RESEARCH

A Deep Dive Into ALPHV/BlackCat Ransomware

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.

SecurityScorecard

Close

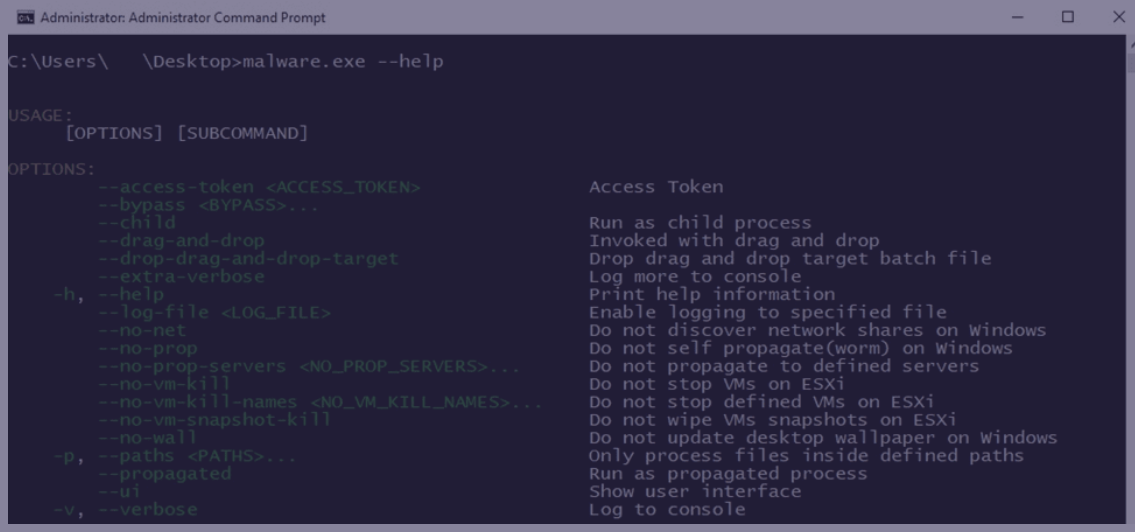


Figure 1
Whether the ransomware is running with no parameters or with an invalid access token, an error message is displayed:

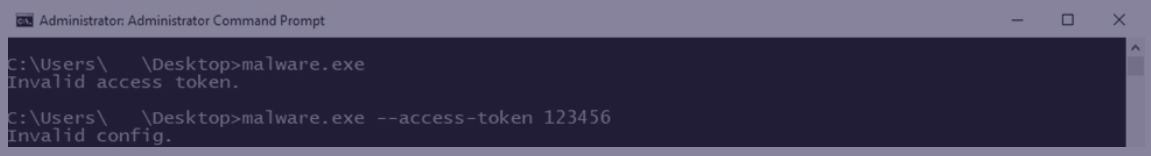


Figure 2
By performing the dynamic analysis, we've found that the access token must be a 32-byte value that is not unique.

SecurityScorecard Close

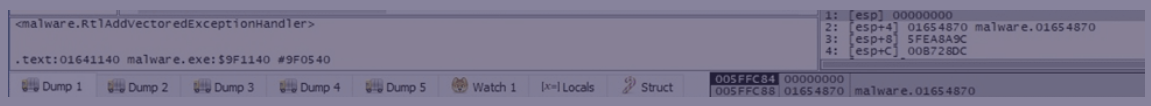


Figure 4
The executable retrieves the command-line string for the process using the GetCommandLineW function:

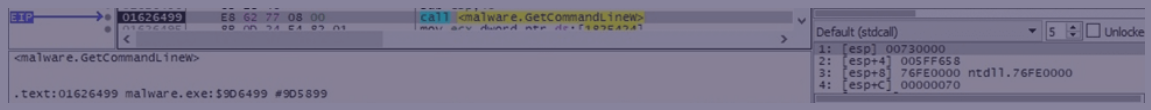
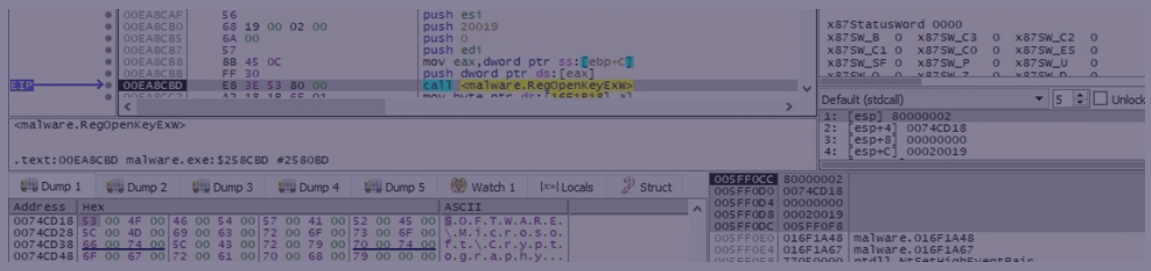


Figure 5
BlackCat opens the “SOFTWARE\Microsoft\Cryptography” registry key by calling the RegOpenKeyExW routine (0x80000002 = **HKEY_LOCAL_MACHINE**, 0x20019 = KEY_READ):



CreateFileW (0x7 = **FILE_SHARE_DELETE | FILE_SHARE_WRITE | FILE_SHARE_READ**, 0x3 = **OPEN_EXISTING**, 0x2000000 = **FILE_FLAG_BACKUP_SEMANTICS**):

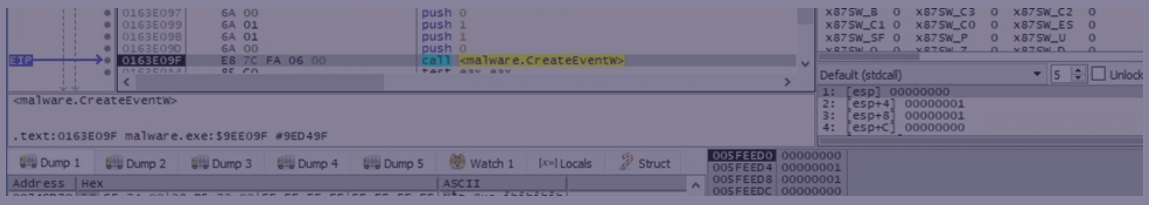


Figure 8
The executable generates 16 random bytes by calling the BCryptGenRandom API (0x2 = **BCRYPT_USE_SYSTEM_PREFERRED_RNG**):

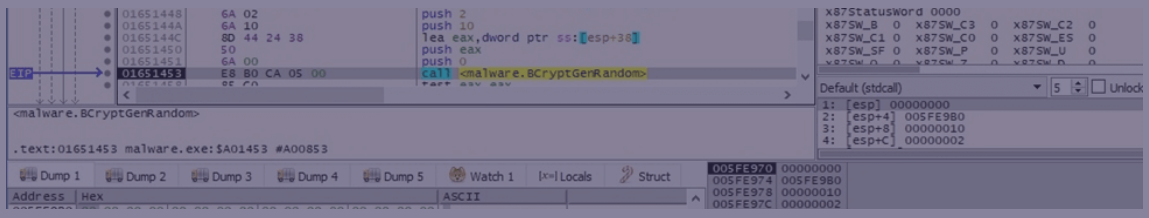


Figure 9
A named pipe whose name contains the current process ID and random bytes generated above is created using

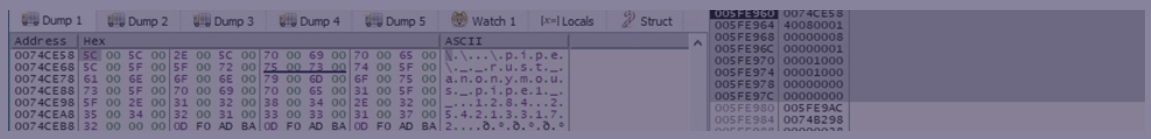


Figure 10
The process opens the named pipe for writing using the CreateFileW routine (0x40000000 = **GENERIC_WRITE**, 0x3 = **OPEN_EXISTING**):

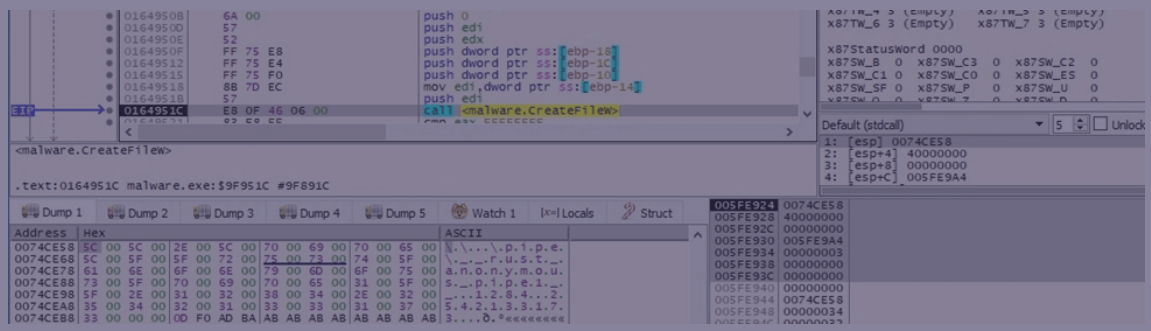


Figure 11
The ransomware creates a read and a write named pipe, respectively.

The wmic process is used to extract the UUID (0x08000400 = **CREATE_NO_WINDOW** | **CREATE_UNICODE_ENVIRONMENT**):

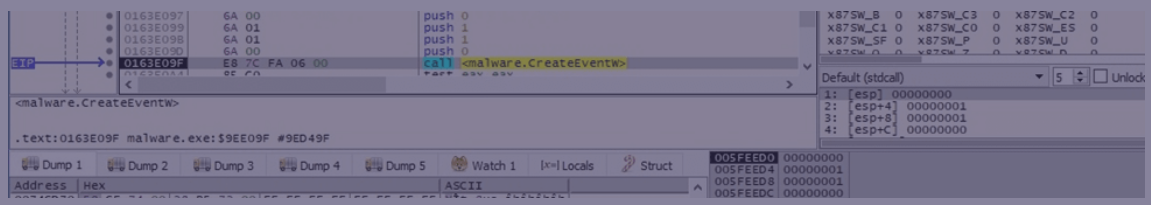


Figure 13
The binary waits until the event objects are in the signaled state by calling WaitForMultipleObjects:

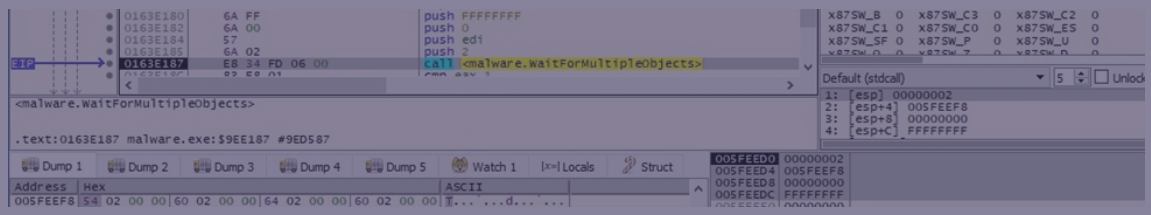
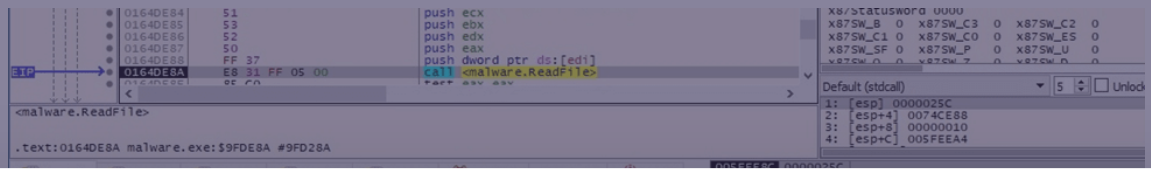


Figure 14
The output of the above process is read from the named pipe using the ReadFile routine:



SecurityScorecard Close

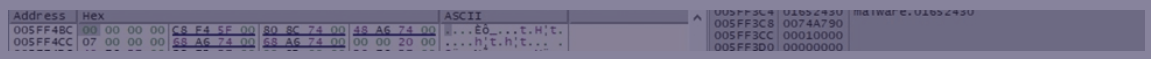


Figure 16

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 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
0074CFC8	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

built-in domain (0x220 = **DOMAIN_ALIAS_RID_ADMINS**):

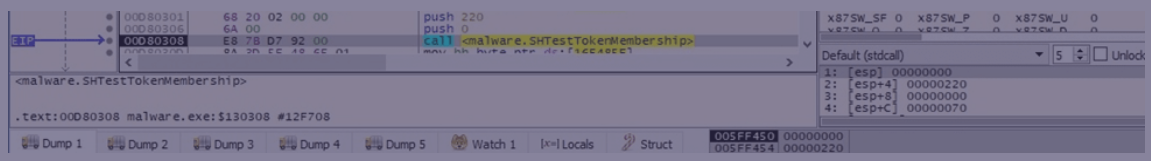


Figure 20

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

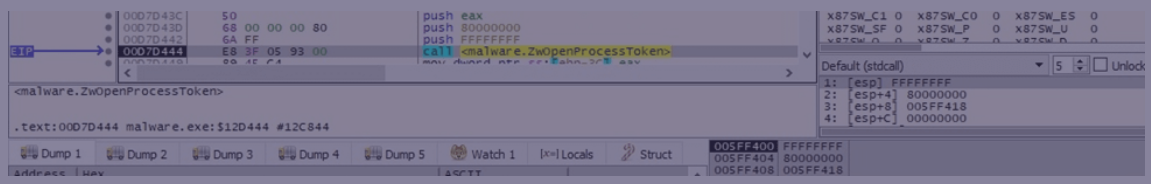
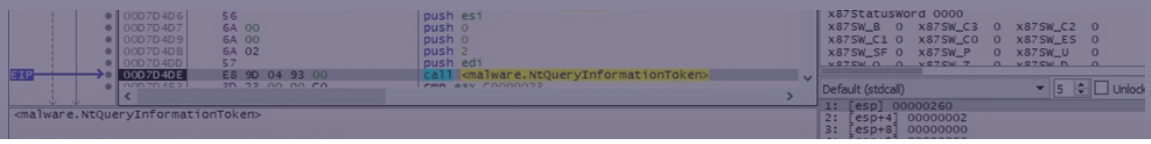


Figure 21

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



SecurityScorecard

Close

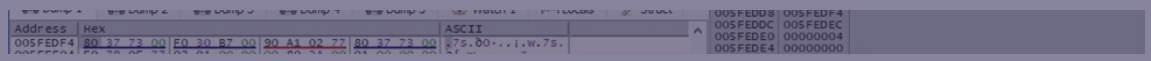


Figure 23
The malicious binary retrieves a pointer to a PEB structure using the ZwQueryInformationProcess routine (0x0 = **ProcessBasicInformation**):

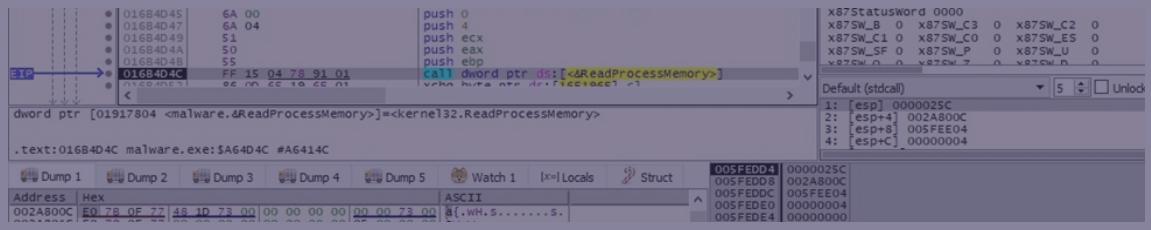
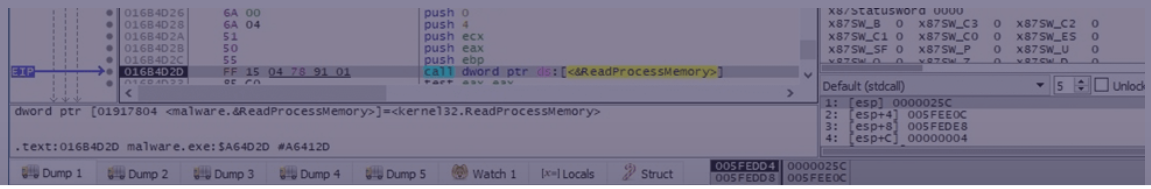


Figure 24
The executable retrieves a pointer to a PEB_LDR_DATA structure containing information about the loaded modules in the process and then to the head of a doubly linked list that contains the loaded modules:



SecurityScorecard

Close

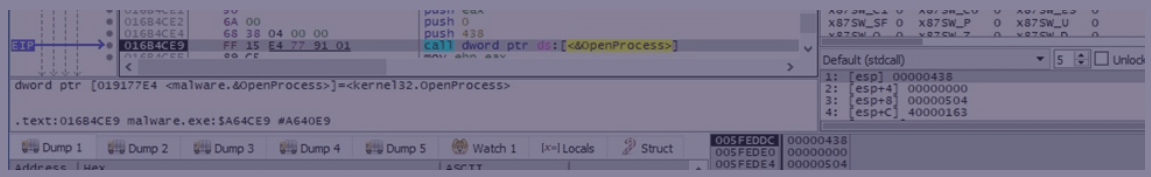


Figure 27

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**):

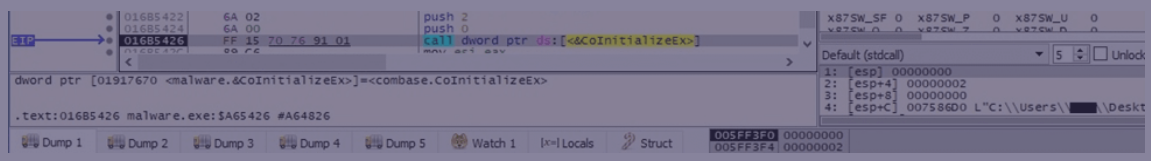


Figure 28
BlackCat ransomware uses the auto-elevated CMSTPLUA interface **{3E5FC7F9-9A51-4367-9063-A120244FBEC7}** in order to escalate privileges:

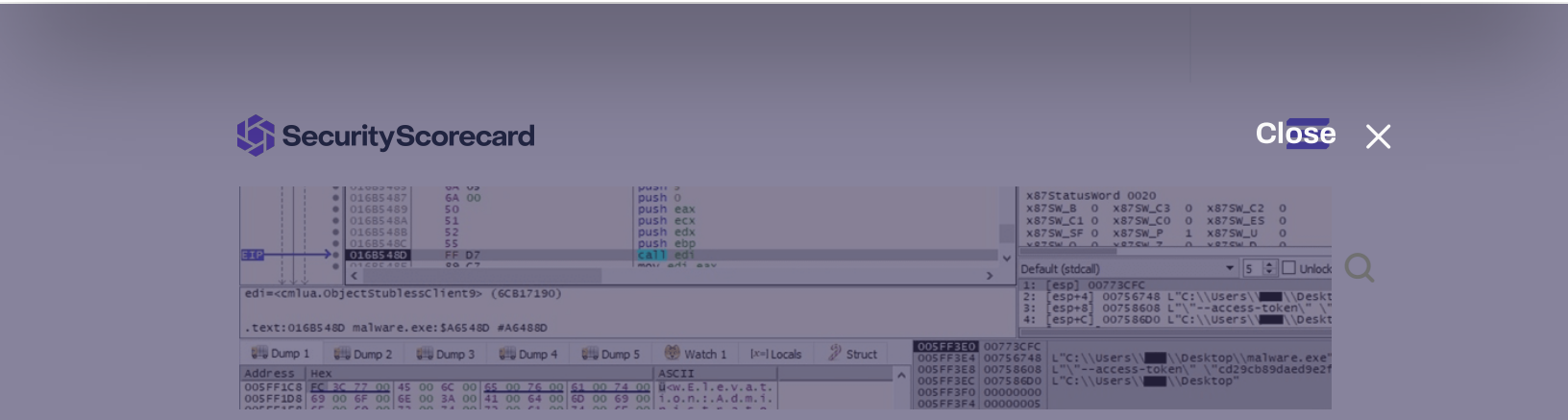


Figure 30
The LookupPrivilegeValueW routine is utilized to retrieve the locally unique identifier that represents the following privileges:

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

SecurityScorecard

Close

Figure 31
All the above privileges are enabled in the access token using AdjustTokenPrivileges:

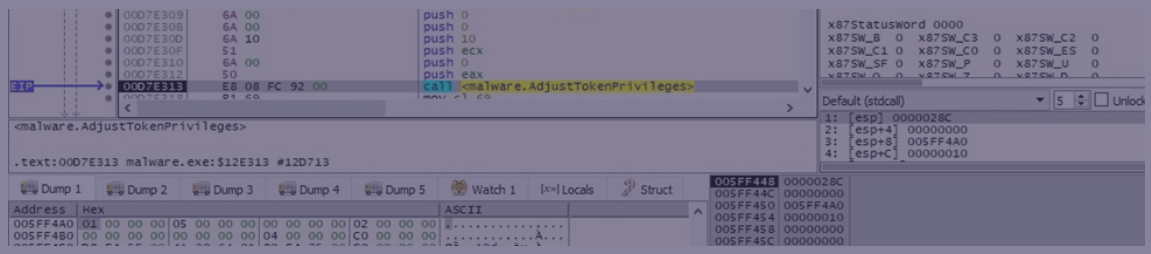
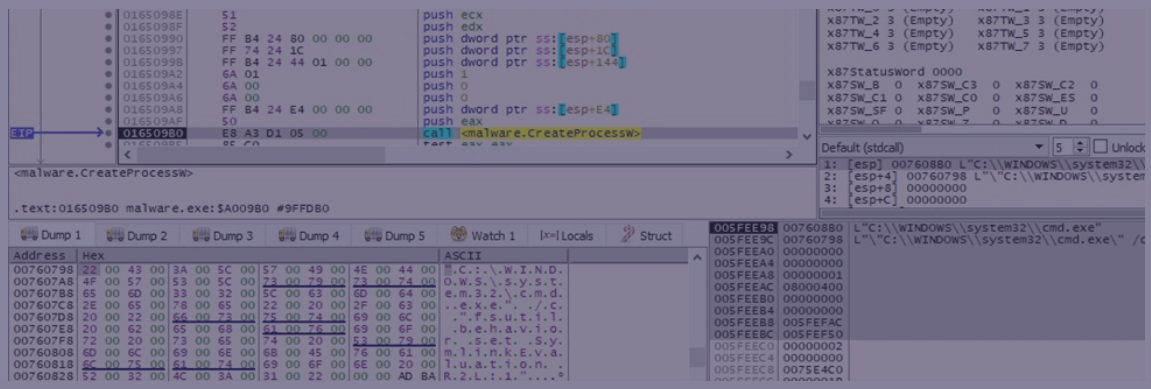


Figure 32
The binary creates the following processes that enable “remote to local” and “remote to remote” symbolic links on the local machine:



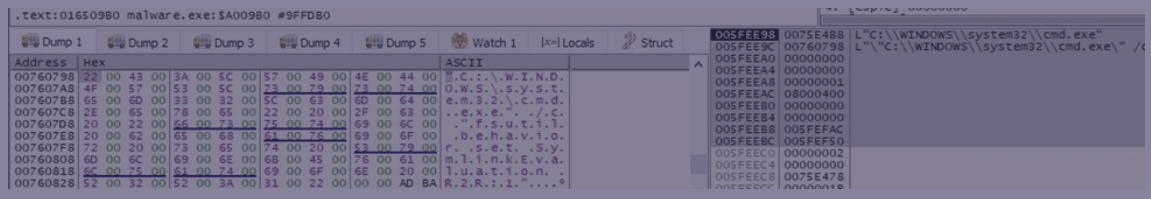


Figure 34
The malware tries to stop the Internet Information service (IIS) using IISReset.exe:

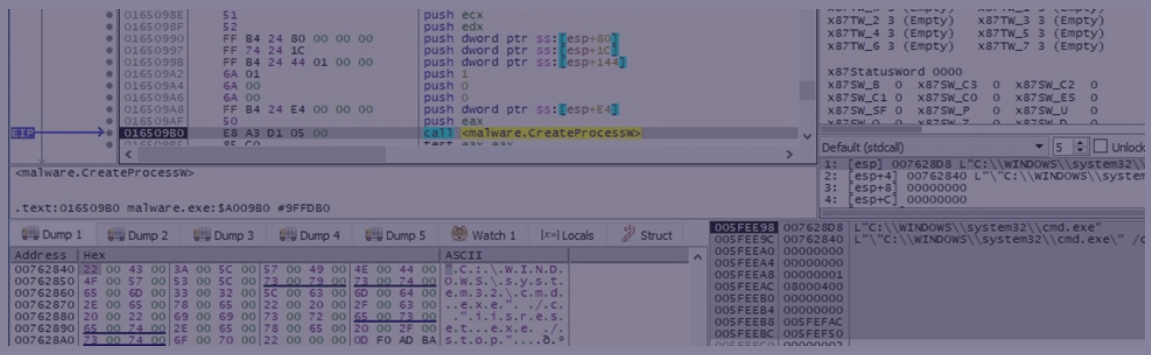
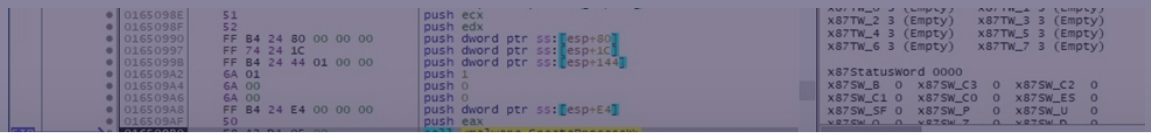


Figure 35
The ransomware deletes all volume shadow copies using the vssadmin.exe utility:



SecurityScorecard Close

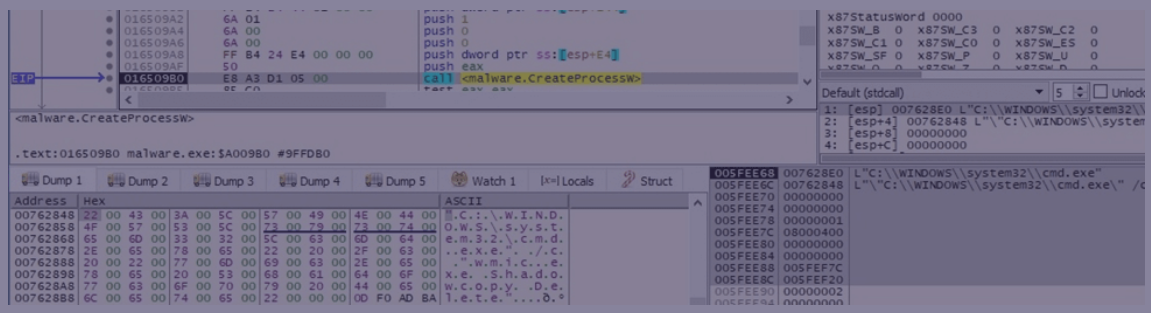


Figure 37

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

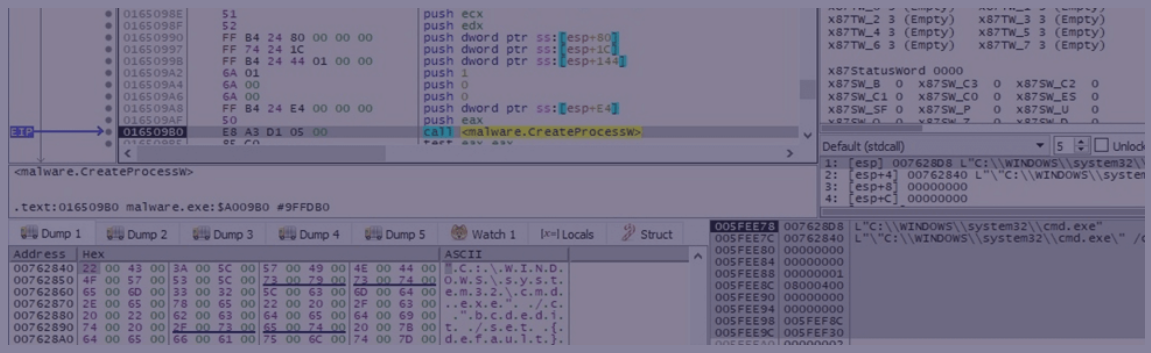
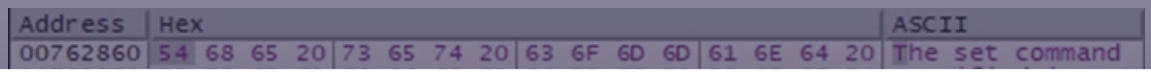


Figure 38



SecurityScorecard

Close

Figure 40

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

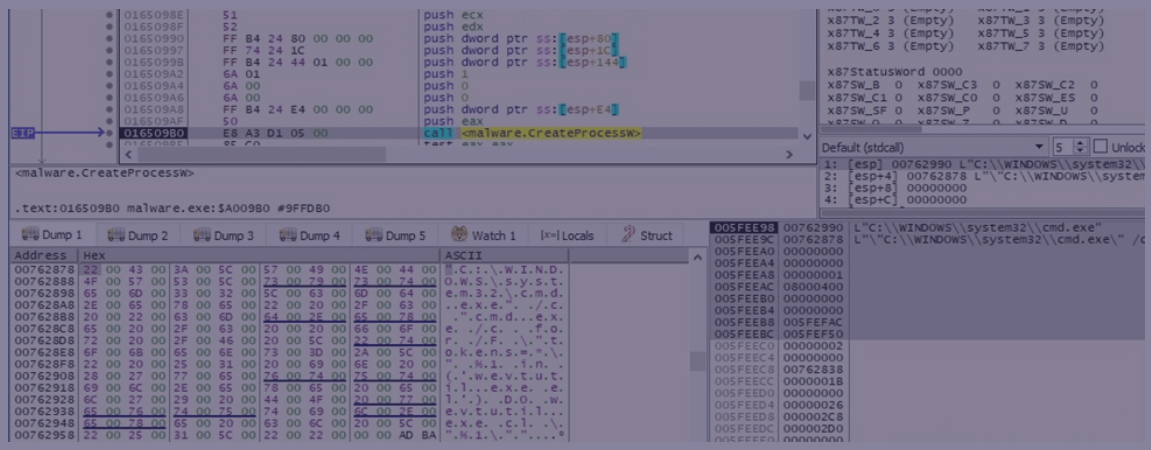
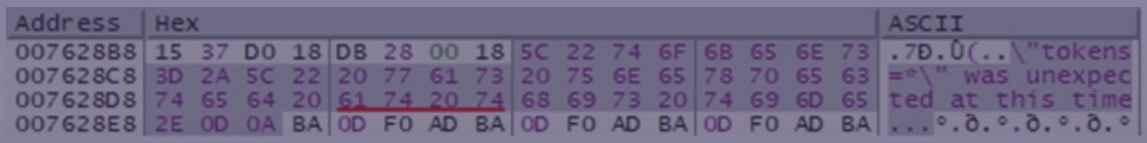


Figure 41



Address	Hex												ASCII
007628B8	15	37	D0	18	DB	28	00	18	5C	22	74	6F	.7Đ.Û(..\"tokens
007628C8	3D	2A	5C	22	20	77	61	73	20	75	6E	65	=*\" was unexpec
007628D8	74	65	64	20	61	74	20	74	68	69	73	20	ted at this time
007628E8	2E	0D	0A	BA	0D	F0	AD	BA	0D	F0	AD	BA	...°.ð.°.ð.°.ð.°

Figure 43
The process obtains a list of active services using EnumServicesStatusExW (0x30 = **SERVICE_WIN32**, 0x1 = **SERVICE_ACTIVE**):

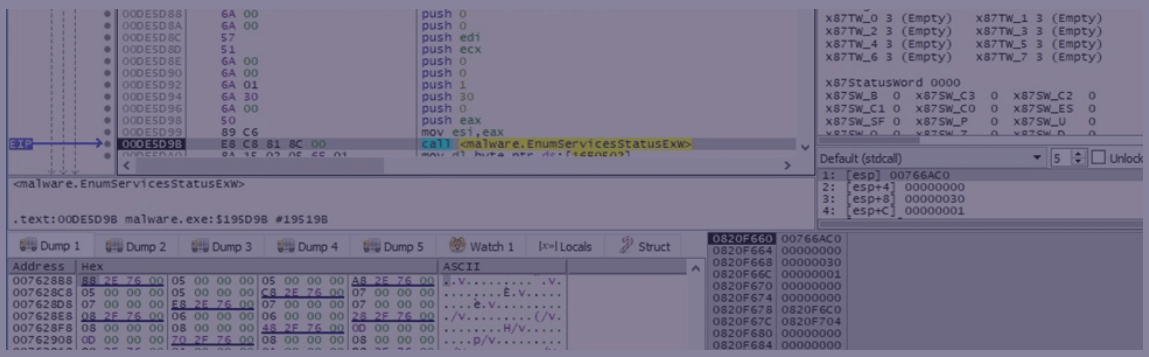
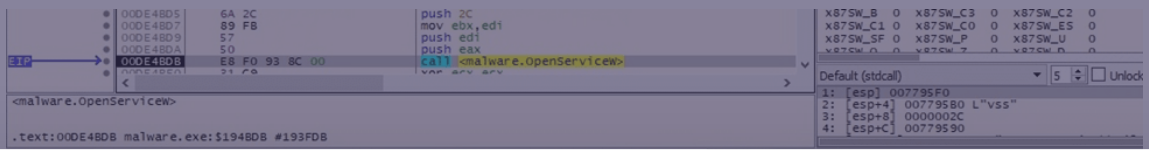


Figure 44
The malware targets the list of services from the kill_services element in the BlackCat configuration.

A targeted service is opened by calling the OpenServiceW routine (0x2c = **SERVICE_STOP | SERVICE_ENUMERATE_DEPENDENTS | SERVICE_QUERY_STATUS**):



SecurityScorecard

Close

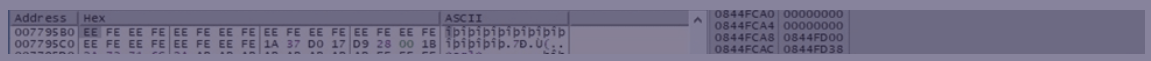


Figure 46
BlackCat stops the targeted service using the ControlService function (0x1 = **SERVICE_CONTROL_STOP**):

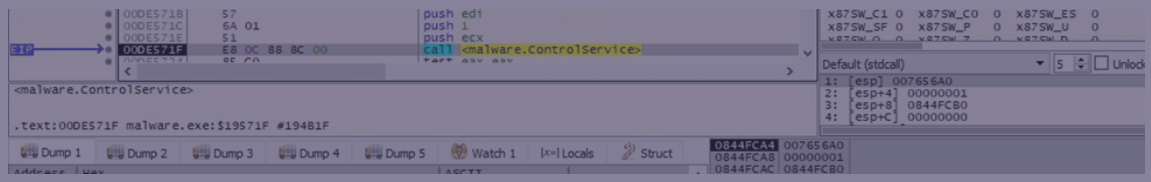


Figure 47

Killing targeted processes

The executable takes a snapshot of all processes and threads in the system (0xF = **TH32CS_SNAPALL**):

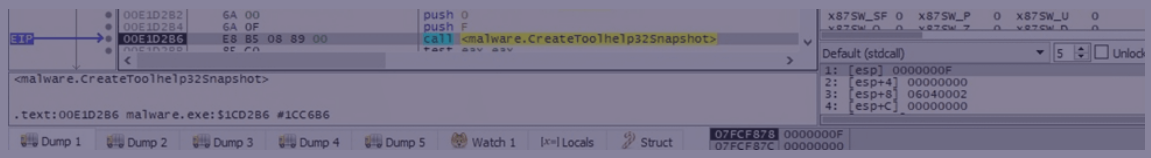


Figure 48
The processes are enumerated using the Process32FirstW and Process32NextW APIs:

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**):

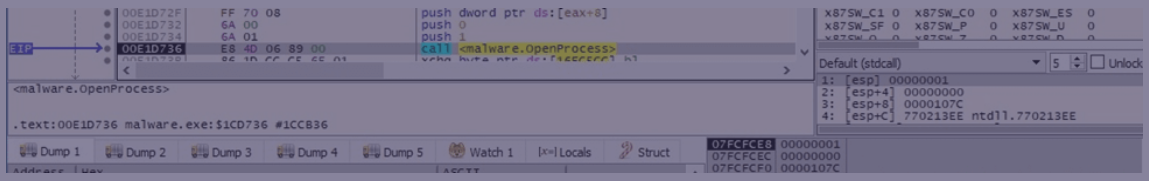


Figure 51
The ransomware terminates the targeted process by calling the TerminateProcess API:

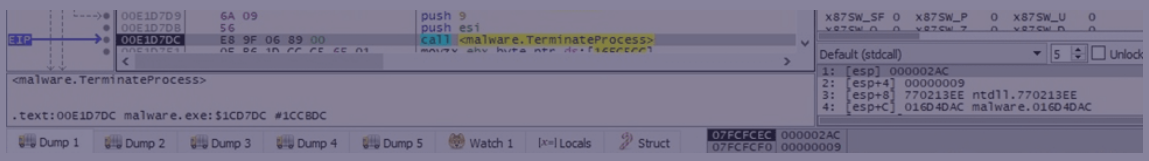


Figure 52
The binary spawns multiple child processes by adding the “–child” parameter to the command line (see figure 53). The new processes run in the security context of credentials that were specified in the credentials entry from the BlackCat configuration.

SecurityScorecard

Close

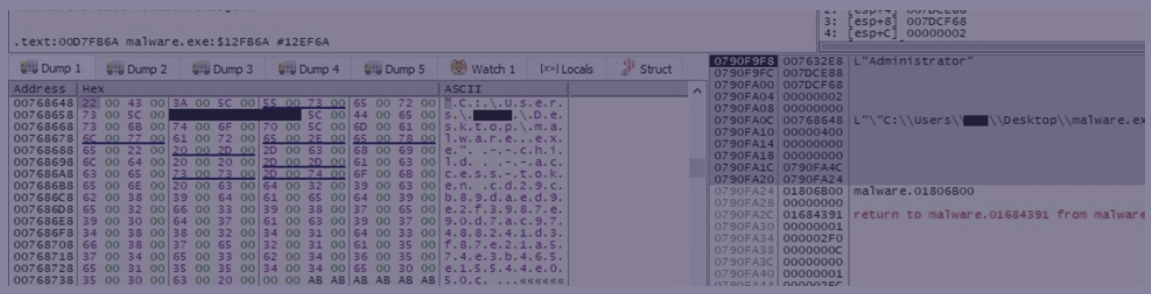


Figure 53
The number of network requests the Server Service can make is set to the maximum by modifying "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxMpxC
Registry value:

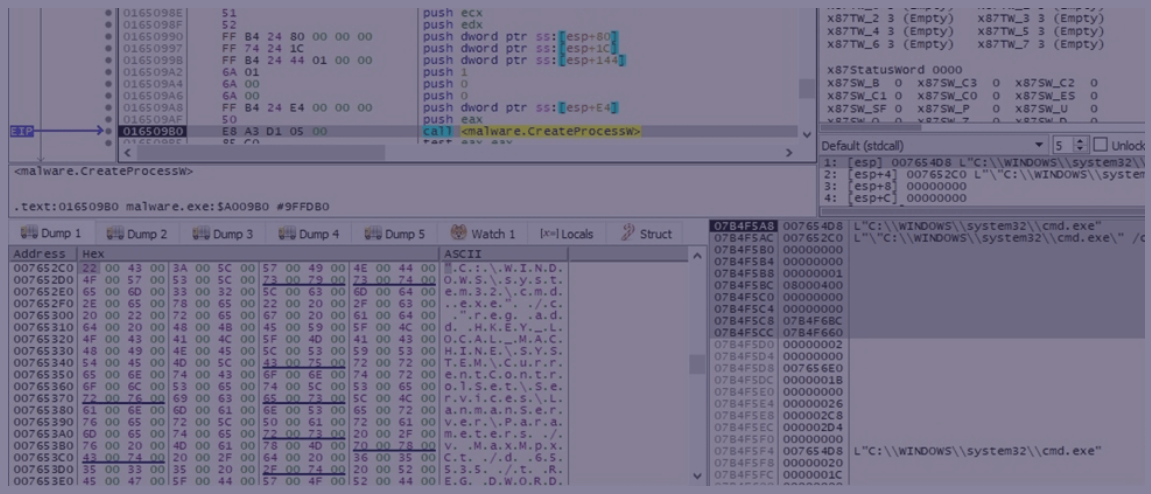


Figure 54

SecurityScorecard

Close

Figure 55
The net use command is utilized to connect to the local computer using different credentials stored in the BlackCat configuration:

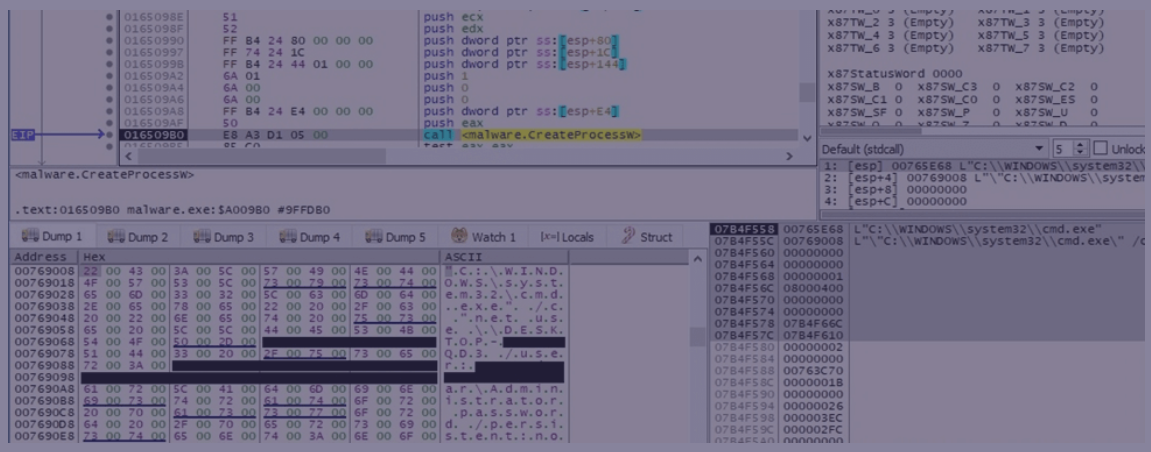
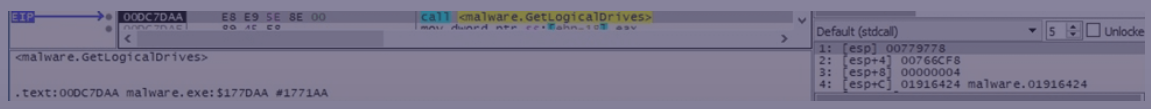


Figure 56
The malware retrieves the currently available disk drives by calling the GetLogicalDrives routine:



SecurityScorecard

Close

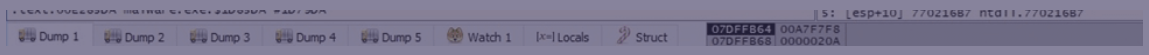


Figure 59
The list of drive letters and mounted folder paths for the above volume is extracted by the malware:

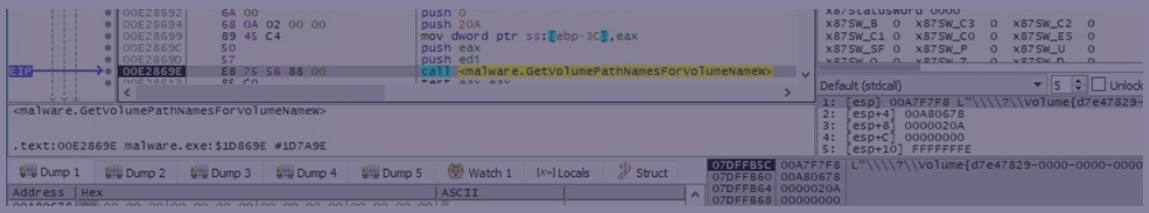


Figure 60
The volume's enumeration continues by calling the FindNextVolumeW function:

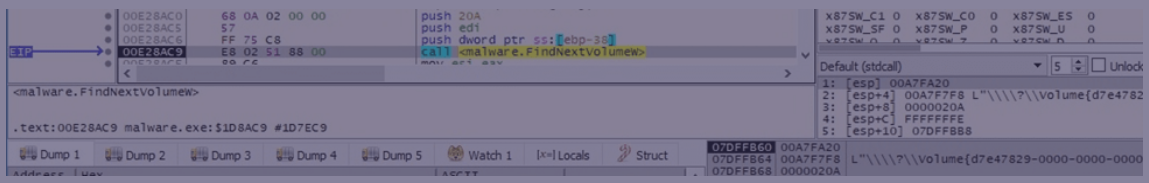


Figure 61
All unmounted volumes are mounted via a function call to SetVolumeMountPointW:

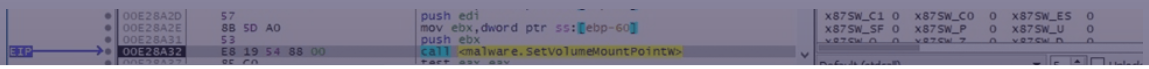


Figure 63

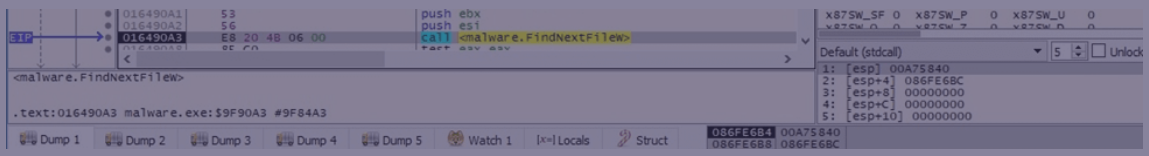


Figure 64

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,

SecurityScorecard

Close

The CreateFileW API is used to open a targeted file (0xC0000000 = **GENERIC_READ | GENERIC_WRITE**, 0x7 = **FILE_SHARE_DELETE | FILE_SHARE_WRITE | FILE_SHARE_READ**, 0x3 = **OPEN_EXISTING**):

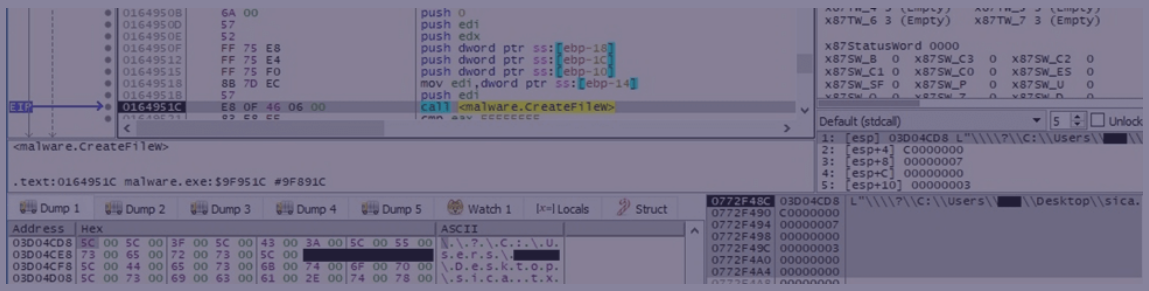
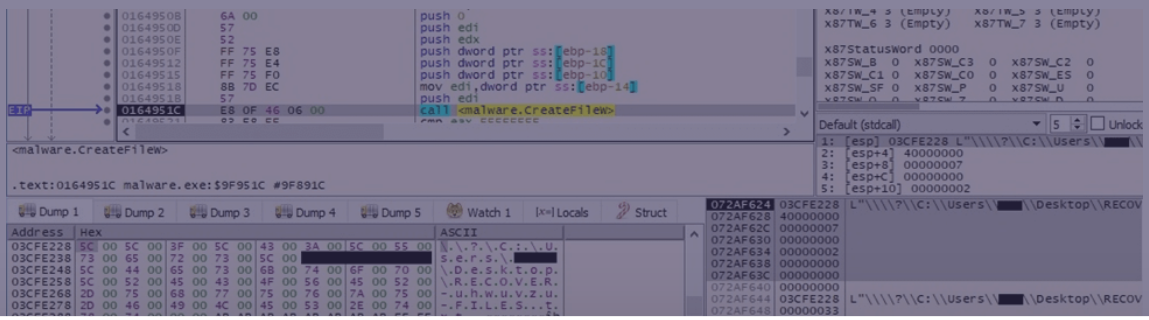


Figure 66

The ransom note is created in every traversed directory (0x40000000 = **GENERIC_WRITE**, 0x7 = **FILE_SHARE_DELETE | FILE_SHARE_WRITE | FILE_SHARE_READ**, 0x2 = **CREATE_ALWAYS**):



SecurityScorecard

Close

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**):

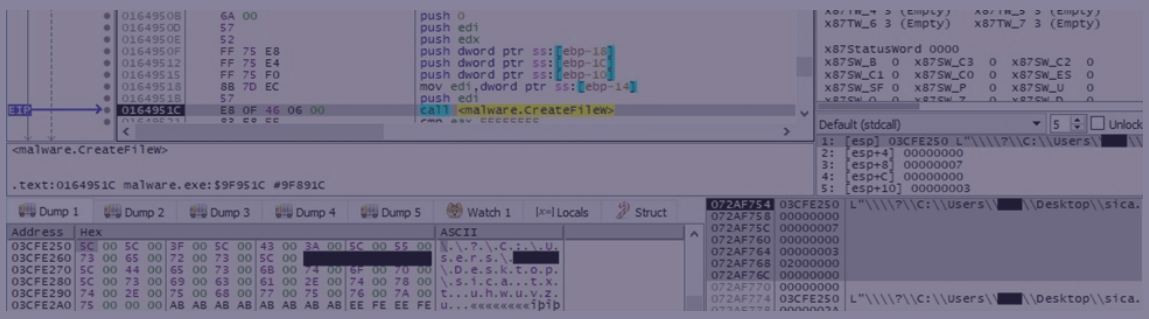


Figure 70
Interestingly, BlackCat creates intermediary files called "checkpoints-<encrypted file name>" during the encryption

SecurityScorecard Close

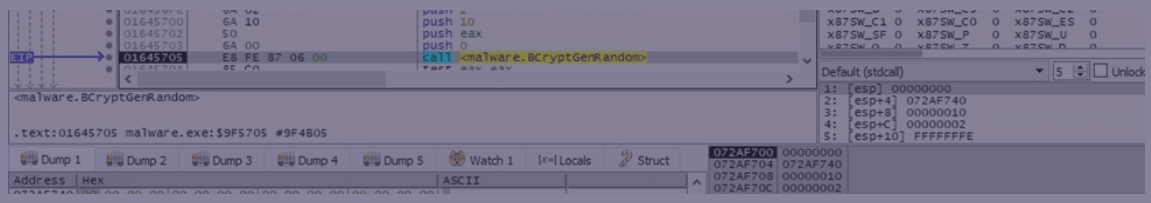


Figure 72
The ransomware moves the file pointer to the beginning of the file by calling the SetFilePointerEx API (0x0 = **FILE_BEGIN**):

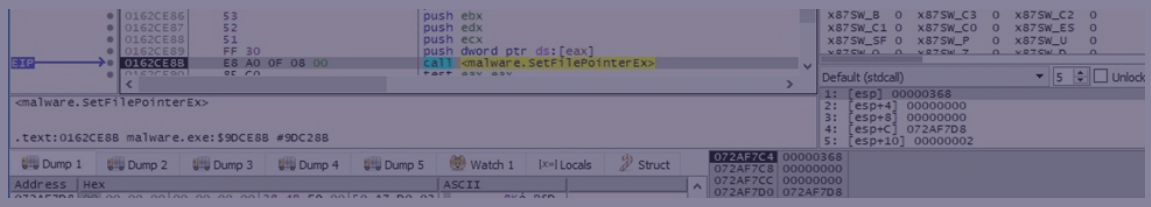


Figure 73
The process reads 4 bytes from the beginning of the file using ReadFile:

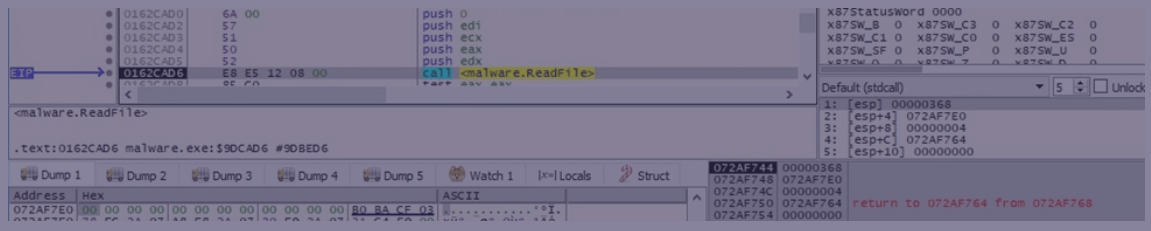


Figure 74

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:

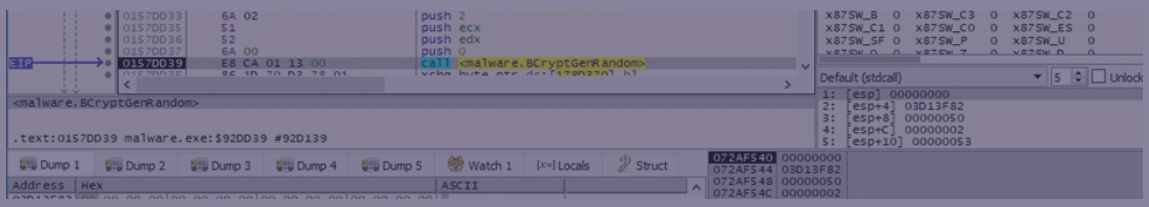


Figure 76

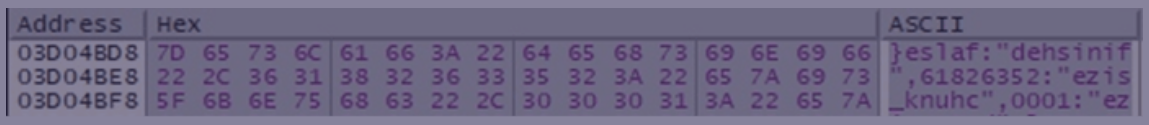


Figure 79
The size of encrypted key (0x100) is written to the file:

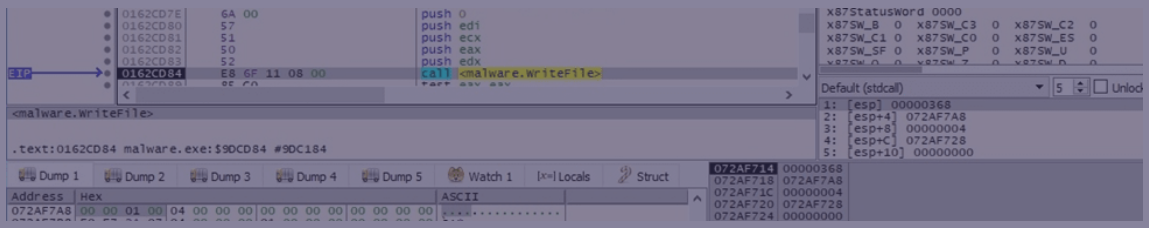
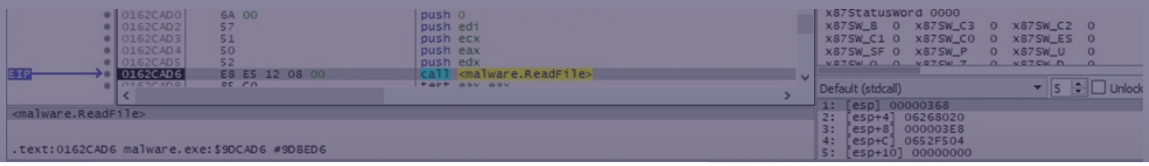


Figure 80
The file content is read by using the ReadFile function:



SecurityScorecard

Close

Figure 82

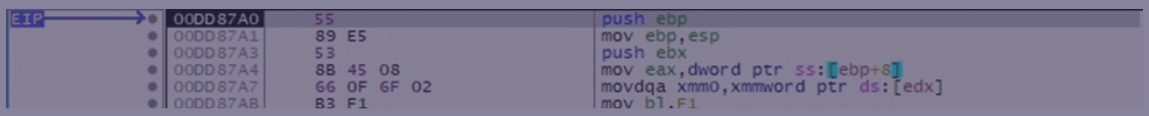
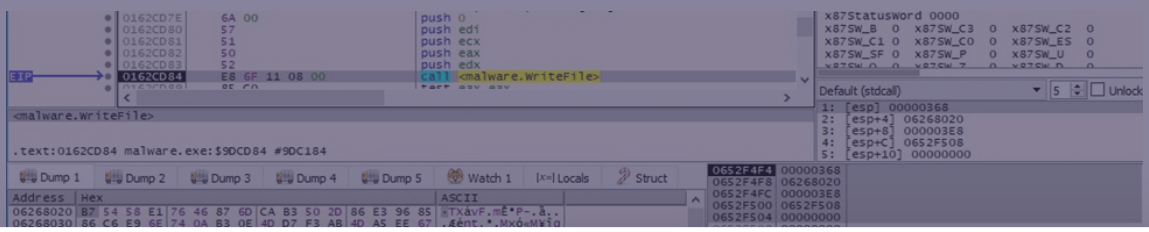


Figure 83

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



SecurityScorecard

Close

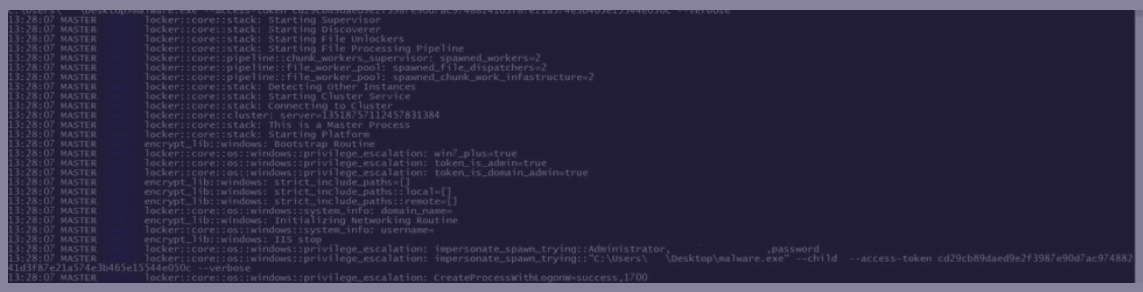


Figure 86

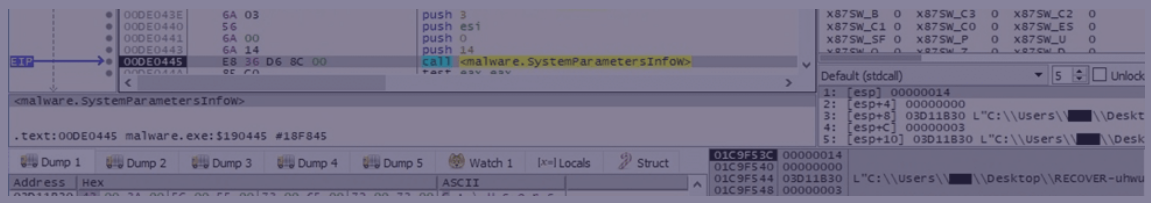
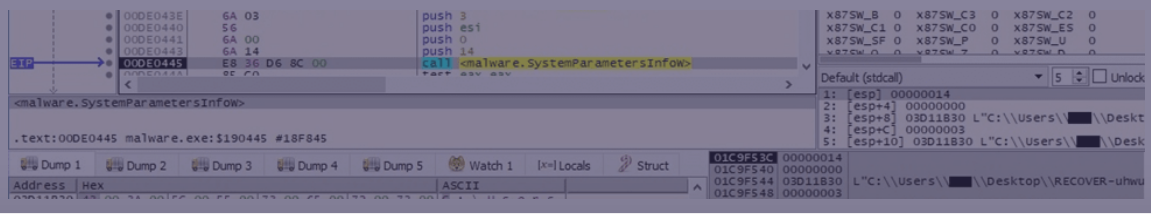


Figure 87

The Desktop wallpaper is changed to the above image by calling the SystemParametersInfoW API (0x14 = **SPI_SETDESKWALLPAPER**, 0x3 = **SPIF_UPDATEINIFILE | SPIF_SENDCHANGE**):



SecurityScorecard

Close

The ransomware writes multiple actions to the command line output:

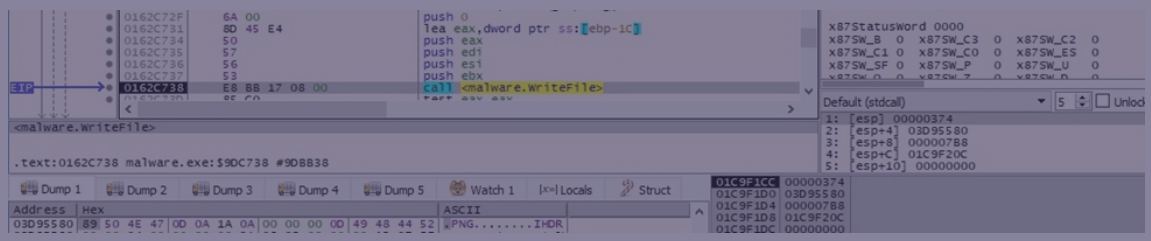


Figure 89

Running with the –extra-verbose –ui parameters

The malware presents the relevant information in the following window:

Figure 90

Indicators of Compromise

SecurityScorecard

Close

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.exe 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”

SecurityScorecard

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