 256 bytes and is rotated using instructions such as pshuflw:

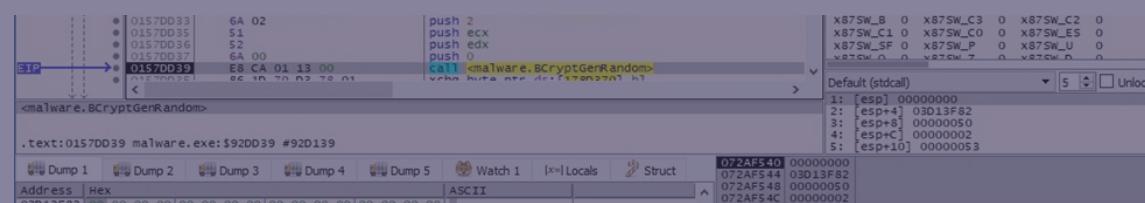


Figure 76

Address	Hex	ASCII
03D04BD8	7D 65 73 6C 61 66 3A 22 64 65 68 73 69 6E 69 66	jeslaf:"dehsinif
03D04BE8	22 2C 36 31 38 32 36 33 35 32 3A 22 65 7A 69 73	",61826352:"ezis
03D04BF8	5F 6B 6E 75 68 63 22 2C 30 30 30 31 3A 22 65 7A	_knuhc",0001:"ez

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 79

The size of encrypted key (0x100) is written to the file:

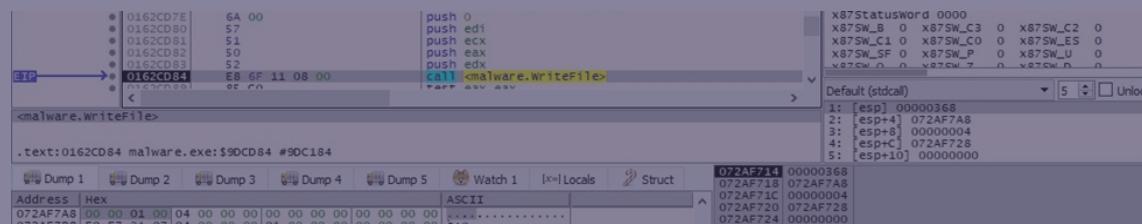
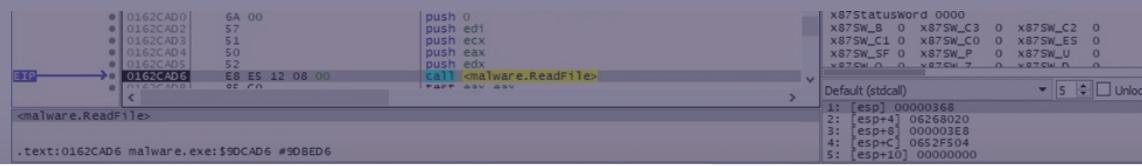


Figure 80

The file content is read by using the ReadFile function:



This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Figure 82

A screenshot of a debugger showing assembly code. The assembly code is:

```
0162CD7E 54 00 push 0
0162CD80 57 push edi
0162CD81 51 push ecx
0162CD82 50 push eax
0162CD83 52 push edx
0162CD84 E8 6F 11 08 00 call malware.writeFile>
```

Figure 83

The encrypted file content is written back to the file using WriteFile:

A screenshot of a debugger showing assembly code. The assembly code is:

```
0162CD7E 54 00 push 0
0162CD80 57 push edi
0162CD81 51 push ecx
0162CD82 50 push eax
0162CD83 52 push edx
0162CD84 E8 6F 11 08 00 call malware.writeFile>
```

Below the assembly code, there is a dump of memory showing the file content being written. The dump shows ASCII data:

```
0652F4F8 00000368 0652F4F8 06268020
0652F4FC 000003E8 0652F500 0652F508
0652F504 00000000 0652F504 00000000
```

#### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

The screenshot shows a log window titled "SecurityScorecard" with a "Close" button and a magnifying glass icon. The log contains numerous entries from a process named "MASTER". The log entries include:

```
13:28:07 MASTER locker::core::stack: Starting Supervisor
13:28:07 MASTER locker::core::stack: Starting Discoverer
13:28:07 MASTER locker::core::stack: Starting File Processors
13:28:07 MASTER locker::core::stack: Starting File Processing Pipeline
13:28:07 MASTER locker::core::pipeline::chunk_workers_supervisor: started_workers=2
13:28:07 MASTER locker::core::pipeline::file_worker_pool: spawned_chunk_work_infrastructure=2
13:28:07 MASTER locker::core::stack: Detecting Other Instances
13:28:07 MASTER locker::core::stack: Connecting to Cluster
13:28:07 MASTER locker::core::cluster: server=1318/7112457831384
13:28:07 MASTER locker::core::os::windows::privilege_escalation: token_is_administrative=true
13:28:07 MASTER locker::core::stack: Starting Platform
13:28:07 MASTER locker::core::os::windows::privilege_escalation: win7_plus=true
13:28:07 MASTER locker::core::os::windows::privilege_escalation: token_is_domain_admin=true
13:28:07 MASTER encrypt_1lib::windows::strict__include_paths::local={}
13:28:07 MASTER encrypt_1lib::windows::strict__include_paths::remote={}
13:28:07 MASTER locker::core::os::windows::privilege_escalation: initializing Networking Routine
13:28:07 MASTER locker::core::os::windows::system_info: username=
13:28:07 MASTER locker::core::os::windows::privilege_escalation: impersonate_spawn_trying::Administrator, --password
13:28:07 MASTER locker::core::os::windows::privilege_escalation: impersonate_spawn_trying::C:\Users\_\Desktop\malware.exe" --child --access-token cd29cb89daed9e2f3987e90d7ac974882
41d3f87e21a574c3b465e15344e0dc
13:28:07 MASTER locker::core::os::windows::privilege_escalation: CreateProcessWithLogonW-success,1700
```

Figure 86

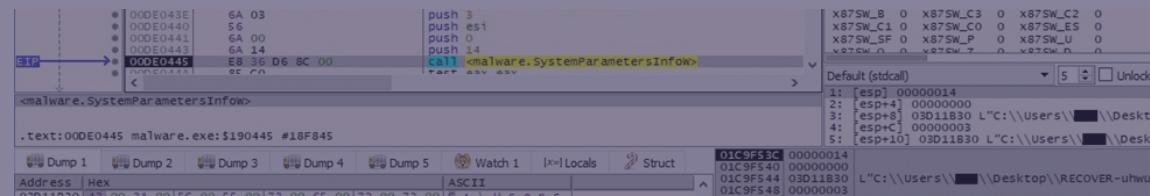
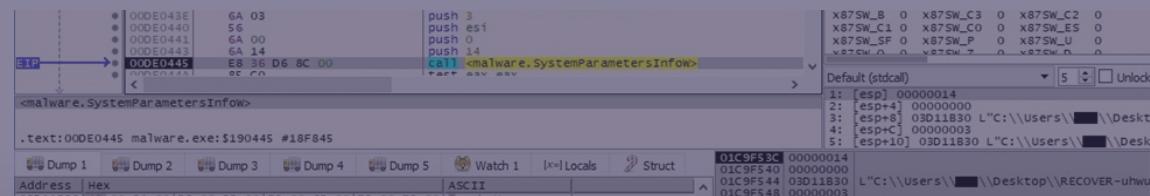


Figure 87

The Desktop wallpaper is changed to the above image by calling the SystemParametersInfoW API (0x14 = SPI\_SETDESKWALLPAPER, 0x3 = SPIF\_UPDATEINIFILE | SPIF\_SENDCHANGE):



## This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

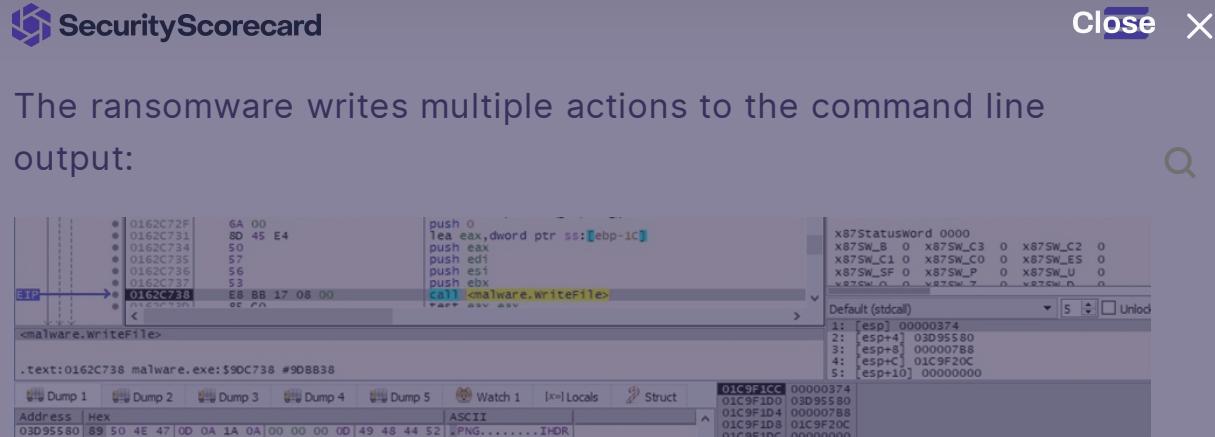


Figure 89

## Running with the –extra-verbose –ui parameters

The malware presents the relevant information in the following window:

This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



SecurityScorecard

[Close](#) X



Figure 90

## Indicators of Compromise

### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



[Close](#) X

## Processes spawned



```
cmd.exe /c "wmic csproduct get UUID"  
cmd.exe /c "fsutil behavior set SymlinkEvaluation R2L:1"  
cmd.exe /c "fsutil behavior set SymlinkEvaluation R2R:1"  
cmd.exe /c "iisreset.exe /stop"  
cmd.exe /c "vssadmin Delete Shadows /all /quiet"  
cmd.exe /c "wmic.exe Shadowcopy Delete"  
cmd.exe /c "bcdedit /set {default}"  
cmd.exe /c "bcdedit /set {default} recoveryenabled No"  
cmd.exe /c for /F "tokens=*" %1 in ('wevtutil.exe el') DO  
wevtutil.exe cl %1  
cmd.exe  
/c "reg add  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Para  
/v MaxMpxCt /d 65535 /t REG_DWORD /f"  
cmd.exe /c "arp -a"
```

### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.



Digital Forensics & Incident Response  
Advisory Services  
Penetration Testing  
Red Team  
Tabletop Exercises

Locate a Partner  
Value-Added Resellers  
Managed Service Providers  
ISAC Partner Program  
Technology Alliances  
SCORE Portal Login

## Resources

Blog  
Research  
Learning Center  
Webinars  
Tools & Documentation  
Public Scorecards

## Company

Leadership  
Press  
Events  
Policy Insights  
Careers  
Contact Us  
Patents



© 2024 SecurityScorecard | [Terms Of Use](#) | [Privacy Policy](#) | [Cookie Preferences](#) | [Patents](#)

### This website uses cookies

We use cookies to personalize content and ads, to provide social media features and to analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.