A Deep Dive Into ALPHV/BlackCat Ransomware

securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware



Skip to main content

- <u>Support</u>
- Login
- <u>Contact</u>
- <u>Blog</u>
- Languages
 - <u>English</u>
 - Français
 - 。<u>日本語</u>
- <u>Request a Demo</u>

Interested in reading the report later? Download it.

Download Now Prepared by: Vlad Pasca, Senior Malware & Threat Analyst

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.

The files are encrypted using the AES algorithm, with the AES key being encrypted using the RSA public key contained in the configuration. The extension of the encrypted files is changed to uhwuvzu by the malware.

Analysis and findings

SHA256: 847fb7609f53ed334d5affbb07256c21cb5e6f68b1cc14004f5502d714d2a456

Administrator: Administrator Command Prompt _ ::\Users\ \Desktop>malware.exe --help [OPTIONS] [SUBCOMMAND] PTIONS: 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 self propagate(worm) on Windows Do not stop VMs on ESXi 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 Run as propagated process Show user interface Log to console

The malware can run with one of the following parameters:

Figure 1

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



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

The binary registers a new top-level exception handler via a function call to SetUnhandledExceptionFilter:

×

ETP	● 00C51241 →● 00C51248	C7 04 24 A0 42 68 01 FF 15 4C 78 91 01	<pre>mov dword ptr ss:[esp],malware.16842A0 call dword ptr ds:[c&SetUnhandledExceptionFilter>]</pre>		275W 0 0 ¥275W 7	0 x 275W D 0
	• • • • • • • • • • • • • • • • • • • •	02 EC 04	euh aen 4	De	fault (stdcall)	▼ 5 € Unlock
dword ptr	[0191784C <malwa< td=""><td>are.&SetUnhandledException</td><td>nFilter>]=<kernel32.setunhandledexceptionfilter></kernel32.setunhandledexceptionfilter></td><td>2: 3: 4:</td><td>[esp+4] 00000002 [esp+8] 00000000 [esp+C] 00000000</td><td></td></malwa<>	are.&SetUnhandledException	nFilter>]= <kernel32.setunhandledexceptionfilter></kernel32.setunhandledexceptionfilter>	2: 3: 4:	[esp+4] 00000002 [esp+8] 00000000 [esp+C] 00000000	
.text:out	SI248 maiware.ext		005FFD00 01	6842A	0 malware.016B42A	0

The AddVectoredExceptionHandler API is utilized to register a vectored exception handler:

570	• 01641139 • 0164113E	68 <u>70</u> 6A 00	48 65 01	pu	sh malware.1 sh 0	165 4870		attend and		x875W_SF 0 x875W	P 0 x875W_U	0
	• 01641140 • 0164114E	00 00	C9 06 00	ta ta	et asv asv	RETADOVECE	oredexceptio	nhand i er >	> ×	Default (stdcall) 1: [esp] 00000000	▼ 5	🗘 🗌 Unlock
<malware.rt< th=""><th>1AddVectored</th><th>ExceptionHa</th><th>#9E0540</th><th></th><th></th><th></th><th></th><th></th><th></th><th>2: [esp+4] 0165487 3: [esp+8] 5FEA8A5 4: [esp+C] 00B728D</th><th>'O malware.0165 K K</th><th>4870</th></malware.rt<>	1AddVectored	ExceptionHa	#9E0540							2: [esp+4] 0165487 3: [esp+8] 5FEA8A5 4: [esp+C] 00B728D	'O malware.0165 K K	4870
. centrozora	240 marma er					1	d	005555084	00000	2000		
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	005FFC88	01654	4870 malware.016548	370	
Figure 4	4											

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

EIP → 01626499 01626495	E8 62 77 08 00 99 00 24 E4 92 01	call cmalware.GetCommandLineW>	>	Default (stdcall)
<pre><malware.getcommandlinew> .text:01626499 malware.exe</malware.getcommandlinew></pre>	e:\$9D6499 #9D5899			1: [csp+4] 005FF658 3: [csp+8] 76FE0000 ntd11.76FE0000 4: [csp+C] 00000070
Figure 5				1

Figure 5

BlackCat opens the "SOFTWARE\Microsoft\Cryptography" registry key by calling the RegOpenKeyExW routine (0x80000002 = HKEY_LOCAL_MACHINE, 0x20019 = KEY_READ):

ODEASCAF ODEASCB0 ODEASCB0 ODEASCB7 ODEASCB3 ODEASCB3	56 68 19 00 02 00 57 57 64 75 75 75 75 75 75 75 75 75 75 75 75 75	push esi push 20019 push edi mov ea,dword ptr ss:[ebp+C] push dword ptr ds:[eax] call -malware.RegopenkeyExw> mov bure otr de:FSEEXES: 3]	× >	x875tatusword 0000 x875w_B 0 x875w_C3 0 x875w_C2 0 x875w_S1C1 0 x875w_C0 0 x875w_E5 0 x875w_SF 0 x875w_P 0 x875w_U 0 v875w 0 0 v875w_P 0 x875w_U 0 Default(stdcall) 1: [esp] 80000002
<malware.regopenkeyexw> .text:00EA8CBD malware.exe</malware.regopenkeyexw>	2:\$258CBD #2580BD			2: [esp+4] 0074CD18 3: [esp+8] 0000000 4: [esp+C] 00020019
Dump 1 Dump 2	Dump 3 💭 Dump 4 💭 Dum	p 5 🛞 Watch 1 🕅 🖉 Struct	005FF0CC 80000 005FF0D0 00740	002 D18
Address Hex 0074CD18 53 00 4F 00 46 00 0074CD28 5C 00 00 69 00 0074CD28 5C 00 4D 00 69 00 0074CD28 5C 00 74 00 5C 00 0074CD28 6F 00 67 00 72 00	0 54 00 57 00 41 00 52 00 4 0 63 00 72 00 6F 00 73 00 6 43 00 72 00 79 00 70 00 7 0 61 00 70 00 68 00 79 00 0	ASCII 00 \.M.1.C.r.0.S.0. 00 \.M.1.C.r.0.S.0. 00 \.M.1.C.r.y.p.t. 00 00 (g.r.a.p.hy)	005FF0D4 00000 005FF0D8 00020 005FF0DC 005FF 005FF0E0 016F1 005FF0E4 016F1	0000 0019 0078 448 malware.016F1A48 1467 malware.016F1A67

Figure 6

The binary extracts the MachineGUID value from the registry:

• OOFAREGO 51 • OOFAREGI 50 • OOFAREGI 53 • OOFAREGI 54 • OOFAREGI 57 • OOFAREGI 56 •	push eck push eax push ebx push eb push ebi call <malware.regqueryvalueexw> call <malware.regqueryvalueexw> push esi</malware.regqueryvalueexw></malware.regqueryvalueexw>	>	x87Statusword 0000 x87Sw_B 0 x87Sw_C0 x87Sw_C1 0 x87Sw_C0 x87Sw_SF 0 x87Sw_P v87Sw 0 x87Sw_P v87Sw 0 x87Sw_P v87Sw 0 x87Sw_P v87Sw 0 0 x87Sw_P v87Sw_P v87Sw 0 x87Sw_P v87Sw 0 x87Sw_P v87Sw 0 x87Sw_P v87Sw 0 x87Sw_P v87Sw 0 x87Sw_P v87Sw 0 x87Sw_P x87Sw_P v87Sw 0 x87Sw_P x87Sw	0 x875₩_C2 0 0 x875₩_E5 0 0 x875₩_U 0 • x875₩_U 0 • x875₩ 0 • 5 ↓ Unlock
Image: Dump 1 Image: Dump 2 Image: Dump 3 Image: Dump 4 Image: Dump 4 Address Hex 0074CEE8 50 30 33 AB <	p5 Image: Constraint of the second sec	000000 0074C1 000000 005FF(007461 005FF(0074C1 000000 000000 000000 000000 000000 0000	254 F48 000 004 728 F48 004 F48 004 000 000 772 malware.016F1A72	

The malicious process searches for cmd.exe in the current directory and then in the System32 directory via a function call to CreateFileW (0x7 = FILE_SHARE_DELETE | FILE_SHARE_WRITE | FILE_SHARE_READ, 0x3 = OPEN_EXISTING, 0x2000000 = FILE_FLAG_BACKUP_SEMANTICS):

<pre></pre>	6A 00 57 FF 75 E8 FF 75 E4 FF 75 F0 88 70 EC 57 E8 0F 46 06 00 e9 c0 cc	push 0 push edi push dword ptr ss: ebp-18 push dword ptr ss: ebp-10 push dword ptr ss: ebp-10 mov edi, dword ptr ss: ebp-14 push edi call «malware.CreateFilew»	, , ,	x87Tw_6 3 (Empty) x x87Tw_6 3 (Empty) x x87StatusWord 0000 x87Sw_2 x87Stw_6 0 x87Sw_2 x87Sw_2 x87Sw_5 0 x87Sw_2 x87Sw_2 y27Sw_8 0 x87Sw_2 x87Sw_2 y27Sw_8 0 x87Sw_2 x87Sw_2 y27Sw_1 0 0 x87Sw_2 x87Sw_2 y27Sw_1 0 0 x87Sw_2 x82Sw_7 y28Sw_1 0 0 x82Sw_1 x82Sw_7 y28Sw_1 0 0 x82Sw_1 x82Sw_7 y28Sw_2 0 0 x82Sw_1 x82Sw_7 y28Sw_2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	orin_o s (Empty) 87TW_7 3 (Empty) 0 x87SW_C2 0 0 x87SW_ES 0 0 x87SW_U 0 0 x87
Dump 1 Em Dump 2	100 Dama 2 100 Dama 4 10	Dura 5 Match 1 (val) and 60 C	005FE958 007	48520 L"C:\\Users\\\\	Desktop\\cmd.exe"
e-e bump 1 e-e bump 2	ere bump 5 ere bump 4 e	Dump 5 Watch 1 IN-I Locals 2 5	005FE95C 000	00000	
Address Hex 005FEAOC 00 00 00 00 005FEAIC 20 00 00 00 22 005FEA2C 50 EA 5F 00 02 005FEA2C 00 00 00 00	0 00 00 00 70 CD 74 00 70 0 00 00 00 80 EF 5F 00 37 CD 74 00 88 CC 74 00 00	ASCII <u>F9 64 01</u>	OOSFE960 000 OOSFE964 000 OOSFE968 000 OOSFE968 000 OOSFE960 020 OOSFE970 000 OSFE970 OSFE970	00000 00003 00000 00000	

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 CreateNamedPipeW (0x40080001 = FILE_FLAG_OVERLAPPED | FILE_FLAG_FIRST_PIPE_INSTANCE | PIPE_ACCESS_INBOUND, 0x8 = PIPE_REJECT_REMOTE_CLIENTS):



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

<pre>malware.Cr .text:01649</pre>	01649508 01649508 01649502 01649502 01649512 01649513 01649518 01649518 01649518 01649518 01649518 eateFilew> s1c malware.e	6A 00 57 52 FF 75 FF 75 FF 75 8B 7D 57 E8 0F • 2 co	E8 F0 EC ee #9F891C	pu pu pu pu pu ca	sh 0 sh edi sh dword pt sh dword pt sh dword pt v edi,dword sh edi 11 <malware< th=""><th>r ss: ebp-1 r ss: ebp-1 r ss: ebp-1 ptr ss: eb CreateFile</th><th>8 0 0 0 14 1 8</th><th>_</th><th>></th><th>x87 x87 x87 x87 x87 x87 x87 x87 x87 x87</th><th>IN 3 (Empty) TW_6 3 (Empty) StatusWord 0000 SW_8 0 x87SW_C3 SW_C1 0 x87SW_C3 SW_C1 0 x87SW_C9 SW_5 0 x87SW_7 SW_5 0 x87SW_7 SW_5 0 x</th><th>x87TW_7 3 (Empty) 0 x87SW_C2 0 0 x87SW_C2 0 0 x87SW_ES 0 0 x87SW_U 0 0 x87SW_</th></malware<>	r ss: ebp-1 r ss: ebp-1 r ss: ebp-1 ptr ss: eb CreateFile	8 0 0 0 14 1 8	_	>	x87 x87 x87 x87 x87 x87 x87 x87 x87 x87	IN 3 (Empty) TW_6 3 (Empty) StatusWord 0000 SW_8 0 x87SW_C3 SW_C1 0 x87SW_C3 SW_C1 0 x87SW_C9 SW_5 0 x87SW_7 SW_5 0 x87SW_7 SW_5 0 x	x87TW_7 3 (Empty) 0 x87SW_C2 0 0 x87SW_C2 0 0 x87SW_ES 0 0 x87SW_U 0 0 x87SW_
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	🛞 Watch 1	[x=] Locals	2 Struct	005FE92	4 0074	CE58		
Address He 0074CE58 5C 0074CE68 5C	x 00 5C 00 2E 00 5F 00 5F	00 5C 00 00 72 00	70 00 69 00	70 00 65 00 74 00 5F 00	ASCII	i.p.e. s.t		005FE92 005FE93 005FE93 005FE93 005FE93	C 0000 0 005F 4 0000 8 0000	0000 E9A4 0003		
0074CE78 61 0074CE88 73 0074CE98 5F 0074CE88 35	00 6E 00 6F 00 5F 00 70 00 2E 00 31 00 34 00 32	00 6E 00 00 69 00 00 32 00 00 31 00 E0 40 84	79 00 6D 00 70 00 65 00 38 00 34 00 33 00 33 00 AB AB AB AB	6F 00 75 00 31 00 5F 00 2E 00 32 00 31 00 37 00 AB AB AB AB	a.n.o.n.y. sp.i.p. 1.2.8. 5.4.2.1.3.	m.o.u. e.1 42. 3.1.7.		005FE93 005FE94 005FE94 005FE94	C 0000 0 0000 4 0074 8 0000	0000 0000 CE58 0034		
Figure '	11	FU AD BA	TO TO AD AD	NO NO NO NO	50. *««	ananag		I OULEEDA	- 10000	0022		

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):

<pre></pre>	51 52 FF 74 24 10 00 00 00 FF 74 24 14 01 00 00 6A 00 6A 00 6A 00 FF 84 24 44 01 00 00 6A 00 6A 00 6A 00 50 8A 30 105 00 8C CO	<pre>push ecx push dword ptr ss: esp+80 push dword ptr ss: esp+12 push dword ptr ss: esp+141 push 1 push 0 push 0 push dword ptr ss:[esp+E4] push eax call amalware.CreateProcessw> tart asy asy</pre>	• •	x87TW_2 3 (Empty) x87TW_3 3 (Empty) x87TW_4 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87SW_5 0 x87SW_C3 0 x87SW_C2 0 x87SW_5 0 x87SW_5
Dump 1 Dump 2	Dump 3 🔛 Dump 4 🔛	Dump 5 💮 Watch 1 🛛 🗐 Locals 🖉 Struct	005FEA08 00748 005FEA0C 00748	298 L"C:\\WINDOWS\\system32\\cmd.exe" 520 L"\"C:\\WINDOWS\\system32\\cmd.exe\" /c
Address Hex 00748520 22 00 43 00 3A 0C 00748530 4F 00 57 00 53 0C 0C	5C 00 57 00 49 00 4E 0 5C 00 73 00 79 00 73 32 00 5C 00 63 00 60 60 65 00 52 00 20 00 26 60 60 60 60 60 63 00 20 63 00 20 63 00 50 63 00 50 63 00	ASCII A 00 44 00 [h.c.t.], W.I.N.D. 10 74 00 [0.W.S.], S.Y.S.T. 00 64 00 [w.m.3.2.], C.m.d. 00 63 00 e.x.e.", /.C. 00 63 00 e.x.e.", /.C. 00 74 00 S.p.r.o.d.u.c.t. 00 74 00 S.p.r.o.d.u.c.t.	005FEA14 00000 005FEA14 00000 005FEA12 08000 005FEA20 00000 005FEA24 00000 005FEA24 005FE 005FEA2C 005FE	000 001 001 000 000 000 BLC ACO

Figure 12

The CreateEventW API is utilized to create two unnamed event objects:

Image: State of the state	Address H	ex	BE 33 001			ASCII			^	005FEED8 0	0000	0001				
Imalware.CreateEventW> Imalware.createEventW> Imalware.createEventW> .text:0163E09F malware.exe:\$9E09F #9ED49F Imalware.createEventW>	Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	🛞 Watch 1	[x=] Locals	2 Struct		005FEED0 00 005FEED4 00	0000	0000				
	<pre>malware.Cr .text:01638</pre>	● 0163E099 ● 0163E099 ● 0163E09D ● 0163E09	6A 01 6A 01 6A 01 E8 7C 85 C0 exe:\$9EE09	FA 06 00 F #9ED49F		ush 1 ush 1 all <malware.< td=""><td>CreateEven</td><td>tw></td><td>_</td><td>></td><td></td><td>x87SW_C1 x87SW_SF x87SW_O Default (stdca 1: [esp] 2: [esp+4 3: [esp+8 4: [esp+C</td><td>0 x875W_C0 0 x875W_P 0 x875W_7 0 0000000 00000000 00000000 00000000 00000</td><td>0</td><td>×87SW_E ×87SW_U ×87SW_D</td><td>S 0 O Unlod</td></malware.<>	CreateEven	tw>	_	>		x87SW_C1 x87SW_SF x87SW_O Default (stdca 1: [esp] 2: [esp+4 3: [esp+8 4: [esp+C	0 x875W_C0 0 x875W_P 0 x875W_7 0 0000000 00000000 00000000 00000000 00000	0	×87SW_E ×87SW_U ×87SW_D	S 0 O Unlod

Figure 13

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

	 0163E180 0163E182 0163E184 0163E185 0163E187 0163E187 (6A FF 6A 00 57 6A 02 E8 34 07 50	FD 06 00	pu pu ca	ish FFFFFFF ish 0 ish edi ish 2 ish 2 ish 2 ish 2 ish 2 ish 2 ish 2 ish 3 ish 5 ish 6 ish 6 ish 6 ish 6 ish 7 ish 7 ish 0 ish 8 ish 0 ish 8 ish 0 ish 10 ish	WaitForMul	tipleObjects	>		~	x875W_B 0 x875W_C1 0 x875W_SF 0 x875W_O 0 Default (stdcall)	x875W_C3 x875W_C0 x875W_P x875W_P	0	x875W_C: x875W_E: x875W_U x875W_U	2 0 5 0 0
<malware.wai< th=""><th>tForMultipl .87 malware.</th><th>leObjects> .exe:\$9EE187</th><th>#9ED587</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>2: [esp+4] 3: [esp+8] 4: [esp+C]</th><th>005FEEF8 00000000 FFFFFFF</th><th></th><th></th><th></th></malware.wai<>	tForMultipl .87 malware.	leObjects> .exe:\$9EE187	#9ED587								2: [esp+4] 3: [esp+8] 4: [esp+C]	005FEEF8 00000000 FFFFFFF			
Dump 1	Dump 2	Dump 3	Dump 4	📖 Dump 5	Watch 1	[x=] Locals	Struct	005FE	EDO (ED4 (ED8 (00000 005FE	002 EF8 000				
005FEEF8 54	02 00 00 60	0 02 00 00 0	54 02 00 00	60 02 00 00	Td			00555	EDC I	FFFFF	FFF				

Figure 14

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

01640E84 51 pp 01640E85 53 pp 01640E85 52 pp 01640E87 52 pp 01640E87 FF 37 pp 01640E88 FF 37 pp 01640	ish eck ish edk ish edk ish eak ish dword ptr ds:[edi] ish dword ptr ds:[edi] ish dword ptr ds:[edi] ish exp	X8/STACUSWORD UUUU X8/STAL 0 X875W_C3 0 X875W_C2 0 X8/SW_C1 0 X875W_C0 0 X875W_E5 0 X8/SW_STAC 0 X875W_U 0 X8
<malware.readfile> .text:0164DE8A malware.exe:\$9FDE8A #9FD28A</malware.readfile>		2: [esp+4] 0074CE88 3: [esp+8] 0000010 4: [esp+C] 005FEEA4
💭 Dump 1 💭 Dump 2 💭 Dump 3 💭 Dump 4 👹 Dump 5	Watch 1 [x=] Locals Ø Struct Ø SFEE90	0000025C 0074CE88
Address Hex	ASCII 005FEE94	00000010
0074CE88 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA		005FEEA4 return to 005FEEA4 from 005FEF1D
Address Hex	ASCII	00740070
00748520 55 55 49 44 20 20 20 20 20 20 20 20 20 20 20 20 20	UUID50F04D5	

Figure 15

The malware creates multiple threads by calling the CreateThread function (0x00010000 = **STACK_SIZE_PARAM_IS_A_RESERVATION**):

	6A 00 68 00 00 01 00 56 68 <u>30 24 65 01</u> 52 6A 00 E8 D9 B7 05 00 ** \$A0238A #A0178A	push 0 push 10000 push esi push malware.1652430 push edx push 0 call emalware.CreateThread>		>	x875tatusWord 0000 x875W_B 0 x875W_C2 0 x875W_C2 0 x875W_C1 0 x875W_C0 0 x875W_E5 0 x875W_SF 0 x875W_P 0 x875W_U 0 v875W 0 v875W_P 0 x875W_U 0 Default (stdcal) ▼ 5 □ Unlock 1: [esp] 00000000 2: [esp+4] 0020000 3: [esp+4] 0020000 4: [esp+c] 0074A790
Dump 1 Dump 2	Dump 3 Dump 4 Dump 5	🛞 Watch 1 🛛 🛛 🖉	Struct 005FF3BC	00000	000
Address Hex		ASCII	005FF3C4	01652	430 malware.01652430
005FF4BC 00 00 00 00 C8 F4	4 5F 00 80 8C 74 00 48 A6 74 0	00ÈÔt.H't.	005FF3C8	0074A	000
005FF4CC 07 00 00 00 68 A	5 74 00 68 A6 74 00 00 00 20 0	00h't.h't	005FF3D0	00000	000
Figure 16					

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

Address	Нех								ASCII
0074CF48	3E 3E	20 57	68 61	74 20	68 61	70 70	65 6E	65 64	>> What happened
0074CF58	3F OA	0A 49	6D 70	6F 72	74 61	6E 74	20 66	69 6C	?Important fil
0074CF68	65 73	20 GF	6E 20	79 GF	75 72	20 GE	65 74	77 GF	es on your netwo
0074CF78	72 GB	20 77	61 73	20 45	4E 43	52 59	50 54	45 44	rk was ENCRYPTED
0074CF88	20 61	6E 64	20 GE	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 GE	73 69	GF GE	ZE OA	49 GE	20 GF	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 60	65 73	20 79	6F 75	20 GE	65 65	64 20	Tiles you need
0074CFD8	74 GF	20 66	OF OC	6C 6F	65 66	69 6E	75 74	12 /5	ctions balow
00740768	25 20	69 6F	GE 73	60 74	60 7C	GF 77	2E UA	74 61	Sensitive Data
00740008	04 04	53 65	GE 72	69 74	69 76	65 20	64 61	74 61	Sensitive data
00740018	20 65	6F 20	79 65	75 72	20 65	65 74	77 65	72 68	on your network
00740028	20 77	61 73	20 44	4F 57	4F 4C	4F 41	44 45	44 2F	Was DOWNLOADED.
0074D038	0A 49	66 20	79 6F	75 20	44 4F	4F 27	54 20	57 41	IT 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 vou have
Figure 1	7								
Address	Hex								ASCII
0074AA98	49 60	70 6	F 72 74	61 GE	74 20	66 69	9 6C 65	5 73 20	Important files
0074AAA8	6F 68	E 20 7	9 6F 75	72 20	6E 65	74 77	6F 72	2 6B 20	on your network
0074AAB8	77 61	L 73 2	0 44 4F	57 4E	4C 4F	41 44	4 45 44	4 20 61	Was DOWNLOADED a
0074AAC8	6E 64	1 20 4	5 4E 43	52 59	50 54	4 45 44	1 2E 0/	4 53 65	nd ENCRYPTEDSe
0074AAD8	65 20	22 5	2 45 43	4F 56	45 52	2 2D 75	68 77	7 75 76	e "RECOVER-uhwuv
0074AAE8	7A 75	5 2D 4	6 49 40	45 53	2E 74	78 74	22 20	0 66 69	Zu-FILES.txt" fi
0074AAF8	6C 65	20 7	4 6F 20	67 65	74 20	66 75	72 74	4 68 65	le to get furthe
0074AB08	72 20	69 6	E 73 74	72 75	63 74	69 68	6E 73	3 2E AE	r instructions.«
Figure 1	8								

The malicious binary obtains information about the current system via a function call to GetSystemInfo:

• 0146847F	50	push eax		V075W 0 0 V075W 7	0 V875W D 0
	DO CC		>	Default (stdcall)	▼ 5 🖶 🗌 Unlock
<malware.getsysteminfo> .text:01468480 malware.ex</malware.getsysteminfo>	(e:\$81B480 #81A880			2: [esp+4] 0000000 3: [esp+8] 0000000 4: [esp+C] 0000000	
	anana	m6)	005FF4AC 005F	F4B0	

Figure 19

There is a call to SHTestTokenMembership that verifies whether the user token is a member of the Administrators group in the built-in domain (0x220 = **DOMAIN_ALIAS_RID_ADMINS**):

EIP	● 00D 80 301 00D 80 306 ● 00D 80 308 ● 00D 80 308 <	68 20 6A 00 E8 7B I	02 00 00 07 92 00 10 65 01		sh 220 sh 0 11 <malware V bb bute of</malware 	SHTestToke	nMembership>	>	~	x875W_SF_0_x875W_P x875W_0_0_x875W_7 Default (stdcall)	0 x875₩_U	0 Unlock
<malware.sh< th=""><th>TestTokenMemb</th><th>ership> exe:\$130308</th><th>#12F708</th><th></th><th></th><th></th><th></th><th></th><th></th><th>1: [esp] 00000000 2: [esp+4] 00000220 3: [esp+8] 0000000 4: [esp+C] 00000070</th><th></th><th></th></malware.sh<>	TestTokenMemb	ership> exe:\$130308	#12F708							1: [esp] 00000000 2: [esp+4] 00000220 3: [esp+8] 0000000 4: [esp+C] 00000070		
Bump 1 Figure 2	Dump 2	Dump 3	Ump 4	Dump 5	🛞 Watch 1	[x=] Locals	Struct	005FF450 00 005FF454 00	0000	20		

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

EIP	 00D7D43C 00D7D43D 00D7D43D 00D7D442 00D7D444 00D7D444 	50 68 00 6A FF E8 3F 66 45	00 00 80 05 93 00		ish eax ish 80000000 ish FFFFFFF all <malware.< th=""><th>ZwOpenProc</th><th>essToken></th><th></th><th>~</th><th>x879 x879 x879</th><th>SW_C1 0 SW_SF 0 SW 0 0</th><th>x87SW_C0 x87SW_P x87SW_7</th><th>0</th><th>x87SW_ES x87SW_U v87SW_D</th><th>0 0 0 0 0</th></malware.<>	ZwOpenProc	essToken>		~	x879 x879 x879	SW_C1 0 SW_SF 0 SW 0 0	x87SW_C0 x87SW_P x87SW_7	0	x87SW_ES x87SW_U v87SW_D	0 0 0 0 0
<malware.zw< td=""><td>OpenProcess</td><td>Foken> .exe:\$12D444</td><td>4 #12C844</td><td></td><td></td><td></td><td></td><td></td><td>,</td><td>1: [2: [3: [4: [</td><td>esp] FF esp+4] esp+8] esp+C]</td><td>FFFFF 80000000 005FF418 00000000</td><td></td><td></td><td></td></malware.zw<>	OpenProcess	Foken> .exe:\$12D444	4 #12C844						,	1: [2: [3: [4: [esp] FF esp+4] esp+8] esp+C]	FFFFF 80000000 005FF418 00000000			
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	005FF400 005FF404	FFFF	FFFF 0000					
Address He	ev.				ASCIT			005FF408	005 FI	F418					

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

0007D4D6 0007D407 0007D409 0007D409 0007D409 0007D40B 0007D40B 0007D40B 0007D40B 0007D40B	56 00 p 6A 00 p 6A 02 p 57 p p 58 90 04 93 00	ush esi ush 0 ush 0 ush 2 ush 2 ush 2 i all malware.NtQueryInformationToke mp exy CODD022	n> v	x875tatusword 0000 x875w_B 0 x875w_C3 x875w_C10 x875w_C0 x875w_SF 0 x875w_P verse 0 verse 7 Default (stdcall)	0 x875W_C2 0 0 x875W_ES 0 0 x875W_U 0 0 x875W_D 0
<malware.ntqueryinformatio< th=""><th>nToken> :\$12D4DE #12C8DE</th><th></th><th></th><th>2: [esp+4] 00000002 3: [esp+8] 0000000 4: [esp+C] 0000000</th><th></th></malware.ntqueryinformatio<>	nToken> :\$12D4DE #12C8DE			2: [esp+4] 00000002 3: [esp+8] 0000000 4: [esp+C] 0000000	
Dump 1 Dump 2	Dump 3 💭 Dump 4 💭 Dump 5	🥮 Watch 1 🛛 🕼 🖉 Struct	005FF3F8 0000 005FF3FC 0000	0260	
Address Hex 005FF434 00 00 00 00 01 00	00 00 00 00 00 00 00 05 96 2	ASCII ,	005FF400 0000 005FF404 0000 005FF408 005F	00000 00000 F434	
Figure 22					

The OpenProcess API is utilized to open a local process object (0x438 =

PROCESS_QUERY_INFORMATION | PROCESS_VM_WRITE | PROCESS_VM_READ | PROCESS_VM_OPERATION):

EIP	• 01684CE1 • 01684CE2 • 01684CE4 • 01684CE4 • 01684CE5 • 01684CE5	50 6A 00 68 38 FF 15	04 00 00 E4 77 91 01		ish eax ish 0 ish 438 iii dword ptr	n ds:[<mark><&Ope</mark>	nProcess>]	_	>	V De	375W_C1 0 375W_SF 0 75W 0 0	x875W_C0 x875W_P	0	x87SW_ES x87SW_U x87SW_D	Unlock
dword ptr (019177E4 <m< td=""><td>alware.&Oper</td><td>nProcess>]=<</td><td>kerne132.0p</td><td>enProcess></td><td></td><td></td><td></td><td></td><td>1: 2: 3: 4:</td><td>[esp+4] [esp+8] [esp+C]</td><td>0000438 000000000 00000504 40000163</td><td></td><td></td><td></td></m<>	alware.&Oper	nProcess>]=<	kerne132.0p	enProcess>					1: 2: 3: 4:	[esp+4] [esp+8] [esp+C]	0000438 000000000 00000504 40000163			
.text:01684	ces maiware	exe: SA64CE	9 #A640E9												
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	005 FED	DC 00	00043	8				
Address H	PV				ASCTT			_ 005FED	E4 00	00050	4				

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:

	push 0 push 4 push ecx push eax push ebp call dword ptr ds:[<&ReadProcessMemory>] eart asy ell32.ReadProcessMemory>	x8/>tratusword UUUU x8/STw_E 0 x87Sw_C2 0 x87Sw_C2 0 x87Sw_C1 0 x87Sw_C0 0 x87Sw_E5 0 x87Sw_C1 0 x87Sw_C 0 x87Sw_U 0 verse 0 x87Sw_U 0 x87Sw_U 0 verse 0 x87Sw_U 0 x87Sw_U 0 verse 0 x87Sw_U 0 x87Sw_U 0 verse 1 x 0 x87Sw_U 0 x87Sw_U 0 x87Sw_U 0 verse 1 x 0 x87Sw_U 0
Image: Second state Image: Second state	Watch 1 [x=] Locals Struct ODSFEDD4 005FEDD2 ASCII ASCII 005FEDD0 005FEDD0 D	0000025C 005FEBC 0005FEB8 00000004
	b a b a	0000000

Figure 25

EIP	● 01684D45 ● 01684D47 ● 01684D49 ● 01684D4A ● 01684D48 ● 01684D48 ● 01684D42 ● 01684D42 ● 01684D42 ● 01684D42	6A 00 6A 04 51 50 55 FF 15	04 78 91 01	pu pu pu ca	sh 0 sh 4 sh ecx sh eax sh ebp 11 dword ptr	ds: [<&Read	ProcessMemo	ry>]	>	x875tatusW x875W_B 0 x875W_C1 0 x875W_SF 0 x875W_SF 0 Default (stdcall)	00025C	0000	x87SW_C2 x87SW_ES x87SW_U x87SW_U	0 0 0 0
dword ptr	[01917804 <ma 34D4C malware.</ma 	alware.&Read	ProcessMemo	ry>]= <kernel< th=""><th>32.ReadProc</th><th>essMemory></th><th></th><th></th><th></th><th>2: [esp+4] 3: [esp+8] 4: [esp+C]</th><th>002A800C 005FEE04 00000004</th><th></th><th></th><th></th></kernel<>	32.ReadProc	essMemory>				2: [esp+4] 3: [esp+8] 4: [esp+C]	002A800C 005FEE04 00000004			
Dump 1	Dump 2	💭 Dump 3	💭 Dump 4	💷 Dump 5	Watch 1	[x=] Locals	Struct	005 FEDD 4 005 FEDD 8 005 FEDDC	00000 002A 005F	025C 800C EE04				
002A800C	EO 78 OF 77 48	3 1D 73 00	00 00 00 00	00 00 73 00	a{.wH.s			005FEDE0 005FEDE4	0000	0004				
Figure	26													

The path of the image file for the current process is retrieved using ReadProcessMemory:



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 ColnitializeEx (0x2 = COINIT_APARTMENTTHREADED):

	 016B5422 016B5424 	6A 02 6A 00		pus	h 2 h 0			_		x875W_SF 0 x875W_F	0 x875W_0	0
BIB	01685426 01605470	FF 15 7	70 76 91 01	Ca mov	dword pt	ds:[<&COI	nitializeEx>		~	Default (stdcall)	- 5	Unlock
dword ptr	[01917670 <ma< td=""><td>lware.&CoIn</td><td>itializeEx>1</td><td>=<combase.c< td=""><td>oInitialize</td><td>Ex></td><td></td><td>,</td><td>-1</td><td>1: [esp] 00000000 2: [esp+4] 00000002</td><td></td><td></td></combase.c<></td></ma<>	lware.&CoIn	itializeEx>1	= <combase.c< td=""><td>oInitialize</td><td>Ex></td><td></td><td>,</td><td>-1</td><td>1: [esp] 00000000 2: [esp+4] 00000002</td><td></td><td></td></combase.c<>	oInitialize	Ex>		,	-1	1: [esp] 00000000 2: [esp+4] 00000002		
										3: [esp+8] 00000000 4: [esp+6] 00758600	L"C .\\Usars\	
.text:010	585426 malware.	exe: \$A65426	#A64826					<u> </u>		4. [esp+c]_00/38600	L C. ((05815)	(Deski
Ump :	1 Dump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	005FF3F0 00 005FF3F4 00	0000	000		
Figure	28											

Figure 28

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

016853DF 50 016853DF 53 016853E0 51 016853E1 55 016853E1 55 016853E1 55 016853E1 55 016853E1 56 016853E2 65 400rd ptr [0191766c <malware.&cogetobject>]=<01832.CoGet .text:016853E2 malware.exe:\$A653E2 #A647E2</malware.&cogetobject>	bush eax bush eax bush eax bush ebx bush ebp dep dep des:[cacogetObject>] how ary dword or referenced tobject>	*	x875w_E0 0 x875w_C1 0 x875w_C2 0 x875w_C1 0 x875w_C2 0 x875w_C5 0 x875w_F0 x875w_F1 x875w_U 0 x875w_U 0 x875w_F1 x875w_U 0 x875w_U 0 0 v875w_F1 x875w_U 0 x875w_U 0 v875w_F1 005FF1CC L"Elevation:Administrator 2: esp+4 005FF1A4 1: esp1 0184F3F4 malware.0184F3F4 4: esp+C 005FF1C8
Ump 1 Ump 2 Ump 3 Ump 4 Ump 5 Address Hex 005FF1CC 145 00 67 00 51 00 74 00 69 06 60 65 00 65 00 74 00 69 06 60 65 00 65 00 74 00 69 00 65 00 65 00 74 00 69 00 65 00 50 00 74 00 69 00 65 00 50 00 74 00 69 00 65 00 50 00 70 04 00 70 04 00 30 04 50 00 50 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Watch 1 [x=]Locals D Struct ASCII 0 E.1.e.v.a.t.1.o. • 0 E.1.e.v.a.t.1.o. • • 0 S.t.r.a.t.o.r.l. • • 0 • • • • 0 • • • • 0 • • • • 0 • • • • 0 • • • • 0 •	005FF194 005F 005FF198 005F 005FF198 005F 005FF196 005FF196 0000 005FF196 0000 005FF196 0000 005FF196 0000 005FF196 0000 005FF196 0000	TICC L"Elevation:Administrator:new:{3E5FC7F5 1A4 1A5F malware.0184F3F4 1C8 0024 0000 0000 0000 0000 0000

Figure 29

The initial executable is spawned with administrative privileges:

edi= <cmlua.0bjectstubless< th=""><th>6A 05 6A 00 50 51 52 55 FF D7 66 77 Client9> (6C817190)</th><th>push 5 push eax push eax push eax push edx push edx call edx</th><th></th><th>></th><th>x87StatusWord 0020 x87Sw_E1 0 x87Sw_E2 0 x87Sw_E5 0 x87Sw_F0 x87Sw_P 1 x87Sw_E0 0 x87Sw_F1 0 x87Sw_P 1 x87Sw_D 0 x87Sw_F2 0 x87Sw_P 1 x87Sw_D 0 x85Sw_F2 0 x87Sw_P 1 x87Sw_D 0 x85Sw_F2 0 x75S808 L"C:\Users\\\Deskt x85Sw_F2 0 x75S808 L"C:\Users\\\Deskt</th></cmlua.0bjectstubless<>	6A 05 6A 00 50 51 52 55 FF D7 66 77 Client9> (6C817190)	push 5 push eax push eax push eax push edx push edx call edx		>	x87StatusWord 0020 x87Sw_E1 0 x87Sw_E2 0 x87Sw_E5 0 x87Sw_F0 x87Sw_P 1 x87Sw_E0 0 x87Sw_F1 0 x87Sw_P 1 x87Sw_D 0 x87Sw_F2 0 x87Sw_P 1 x87Sw_D 0 x85Sw_F2 0 x87Sw_P 1 x87Sw_D 0 x85Sw_F2 0 x75S808 L"C:\Users\\\Deskt x85Sw_F2 0 x75S808 L"C:\Users\\\Deskt
Address Hex 005FF1C8 FC 3C 77 00 45 0 005FF1C8 FC 3C 77 00 45 0 005FF108 69 00 6F 00 6E 0 Figure 30	Dump 3 Dump 4 Dump 4 Dump 4 Dump 3 Dump 4 Du	mp 5 🛞 Watch 1 x= Locals ASCII 74 00 Ūdv.E.l.e.v.a.t. 69 00 1.0.n.:.A.d.m.i.	Ø05FF3E0 005FF3E0 005FF3E0 005FF3E0 005FF3E0 005FF3E0 005FF3F0 005FF3F0 005FF3F4	007736 00756 00758 00758 00758 000000	<pre>IFC L"C:\\Users\\\\Desktop\\malware.exe" S08 L"\"access-token\" \"cd29cb89daed9e2f S00 L"C:\\Users\\\\Desktop" 000 005</pre>

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 SeImpersonatePrivilege SeCreateGlobalPrivilege
- SeIncreaseWorkingSetPrivilege SeTimeZonePrivilege
- SeCreateSymbolicLinkPrivilege SeDelegateSessionUserImpersonatePrivilege

<pre><malware.log .text:00d7e<="" pre=""></malware.log></pre>	CE malware.ex	valuew> xe:\$12E2CE	#12D6CE					>	Default (stdcall) ▼ [5] 1: [esp] 000000000 2: [esp+4] 0075DE88 L"SeIncreaseQuo 3: [esp+4] 005FF498 4: [esp+C] 000000C0	L Unlock
	00D7E2CA 00D7E2CB 00D7E2CC 00D7E2CC 00D7E2CE 00D7E2CE	50 56 6A 00 E8 E5	FC 92 00	push push push call	eax esi 0 <malware.< td=""><td>LookupPriv</td><td>ilegeValueW></td><td></td><td>x875W_C1 0 x875W_C0 0 x875W_E5 x875W_5F 0 x875W_P 0 x875W_U x875W 0 x875W 0 x875W 0</td><td></td></malware.<>	LookupPriv	ilegeValueW>		x875W_C1 0 x875W_C0 0 x875W_E5 x875W_5F 0 x875W_P 0 x875W_U x875W 0 x875W 0 x875W 0	

Figure 31

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

<pre></pre>	push 0 push 10 push 12 push ex push eax call cmalware.AdjustTokenPrivileges>	x875tatusWord 0000 x875W_E8 0 x875W_C3 0 x875W_C2 0 x875W_C1 0 x875W_C0 0 x875W_E5 0 x875W_C1 0 x875W_C 0 x875W_U 0 v875W_0 0 v875W_0 0 Default (stdcall) v 5 0 Unloch 1: [esp1 0000028C 2: [esp+4] 0000000 3: [esp+4] 0005FF4A0 4: [esp+C] 0000010
💭 Dump 1 💭 Dump 2 💭 Dump 3 💭 Dump 4 💭	Dump 5 🛞 Watch 1 🛛 🖉 Struct	005FF448 0000028C 005FF44C 00000000
Address Hex	ASCII	005FF450 005FF4A0
005FF4A0 01 00 00 00 05 00 00 00 00 00 00 00 02 00	00 00	005FF458 0000000
		005FF45C 00000000

Figure 32

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

	x87TW_2 3 (Empty) x87TW_3 3 (Empty) x87TW_4 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87SW_6 0 x87SW_20 0 x87SW_20 0 x87SW_5 0 x87SW_20 0 x87SW_20 0 x87SW_5 0 x87SW_7 0 x87SW_0 0 x87SW_0 0 x87SW_0 0 x87SW_5 0 x87SW_7 0 x87SW_0 0 x87SW_0 0 x87SW_5 0 x87SW_0 0 x87SW_0 0 x87SW_0 0 x87SW_5 0 x87SW_1 0 x87SW_0 0 x87SW_0 0 x1 [sps+8] 00760785 L"'C'\WINDOWS\\system x87SV_system x1 [sps+8] 00000000 x87SW_0 0 x1 [sps+8] 00000000 x87SW_1 0 x1 [sps+8] 00000000 x87SW_1 0
💭 Dump 1 💭 Dump 2 💭 Dump 3 💭 Dump 4 💭 Dump 5 🧐 Watch 1 💷 Locals 🖉 Struct 005FEE93 0	0760880 L"C:\\WINDOWS\\system32\\cmd.exe" 0760798 L"\"C:\\WINDOWS\\system32\\cmd.exe\" /c
Address Hex ASCII O05FEEA0 0005FEEA0 0005FEEA0 </td <td>0000000 0000000 0000000 0000000 0000000</td>	0000000 0000000 0000000 0000000 0000000
00760818 6 <u>C 00 75 00 61 00 74 00</u> 69 00 6F 00 6E 00 20 00 1.u.a.t.1.o.n 00760828 52 00 32 00 4C 00 3A 00 31 00 22 00 00 0A DBA R.2.L.:.1."	075E4C0
Figure 33	
0165098E 51 push ecx 0165098F 52 push ecx 01650990 FF 84 24 80 00 00 00 01650990 FF 74 24 1C push dword ptr ss: esp+80 01650998 FF 74 24 1C push dword ptr ss: esp+1C 01650990 FF 74 24 1C push dword ptr ss: esp+1C 0165094 6A 01 push 0 01650945 6A 00 push 0 01650945 6A 00 push 0 01650945 6A 00 push 0 01650946 6A 00 push 0 01650947 9E 6A 21 05 00 push 0 01650948 FB 4 24 E4 00 00 00 push 0 01650947 9E 6A push 0 01650948 FB 4 24 E4 00 00 00 push 0 01650947 9E 6A push 0 016509480 9E 6A push 0 01650950 9E 6A push 0 016509480 9E 6A push 0 01650950 9E 6A push 0 01650950 9E 6A 10 50 0 016509480 9E 6A 10 50 0 0	x87TW_2 3 (Empty) x87TW_3 3 (Empty) x87TW_4 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87STL x87SW_C1 0 x87SW_C2 0 x87SW_5 0 x87SW_C0 0 x87SW_E 0 x87SW_10 0 x87SW_5 0 x87SW_0 x87SW_10 0 x87SW_10 0 x87SW_2 0 x87SW_10 0 x87SW_10 0 x87SW_10 0 x87SW_10 0 x87SW_10 0 x87SW_10 0 x87SSW_10 0 x87SW_10 0 x87SW_10 0 <td< td=""></td<>
Dump 1 1 Dump 2 1 Dump 2 1 Dump 4 1 Dump 5 1 Withh 1 (valiance 9 Struct 005FEE98 0	075E4B8 L"C:\\WINDOWS\\system32\\cmd.exe"
Address Hex Ascri Ascr Ascri Ascri	0760798 L"\"C:\\WINDOWS\\system32\\cmd.exe\" /0 00000000 00000000 00000000 00000000 0000

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

<pre></pre>	51 52 FF 84 24 80 00 00 00 FF 74 24 1C FF 84 24 44 01 00 00 6A 00 6A 00 6F 04 24 E4 00 00 00 50 55 54 54 54 55 55 55 55 55 55	push ecx push dword ptr ss: esp+80 push dword ptr ss: esp+10 push dword ptr ss: esp+141 push 1 push 0 push 0 push dword ptr ss: esp+E4 push eax call cmalware.CreateProcessw> tert eav eav	*	x87TW_2 3 (Empty) x87TW_3 3 (Empty) x87TW_4 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87SW_5 0 x87SW_5 0 x87SW_5 0 x87SW_5 0 x87SW_5 0 x87SW_2 0 x87SW_5 0 x87SW_2 0 x87SW_5 0 x87SW_2 0 x87SW_5 0 x87SW_0 0 x87SW_5 0
💭 Dump 1 💭 Dump 2 💭 I	Dump 3 💭 Dump 4 💭 Dump	p 5 🛞 Watch 1 🛛 🕅 🖉 Struct	005FEE98 0076 005FEE9C 0076	28D8 L"C:\\WINDOWS\\system32\\cmd.exe" 2840 L"\"C:\\WINDOWS\\system32\\cmd.exe\" /c
Address Hex 00762840 22 00 43 00 3A 00 00762850 65 00 00 53 00 00762850 25 00 50 07 83 00 00762850 25 00 60 07 80 07 00 <	SC 00 57 00 49 00 4E 00 73 00 74 00 73 00 73 00 73 00 73 00 73 00 73 00 73 00 74 00 73 00 74 00 74 00 74 00 73 00 73 00 72 00 73 00 70 00 20 00 27 00 00 00 00 00 76 00 73 00 70 00 70 00 20 00 20 00 20 00 21 00 00 00 00 00 00 70 42 20 20 21 20 21 20 21 20 21 21 21 21 21 21 21 21 21 21 21 21 21 21 21 21 21<	ASCII 000 T.C.:.\W.I.N.D. 000 O.W.S.\.S.Y.S.T. 000 e.m.3.2.\.C.m.d. 00e.x.e."/.C. 00".1.1.S.r.e.S. 00 e.te.x.e/. BA 5.t.o.p."	▲ 005FEEA0 0000 005FEEA4 0000 005FEEA8 0000 005FEEA0 0000 005FEEB0 0000 005FEEB4 0000 005FEEB8 005F 005FEEBC 005F	0000 0000 0001 0400 0000 0000 EFAC EFS0

Figure 35

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

	0165098E 01650990 01650990 01650990 01650998 01650982 01650984 01650984 01650984 01650985 01650985 01650985 01650985	51 52 FF 74 24 80 00 FF 74 24 1C FF 74 24 1C GA 01 GA 00 FF 84 24 44 01 GA 00 FF 84 24 E4 00 50 E8 A3 D1 05 00 er 0	push push push push push push push push	ecx edx dword ptr ss: dword ptr ss: 1 0 dword ptr ss: eax eax eax eax eax eax	esp+80 esp+1C esp+144 esp+144 esp+E4 ateProcessw>		> ~	x87TW_2 3 x87TW_4 3 x87TW_6 3 x87TW_6 3 x87Statusw x87SW_B 0 x87SW_C1 0 x87SW_C1 0 x87SW_C1 0 x87SW_SF 0 x87SW	(Empty) ((Empty) ((Empty) ((Empty) ((Empty) (x875W_C0 (x875W_P (x875W	0 x875w_2 (Empty 877w_3 (Empty 877w_7 3 (Empty 0 x875w_C2 0 0 x875w_ES 0 0 x875w_ES 0 0 x875w_U 0 0 x875w_U 0 x875w_U 1 x y y y y y y y y y y y y y y y y y y))) Unlock :em32\\
kind Iware. creat	errocesswa							2: [esp+4] 3: [esp+8]	00762850 L 00000000	"\"C:\\WINDOWS\\	system
.text:01650980	malware.exe:	\$A009B0 #9FFDB0						4: [esp+c]	0000000		
Dump 1	Dump 2	Dump 3 🛛 💭 Dump 4	Dump 5	🖲 Watch 1 🛛 🛛 🕅	Locals 🖉 Struct	005FEE68 005FEE6C	007629	968 L"C:\\ 350 L"\"C:	WINDOWS\\sy \\WINDOWS\\	stem32\\cmd.exe' system32\\cmd.ex	
Address Hex			A	SCII		A 005FEE70	000000	000			
00762850 22 00	0 43 00 3A 00	5C 00 57 00 49 0	0 4E 00 44 00 🛗	.C.:.\.W.I.N.C).	005FEE78	000000	001			
00762860 4F 00	57 00 53 00	5C 00 73 00 79 0	0 73 00 74 00 0	W.S.\.S.y.s.1		005FEE7C	080004	100			
00762880 2E 00	65 00 78 00	65 00 22 00 20 0	0 2F 00 63 00 .	.e.x.e."/.0		005FEE80	000000	000			
00762890 20 00	22 00 76 00	73 00 73 00 61 0	0 64 00 6D 00	.".v.s.s.a.d.m	n.	005FEE84	005555	70			
007628A0 69 00	0 6E 00 2E 00	65 00 78 00 65 0	0 20 00 44 00 1	.ne.x.e[005FEE8C	OOSFER	20			
00762880 65 00	64 00 65 00	77 00 73 00 20 0	0 2F 00 61 00 a	d.o.w.s. ///		005FEE90	000000	002			
007628D0 6C 00	6C 00 20 00	2F 00 71 00 75 0	0 69 00 65 00 1	.1/.q.u.i.e		005FEE94	000000	000			
007628E0 74 00	22 00 00 00	AD BA OD FO AD B	A OD FO AD BA t		•	005FEE56	000/020	10			
Figure 36	5										

There is also a second process that is responsible for deleting all volume shadow copies with wmic:

<pre></pre>	1 2 4 4 5 7 4 4 4 4 0 0 0 4 00 4 00 4 00 4 00 0 0 0 0 0 0 0 0 0 0 0 0	push ecx push dword ptr ss: esp+80 push dword ptr ss: esp+141 push dword ptr ss: esp+144 push l push dword ptr ss: esp+E41 push dword ptr ss: esp+E41 ptr esp str esp s	× 1	x87TW_2 3 (Empty) x87TW_3 3 (Empty) x87TW_4 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_5 3 (Empty) x87TW_8 0 x87TW_7 3 (Empty) x87SW_8 0 x87SW_20 0 x87SW_8 0 x87SW_20 0 x87SW_8 0 x87SW_20 0 x87SW_9 0 x87SW_9 0 x87SW_9 0 x87SW_9 0 vertwo 0 vertwo 0 <
Dump 1 Dump 2 Dump 2	mp 3 🗰 Dump 4 🗰 Dump 5	🛞 Watch 1 🛛 🗱 🖉 Strue	t 005FEE68 007620 005FEE6C 007620	<pre>BE0 L"C:\\WINDOWS\\system32\\cmd.exe" 848 L"\"C:\\WINDOWS\\system32\\cmd.exe\" /</pre>
Address Hex 00762358 (22) 00 3.00 5C 00762358 (47) 00 5.00 5C 00762358 (47) 00 5.30 5Z 00762358 (47) 00 5.30 5Z 00762368 (50) 00 0.03 0.03 3Z 00762368 (20) 05 00 70 06 00 00762368 (20) 0.22 0.76 00 6Z 00 70 00 6D 00762368 (77) 00 6D 00 70 00 6Z 00762368 (77) 00 63 00 67 00 73 00762388 (70) 06 500 74 00 6S	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	ASCII 00 [].(.:.,.w.I.N.D.) 10 0 w.S.,.s.y.s.t. 10 0 e.m.3.2.,.c.m.d. 10	005FEE70 000000 005FEE78 00000 005FEE78 00000 005FEE88 00000 005FEE88 00000 005FEE88 005FEI 005FEE88 005FEI 005FEE80 005FEI	100 100 101 100 100 100 77C 720 002

Figure 37

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



The binary disables Automatic Repair using the bcdedit tool:

cmalware.	•••••••••••••••••••••••••••••									y) x87TW_S 3 (Empt y) x87TW_S 3 (Empt y) x87TW_S 3 (Empt 0000 (SW_C3 0 x87SW_C2 (SW_C0 0 x87SW_C2 (SW	y) y) y) y) unlock stem32\\ \\system
Dump 1	Dump 2	Dump 3	Dump 4	📖 Dump 5 🛛 🧶 Wa	tch 1 [x=] Local	s 🖉 Struct	005FEE78 005FEE7C	007624	A00 L"C:\\WINDO	WS\\system32\\cmd.ex@ DOWS\\system32\\cmd.e	e" exe∖" ∕o
Address	Нех			ASCII			A 005FEE80	000000	000		
007628E8	22 00 43 00 3A	00 5C 00 57	00 49 00 4E	00 44 00 M.C.:.	.W.I.N.D.		005FEE88	000000	001		
00762908	65 00 6D 00 33	00 32 00 5C	00 63 00 6D	00 64 00 e.m.3.	2.\.c.m.d.		005FEE8C	080004	400		
00762918	2E 00 65 00 78	00 65 00 22	00 20 00 2F	00 63 00e.x.	e."/.c.		005FEE94	000000	000		
00762928	20 00 22 00 62 74 00 20 00 2F	00 63 00 64	00 65 00 64	00 69 00b.	c.d.e.d.1.		005FEE98	005FEF	-8C		
00762948	64 00 65 00 66	00 61 00 75	00 GC 00 74	00 7D 00 d.e.f.	a.u.1.t.}.		005FEE9C	005FEF	-30 002		
00762958	20 00 72 00 65	00 63 00 6F	00 76 00 65	00 72 00 .r.e.	c.o.v.e.r.		005FEEA4	000000	000		
00762978	20 00 4E 00 6F	00 22 00 00	00 AD BA OD	FO AD BA .N.O.	°"		005FEEA8	007628	SAS		
	40										

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

	push ecx push edx push dword ptr ss: esp+80 esp+10 push dword ptr ss: 4 01 00 00 push dword ptr ss: esp+144 push 1 push 0 push dword ptr ss: 4 00 00 00 push dword ptr ss: esp+144 push 1 push 0 push dword ptr ss: 5 00 cal 4 malware.CreateProcessw>	x87TW_2 3 (Empty) x87TW_3 3 (Empty) x87TW_4 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_5 3 (Empty) x87SW_6 0 x87SW_C3 0 x87SW_C2 0 x87SW_5 0 x87SW_C5 0 x87SW_5 0 x87SW_5 0 x87SW_7 0 x87SW_0 0 x87SW_6 0 0 x87SW_6 0 x87SW_7 0 x87SW_0 0 x87SW_6 0 0 x87SW_6 0 x87SW_7 0 x87SW_0 0 x87SW_6 0 0 x87SW_6 0 x87SW_7 0 x87SW_0 0 x87SW_6 0 0 x87SW_6 0 x87SW_7 0 x87SW_0 0 x87SW_6 0 0 x87SW_6 0 x87SW_7 0 x87SW_0 0 x87SW_6 0 0 x87SW_6 0 x87SW_7 0 x87SW_0 0 x87SW_6 0 0 x87SW_6 0 x87SW_7 0 x87SW_7 0 x87SW_0 0 x87SW_7 0 x87SW_6 0 x87SW_6 0 x87SW_7 0 x87SW_7 0 x87SW_7 0 x87SW_7 0 x87SW_7 0 x87SW_7 0 x87SW_7 0 x87SW_7 0 x87SW_6 0 x87SW_7 0 x
Dump 1 1 Dump 2 1 Dump 3	Dump 4 IIII Dump 5 🛞 Watch 1 Ix=I Locals 🎾 Stru	005FEE98 00762990 L"C:\\WINDOWS\\system32\\cmd.exe"
Address Hex Address Hex 00762878 22 0 43 00 52 00 57 00 00762878 4F 00 70 53 00 52 00 72 00 00 33 00 20 00 52 00	ASCII 0 49 00 4E 00 44 00 [].c.:.,W.I.N.D. 79 00 73 00 74 00 [].w.S.,S.y.s.t. 163 00 6D 00 64 00 [].e.:.,W.I.N.D. 20 00 2F 00 63 00 [].e.:.,V.C. 20 00 2F 00 63 00 [].e.:.,V.C. 20 00 65 00 78 00 [].e.:., 30 00 2A 00 5C 00 [].e.:., 30 00 2A 00 5C 00 [] 90 00 6E 00 20 00 [] 150 00 2A 00 5C 00 [] 95 00 06 E0 02 00 [] 11 e.x.e. 46 00 20 00 65 00 [] 11 e.x.e. 46 00 20 00 65 00 [] 12 e.x.e. 47 00 20 00 65 00 [] 12 e.x.e. 46 00 20 00 65 00 [] 12 e.x.e. 47 00 20 00 55 00 [] 12.0 00 50 00 50 00 [] 12.0 00 50 00 50 00 [] 12.0 00 50 00 50 00 [] 12.0 00 50 00 50 00 [] 12.0 00 00 50 00 []	005FEEA 00000000 005FEEA 00000000 005FEEA 00000000 005FEEA 00000000 005FEEA 00000000 005FEEA 00000000 005FEEA 0000000 005FEEA 0000000 005FEEA 0000000 005FEEA 00762838 005FEEA 0000000 005FEEA 0076288 005FEEA 0000000 005FEEA 0000000 005FEEA 0000000 005FEEA 0000000 005FEEA 0000000 005FEEA 0000000 005FEEA 0000000 005FEEA 0000000
Address Hex	ASCII	I
00762888 15 37 D0 18 D8 28 00762888 3D 2A 5C 22 20 77 00762808 74 65 64 20 61 74 00762888 2E 0D 0A BA 0D F0 Figure 42	00 18 5C 22 74 6F 6B 65 6E 73 .70.0 61 73 20 75 6E 65 78 70 65 63 =*\" 20 74 68 69 73 20 74 69 6D 65 ted a AD BA 0D F0 AD BA 0D F0 AD BA°.	0(\"tokens was unexpec at this time .ð.°.ð.°.ð.°

Killing targeted services

The binary opens the service control manager database via a function call to OpenSCManagerW (0xF003F = **SC_MANAGER_ALL_ACCESS**):

EIP	OODESD38 OODESD43 OODESD43 OODESD43 OODESD43 OODESD44	68 3F 6A 00 6A 00 E8 7C P1 01	00 OF 00 82 8C 00		sh FOO3F sh O sh O 11 <malware< b="">.</malware<>	.OpenSCMana	gerW>	_		V Defa	7SW_C1 0 7SW_SF 0 7SW 0 0	x875W_C0 x875W_P x875W_7	0 x875W 0 x875W 0 x875W	ES 0 _U 0 5 🗘 🗌 Unlock
<pre>.text:00DE5</pre>	enSCManager	W> .exe:\$195D4	7 #195147						/	1: 2: 3: 4:	[esp] 00 [esp+4] [esp+8] [esp+C]	000000 00000000 000F003F 56C40F48		
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	🛞 Watch 1	[x=] Locals	2 Struct	0820F67 0820F68	C 000	00000				
Address He					ASCTT	1		. 0820F68	4 000	F003F				

Figure 43

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

cma]ware.EnumS	000E5D88 000E5D82 000E5D82 000E5D82 000E5D82 000E5D93 000E5D93 000E5D94 000E5D94 000E5D99 000E5D99 000E5D99 000E5D99 000E5D99 000E5D99 000E5D99 000E5D99 000E5D99 000E5D99 000E5D99 000E5D98 000E5D98 000E5D98 000E5D98 000E5D98 000E5D98 000E5D98 000E5D88 000E5D88 000E5D88 000E5D88 000E5D88 000E5D88 000E5D82 000E5D92 000E5D92 000E5D92 000E5D92 000E5D92 000E5D92 000E5D92 000E5D92 000E5D92 000E5D92 000E5D92 000E5D92 000E5D98 000E5D98 000E5D94 000E5D98 000E5D88 000E508 000E508 000E508 000E5080 000E5080 000E5	6A 00 6A 00 57 51 6A 00 6A 01 6A 30 6A 01 6A 30 6A 00 6A 01 6A 30 6A 00 6A 01 6A 30 6A 01 6A 30 6A 01 6A 10 6A 00 50 50 57 51 51 57 51 57 51 57 51 57 51 57 57 51 57 57 51 57 57 51 6 6 7 57 57 57 57 57 57 57 57 57 57 57 57 5	81 8C 00	M	push 0 push 0 push edi push ecx push 0 push 0 push 1 push 30 push 30 push eax nov esi,eax all <u>cmalwar</u>	e.EnumServic	esStatusExW3	•		>	x87TW_ x87TW_ x87TW_ x87TW_ x87Sta x87SW_ x8	0 3 (2 3 (4 3 (6 3 (tuswo B 0 C1 0 SF 0 C1 0 c1 0 c1 0 c1 0 c1 0 c1 0 c1 0 c1 0 c	Empty) Empty) Empty) Empty) rd 0000 x87SW_C: x87SW_C x87SW_C x87SW_C 766AC0 00000000 00000000	x87Ti x87Ti x87Ti x87Ti x87Ti x87Ti 0 0 0 0	↓ 1 3 (E ↓ 3 3 (E ↓ 5 3 (E ↓ 7 3 (E x87SW_C x87SW_E x87SW_E x87SW_U x87SW_	mpty) mpty) mpty) 2 0 5 0 0 0	k
.text:00DE5D9B	malware.exe	:\$195D9	B #19519B							i i							-
How p Her Address Hex 00762808 88 22 00762808 05 00 00762808 08 00 00762808 08 00 00762808 08 00 00762808 00 00 00762808 00 00 00762808 00 00	Dump 2 Image: Constraint of the second	Dump 3	05 00 00 00 C8 2E 76 0 07 00 00 0 06 00 00 0 48 2F 76 0 08 00 00 0 08 00 00 0	A8 2E 76 0 0 A8 2E 76 0 0 07 00 00 0 0 28 2F 76 0 0 00 00 00 0 0 0 28 2F 76 0 0 0 0 00 00 00 0	Watch : ASCII 0	1 [x=1 Locals	2 Struct	*	820F660 820F664 820F668 820F66C 820F670 820F674 820F678 820F67C 820F680 820F684	00766 00000 00000 00000 00000 0820F 0820F 00000 00000	AC 0 000 030 001 000 000 6C 0 704 000 000						

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):

Address H	ey .				ASCIT			0844FD3	8 0000	002C					
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	0844FD3 0844FD3	0 0077	95F0 95B0	L"vss"				
<pre><malware.0 .text:00de<="" pre=""></malware.0></pre>	OODE4BD3 OODE4BD3 OODE4BDA	exe: \$1948D	93 8C 00		sh edi sh eax 11 <malware< th=""><th>. OpenServic</th><th>ew></th><th></th><th>></th><th>X87 X87 Defau 1: [2: [3: [4: [</th><th>sw_CI 0 Sw_SF 0 [stdcall] [esp] 00 [esp+4] [esp+8] [esp+C]</th><th>7795F0 0007795B0 000779590</th><th>0 0 L"VS:</th><th>x875₩_U x875₩_U x875₩_U x875₩_D</th><th>€ Unlock</th></malware<>	. OpenServic	ew>		>	X87 X87 Defau 1: [2: [3: [4: [sw_CI 0 Sw_SF 0 [stdcall] [esp] 00 [esp+4] [esp+8] [esp+C]	7795F0 0007795B0 000779590	0 0 L"VS:	x875₩_U x875₩_U x875₩_U x875₩_D	€ Unlock
	00DE48D5	6A 2C		pu	sh 2C					X87	SW_B 0	x875W_C3	0	x875W_C2	0

Figure 45

EnumDependentServicesW is utilized to retrieve the active services that depend on the targeted service (0x1 = **SERVICE_ACTIVE**):



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

EIP	 00DE5718 00DE5718 00DE5718 00DE5718 00DE5718 	57 6A 01 51 E8 0C	88 8C 00	pus pus cal	sh edi sh 1 sh ecx I <malware< th=""><th>.ControlSer</th><th>/ice></th><th></th><th>~</th><th>x875W_C1 0 x875W_C0 x875W_SF 0 x875W_P x875W 0 0 x875W_P x875W 0 0 x875W 7 Default (stdcall)</th><th>0 x87SW_ES 0 0 x87SW_U 0 • x87SW_D 0</th></malware<>	.ControlSer	/ice>		~	x875W_C1 0 x875W_C0 x875W_SF 0 x875W_P x875W 0 0 x875W_P x875W 0 0 x875W 7 Default (stdcall)	0 x87SW_ES 0 0 x87SW_U 0 • x87SW_D 0
<pre><malware.co .text:00de5<="" pre=""></malware.co></pre>	71F malware	e>	- #194B1F	_						1: [esp] 007656A0 2: [esp+4] 00000001 3: [esp+8] 0844FCB0 4: [esp+C] 00000000	
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	🛞 Watch 1	[x=] Locals	2 Struct	0844FCA4 0	0765	6A0 0001	
Address He				1	ASCTT	1		0844FCAC 0)844F	CBO	

Figure 47

Killing targeted processes

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

EIP	• 00E1D2B2 00E1D2B4 • 00E1D2B6 • 00E1D2B6 • 00E1D2B6	6A 00 6A 0F E8 B5	08 89 00		ISh 0 ISh F Il <malware.< th=""><th>.CreateTool</th><th>help32Snapsh</th><th>ot></th><th>~</th><th>x87SW_SF 0</th><th>X875W_P</th><th>0</th><th>×875₩_U ×875₩ D</th><th>0 Unlock</th></malware.<>	.CreateTool	help32Snapsh	ot>	~	x87SW_SF 0	X875W_P	0	×875₩_U ×875₩ D	0 Unlock
<malware.co< th=""><th>reateToolhelp D2B6 malware.</th><th>32Snapshot> exe:\$1CD2B6</th><th>#1CC6B6</th><th></th><th></th><th></th><th></th><th></th><th></th><th>1: [esp] 00 2: [esp+4] 3: [esp+8] 4: [esp+C]</th><th>00000F 00000000 06040002 00000000</th><th></th><th></th><th></th></malware.co<>	reateToolhelp D2B6 malware.	32Snapshot> exe:\$1CD2B6	#1CC6B6							1: [esp] 00 2: [esp+4] 3: [esp+8] 4: [esp+C]	00000F 00000000 06040002 00000000			
Figure	Ump 2 2	Dump 3	Dump 4	Dump 5	🛞 Watch 1	[x=] Locals	2 Struct	07FCF878 00 07FCF87C 00	00000	00F				

The processes are enumerated using the Process32FirstW and Process32NextW APIs:

EIC	• 00E1D33B • 00E1D33C • 00E1D33F • 00E1D340 • 00E1D245 <	50 89 7D 57 E8 4B	FO DA 89 00	pu mo ca	sh eax v dword ptr sh edi 11 <malware.< th=""><th>ss: ebp-10</th><th>,edi irstW></th><th>2</th><th>*</th><th>x875w_C1 0 x875w_C0 0 x875w_ES 0 x875w_SF 0 x875w_P 0 x875w_U 0 v875w 0 v875w 7 v875w 0 Default (stdcall) ▼ 5 ↓ Unloc</th></malware.<>	ss: ebp-10	,edi irstW>	2	*	x875w_C1 0 x875w_C0 0 x875w_ES 0 x875w_SF 0 x875w_P 0 x875w_U 0 v875w 0 v875w 7 v875w 0 Default (stdcall) ▼ 5 ↓ Unloc
<malware.pr< th=""><th>nocess32First 0340 malware.</th><th>w> exe:\$1CD340</th><th>#1CC740</th><th></th><th></th><th></th><th></th><th></th><th></th><th>2: [esp+4] 07FCFAAC 3: [esp+8] 06040002 4: [esp+C] 00000000</th></malware.pr<>	nocess32First 0340 malware.	w> exe:\$1CD340	#1CC740							2: [esp+4] 07FCFAAC 3: [esp+8] 06040002 4: [esp+C] 00000000
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	07FCF878 0 07FCF87C 0	0000 7FCF	02D8 FAAC
Figure	49 00E1D3E1 00E1D3E2 00E1D3E5	50 88 7D 1 57	F0	pu mo pu	sh eax v edi,dword sh edi	ptr ss:[eb	0-10]			x875W_C1 0 x875W_C0 0 x875W_ES 0 x875W_SF 0 x875W_P 0 x875W_U 0
	000010200	00 00		+4	F# ASV ASV	in occossion.	CA CHP	2	. *	Default (stdcall) 🔻 5 💠 🗌 Unloc
<malware.pr< td=""><td>D3E6 malware.</td><td>> exe:\$1CD3E6</td><td>#1CC7E6</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1: [esp] 0000208 2: [esp+4] 07FCFAAC 3: [esp+8] 0000022C 4: [esp+C] 00000000</td></malware.pr<>	D3E6 malware.	> exe:\$1CD3E6	#1CC7E6							1: [esp] 0000208 2: [esp+4] 07FCFAAC 3: [esp+8] 0000022C 4: [esp+C] 00000000
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	07FCF878 0	0000	02D8
Eiguro	50							01101010		

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:

>00E1D7D9 00E1D7DB	6A 09	push 9 push esi		X875W_SF 0 X875W_	P 0 x875W_U 0
		moury aby bute atr de: [160000]	>`	Default (stdcall) 1: [esp] 000002AC	▼ 5 🖨 🗌 Unlock
<pre><malware.terminateprocess: .text:00E1D7DC malware.exe</malware.terminateprocess: </pre>	e:\$1CD7DC #1CCBDC			2: [esp+4] 0000000 3: [esp+8] 770213E0 4: [esp+C] 016D4DA0	9 ntdll.770213EE malware.016D4DAC
Dump 1 Dump 2	Dump 3 💭 Dump 4	Dump 5 🛞 Watch 1 🛛 🕸 Struct	07FCFCEC 00000 07FCFCF0 00000	02AC	

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.

	push eax push esi push 0 push 0 push 40 push 40 push esi push esi push esi push dword ptr ss: ebp-4C push dword ptr ss: ebp-50 push dword ptr ss: ebp-54 call «malware.CreateProcesswithLogonw> terr av av	x87TagWord FFFF x87Tw_0 3 (Empty) x87Tw_1 3 (Empty) x87Tw_2 3 (Empty) x87Tw_3 3 (Empty) x87Tw_4 3 (Empty) x87Tw_5 3 (Empty) x87Tw_6 3 (Empty) x87Tw_5 3 (Empty) x875w_5 0 (Empty) x87Tw_5 0 (Empty) x875w_5 0 (2000) x875w_5
.text:00D7F86A malware.exe:\$12F86A #12EF6A	mp 5 🛞 Watch 1 [X=] Locals 🖉 Struct 0790F9F6 01 0790F9F6 01	3: [esp+6] 0070CF68 4: [esp+C] 00000002 J7502E8 L"Administrator" J750CE88
Address Hex 00768648 22 00 30 03 A 00 5C 00 73 00 6D 73 00 5C 00 74 00 6D 00 74 00 6D 00 74 00 6D 00 70 00 5C 00 73 00 6D 00 70 00 5C 00 72 00 5C 00 72 00 5C 00 72 00 5D 02 70	ASCII 0730FA00 0730FA04 0730FA02 0730FA02 0730FA02 0730FA10 0730FA10 0730FA10 0730FA10 0730FA10 0730FA10 0730FA16 0730FA16 0730FA18 0730FA18 0730FA12 0730FA20 0730FA20 <t< th=""><th>170CF68 1000000 1768648 L"\"C:\\Users\\mm\\Desktop\\malware.ex 1000400 1000000 190FA4C 190FA4C</th></t<>	170CF68 1000000 1768648 L"\"C:\\Users\\ mm \\Desktop\\malware.ex 1000400 1000000 190FA4C 190FA4C
00768658 65 00 62 00 30 06 4 00 32 03 30 00 007686508 62 00 30 00 40 06 10 65 00 40 06 10 65 00 40 05 10 65 00 30 00 40 05 10 65 00 30 30 30 30	33 000 e.n. .c.d.2.9.C. 0730FA24 00 35 001 b.8.9.d.a.e.d.9. 0730FA28 00 55 000 e.2.f.3.9.8.7.e. 0730FA2C 01 700 9.0.d.7.a.c.9.7. 0730FA32 01 030FA32 01 33 00 4.8.6.2.4.1.d.3. 0730FA34 01 0730FA34 01 55 00 f.8.7.e.2.1.a.5. 0730FA34 01 0730FA34 01 55 00 f.4.e.3.b.4.6.5. 0730FA35 01 0730FA36 01 50 00 e.4.e.3.b.4.6.5. 0730FA36 01 0730FA36 01 84 84 S.0.c	S06800 malware.01806800 1000000 Icelurn to malware.01684391 from malware 1000026 1000026 10000000 1000000 10000000 1000000
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\MaxMpxCt" Registry value:

<pre>malware.Cr .text:01650</pre>	O155098E O155098F O1550990 O1550997 O1550939 O1550942 O1550944 O1550946 O1550946 O1550946 O1550946 O1550946 O1550946 O1550946 O1550946 O1550948 O155094 O155	51 52 FF B4 FF 74 FF 6A 01 6A 00 6A 00 FF B4 50 E8 A3 e5 C0	24 80 00 00 24 1C 24 44 01 00 24 E4 00 00 D1 05 00	00 pui 00 pui 00 pui 00 pui 00 pui 00 pui 00 pui 00 pui 00 pui	h ecx h dword ptr h dword ptr h dword ptr h dword ptr h 1 h 0 h 0 h dword ptr h 1 malware,	SS: esp+84 SS: esp+10 SS: esp+1 SS: esp+E CreateProc	4] 4] essw>		_	× x x x x x x x x x x x x x x x x x x x	37TW_2 3 37TW_4 3 37TW_6 3 37StatusW 37SW_B 0 37SW_C1 0 37SW_SF 0 37SW_SF 0 57SW_0 0 57	(Empty) (Empty) (Empty) (Empty) ord 0000 x875W_C x875W_C x875W_C x875W_C 007654D8 L 007654D8 L 00000000 00000000	x87TW_3 x87TW_5 x87TW_5 x87TW_7 3 0 x87 0	3 (Empt 3 (Empt 3 (Empt 5W_C2 5W_ES 7SW_U 7SW_U 5 0WS\\sy! WINDOWS	y) y) y) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	👹 Watch 1	[x=] Locals	2 Struct	07B	4F5A8	007654D	B L"C:\\\	VINDOWS	system32\ \\svstem3	\cmd.exe	" exe\" /o
Address Het 007652C0 22 007652C0 22 007652C0 22 007652C0 22 007652C0 22 007653C0 20 007653C0 20 00765320 4F 00765320 4F 00765320 45 00765320 45 00765	X 00 43 00 32 00 67 00 57 00 50 00 67 00 55 00 60 01 71 00 65 00 70 52 00 65 00 74 00 20 01 74 00 30 41 00 45 00 45 00 45 00 45 00 66 00 67 00 66 00 75 00 65 00 7 00 65 00 7 00 65 00 7 00 65 00 7 00 65 00 7 00 20 00 30 02 02 00 30 02 00 30 03 00 45 00 47 00 5 00 30 03 00 47 00 5 00 47 00	00 5C 00 5 00 5C 00 5 00 5C 00 5 00 65 00 5 00 65 00 5 00 48 00 4 00 48 00 4 00 43 00 5 00 5C 00 5 00 45 00 5 00 65 00 5 00 65 00 5 00 65 00 5 00 65 00 5 00 65 00 5 00 27 00 27 00 27 00 5 00 24 00 5 00 44 00 5	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	ASCII 	N.D. S.T. 		 O78 O78	4F580 4F588 4F588 4F580 4F500 4F500 4F500 4F500 4F500 4F500 4F500 4F500 4F500 4F500 4F500 4F500 4F500 4F500 4F560	0000000 0000000 0000000 0000000 0784F68 0784F68 0700000 0000000 0000000 0000000 0000000	000 1000 000 000 000 000 000 000 000 00	VINDOWS\\	system32\	\cmd.exe	

Figure 54

The malicious process obtains the ARP table using the arp command, as shown below:

<pre>cmalware.Cr .text:01650</pre>	 1165098E 0165098F 01650997 01650997 01650998 01650984 01650985 01650985<	51 52 FF 84 2 FF 74 2 FF 84 2 6A 01 6A 00 6A 00 FF 84 2 50 E8 A3 0 E8 A3 E8 A3	24 80 00 00 24 1C 24 44 01 00 24 E4 00 00 21 05 00 #9FFDB0	00 pu 00 pu 00 pu 00 pu 00 pu 00 pu 00 pu 00 pu 00 pu 00 pu	sh ecx sh dword ptr sh dword ptr sh dword ptr sh 1 sh 0 sh 0 sh dword ptr sh eax 11 cmalware.(ss: esp+8 ss: esp+1 ss: esp+1 ss: esp+E reateProce	4] 4] essw>			>	x87Tw_2 3 (E x87Tw_4 3 (E x87Tw_6 3 (E x87Tw_6 3 (E x87Sw_6 3 (E x87Sw_6 1 0 x87Sw_6 1 0 x87Sw_6 1 0 x87Sw_5 0 x87Sw_6 1 0 x87Sw_5 0 x87Sw_6 1 0 x87Sw	mpty) :: mpty) :: mpty) :: mpty) : d 0000 x87SW_C3 x87SW_C3 x87SW_C3 x87SW_P x87SW_P x87SW_P x87SW_P x87SW_P x87SW_P x87SW_2 x87SW_0 x	(87TW_3 3 ((87TW_5 3 ((87TW_5 3 (0 x875W_ 0 x875W	Empty) Empty) Empty) Empty) C2 0 ES 0 U 0 5 5 5 1 10lock (\system32\\ DOWS\\system
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	🛞 Watch 1	[x=] Locals	2 Struct	076	84F478	00765	7D8 L"C:\\WI	NDOWS\\sy WINDOWS\\	stem32\\cm	d.exe" cmd.exe\" /c
Address He 00765740 22 00765750 4F 00765760 65 00765770 2E 00765770 2E 00765790 22 00765790 22	x 00 43 00 3A 0 00 57 00 53 0 00 65 00 33 0 00 65 00 78 0 00 02 00 61 0 00 00 00 00 F	00 5C 00 5 00 5C 00 7 00 32 00 5 00 65 00 2 00 72 00 72 00 AD BA 0	7 00 49 00 4 3 00 79 00 2 2 00 63 00 0 2 00 20 00 2 0 00 20 00 2 0 F0 AD BA 0	E 00 44 00 3 00 74 00 D 00 64 00 F 00 63 00 D 00 61 00 D F0 AD BA F 0 AD BA	ASCII 	N.D. s.t. m.d. /.c. a. 0.0.°		076 076 076 076 076 076 076 076 076	B4F480 B4F484 B4F488 B4F486 B4F490 B4F490 B4F496 B4F49C	00000 00000 00000 00000 00000 00000 0784F 0784F	000 000 001 1400 000 58C 530			

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

<pre><malware.createprocessw></malware.createprocessw></pre>		push ecx push dword ptr ss: esp+80 push dword ptr ss: esp+10 push dword ptr ss: esp+141 push 0 push 0 push 0 push dword ptr ss: esp+E4 push eax call cmalware.CreateProcessw>	<pre>x87TW_2 3 (Empty) x87TW_3 3 (Empty) x87TW_4 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87TsLatuSWord 0000 x87SW_5 0 x87SW_5 0 x87SW_2 0 x87SW_2 0 x87SW_5 0 x87SW_9 0 x87SW_2 0 Default (stdcall) > D</pre>
## Dump 1 ## Dump 2 ## Dump 4 ## Dump 5 @W Watch 1 Ix=lLocals >> Struct 0784F55C 00765E68 L"C::\\WINDOWS\\system32\\cmd.exe" 00769008 122 00 43 00 3A 00 5C 00 57 00 49 00 44 00 44 00 #C.:.\\WI.N.D.C. 00784F55C 00000000 0784F55C 000000000 0784F55C 000000000	Hex Dump 1 Hex Dump 3 Hex Dump 4 Dump 4	S Image: Second se	4F353 00765E68 L"C:\\WINDOWS\\system32\\cmd.exe" 4F55C 00060000 L"\"C:\\WINDOWS\\system32\\cmd.exe\" /c 4F564 0000000 4F564 4F55C 0000000 4F564 4F565 0000000 4F564 4F564 0000000 4F574 4F570 0000000 4F574 4F574 0000000 4F574 4F574 0000000 4F574 4F584 0000000 4F584 4F584 0000002 4F584

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

EIP 000C7DAA E8 E9 5E 8E 00	call <malware.getlogicaldrives></malware.getlogicaldrives>	>	Default (stdcall)
<pre><malware.getlogicaldrives> .text:00DC7DAA malware.exe:\$177DAA #1771AA</malware.getlogicaldrives></pre>			1: [csp14] 00766CF8 3: [csp14] 00766CF8 4: [csp14] 00000004 4: [csp14] 01916424 malware.01916424
Figure 57			

The GetDriveTypeW API is utilized to obtain the drive type:

EIP	00DC 9805	56 E8 3D	44 8E 00		ush esi all <malware.< th=""><th>GetDriveT</th><th>pew></th><th></th><th>~</th><th>Default (sto</th><th>call)</th><th>0 2075</th><th>5</th><th>O Unlock</th></malware.<>	GetDriveT	pew>		~	Default (sto	call)	0 2075	5	O Unlock
<malware.ge< th=""><th>tDriveTypeW></th><th>exe: \$179800</th><th>5 #178006</th><th></th><th></th><th></th><th></th><th></th><th>></th><th>1: [esp] 2: [esp4 3: [esp4 4: [esp4</th><th>04173E88 4] 04173E88 8] 00000001 C] 00000001</th><th></th><th></th><th></th></malware.ge<>	tDriveTypeW>	exe: \$179800	5 #178006						>	1: [esp] 2: [esp4 3: [esp4 4: [esp4	04173E88 4] 04173E88 8] 00000001 C] 00000001			
Dump 1	Dump 2	Dump 3	📖 Dump 4	🕮 Dump 5	Watch 1	[x=] Locals	Struct	0609F820 0609F824 0609F828	04173 04173 00000	E88 E88 001	10] 041/3248			
04173E88 41	00 00 00 AE	AB AB AB	AB AB AB AB	AB AB AB AB	A««««««««			0609F82C	00000	001 E40				

Figure 58

The ransomware starts scanning the volumes on the local machine using FindFirstVolumeW:

	 00E285D4 00E285D9 	68 0A	02 00 00	pu	sh 20A sh edi	FindFinanti	- Trumpite			x875W_SF 0 x875W_P	0 x87SW_	J 0
ETLA	00E28SDA	E8 E1	55 88 00	6		.FindFirstv	olumew>	>	× C	efault (stdcall)	▼ [5	Unlock
<malware.ft< th=""><th>indFirstVolum 35DA malware.</th><th>neW> .exe:\$1D85D/</th><th>4 #1D79DA</th><th></th><th></th><th></th><th></th><th></th><th></th><th>2: [esp+4] 0000020A 3: [esp+8] FFFFFFE 4: [esp+C] 07DFFBB8 5: [esp+10] 77021687</th><th>ntdll.77021</th><th>687</th></malware.ft<>	indFirstVolum 35DA malware.	neW> .exe:\$1D85D/	4 #1D79DA							2: [esp+4] 0000020A 3: [esp+8] FFFFFFE 4: [esp+C] 07DFFBB8 5: [esp+10] 77021687	ntdll.77021	687
Dump 1	Dump 2	Dump 3	💷 Dump 4	Ump 5	👹 Watch 1	[x=] Locals	2 Struct	07DFFB64 00A 07DFFB68 000	7F7	F8 0A		
Figure	59											

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

EIP <ma< th=""><th>]ware.G</th><th>00228692 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 002869 002869</th><th>6A 00 68 0A 89 45 50 57 E8 75 87 70 NamesForVol</th><th>02 00 00 C4 56 88 00</th><th>pus pus mov pus cal</th><th>h 0 h 20A dword ptr h eax h edi cmalware</th><th>ss:[ebp-3C .GetVolumeP</th><th>],eax athNamesFor</th><th>rvolu</th><th>imeNameW></th><th>></th><th>x87 x87 x87 x87 x87 x87 Defa</th><th>SW_B 0 SW_C1 0 SW_SF 0 SW_SF 0 ult (stdcall) [esp] 00</th><th>x87SW_C x87SW_C x87SW_P x87SW_P x87SW_P</th><th>3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</th><th>x87SW_C x87SW_E x87SW_U x87SW_U x87SW_D 5 5 2\\Volume</th><th>2 0 5 0 0 2 4 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</th></ma<>]ware.G	00228692 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 0022869 002869 002869	6A 00 68 0A 89 45 50 57 E8 75 87 70 NamesForVol	02 00 00 C4 56 88 00	pus pus mov pus cal	h 0 h 20A dword ptr h eax h edi cmalware	ss: [ebp-3C .GetVolumeP],eax athNamesFor	rvolu	imeNameW>	>	x87 x87 x87 x87 x87 x87 Defa	SW_B 0 SW_C1 0 SW_SF 0 SW_SF 0 ult (stdcall) [esp] 00	x87SW_C x87SW_C x87SW_P x87SW_P x87SW_P	3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	x87SW_C x87SW_E x87SW_U x87SW_U x87SW_D 5 5 2\\Volume	2 0 5 0 0 2 4 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
.te	xt:00E2	869E malware	.exe:\$1D8698	E #1D7A9E								3: 4:	[esp+8] [esp+C]	0000020A 00000000 FFFFFFF			
0	Dump 1	Dump 2	Ump 3	Dump 4	Ump 5	🛞 Watch 1	[x=] Locals	2 Struct		07DFFB5C (07DFFB60 (07DFF))))))))	00A7F	7F8 678	L"////?	\\Volume	d7e4	7829-0000	-0000-0000
Add	ress H	ex	0.00.00.001	00 00 00 00	00 00 00 00	ASCII			^	07DFFB64 (07DFFB68 (00000	20A					

Figure 60

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

EIP	 00E28AC0 00E28AC0 00E28AC0 00E28AC0 00E28AC0 	68 0A 57 5 FF 75 E8 02	02 00 00 C8 51 88 00	pus pus pus	h 20A h edi h dword ptr	ss:[ebp-3	8] 1umeW>	_		x875W_C1 0 x875W_C0 x875W_SF 0 x875W_P x875W 0 0 x875W 7	0 0 x87SW_ES 0 0 x87SW_U 0 0 x87SW_D 0	
	• • • • • • • • • • • • • • • • • • • •	00		200	ari asv			>	1	Default (stdcall)	▼ 5 🖨 🗆	Unlock
<malware.fi< td=""><td>ndNextVolum</td><td>ew> .exe:\$1D8AC</td><td>9 #1D7EC9</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1: [esp] 00A7FA20 2: [esp+4] 00A7F7F8 3: [esp+8] 0000020A 4: [esp+C] FFFFFFE 5: [esp+10] 07DFFBB8</td><td>L"\\\\?\d7</td><td>e4782</td></malware.fi<>	ndNextVolum	ew> .exe:\$1D8AC	9 #1D7EC9							1: [esp] 00A7FA20 2: [esp+4] 00A7F7F8 3: [esp+8] 0000020A 4: [esp+C] FFFFFFE 5: [esp+10] 07DFFBB8	L"\\\\?\d7	e4782
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	🛞 Watch 1	[x=] Locals	Struct	07DFFB60 00 07DFFB64 00 07DFFB68 00	A7FA A7F7	A20 7F8 L"\\\\?\	d7e47829-0000-0000-	-0000

Figure 61

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

EIP	00E28A20 00E28A20 00E28A3 00E28A3 00E28A3 00E28A3 00E28A3 00E28A3	57 88 5D 53 2 E8 19	A0 54 88 00		sh edi v ebx,dword sh ebx 11 <malware< th=""><th>ptr ss:[eb</th><th>p-60] ountPointW></th><th></th><th>X8 X8 Defa</th><th>7 SW_C1 0 7 SW_SF 0 7 SW 0 0</th><th>x875W_C0 x875W_P</th><th>0 x875W 0 x875W 0 x875W</th><th>_ES _U 5 🗘</th><th>Unlock</th></malware<>	ptr ss:[eb	p-60] ountPointW>		X8 X8 Defa	7 SW_C1 0 7 SW_SF 0 7 SW 0 0	x875W_C0 x875W_P	0 x875W 0 x875W 0 x875W	_ES _U 5 🗘	Unlock
<pre><malware.setvolumemountpointw> .text:00E28A32 malware.exe:\$1D8A32 #1D7E32</malware.setvolumemountpointw></pre>								1: 2: 3: 4: 5:	[esp] 00 [esp+4] [esp+8] [esp+C] [esp+10]	00A7A9F8 L"2 00A7F7F8 L 00A74290 00000003 00000003	"\\\\?\\W	olume{	d7e4782	
Dump 1	Ump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	07DFFB64 00A7 07DFFB68 00A7	A9F8	L"Z:\\" L"\\\\?	\c	7e47829-00	000-00	00-0000
Figure	62													

BlackCat traverses the file system using the FindFirstFileW and FindNextFileW APIs:

0164994E 53 0164994F 89 75 D4 01649952 56 01649952 56 01649953 E8 60 42 06 00	push ebx mov dword ptr ss:[ebp-2C],esi push esi call amalware.FindFirstFilew> cmm esy CCCCCCCC	x875W_C1 0 x875W_C0 0 x875W_E5 0 x875W_SF 0 x875W_P 0 x875W_U 0 v275W 0 0 v275W 0 Default (stdcall) v15 0 Unlock
<malware.findfirstfilew> .text:01649953 malware.exe:\$9F9953 #9F8D53</malware.findfirstfilew>		1: [esp1 00475638 L*C:\\USErS\\"" 2: [esp+4] 056FE558 3: [esp+5] 00000000 4: [esp+C] 00000000 5: [esp+10] 00000000
## Dump 1 ## Dump 2 ## Dump 3 ## Dump 4 ## C Figure 63	ump 5 🔞 Watch 1 🕼 I Locals 🎾 Struct	DEGEEBSU 00475638 ["C:\\USers\\"" 1086FEB54 086FEB58
	push ebx push esi call <malware.findnextfilew></malware.findnextfilew>	x875W_SF 0 x875W_P 0 x875W_U 0 v275W_0 0 x275W_7 0 x275W_0 0 Default (stdcall)
<malware.findnextfilew> .text:016490A3 malware.exe:\$9F90A3 #9F84A3</malware.findnextfilew>		2: [csp+4] 056FE6BC 3: [csp+4] 056FE6BC 4: [csp+2] 00000000 5: [csp+10] 00000000
## Dump 1 ## Dump 2 ## Dump 3 ## Dump 4 ## Dump 4 Figure 64 ## Dump 3 ## Dump 4 ## Dum	Dump 5 🔮 Watch 1 🛛 🕸 I Locals 🖉 Struct	USSESSE 00A75840 086FE6B8 086FE6BC

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, excluding VMware ESXi virtual machines from termination



Files encryption

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):

<pre></pre>	6A 00 57 52 FF 75 E8 FF 75 E4 FF 75 F0 88 70 EC 57 E8 0F 46 06 00 e9 c0 cc xe:\$9F951C #9F891C	push o push edi push dword ptr ss push dword ptr ss push dword ptr ss mov edi dword ptr push edi call smalware.Cre	: ebp-18 : ebp-12 : ebp-20 : ss: gebp-14 sateFilew>	×	x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty) x87Statusword 0000 x87SW_2 0 x87SW_8 0 x87SW_2 0 x87SW_2 0 x87SW_6 0 x87SW_P 0 x87SW_2 0 x87SW_6 0 x87SW_P 0 x87SW_2 0 y87SW_6 0 x87SW_P 0 x87SW_2 0 x87SW_8 0 x87SW_8 0 x87SW_8 0 x87SW_8 0 x87SW_8 0
			(3)	0772E48C 03D0	4CD8 L"\\\?\\C:\\Users\\\\Desktop\\sica.
Dump 1 Dump 2	Dump 3 Dump 4	Ump 5 Watch 1	=l Locals 🧳 Struct	0772F490 C000	0000
Address Hex		ASCII		0772F494 0000	0007
03D04CD8 5C 00 5C 00 3F	00 5C 00 43 00 3A 00 5	C 00 55 00 N.\.?.\.C.:.\.	U.	0772F49C 0000	0003
03D04CE8 73 00 65 00 72 03D04CE8 5C 00 44 00 65	00 73 00 50 00 74 00 0	SE 00 70 00 \.D.e.s.k.t.0.	D.	0772F4A0 0000	0000
03D04D08 5C 00 73 00 69	00 63 00 61 00 2E 00	4 00 78 00 \.s.i.c.at.	x.	0772F4A4 0000	0000

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**):



The ransom note is populated using the WriteFile routine:

	> Def 1: 2: 3: 4: 5:	>>statusword 0000 >>statusword 0000 >>statusword va875w_C1 >>statusword va87sw_C2 >>sws_statusword va87sw_C2 >>ws7sw_C1 va87sw_C2 >>ws7sw_C2 va87sw_C2 >>ws7sw_C2 va87sw_C2 ault(stdcal)	0 x875W_C2 0 0 x875W_E5 0 0 x875W_U 0 0 x8
🗱 Dump 1 🗱 Dump 2 🗱 Dump 3 🗱 Dump 4 👪 Dump 5 🛞 Watch 1 💷 Locals 🖉 Struct 072AF640	00000368		
Address Hex ASCII 072AF64	00000528		
03D10A08 3E 3E 20 57 68 61 74 20 68 61 70 70 65 6E 65 64 ≥> What happened 03D10A18 3F 0D 0A 0D 0A 4 9 6D 70 6F 72 74 61 6E 74 20 66 72Important f	00000000		
03D10A28 69 6C 65 73 20 6F 6E 20 79 6F 75 72 20 6E 65 74 11es on your net	00000000		
Figure 68			
RECOVER-AwaveFills M 3			
Theorem file of your persons was PNSVETD and now they have "shoures" extension.			
In order to recover your files you need to follow instructions below.			
6 >> Sensitive Data			
Sensitive data on your network was DONNIGADED. If you DON'T KANT your sensitive data to be FUBLISHED you have to act quickly.			
1 Data includes			
13 = Floodatary			
14 = Confidential data; 15 = Projects;			
16 - Blueprints; 17 - Database;			
10 - Contracts and agreements; 19 - Percond data;			
20 - Reports			
- And Roser:			
23 Dampies are available on your personal web page linked below.			
23 >> CAUTION 24			
 DO NOT MODITY ENKRYPTED FILLS YOURSELF. DO NOT WOITY ENKRYPTED FILLS YOURSELF. YOU HAY CANAGE YOUR FILES, IT WILL RESULT IN PERGAMENT DATA LOSS. 			
11 >> What should I do next?			
3 1) Download and install Tor Browser from: https://torproject.org/			
(3) 4) WATGREE to: http://webspljiekldooflutButoch473jglpldmgsFrjhyrwnydonkgvd.onLon/Facess-key- ofLiMmL57j7wyH27LIjComEXtrgAnloin+ObmScQ4285Ch25JHWc05Fr9MH1HTjpl1EBH2K4HWC0KUVyj7K4A2F2qUWHT065ygKKe2WtQ5kyvxEBo428046j7gpA2Fxx1fUcrQ5kn2IHrCOnYseT4A	j53N01r52Cm%2Fq	xIlVI53MPlq4bfDw6Nu2A3IddOmQr0	xHK8qHnUqKEHY3pmQ43D43D

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):

• 0164 • 0166 •	9508 6A 00 9500 57 950F 52 951F FF 75 9518 FF 75 9518 57 9512 FF 75 9513 FF 75 9514 FF 75 9515 FF 75 9518 57 9512 FF 75 9518 57 9514 E8 0F 9514 9 00 9514 9 00 9518 57 9514 80 00 9518 9 00 9519 9 00 9510 9 00 9511 9 00 9 00 9 00 9 00 9 00 9 00 9 00	E8 E4 F0 EC 46 06 00 cc #9F891C	push 0 push edi push dovrd ptr push dword ptr push dword ptr mov edi dword p push edi call qmalware.C	ss:[ebp-18] ss:[ebp-10] ss:[ebp-10] tr ss:[ebp-14] reateFilew> c		>	x875W_6 x875W_6 x875W_1 x875W_2 x875W_21 x875W_5 v875W_5 v875W_6v875W_6 v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6v875W_6v875W_6 v875W_6v875W_6v875W_6v875W_6 v875W_6v875W	s (Empty) 3 (Empty) sword 0000 0 x875W_C 0 x875W_C 0 x875W_P 0 x875W_P 0 x875W_P 1 0000000 3 00000007 1 00000000 3 00000007	xx87TW_7 3 xx87TW_7 3 0 xx87SW 0 xx87SW 0 x87SW 0 x87SW 0 x87SW 0 x87SW 0 x87SW	(Empty) (22 0 (ES 0 (U 0 5 0 (Users)
Dump 1 Dump	2 💭 Dump 3	Dump 4 Dump	5 💮 Watch 1	[x=] Locals	Struct	072AF754 03CF 072AF758 0000	E250 L"\\\ 0000	\?\\C:\\Use	rs////De	sktop\\sica
Address Hex			ASCII	1		072AF75C 0000	0007			
03CFE250 5C 00 5C 0	0 3F 00 5C 00	43 00 3A 00 5C 00 55	00 N.\.?.\.C.:.\	.U.		072AF760 0000 072AF764 0000	0000			
03CFE260 73 00 65 0 03CFE270 5C 00 44 0	0 65 00 73 00	6B 00 74 00 6F 00 70	00 \.D.e.s.k.t.0	0.0.		072AF768 0200	0000			
03CFE280 5C 00 73 0	0 69 00 63 00	61 00 2E 00 74 00 78	00 \.s.i.c.at	t.x.		072AF76C 0000	0000			
03CFE290 74 00 2E 0 03CFE2A0 75 00 00 0	0 75 00 68 00 0 0 AB AB AB AB	77 00 75 00 76 00 7A AB AB AB AB AB EE FE EE	00 tu.n.w.u.v	ibib		072AF774 03CF	E250 L"\\\	\?\\C:\\Use	rs\\ \\De	sktop\\sica
Figure 70						1777657701 nnnn				

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



The malware generates 16 random bytes that will be used to derive the AES key:



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:

EIP	 0162CAD0 0162CAD2 0162CAD3 0162CAD4 0162CAD5 0162CAD6 0162CAD6 0162CAD6 0162CAD6 	6A 00 57 51 50 52 E8 E5 12 08 (0 Ca	sh 0 sh edi sh ecx sh eax sh edx 11 <malware< th=""><th>.ReadFile></th><th></th><th>_</th><th></th><th>></th><th>×87 ×87 ×87 ×87 ×87</th><th>StatusWe SW_B 0 SW_C1 0 SW_SF 0 SW_SF 0</th><th>000268</th><th>0</th><th>x87SW_C2 x87SW_ES x87SW_U x87SW_U</th><th>0 0 0 • Unlock</th></malware<>	.ReadFile>		_		>	×87 ×87 ×87 ×87 ×87	StatusWe SW_B 0 SW_C1 0 SW_SF 0 SW_SF 0	000268	0	x87SW_C2 x87SW_ES x87SW_U x87SW_U	0 0 0 • Unlock
<malware.< th=""><th>ReadFile> 2CAD6 malware.e></th><th>(e:\$9DCAD6 #9DBE</th><th>16</th><th></th><th></th><th></th><th></th><th></th><th></th><th>2:3:4:5:</th><th>[esp+4] [esp+8] [esp+C] [esp+10]</th><th>072AF7E0 00000004 072AF764 00000000</th><th></th><th></th><th></th></malware.<>	ReadFile> 2CAD6 malware.e>	(e:\$9DCAD6 #9DBE	16							2:3:4:5:	[esp+4] [esp+8] [esp+C] [esp+10]	072AF7E0 00000004 072AF764 00000000			
Dump 1	Dump 2	Dump 3 💭 Dur	np 4 👹 Dump 5	🛞 Watch 1	[x=] Locals	2 Struct		072AF744 072AF748	00000 072AF	368 7E0					
Address 072AF7E0	Hex 00 00 00 00 00 00	0 00 00 00 00 0	00 BO BA CF 03	ASCII			^	072AF74C 072AF750 072AF754	00000 072AF 00000	004 764 000	return	to 072AF76	4 fro	m 072AF7	68

Figure 74

A JSON form containing the encryption cipher (AES), the AES key used to encrypt the file, the data, and the chunk size, is constructed in the process memory:

Address	He	Hex															ASCII
03D13F80	7B	22	76	65	72	73	69	6F	6E	22	ЗA	30	2C	22	6D	6F	{"version":0,"mo
03D13F90	64	65	22	3A	22	46	75	6C	6C	22	2C	22	63	69	70	68	de":"Full","ciph
03D13FA0	65	72	22	3A	22	41	65	73	22	2C	22	70	72	69	76	61	er":"Aes","priva
03D13FB0	74	65	5F	6B	65	79	22	3A	5 B	31	38	34	2C	31	32	39	te_key":[184,129
03D13FC0	2C	31	34	37	2C	31	31	36	2C	34	32	2C	32	31	31	2C	,147,116,42,211,
03D13FD0	35	35	2C	38	31	2C	34	33	2C	31	39	37	2C	31	35	2C	55,81,43,197,15,
03D13FE0	32	34	33	2C	31	31	30	2C	32	33	33	2C	32	33	36	2C	243,110,233,236,
03D13FF0	31	37	35	5D	2C	22	64	61	74	61	5F	73	69	7A	65	22	175],"data_size"
03D14000	3A	31	30	30	30	2C	22	63	68	75	6E	6B	5F	73	69	7A	:1000,"chunk_siz
03D14010	65	22	ЗA	32	35	33	36	32	38	31	36	2C	22	66	69	6E	e":25362816,"fin
03D14020	69	73	68	65	64	22	3A	66	61	6C	73	65	7D	FO	AD	BA	ished":false}0.°
																	-

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:





Address	He	ĸ							9.9				2				ASCII
03D04BD8	7D	65	73	6C	61	66	3A	22	64	65	68	73	69	6E	69	66	}eslaf:"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
03D04C08	69	73	5F	61	74	61	64	22	2C	5D	35	37	31	2C	36	33	is_atad",]571,63
03D04C18	32	2C	33	33	32	2C	30	31	31	2C	33	34	32	2C	35	31	2,332,011,342,51
03D04C28	2C	37	39	31	2C	33	34	2C	31	38	2C	35	35	2C	31	31	,791,34,18,55,11
03D04C38	32	2C	32	34	2C	36	31	31	2C	37	34	31	2C	39	32	31	2,24,611,741,921
03D04C48	2C	34	38	31	5 B	3A	22	79	65	6B	5F	65	74	61	76	69	,481[:"yek_etavi
03D04C58	72	70	22	2C	22	73	65	41	22	3A	22	72	65	68	70	69	rp","seA":"rehpi
03D04C68	63	22	2C	22	6C	6C	75	46	22	3A	22	65	64	6F	6D	22	<pre>c","lluF":"edom"</pre>
03D04C78	2C	30	3A	22	6E	6F	69	73	72	65	76	22	7B	00	80	6A	,0:"noisrev"{j
03D04C88	64	88	A7	F6	63	51	17	91	B9	9F	6C	4E	BC	CC	78	CF	d.§öcQIN%İXİ
03D04C98	FB	AA	CF	08	B 8	9F	6F	02	78	DO	E9	02	70	FB	F2	B6	û°Îo.xĐé.pûò¶
03D04CA8	B4	98	C5	87	2C	C4	BD	EE	8D	B 8	3D	4F	8E	25	64	9C	.A.,A%1. =0.%d.
03D04CB8	FO	6F	3A	2C	F3	71	99	C3	C1	B 8	C4	01	AF	C1	DC	5D	do:,óq.AA Ä. ÄÜ]
03D04CC8	61	41	50	2D	62	46	28	08	10	9D	F7	8F	51	8E	02	00	aAP-bF(÷.Q
Figure 7	7																

A 4-byte border "19 47 B2 CE" that separates the encrypted file content from the encrypted AES key is written to the file:



Figure 78

The buffer that contains the AES key presented in figure 77 is encrypted with the RSA public key from the BlackCat configuration. The result is written to the file using WriteFile:



Figure 79

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

<pre></pre>	6A 00 57 51 50 52 88 6F 11 08 00 95 70 85 900084 #900184	push o push edi push ecx push eax push eax cal amalware.writeFi	le>	>	x87Stat x87SW_B x87SW_C x87SW_C x87SW_C x87SW_C y97SW_C y97SW_C y97SW_C y97SW_C y97SW_	usword 0000 0 x875W_C0 F 0 x875W_P 0 x875W_C0 10 0 x875W_C 0 x875W_E 0 x875W_U 0 x875W_U • x875W_D	2 0 5 0 0 0	
Dump 1 Dump 2	Dump 3 🔛 Dump 4 🕮 Dump	5 🛞 Watch 1 [x=] Loca	ls 🖉 Struct	072AF714 000 072AF718 072 072AF71C 000	00368 AF7A8 00004			
072AF7A8 00 00 01 00 04 00	00 00 00 00 00 00 00 00 00	00	⁽¹⁾	072AF720 072 072AF724 000	AF728 00000			

Figure 80

The file content is read by using the ReadFile function:



The file content is encrypted using the AES-128 algorithm. The malware uses the aesenc and aesenclast instructions for this purpose:

	00DD84C	7 66 OF 38 D	C DO	aesenc xmm2,xmm0
	00DD84C	66 OF 38 D	C D8	aesenc xmm3, xmm0
	00DD84D	1 66 OF 38 D	C EO	aesenc xmm4, xmm0
	00DD 84D	66 OF 38 D	C ES	aesenc xmm5, xmm0
	0000840	66 OF 38 D	C EO	aesenc xmm6, xmm0
	00000845	66 0F 38 D	C ES	
	0000845	66 0F 38 D	C C8	aesenc ymm1 ymm0
	00000046	66 OF 75 1	4 24	movide ymmuord ata ss: [asa] ymm2
	00000346		4 24 40	
	• 000D84E	66 UF 6F 5	4 24 10	movada xmm2, xmmword ptr ss: [esp+10]
	• 000D84F	66 UF 38 D	C DO	aesenc xmm2, xmm0
	00DD84F	66 OF 6F 4	1 20	movdqa xmmo, xmmword ptr ds: [ecx+20]
	00DD84F	66 OF 7F 5	4 24 10	movdqa xmmword ptr ss: esp+10, xmm2
	00DD 850	66 OF 6F 1	4 24	movdqa xmm2,xmmword ptr ss:[esp]
	00DD 85 0.	A 66 OF 38 D	C D8	aesenc xmm3,xmm0
	00DD 85 0	F 66 0F 38 D	C EO	aesenc xmm4,xmm0
	00DD851	4 66 OF 38 D	C E8	aesenc xmm5,xmm0
	00DD851	9 66 0F 38 D	C FO	aesenc xmm6, xmm0
	0000851	E 66 0F 38 D	C F8	aesenc xmm7, xmm0
	00DD852	66 OF 38 D	C C8	aesenc xmm1, xmm0
	00DD852	66 OF 38 D	C DO	aesenc xmm2.xmm0
	00000852	66 OF 7F 1	4 24	movdga xmmword ptr ss: [esp], xmm2
	0000853	66 OF 65 5	4 24 10	movdga xmm2 xmmword ptr ss: esp+10
	00000853	66 0F 38 D	0 00	assanc ymm2 ymm0
	00000853		1 20	movidaa ymm0 ymmword atr ds:[acy+20]
	0000035		4 34 10	movida versiond at scillasation versi
	0000854	66 UF /F 5	4 24 10	movdga xmmword ptr ss: esp+10, xmm2
Fi	auro 82			
;	guicoz			
le r				and the
EI	P 000087A	55		push eop
	00DD87A	1 89 E5		mov epp,esp
	00DD87A	3 53		push ebx
	00DD87A	4 8B 45 08		mov eax, dword ptr ss:[ebp+8]
	00DD87A	7 66 OF 6F 0	2	movdqa xmm0, xmmword ptr ds:[edx]
	00DD87A	B B3 F1		mov bl,F1
	00DD87A	66 OF EF 0	0	pxor xmm0, xmmword ptr ds:[eax]
	00DD87B	1 66 OF 38 D	C 42 10	aesenc xmm0, xmmword ptr ds:[edx+10]
	00DD87B	7 66 OF 38 D	C 42 20	aesenc xmm0, xmmword ptr ds: [edx+20]
	00DD87B	66 0F 38 D	42 30	aesenc xmm0, xmmword ptr ds:[edx+30]
				and and summary and atta day forder to 1
	0000.87C	31 66 0F 38 D	C 42 40	aesenc xmmu, xmmword prr ds:ledx+401
	00DD 87C 00DD 87C	66 OF 38 D	C 42 40 C 42 50	aesenc xmm0, xmmword ptr ds:[edx+40]
	00DD 87C 00DD 87C 00DD 87C 00DD 87C	66 0F 38 D 66 0F 38 D 66 0F 38 D	C 42 40 C 42 50 C 42 60	aesenc xmm0, xmmword ptr ds:[edx+40] aesenc xmm0, xmmword ptr ds:[edx+50]
	 00DD 87C 00DD 87C 00DD 87C 00DD 87C 	66 0F 38 D 66 0F 38 D 66 0F 38 D 66 0F 38 D	C 42 40 C 42 50 C 42 60 C 42 70	aesenc xmm0, xmmword ptr ds: [edx+40] aesenc xmm0, xmmword ptr ds: [edx+50] aesenc xmm0, xmmword ptr ds: [edx+60]
	00DD 87C 00DD 87C 00DD 87C 00DD 87C 00DD 87C 00DD 87D 00DD 87D	66 OF 38 D 66 OF 38 D 66 OF 38 D 66 OF 38 D 66 OF 38 D	C 42 40 C 42 50 C 42 60 C 42 70 C 42 70	aesenc xmm0, xmmword ptr ds: [edx+40] aesenc xmm0, xmmword ptr ds: [edx+50] aesenc xmm0, xmmword ptr ds: [edx+60] aesenc xmm0, xmmword ptr ds: [edx+70]
	00DD 87C 00DD 87C 00DD 87C 00DD 87C 00DD 87C 00DD 87C 00DD 87D 00DD 87D 00DD 87D 00DD 87D	66 OF 38 D 66 OF 38 D	C 42 40 C 42 50 C 42 60 C 42 70 C 42 70 C 82 80 00 00	aesenc xmm0, xmmword ptr ds: [edx+40] aesenc xmm0, xmmword ptr ds: [edx+50] aesenc xmm0, xmmword ptr ds: [edx+60] aesenc xmm0, xmmword ptr ds: [edx+80]
	ODD 87C ODD 87C ODD 87C ODD 87C ODD 87C ODD 87D ODD 87D ODD 87D ODD 87D	66 0F 38 D 66 0F 38 D 66 0F 38 D 66 0F 38 D 66 0F 38 D 8 66 0F 38 D 8 66 0F 38 D 4 86 1D <u>FE 8</u>	C 42 40 C 42 50 C 42 60 C 42 70 C 82 80 00 00 B 6E 01	aesenc xmm0, xmmword ptr ds: [edx+40] aesenc xmm0, xmmword ptr ds: [edx+50] aesenc xmm0, xmmword ptr ds: [edx+60] aesenc xmm0, xmmword ptr ds: [edx+80] xchg byte ptr ds: [16E8BFE] b1
	ODD 87C ODD 87C ODD 87C ODD 87C ODD 87C ODD 87D ODD 87D ODD 87E ODD 87E	3 66 0F 38 D 9 66 0F 38 D 9 66 0F 38 D 66 0F 38 D 38 D 5 66 0F 38 D 66 0F 38 D 38 D 66 0F 38 D 58 D 4 86 1D FE 8 66 0F 38 D 58 D	C 42 40 C 42 50 C 42 60 C 42 70 C 82 80 00 00 <u>B 6E 01</u> C 82 90 00 00	<pre>aesenc xmm0,xmmword ptr ds:[edx+40] aesenc xmm0,xmmword ptr ds:[edx+50] aesenc xmm0,xmmword ptr ds:[edx+60] aesenc xmm0,xmmword ptr ds:[edx+70] 00 aesenc xmm0,xmmword ptr ds:[edx+80] xchg byte ptr ds:[16E8BEE],b1 00 aesenc xmm0,xmmword ptr ds:[edx+90]</pre>
	ODD S7C ODD S7C ODD S7C ODD S7C ODD S7D ODD S7D ODD S7D ODD S7E ODD S7E ODD S7E ODD S7E ODD S7E	66 0F 38 D 66 0F 38 D 66 0F 38 D 66 0F 38 D 66 0F 38 D 8 66 0F 38 D 8 66 0F 38 D 4 86 1D FE 8 A 66 0F 78 D 3 66 0F 77 0	C 42 40 C 42 50 C 42 60 C 42 70 C 82 80 00 00 B 6E 01 C 82 90 00 00 0	<pre>aesenc xmm0, xmmword ptr ds: [edx+40] aesenc xmm0, xmmword ptr ds: [edx+50] aesenc xmm0, xmmword ptr ds: [edx+60] aesenc xmm0, xmmword ptr ds: [edx+80] xchg byte ptr ds: [16E8BFE], b1 00 aesenc xmm0, xmmword ptr ds: [edx+90] movdqa xmmword ptr ds: [eax], xmm0</pre>
	 00DD 87C 00DD 87C 00DD 87C 00DD 87C 00DD 87D 00DD 87D 00DD 87E 00DD 87F 00DD 87F 00DD 87F 	3 66 0F 38 D 9 66 0F 38 D 5 66 0F 38 D 6 0 F 38 D 5 66 0F 38 D 6 0 F 38 D 4 86 1D FE 8 A 66 0 F 38 D 3 66 0 F 38 D 7 66 0 F 38 D	$ \begin{array}{cccc} 42 & 40 \\ C & 42 & 50 \\ C & 42 & 60 \\ C & 42 & 70 \\ C & 82 & 80 & 00 & 00 \\ \hline C & 82 & 90 & 00 & 00 \\ C & 82 & 90 & 00 & 00 \\ 0 & 0 \\ \end{array} $	<pre>aesenc xmm0,xmmword ptr ds:[edx+40] aesenc xmm0,xmmword ptr ds:[edx+50] aesenc xmm0,xmmword ptr ds:[edx+60] aesenc xmm0,xmmword ptr ds:[edx+70] xchg byte ptr ds:[16E8BFE],b1 00 aesenc xmm0,xmmword ptr ds:[edx+90] movdqa xmmword ptr ds:[edx+90] 00 aesenclast xmm0,xmmword ptr ds:[edx+A0]</pre>

Figure 83

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

Ols2CD7E 6A 00 Ols2CD7E 6A 00 Ols2CD80 57 Ols2CD81 51 Ols2CD81 52 Ols2CD82 50 Ols2CD83 52 Ols2CD83 Ols2CD83	push 0 push edi push ecx push eax push edx call cmalware.writeFile>	x875%LE0 0000 x875%LE0 x875%LC2 0 x875%LC1 0 x875%LC3 0 x875%LC2 0 x875%LC1 0 x875%LC0 0 x875%LE 0 x875%L5F 0 x875%LE 0 0 x875%L5F 0 x875%LE 0 0 befault (stdcall)
<malware.writefile> .text:0162CD84 malware.exe:\$90CD84 #90C184</malware.writefile>		1: [esp] 0000368 2: [esp+4] 06268020 3: [esp+8] 00003E8 4: [esp+5] 0652F508 5: [esp+10] 0000000
Image: Constraint of the state of	Dump 5 1 Ix= Locals 2 Struct 053 055 ASCII ASCII 0	24521 0000368 24480 06268020 24470 006258020 25400 0652508 25500 0652508 25500 0000000 25500 0652508

An example of an encrypted file is displayed below:

sica.txt.uhwuvzu

$\begin{array}{c} 000001100 \\ 000001100 \\ 000001100 \\ 18 & C BB F 0 38 C D T EB 79 F6 C CA 2E 3C CE 96 12 84 78 CO KG=062(TÅN 56.A.') \\ 000001100 \\ 18 & C BB F 0 38 76 C D C EA A CA 46 40 87 56 59 08 \\ KG=062(TÅN 56.A.') \\ 000001100 \\ 19 126 2A 78 129 03 029 40 B9 95 CT 8 EE D 75 A CO CC TÅN 56.A.') \\ 00000210 \\ 91 26 2A 78 129 22 38 6E 91 5A 43 E9 4F B1 A7 AA CB '+x.5n.'2C6045*E \\ 00000220 \\ 92 51 9B 53 1B D8 19 50 EF FA 61 2F 41 DF CE 94 20.5.0.F1da(A.f., 00000230 \\ 69 84 2C 8B 20 0C E8 79 FD 01 17 42 24 AA 61 CD \\ 1, '.eyy.B5*af \\ 00000220 \\ 69 84 2C 8B 20 0C E8 79 FD 01 17 42 24 AA 61 CD \\ 1, '.eyy.B5*af \\ 00000230 \\ 69 A1 E4 2C 73 30 7E B1 87 78 7B 9D AD 4D 8A 75 1;A,60-±se(ÅE1 00000240 \\ 69 A1 E4 2C 73 30 7E B1 87 78 7B 9D AD 4D 8A 75 1;A,60-±se(ÅE1 00000240 \\ 84 E2 B6 2A 661 80 33 AF P0 A1C 65 55 E8 75, A(F.',, *$	Offset(h)	00	01	02	03	04	05	06	07	08	09	OA	OВ	oc	OD	OE	OF	
$\begin{array}{c} 00000100 \\ 0000100 \\ 0000100 \\ 017 $	000001B0	DD	63	AC	D7	EB	79	F6	CA	2E	3C	CE	98	12	84	78	CO	Ýc¬×ëyöÊ.<î~."xÀ
$\begin{array}{c} 0 = 0 = 0 = 0 \\ 0 = 0 = 0 = 0 \\ 0 = 0 =$	000001C0	4B	80	BB	FO	38	76	CD	CE	AA	CA	46	4D	87	56	59	08	KŒ>ð8vÍÎ*ÊFM‡VY.
$\begin{array}{c} 000001E0 & C0 & 69 & 43 & E9 & 05 & 09 & 30 & 29 & 40 & B9 & 95 & CE & 78 & EE & D9 & Ab & Åicé0) e^{1+ExiO^+} \\ 00000210 & 68 & 31 & A7 & 1C & 32 & 2C & 59 & 16 & 9C & 53 & CE & 2A & 06 & 2D & B6 & D^+ & LS & 15 & 2.5 & 2.5 & 2.5 & 2.5 & 2.6 & 2.0 & 2.6 & 2.5$	000001D0	E7	51	F8	C7	3A	9F	C4	4E	88	8A	F2	1E	41	5F	B7	7D	çQøÇ:ŸÄN^Šò.A ·}
$\begin{array}{c} 000001F0 & 91 \ 26 \ 2A \ 78 \ 2E \ 38 \ 6E \ 91 \ 5A \ 43 \ E9 \ 4F \ B1 \ A7 \ AA \ CB \ '4*x. 9n `2C604s \ E \\ 00000220 & 9E \ 51 \ 9B \ 53 \ 1B \ D8 \ 19 \ 50 \ EF \ FA \ 61 \ 2F \ 41 \ 0F \ CE \ 84 \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 20 \ S. 9F \ 1a \ AA \ AC \ 1a \ 1a \ AA \ AC \ AA \ AC \ AA \ AC \ AA \ AC \ AA \ AC \ AA \ AC \ AA \ AC \ AA \ AC \ AA \ AC \ AA \ AA \ AC \ AA \ $	000001E0	CO	69	43	E9	05	09	30	29	40	B9	95	CB	78	EE	D9	A8	ÀiCé0)@'•ËxîÙ"
$\begin{array}{c} 00000200 \\ 0 = 0 & 51 & A7 & 1C & 32 & 2C & 59 & 16 & 9C & 53 & C8 & 2A & 06 & 2D & B6 & 07 \\ 00000220 & 27 & 66 & F4 & E8 & 1A & F1 & E7 & 82 & 9E & C8 & 1A & D0 & B9 & 83 & C0 & 51 \\ 00000220 & 55 & 01 & 4E & C4 & D5 & D2 & 85 & 52 & 63 & 03 & F0 & B9 & 1D & 8D & E8 & A1 \\ 00000240 & 55 & 01 & 4E & C4 & D5 & D2 & 85 & 52 & 63 & 03 & F0 & B9 & 1D & 8D & E8 & A1 \\ 00000250 & 69 & A1 & E2 & C6 & C8 & 79 & D1 & 17 & 22 & 4A & 61 & CD \\ 00000220 & C7 & B8 & B7 & 46 & D5 & 95 & BA & A1 & C6 & 69 & 56 & E8 & 75 \\ 00000220 & AC & TB & 83 & F7 & 60 & 51 & 64 & 30 & A2 & F7 & F3 & A1 \\ 00000220 & AC & TB & 83 & F7 & 60 & B1 & 47 & F7 & 78 & BA & D4 & D4 & 87 & 71 \\ 00000220 & AC & TB & 83 & F7 & 66 & 18 & 03 & 35 & FA & 2D & F7 & 61 & 15 & 47 & 22 & -4f^{+1}, -c. & -i. & 0'. \\ 00000200 & AC & CB & S0 & 9 & B6 & A3 & 5C & A2 & DF & 9F & 81 & 3E & A2 & F7 & FA \\ 00000200 & A7 & CF & CS & BC & 09 & FC & 81 & 98 & 81 & B0 & 01 & 57 & EC & 20 & 2T & 71 & 25 & 74 & -2. \\ 00000200 & A7 & CF & CS & BC & 09 & FC & 81 & 98 & 81 & ED & CP & DE & 59 & 11 & 41 & UADA2. & 0'IDA2. & 0'$	000001F0	91	26	2A	78	2E	38	6E	91	5A	43	E9	4F	Bl	A7	AA	CB	`&*x.8n`ZCéO±§ªË
00000210 9E 51 98 53 18 D8 19 50 EE FA 61 2F 41 0F CE 44 20>.6.Piúa/A.f. 00000220 27 66 F4 E8 1A F1 E7 89 92 C8 1A D0 B9 83 C0 51 'fde.hd.ZE.brjAQ 00000220 65 84 2C 88 20 0C E8 79 FD 01 17 42 24 AA 61 D DN B0 E8 A1 U.NÅČ.R.cðt.ei 00000250 65 A1 E4 2C F3 30 7E B1 87 F8 7B 9D AD 4D 8A 75 I;A,óo-±±e(.MŠu 00000270 AC 7B 83 B7 46 05 19 63 2B A4 8D 84 A9 27 18 27 Catter 1fvèu 00000280 42 EE 87 68 B3 D4 67 8D 84 7E 70 3C C9 51 04 10 BiŽvidgmpcÉ0 00000280 A2 EE 87 76 B3 D4 67 8D 84 7E 70 3C C9 51 04 10 BiŽvidgmpcÉ0 00000280 A2 CE 80 76 16 B3 95 8A 32 B8 90 15 7E EC 0 CHT 2.o-Sjm1 00000280 A7 CE 7C 5 BC 09 7E C8 19 83 ED CD 2C 42 76 1E 94 IfAi2.fij.Bv." 00000280 A2 CE 7 37 C8 33 BC C9 2D 75 1F 2F A4 E1 3D 02 A 4C C1 Iu.1:.0265.a.*x4 00000280 D2 T 16 E8 75 EA 13 B3 1D 18 8A 53 E9 12 AA 4C C1 Iu.1:.1:.0265.a.*x4 00000280 D2 T 16 E8 7F EA 8E 31 83 1C 11 18 B3 EF 3C 90 27 #280.d.*.E1/J.P.M*. 00000300 D2 38 06 16 50 E7 12 C 92 55 0B A3 7 #3.of A.d.Acdata	00000200	68	31	A7	1C	32	2C	59	16	9C	53	C8	2A	06	2D	B6	OF	hl§.2,Y.œSÈ*¶.
$\begin{array}{c} 00000220 & 27 & 66 & F4 E8 & 1A F1 E7 & 82 & 9E C8 1A D0 B9 & 83 c0 3 \\ 00000240 & 55 & 01 & 4E C4 D5 & 82 & 85 & 52 & 63 & 03 F0 B9 1D & 8D F8 & 11 \\ 00000260 & 69 & 14 E 4 C F3 & 30 & 7E B1 87 F8 7B & 9D & D0 & 8A 75 \\ 1; & 00-x^{+}ef (K) \\ 00000260 & 44 E2 B6 & 2A & 66 18 & 03 & 3A FB & 0A 1C & 66 & 69 & 56 & F3 \\ 00000260 & 42 & EE & 87 & 6B & 04 & 67 & 8D & 84 & 80 & 27 & 18 & 22 \\ 00000260 & 42 & EE & 87 & 6B & 04 & 67 & 8D & 84 & 80 & 27 & 18 & 22 \\ 00000260 & 42 & EE & 87 & 6B & 04 & 67 & 8D & 84 & 80 & 27 & 18 & 22 \\ 00000260 & 42 & EE & 87 & 6B & 30 & 67 & 8D & 84 & 8D & 74 & 97 & 77 &K & 3] & 68 \\ 00000260 & 42 & EE & 82 & 76 & B3 & 24 & 2D & 97 & 81 & 3E & 4A & 2F & 7E & 7A \\ 00000260 & 3C & 48 & CB & 7C & 16 & 2B & 95 & 8A & 3B & B9 & 91 & 57 & FZ & C2 & 0 \\ 00000220 & 5E & 77 & C3 & 90 & CS & 21 & 9 & 91 & 6A 7A & 16 & FZ & ED 1 & 94 \\ (WADA2.0') & $	00000210	9E	51	9B	53	1B	D8	19	50	EE	FA	61	2F	41	OF	CE	84	žQ>S.Ø.Pîúa/A.΄
00000230 65 84 2C 88 20 0C E8 79 FD 01 17 42 24 AA 61 CD i.,, eyyBs*ai 00000250 65 A1 E4 2C F3 30 7E B1 87 F8 7B 9D AD 4D 8A 75 1;8,60~±±0(.MŠu 00000260 84 E2 B6 2A 66 18 03 3A FB 0A 1C 66 69 56 E8 75 ,, 00000270 AC 7B 83 B7 46 05 19 63 2B A4 8D B4 A9 27 18 22	00000220	27	66	F4	E8	1A	Fl	E7	8E	9E	C8	1A	DO	B9	83	CO	51	'fôè.ñ玞È.Đ`fÀQ
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000230	69	84	2C	8B	20	0C	E8	79	FD	01	17	42	24	AA	61	CD	i",≺ .èyýB\$ªaÍ
$\begin{array}{c} 00000250 & 69 \ Al \ E4 \ 2C \ F3 \ 30 \ 7E \ Bl \ 87 \ F8 \ 7B \ 9D \ AD \ 4D \ 87 \ 75 \ i, i, do-\pm i, i, i, fi Veu Agtr.iu.fiVeu \ Agtr.iu.fiveu \ Agtr.fiveu \ Agtr.iu.fiveu \ Agtr.fiveu \ Agtr$	00000240	55	01	4E	C4	D5	B2	85	52	63	03	FO	B9	lD	8D	E8	Al	U.NÃÕ ⁴ Rc.ð ¹ è;
$\begin{array}{c} 00000260 & 84 \ E2 \ B6 \ 2A \ 66 \ 18 \ 03 \ 3A \ FB \ 0A \ 1C \ 66 \ 69 \ 56 \ E7 \ 75 \ , \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $	00000250	69	Al	E4	2C	F3	30	7E	Bl	87	F8	7B	9D	AD	4D	8A	75	i;ä,ó0~±≠ø{MŠu
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000260	84	E2	B6	2A	66	18	03	ЗA	FB	OA	1C	66	69	56	E8	75	"â¶*f:ûfiVèu
$\begin{array}{c} 00000220 & 42 \ EE \ 8E \ 76 \ B3 \ D4 \ 67 \ 8D \ B4 \ 7E \ 70 \ 3C \ C9 \ 51 \ 04 \ 10 \ Bi2v^0 \ Gr (~p$	00000270	AC	7B	83	B7	46	05	19	63	2B	A4	8D	B4	A9	27	18	22	¬{f · Fc+¤. '©'."
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000280	42	EE	8E	76	B 3	D4	67	8D	B4	7E	70	3C	C9	51	04	10	BîZv'Og. ~p <eq< td=""></eq<>
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	00000290	08	AO	99	9B	6A	33	5C	A2	DF	9F	81	3E	4A	2F	7E	7A	™>j3\¢BY.>J/~z
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	000002A0	8C	48	8C	B7	C8	16	D3	95	8A	83	BB	90	15	7E	EC	20	CHE E.O.Sf»~1
$\begin{array}{c} 000002C0 & 58 \ 77 \ C3 \ D9 \ C5 \ 32 \ 19 \ D3 \ 91 \ 6A \ 7A \ 16 \ F2 \ AE \ D1 \ 94 \ [vAUA2.0^{+}z.68N^{+}.selfdegG\\ 000002E0 \ A2 \ CF \ 8A \ RA \ 22 \ 18 \ 8A \ EA \ CF \ DE \ P9 \ 14 \ 7I \ 4EXU6^{+}v^{+}.selfdegG\\ 000002E0 \ A2 \ CF \ 37 \ C8 \ 33 \ BC \ C9 \ 2D \ 75 \ 1F \ 2F \ A4 \ E1 \ 3D \ 02 \ A9 \ c17E346_{-}u,/Aa_{-}Ge\\ 00000300 \ 32 \ 38 \ D6 \ 15 \ D4 \ 3C \ 94 \ 2A \ C8 \ 1E \ 55 \ 27 \ 11 \ B6 \ 63 \ 10 \ 286.6^{-}v^{E}.U.gGe.\\ 00000300 \ 32 \ 38 \ D6 \ 15 \ D4 \ 3C \ 94 \ 2A \ C8 \ 1E \ 55 \ 27 \ 11 \ B6 \ 63 \ 10 \ 286.6^{-}v^{E}.U.gGe.\\ 00000300 \ 32 \ 38 \ D6 \ 15 \ D4 \ 3C \ 94 \ 2A \ C8 \ 1E \ 55 \ 27 \ 11 \ B6 \ 63 \ 10 \ 286.6^{-}v^{E}.U.gGe.\\ 00000300 \ 87 \ 1E \ 87 \ FE \ A8 \ E3 \ 183 \ 1C \ 11 \ B3 \ EF \ 3C \ 90 \ 27 \ 1.4.e^{2}15, \ N.^{+}c.'\\ 00000330 \ B0 \ A1 \ 05 \ 9A \ 92 \ 30 \ F1 \ 60 \ 50 \ E7 \ 25 \ 50 \ BA \ 37 \ ^{\circ} \ .5^{\circ} 06 \ F. \ 66 \ F. \ 66 \ FE \ 96 \ 75 \ 67 \ F. \ 67 \ F. \ 70 \ 70 \ 70 \ 70 \ 63 \ 88 \ 7C \ AC \ 84 \ F0 \ EB \ A0 \ 25 \ 13 \ 56 \ 63 \ 91 \ F6 \ \ 1c^{-}, \ -, \ 70^{-} \ -, \ 70^{-} \ 8.^{+} \ VC^{+} \ 00000380 \ 04 \ 31 \ 09 \ 56 \ 59 \ 49 \ CD \ 1F \ 00 \ 65 \ 33 \ 34 \ 0E \ F7 \ 99 \ 13 \ .1.VYIIe34.+^{\rm m}.\\ 00000380 \ 04 \ 31 \ 09 \ 56 \ 59 \ 49 \ CD \ 1F \ 00 \ 65 \ 33 \ 34 \ 0E \ F7 \ 99 \ 13 \ .1.VYIIe34.+^{\rm m}.\\ 00000380 \ 04 \ 41 \ 5C \ 85 \ 49 \ 5D \ 1F \ 60 \ 71 \ 70 \ 70 \ 70 \ 1.8V^{+} \ 1.8V^{+} \ 70 \ 70 \ 70 \ 70 \ 70 \ 70 \ 70 \ 7$	000002B0	A7	CF	C5	BC	09	7E	C8	19	83	ED	CD	2C	42	76	1E	94	SIA4.~E.fiI,Bv."
$\begin{array}{c} 000002D0 \\ 00002D0 \\ b 5 23 C 6 F C F 6 AA FA 22 1A 8A EB CF DB F9 71 47 \\ 0FRUATUR SETURATION OF THE ST AT A ST A THE ST AT A THE ST A ST A A THE ST A ST A A THE ST A ST A A THE ST A ST A A THE ST A ST A A THE ST A ST A A ST A ST A ST A ST A ST A S$	000002C0	5B	77	C3	D9	C5	32	19	D3	91	6A	7A	16	F2	AE	D1	94	[wAUA2.0'jz.0@N"
$\begin{array}{c} 000002E0 & A2 \ CF 37 \ CS 33 \ BC \ C9 \ 2D \ 75 \ 1F \ 2F \ A4 \ E1 \ 3D \ 02 \ A4 \ C1 \ 10.025A \\ 00000300 \ 32 \ 32 \ 32 \ BC \ 15 \ D4 \ 3C \ 94 \ 2A \ C8 \ 1E \ 55 \ 82 \ 71 \ D8 \ 63 \ 10 \ 280 \ 0^{$	000002D0	55	23	C6	FC	F6	AA	FA	22	IA	AS	EB	CF	DB	E9	71	47	U#Euo-u".SelUeqG
$\begin{array}{c} 0000002F0 & \text{EF} \ F9 \ 0A \ 7E \ 6C \ 3A \ 1D \ S1 \ D8 \ SA \ 53 \ E4 \ 2D \ 2A \ A4 \ C1 & 10.~11. \ (DSSA-*HA \\ 00000310 & C2 \ A6 \ 60 \ D9 \ 6F \ 9B \ 55 \ 63 \ A1 \ 3B \ A7 \ 39 \ DB \ A3 \ C6 \ 00 & $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$	000002E0	A2	CF	37	C8	33	BC	C9	2D	75	lF	2F	A4	El	3D	02	A9	¢I7E34E-u./#a=.©
$\begin{array}{c} 00000300 & 32 & 38 & D6 & 15 & D4 & 3C & 94 & 2A & C8 & 1E & 55 & 82 & 71 & D8 & 63 & 10 & 280 & 0.0 < m^{+}E. 0, qdc. \\ 00000320 & 87 & 1E & E8 & 7F & EA & 8E & 31 & 83 & 1C & D1 & 1B & B3 & EF & 3C & 90 & 27 & + .e. & .21f. & .* & .* \\ 00000330 & B0 & A1 & 05 & 9A & 92 & 30 & F1 & 60 & 50 & E7 & 25 & 50 & BA & 37 & '; & .s' of `Pckk PP ^ 7 \\ 00000340 & 9C & 08 & 35 & D6 & 66 & A0 & CB & 1F & CE & 36 & 5B & E1 & 0B & 1C & FE & 09 & & .5' of `Pckk PP ^ 7 \\ 00000350 & CA & 41 & AC & D4 & 8C & 8C & E5 & 52 & 71 & 1F & B6 & 11 & EA & 2F & 5B & C9 & & .* & .* & .* & .* & .* \\ 00000370 & EC & 00 & DF & EF & A1 & 0C & 60 & 71 & 4C & 41 & 0 & 82 & 44 & D7 & 9A & 07 & .* & .* & .* & .* & .* & .* & .* \\ 00000380 & 04 & 31 & 09 & 56 & 59 & 49 & CD & 1F & 0D & 65 & 33 & 34 & 0E & F7 & 99 & 13 & & & & .* & .* & .* & .* $	000002F0	EE	F9	OA	7E	6C	3A	1D	51	DS	AS	53	E4	2D	2A	A4	Cl	iu.~1:.QØSSā-*¤A
$\begin{array}{c} 00000310 \\ 00000320 \\ 00000320 \\ 00000320 \\ 00000330 \\ 0000330 \\ 0000330 \\ 0000330 \\ 0000330 \\ 0000330 \\ 0000340 \\ 0000340 \\ 0000340 \\ 0000350 \\ 014 \\ F5 \\ 22 \\ 14 \\ F1 \\ 00000380 \\ 04 \\ 31 \\ 09 \\ 55 \\ 53 \\ 14 \\ F5 \\ 22 \\ 14 \\ F1 \\ 0000380 \\ 014 \\ F5 \\ 22 \\ 14 \\ F1 \\ 0000380 \\ 014 \\ F5 \\ 22 \\ 14 \\ F1 \\ 0000380 \\ 014 \\ F5 \\ 22 \\ 14 \\ F1 \\ 0000380 \\ 014 \\ F5 \\ 22 \\ 14 \\ F1 \\ 0000380 \\ 014 \\ F5 \\ 22 \\ 14 \\ F1 \\ 0000380 \\ 014 \\ F5 \\ 22 \\ 14 \\ F1 \\ 0000380 \\ 014 \\ F5 \\ 22 \\ 14 \\ F1 \\ 0000380 \\ 014 \\ F1 \\ F1 \\ F1 \\ F1 \\ F1 \\ F1 \\ F1 \\ $	00000300	32	38	De	15	D4	30	94	ZA	C8	1E	55	82	71	DS	63	10	280.0<"*E.U,qØC.
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000310	C2	Ab	60	D9	6F.	98	55	63	AL	38	A./	39	DB	A3	C6	00	A; UOSUC; SULA.
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000320	87	1E	E8	7F	EA	8E	31	83	10	DI	18	B3	EF	30	90	27	‡.e.eZlf.N.ºi<.'
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000330	BO	AL	05	9A	92	30	FI	60	50	E7	25	69	25	50	BA	37	i.s' On PC%E%P07
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000340	90	80	35	De	66	AO	CB	IF	CE	36	58	EL	OB	IC	FE	09	œ.501 E.16[ap.
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000350	CA	41	AC	D4	80	80	ES	52	71	TE	Bo	11	EA	21	58	09	EA-OEEaRq.4.e/[E
$\begin{array}{c} 00000380 & 04 & 31 & 09 & 56 & 59 & 49 & CD & 1F & 0D & 65 & 33 & 34 & 0E & F7 & 99 & 13 & 1.81', & qLA, D×S. \\ 00000380 & 14 & F5 & 22 & 14 & F1 & 0D & CA & C5 & 35 & 8D & 2A & 70 & B6 & 60 & AA & A3 & .5".f. & EAS.*pT`*£ \\ 000003B0 & 04 & 69 & 6D & 4A & 5A & F3 & 83 & 94 & 1D & 58 & E0 & FE & 2C & E1 & FD & 89 & .imJZ6f". Xàþ, áýt \\ 000003C0 & E7 & 9C & E4 & 72 & 5E & AA & CB & 76 & 74 & 27 & F1 & 99 & 28 & 98 & 7D & 13 & .cmZ76f".Xàþ, áýt \\ 000003D0 & E2 & A5 & EF & 53 & 1A & 57 & B6 & BA & 1F & 38 & 12 & 07 & EF & BD & 0E & 71 &$	00000360	70	70	63	88	10	AC	84	FU	EB	AU	25	13	50	63	91	FO	p c -,,0e %.vc 0
$\begin{array}{c} 0.0000390 & 14 \ F5 \ 22 \ 14 \ F1 \ 0D \ c3 \ 53 \ 54 \ 0D \ F7 \ 99 \ 13 \\ .1. \ 11. \ 12. \ 14. \ 53 \ .1. \ 11. \ 11. \ 12. \ 14. \ 15. \ 12. \ 14. \ 15. \ 12. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 14. \ 15. \ 15. \ 14. \ 15. \ 15. \ 14. \ 15. \ 15. \ 14. \ 15. \ 15. \ 14. \ 15. \ 15. \ 14. \ 15. \ 15. \ 14. \ 15. \ 15. \ 14. \ 15. \ 15. \ 14. \ 15. \ 15. \ 15. \ 14. \ 15. \ 15. \ 15. \ 15. \ 14. \ 15. \ 1$	00000370	EC	21	DE	EE	AL	10	CD	11	40	C4	20	24	44	57	9A	12	1.51; . qLA., D×S.
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000380	14	D1	22	14	59	49	CD	CE	25	00	22	70	DE	50	33	10	AN & \$35 *= 0.20
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000390	D.C	AF	22	17	C 0	00	72	25	33	42	CE.	07	E0	01	0.0	01	TN FFFFF7Patio
$\begin{array}{c} 00000300 & \text{EV} \ 164 \ 054 $	00000380	04	46	ED.	47	57	53	02	23	10	12	FO	57	20	51	FD	01	imT764" Vab ave
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000360	57	90	F4	72	SR	77	CB	76	74	27	FI	GG	20	0.0	70	12	cmar aFret 16PM (~)
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000300	E7	75	FF	53	17	57	BE	BA	15	30	12	07	FF	BD	OF	71	SYNS WOR & NE C
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	000003E0	OF	OF	54	09	64	FR	06	93	19	47	B2	CE	AF	69	00	OB	Z.do.".Gft_i
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	000003F0	A6	20	03	E7	79	0C	OD	AC	FD	3B	98	6B	DD	18	90	BE	.cv¬ý:~ký%
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000400	97	30	3B	44	D2	43	1D	OC	04	2D	34	74	8A	F8	6E	FD	-0; DÒC4tŠøný
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	00000410	48	19	DF	AE	9E	74	AO	F7	B5	8B	CF	80	80	44	8E	9E	H.BOŽt ÷u« ÏŒEDŽž
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000420	EA	70	EE	36	75	80	AO	2D	DD	F6	BB	B2	CA	05	BB	03	êpî6u€ -Ýö»°Ê.».
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000430	A4	F2	AO	78	13	35	89	95	EF	6F	86	26	99	F3	66	9F	¤ò x.5‰•ïot&™ófŸ
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000440	FE	7F	BE	14	28	20	90	F9	5C	28	B2	OC	7F	63	38	5B	þ.¾.(.ù\(°c8[
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00000450	FO	5F	03	98	7D	F8	87	75	9A	23	EA	3A	CD	75	94	18	ð ."}ø‡uš#ê:Íu".
00000470 53 B3 D0 F0 34 0F C9 F2 76 57 A8 66 B6 17 AA E5 S*Đ&4.ÉovW f⊈.*å 00000480 6F 29 3E DE 02 60 0A 5C A6 19 37 D7 E7 45 B1 CE o)>Þ.`.\!.7×çE±1 00000400 76 DC E4 DC DA 2B 9A 1D 16 A3 CC AE E6 64 0B B0 vÜäÜÚ+š£Ì@æd.° 00000420 BD 2C 27 E0 2B 17 13 88 6F 80 7E 1C 3F 66 9B 75 s,'à+°o€~.?f×u 00000420 C0 0C 3F 9A 4C 6C 04 7B 1B 18 89 29 46 AD 25 DD à.?šL1.(h)F.%Ý 00000420 5D 60 EE 6A 89 9B E5 34 85 74 CB 67 87 79 3A F4]`ijt>å4tÉg‡y:ô 00000420 BE 49 98 4B 9D 85 6D 3C FC 3D 16 7F 00 00 01 00 su@+ûêU[oàNVnû 0000044F0 I9 47 B2 CE	00000460	55	C3	61	9A	F8	5C	69	94	AD	1A	E7	69	5B	02	9A	F5	UÃašø\i″çi[.šõ
00000480 6F 29 3E DE 02 60 0A 5C A6 19 37 D7 E7 45 B1 CE 0)>F.`.\\:.7×çE±Î 00000490 76 DC E4 DC DA 2B 9A 1D 16 A3 CC AE E6 64 0B B0 vÜäÜÚ+š£Ì®æd.° 00000400 BD 2C 27 E0 2B 17 13 88 6F 80 7E 1C 3F 66 9B 75 's,'à+^o€~.?f>u 000004B0 CO 0C 3F 9A 4C 6C 04 7B 1B 18 89 29 46 AD 25 DD 's.?åL1(b)F.%Ý 000004D0 SD 60 EE 6A 89 9B E5 34 85 74 CB 67 87 79 3A F4]`ijt*å4tEg≠y:ô 000004D0 A7 85 FB AE F7 FB CA DC 5B F2 16 C0 4E 56 6E DB Sû@+ûÊÜ[∂.ÀNVnÛ 000004F0 BE 49 98 4B 9D 85 6D 3C FC 3D 16 7F 00 00 01 00 *irKm<<ü=	00000470	53	B 3	DO	FO	34	OF	C9	F2	76	57	A8	66	B6	17	AA	E5	S'Đ84.ÉòvW"f¶.ªå
00000490 76 DC E4 DC DA 2B 9A 1D 16 A3 CC AE E6 64 0B B0 vÜäÜÚ+š£Ì⊗æd.° 000004A0 BD 2C 27 E0 2B 17 13 88 6F 80 7E 1C 3F 66 9B 75 's,'à+^o€~.?f>u 000004B0 CO 0C 3F 9A 4C 6C 04 7B 1B 18 89 29 46 AD 25 DD À.?šLl.(m)F.%Ý 000004D0 SD 60 EE 6A 89 9B E5 34 85 74 CB 67 87 79 3A F4)`jìm>å4tËg‡y:ô 000004D0 A7 85 FB AE F7 FB CA DC 5B F2 16 C0 4E 56 6E DB Sû⊗÷ûÊÜ[∂.ÀNVnÛ 000004E0 BE 49 98 4B 9D 85 6D 3C FC 3D 16 7F 00 00 01 00 's'I~Km< <u=< td=""><td>00000480</td><td>6F</td><td>29</td><td>3E</td><td>DE</td><td>02</td><td>60</td><td>OA</td><td>5C</td><td>A6</td><td>19</td><td>37</td><td>D7</td><td>E7</td><td>45</td><td>Bl</td><td>CE</td><td>o)>₱.`.\¦.7×çE±Î</td></u=<>	00000480	6F	29	3E	DE	02	60	OA	5C	A6	19	37	D7	E7	45	Bl	CE	o)>₱.`.\¦.7×çE±Î
000004A0 BD 2C 27 E0 2B 17 13 88 6F 80 7E 1C 3F 66 9B 75 \frac{1}{2}, \\dot{\alpha}, \\dot{\alph}, \\dot{\alpha}, \\dot{\alpha}, \\alp	00000490	76	DC	E4	DC	DA	2B	9A	1D	16	A3	CC	AE	E6	64	OB	BO	vÜäÜÚ+š£Ì®æd.°
000004B0 C0 0C 3F 9A 4C 6C 04 7B 1B 18 89 29 46 AD 25 DD À.?šLl.(t)F.%Ý 000004C0 5D 60 EE 6A 89 9B E5 34 85 74 CB 67 87 79 3A F4]`1jt>å4tëg‡y:ô 000004C0 A7 85 FB AE F7 FB CA DC 5B F2 16 C0 4E 56 6E DB §û⊗÷ûÊÜ[ô.ÀNVnû 000004E0 BE 49 98 4B 9D 85 6D 3C FC 3D 16 7F 00 00 01 00 ¾I~Km<ú=	000004A0	BD	2C	27	EO	2B	17	13	88	6F	80	7E	1C	ЗF	66	9B	75	½,'à+^o€~.?f>u
000004C0 5D 60 EE 6A 89 9B E5 34 85 74 CB 67 87 79 3A F4]`îjta>å4tËg‡y:ô 000004D0 A7 85 FB AE F7 FB CA DC 5B F2 16 C0 4E 56 6E DB §û®÷ûÊÜ[ò.ÀNVnÛ 000004E0 BE 49 98 4B 9D 85 6D 3C FC 3D 16 7F 00 00 01 00 %I~Km<ü=	000004B0	CO	oc	3F	9A	4C	6C	04	7B	18	18	89	29	46	AD	25	DD	À.?šLl.{%)F.%Ý
000004D0 A7 85 FB AE F7 FB CA DC 5B F2 16 C0 4E 56 6E DB \$û⊗÷ûÊÜ[ò.ÀNVnÛ 000004E0 BE 49 98 4B 9D 85 6D 3C FC 3D 16 7F 00 00 01 00 %I~Km<<ü=	000004C0	5D	60	EE	6A	89	9B	E5	34	85	74	CB	67	87	79	зA	F4]`îj\$\$>å4tËg‡y:ô
000004E0 <u>BE 49 98 4B 9D 85 6D 3C FC 3D 16 7F 00 00 01 00</u> %I [~] Km<ü= 000004F0 <u>19 47 B2 CE</u>	000004D0	A7	85	FB	AE	F7	FB	CA	DC	5B	F2	16	CO	4E	56	6E	DB	§…û⊗÷ûÊÜ[ò.ÀNVnÛ
000004F0 <u>19 47 B2 CE</u>	000004E0	BE	49	98	4B	9D	85	6D	3C	FC	3D	16	7F	00	00	01	00	¾I″Km<ü=
	000004F0	19	47	B2	CE													.G⁴Î

Figure 85

The ransomware creates a PNG image called "RECOVER-uhwuvzu-FILES.txt.png":



Figure 87

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



Figure 88

Running with the --verbose parameter

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

Pipe

\\.\pipe__rust_anonymous_pipe1__.<Process ID>.<Random number>

BlackCat Ransom Note

RECOVER-uhwuvzu-FILES.txt

Files created

checkpoints-<Filename>.uhwuvzu

RECOVER-uhwuvzu-FILES.txt.png

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\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f"

cmd.exe /c "arp -a"

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.

The files are encrypted using the AES algorithm, with the AES key being encrypted using the RSA public key contained in the configuration. The extension of the encrypted files is changed to uhwuvzu by the malware.

Download Now



SecurityScorecard

ecurityScorecard.com securityscorecard.com Tower 49 12 E 49* Street Suite 15-001 New York, NY 10017

Join us in making the world a safer place.

Free Account Sign Up