

# BlackCat ransomware technical analysis

Additional reading



17

122223

# About BlackCat ransomware

The BlackCat ransomware, also known as ALPHV, is a potent strain of malware that targets and encrypts critical data on an infected system, subsequently demanding a ransom payment for decryption. It typically propagates through phishing campaigns, malicious downloads or exploit kits. By leveraging advanced encryption algorithms typically Rivest-Shamir-Adleman (RSA) or Advanced Encryption Standard (AES), BlackCat makes user files inaccessible and leaves ransom notes with instructions for the victim to follow to retrieve their encrypted data, usually involving payment in cryptocurrency for the decryption key.



### Technical analysis

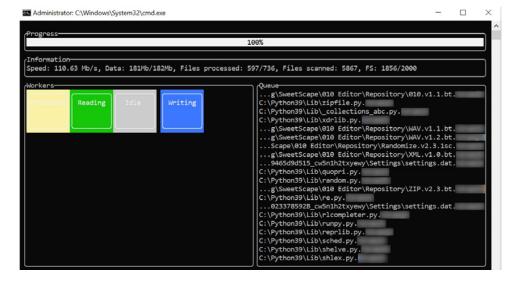
The ransomware is a significant and adaptable cyber threat, engineered in the Rust programming language, which is renowned for its performance efficiency and superior memory management. This combination facilitates the ransomware to operate seamlessly and elude standard cybersecurity scrutiny. Furthermore, Rust's inherent customization capabilities permit the ransomware to tailor its operational techniques and encryption methodologies for specific targets.



### Image 1: Help configurations

The previous iterations of the BlackCat ransomware exhibited a security flaw due to a lack of checks on the access token. However, the latest versions have eliminated this susceptibility by mandating the input of a 32-character access token for execution. This token is exclusively distributed to authorized users who have procured the ransomware usage rights. It is subsequently utilized to decrypt covert configurations nested within the ransomware infrastructure.

Moreover, the stipulation of an access token inadvertently fortifies the ransomware's resistance against automated cybersecurity mechanisms. Such mechanisms, unless specifically programmed to deliver the access token, remain unsuccessful in deriving pertinent information from the ransomware sample.



### Image 2: User interface

Upon successful input of the correct access token, the ransomware decrypts the configuration file that determines its operational parameters. Within this file are essential details like the public encryption key, the file extension utilized during encryption, identification credentials and a list of services and processes to disable, among other settings.

### Image 3: Configuration file

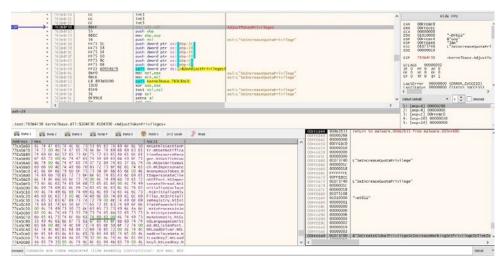


If the malware is activated without appropriate administrative permissions, it utilizes a specific exploitative technique involving Windows User Account Control (UAC) framework. More specifically, it employs the Component Object Model (COM) interface of the Centralized Manageability and Security Technology Policy LUA (CMSTPLUA), conveniently bypassing UAC restrictions and, hence attaining elevated privileges.

### Image 4: Privilege escalation using UAC bypass

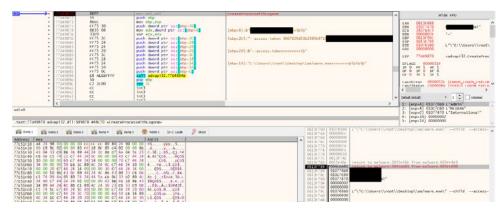


### Image 5: Respawning with additional privileges





Upon securing administrative privileges, the ransomware spawns child processes with administrative privileges to perform numerous tasks comprise but are not limited to eliminating Volume Shadow Copies (VSS), instituting registry keys and erasing event logs. To disseminate, the malware periodically tries to access other accounts on the same device using the "net use" command and attempts to mount hidden partitions.



### Image 6: Spawning child processes

Image 7: Deleting all Shadow Copy backups

P	761D88E0	8BFF	mov_edi,edi	CreateProcessW
	761D88E2	55	push ebp	
	761D88E3	8BEC	mov ebp,esp	
	761D88E5	5D	pop ebp	
	761D88E6	<ul> <li>FF25 <u>88152476</u></li> </ul>	jmp dword ptr ds:[<&CreateProcessW>]	JMP.&CreateProcessW
•	761D88EC	CC	int3	Street and the second second second
	761D88ED	CC	int3	
	761D88EE	CC	int3	
	761D88EF	CC	int3	
•	761D88F0	CC	int3	
	761D88F1	CC	int3	
	761D88F2	CC	int3	
	761D88F3	CC	int3	
	761D88F4	CC	int3	
	761D88F5	cc	int3	
	761D88F6	CC	int3	
	761D88F7	cc	int3	
	761D88F8	CC	int3	
	761D88F9	CC	int3	
	761D88FA	CC	int3	
	761D88FB	CC	int3	
	75100000	~~	3+3	1
	<			
ti=006834E8 "vss	admin.exe Dele	te Shadows /all /quie	tshadow_copy::remove_all_vss="	
		· · · · · · · · · · · · · · · · · · ·		
CONTRACT CONTRACTOR	and an an array	and the second second		
text:761D88E0 ker	me132.dll:\$18	8E0 #98E0 <createproc< td=""><td>essW&gt;</td><td></td></createproc<>	essW>	
Dump 1 Dump 1	mp 2 🔛 Dump	3 🔛 Dump 4 🔛 Dum	np 5 👼 Watch 1 🛛 🗱 🚽 Locals 🎾 Struct	
-a comp -	ing z	S Will Domp 4 Will Dom	10.0 March 1 Ivel Locals 2 Sudd	

### Image 8: Updating a registry key

	<ul> <li>761p88p7</li> </ul>	CC	l int3	
	<ul> <li>76108808</li> </ul>	CC	int3	
	<ul> <li>76108809</li> </ul>	CC	int3	
	<ul> <li>7610880A</li> </ul>	CC	int3	
	<ul> <li>76108808</li> </ul>	CC	int3	
	<ul> <li>7610880C</li> </ul>	CC	int3	
	<ul> <li>76108800</li> </ul>	CC	int3	
	<ul> <li>761D88DE</li> </ul>	CC	int3	
	• 761D88DF	CC CC CC CC	int3	
$\rightarrow$		SEFF	sov edi.edi	CreateProcessW
	<ul> <li>761D88E2</li> </ul>	55	push cbp	
	<ul> <li>761D88E3</li> </ul>	SBEC	mov ebp, esp	
	<ul> <li>76108865</li> </ul>	5D	pop ebp	
	<ul> <li>761088E6</li> </ul>	<ul> <li>FF25 88152476</li> </ul>	jnp dword ptr ds:[<&CreateProcessM>]	3NP.&CreateProcessW
	<ul> <li>761088EC</li> </ul>	CC	int3	
	<ul> <li>761D88ED</li> </ul>	cc	int3	
	<ul> <li>761088EE</li> </ul>	CC	int3	
	<ul> <li>761088EF</li> </ul>	CC	int3	
	<ul> <li>761088F0</li> </ul>	CC	int3	
	<ul> <li>761088F1</li> </ul>	CC	int3	
	<ul> <li>761088F2</li> </ul>	CC	int3	
	· Trincers	~~	1.4.5	
	<			>



The ransomware administers a multi-vector approach designed to neutralize the host's security defenses and mitigate potential disruption of file-locking mechanisms that could compromise its encryption efficacy. To achieve this, it terminates specific system services as well as currently active process threads that is listed in the configurations in the two tables.

### Image 9: OpenSCManagerW enumerate all services



Image 10: Checking if the service is active using EnumDependentServicesW Function (0x01 would mean that the service is active)



## Image 11: Stopping the service with ControlService Function 0x01 (Service\_Control\_Stop)

	<ul> <li>765854A0</li> </ul>	6A 10	push 10	ControlService	
1	<ul> <li>765854A2</li> </ul>	68 A0406076	push sechost.766040A0		
	<ul> <li>765854A7</li> </ul>	E8 F81F0100	call sechost.765C74A4		
	<ul> <li>765854AC</li> </ul>	8365 FC 00	and dword ptr ss:[ebp-4],0		
1	<ul> <li>76585480</li> </ul>	FF75 10	push dword ptr ss:[ebp+10]		
	<ul> <li>76585483</li> </ul>	FF75 OC	push dword ptr ss:[ebp+C]		
	1				>

.text:765B54A0 sechost.dll:\$154A0 #148A0 <ControlService>

Services targeted		
acronisagent	gxcvd	mvarmor64
acrsch2svc	gxfwd	mysql
backup	gxmmm	mysql\$
backupexecagentaccelerator	gxvss	pdvfsservice
backupexecagentbrowser	gxvsshwprov	qbcfmonitorservice
backupexecdivecimediaservice	mepocs	qbdbmgrn
backupexecjobengine	memtas	qbidpservice
backupexecmanagementservice	msexchange	sap
backupexecrpcservice	msexchange\$	sap\$
backupexecvssprovider	mvarmor	sapd\$
gxblr	mvarmor64	saphostcontrol
gxclmgrs	mysql	saphostexec
gxcimgr	mysql\$	sophos

### Table 1: Services targeted threads

### Image 12: Gathering a snapshot of all current processes



### Image 13: Selecting a process via OpenProcess function

<ul> <li>77057270</li> <li>77057272</li> <li>77057273</li> </ul>	88FF 55 88EC	mov edi,edi push ebp mov ebp,esp	OpenProcess	
• 77057275 • 77057278 • 77057278	83EC 24 8845 10 33C9	<pre>sub esp,24 mov eax,dword ptr ss:[ebp+10] xor ecx,ecx</pre>		
<				

## Image 14: Terminating the function selected with TerminateProcess function

	77045893 77045895 77045899 7704589F	8BEC 837D 08 00 • 0F84 EDE90500 FF75 0C	<pre>mov ebp.esp cmp dword ptr ss:[ebp+8],0 je kernelbase.770A458C push dword ptr ss:[ebp+C]</pre>	[ehnac]+"M7"	
1	<				>

.text:77045890 kernelbase.dll:\$105890 #104F90 <TerminateProcess>

Processes targeted		
sql	cvfwd	onenote
agntsvc	cvmountd	oracle
avagent	cvods	outlook
avscc	dbeng50	powerpnt
bedbh	dbsnmp	pvlsvr
benetns	dellsystemdetect	qbcfmonitorservice
bengien	encsvc	qbdbmgrn
beserver	enterpriseclient	qbidpservice
cagservice	excel	raw_agent_svc
cvd	firefox	sap

### Table 2: Processes targeted threads

The ransomware then clears logs and attempts to propagate to other computers within the networks with "net use" command.

### Image 15: Clearing AMSI Debug Logs



### Image 16: Clearing Application Logs

IP	<ul> <li>759488</li> <li>759488</li> <li>759488</li> <li>759488</li> <li>759488</li> </ul>	CC         88FF           4E2         55           4F3         88EC	int3 mov edi.edi push ebp mov ebp.esp	CreateProcessw
1: 01000.30 "		cation\"ðº\r𺫫««««««	ībīb"	

### Image 17: Using "Net Use" to move to other networks

	1	759488DF	CC	int3	
P	$\rightarrow$	759488E0	8BFF	nov edi,edi	CreateProcessW
		759488E2 759488E3	55 8BEC	push ebp mov ebp.esp	
	1	<			
i=01605D28 "net	use \\\\DESH	TOP- /	user:	/persistent:noð%\rð	"didi»»»»»»°61/°61/°61/°61/°61/°61/°61/°61/°61/°61/

The ransomware traverses every directory within the system and drops its ransom note.

1		1 //05	/40F		CC			1	1nt3				
		7705	7410		6A ]				push				WriteFile
		7705 7705 7705 7705 7705 7705 7705 7705	7417 741c 741e 7421 7424 7429 7429 7429 7429 7420 7420 7430 7430 7433 7439 7430	× × × :	E8 3 33C9 8940 8940 8875 85F6 74 0 8906 8870 83FF 0F84 83FF 0F84 83FF	0 E0 E4 14 02 08 F4 0314 F5 E913	0500 0500		call xor e mov c mov e test je ke cmp e je ke cmp e je ke cmp e	kernelbase.77 kernelbase.77 kov,ecx word ptr ss: si,dword ptr ss: esi,esi ernelbase.770 word ptr ds: fi,dword ptr di,FFFFFF4 ernelbase.770 di,FFFFFF5 melbase.770 di,FFFFFF5	709E2B0 ebp-20 bp-1C ss:eb 5742D (esi),e ss:eb A883C A882B	,ecx ,ecx pp+14	edi:">> What happened?\r\n\ edi:">> What happened?\r\n\ edi:">> What happened?\r\n\
	7470.1					****							
text:77057	7410 ke			11: <b>\$</b> 1 Dump 3		#1168		iteFi Dump5		Watch 1 [x=]	Locals	Struct	
Dump 1										Watch 1 [x=]	Locals	y struct	
Dump 1 dress H 16676F0 3	Hex 3E 3E 2	ump 2	<b>68</b> 61	2000 3	20 68	Dump 4	70 65	Dump 5	5 64	ASCII	pened	🐉 Struct	
Dump 1 ddress H 16676F0 3 1667700 3	Hex BE 3E 2 3F 0D 0	ump 2 20 57 0A 0D	68 61 0A 49	74 6D	20 68 70 6F	Dump 4	70 65 61 68	Dump 5	5 64 0 66	ASCII >> What happ ?Importa	pened ant f	🚀 Struct	
Dump 1 ddress H 16676F0 3 1667700 3 1667710 6	Hex 3E 3E 2 3F 0D 0 69 6C 0	ump 2 20 57 0A 0D 65 73	68 61 0A 49 20 6F	74 6D 6E	20 68 70 6F 20 79	Dump 4	70 65 61 68 72 20	Dump 5 6 6E 6 74 2 6 6E 6	5 64 0 66 5 74	ASCII >> What happ ?Importa	pened ant f r net	🎾 Struct	
Dump 1 ddress H 16676F0 3 1667700 3 1667710 6 1667720 7	Hex 3E 3E 2 3F 0D 0 69 6C 6 77 6F 7	ump 2 20 57 0A 0D 65 73 72 68	68 61 0A 49 20 6F 20 77	74 60 61	20 68 70 6F 20 79 73 20	Dump 4 61 70 72 74 6F 75 45 4E	70 65 61 66 72 20 43 52	Dump 5 6 6E 6 74 2 6 6E 6 2 59 5	5 64 0 66 5 74 0 54	ASCII >> What happ ?Importa iles on your work was ENG	pened ant f r net CRYPT	y struct	
Dump 1 ddress H 16676F0 3 1667700 3 1667710 6 1667720 7 1667730 4	Hex 3E 3E 2 3F 0D 0 69 6C 6 77 6F 7 45 44 2	ump 2 20 57 0A 0D 65 73 72 6B 20 61	68 61 0A 49 20 6F 20 77	74 60 61	20 68 70 6F 20 79 73 20	Dump 4 61 70 72 74 6F 75 45 4E	70 65 61 66 72 20 43 52	Dump 5 6 6E 6 74 2 6 6E 6 2 59 5 8 65 7	5 64 0 66 5 74 0 54 9 20	ASCII >> What happ ?Importa iles on your work was ENG ED and now	pened ant f r net CRYPT	2 struct	
Dump 1           Idress         H           16676F0         3           1667700         3           1667710         6           1667720         7           1667730         4           1667740         6	Hex 3E 3E 2 3F 0D 0 69 6C 6 77 6F 7 45 44 2 68 61 7	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65	68 61 0A 49 20 6F 20 77 6E 64	74 6D 6E 61 20	20 68 70 6F 20 79 73 20 6E 6F	Dump 4 61 70 72 74 6F 75 45 4E 77 20	70 65 61 66 72 20 43 52 74 68	Dump 5 6 6E 6 74 2 6E 6 2 59 5 8 65 7 2	5 64 0 66 5 74 0 54 9 20 0 65	ASCII >> What happ ?Importa iles on your work was ENK ED and now 1 have 1	pened ant f r net CRYPT they e	y Struct	
Dump 1           Idress         H           16676F0         3           1667700         3           1667710         6           1667730         4           1667740         6           1667730         4           1667750         7           1667750         7	Hex 3E 3E 2 3F 0D 0 69 6C 6 77 6F 7 45 44 2 68 61 7 78 74 6	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E	68 61 0A 49 20 6F 20 77 6E 64 73 69	74 6D 6E 61 20 6F	20 68 70 6F 20 79 73 20 6E 6F 6E 2E	Dump 4 61 70 72 74 6F 75 45 4E 77 20 0D 0A	70 65 61 66 72 20 43 52 74 68	Dump 5 6 6E 6 74 2 6 6E 6 2 59 5 8 65 7 2 2 20 6	5 64 0 66 5 74 0 54 9 20 0 65 F 72	ASCII >> What happ ?Importa iles on your work was ENC ED and now have xtension	pened ant f r net CRYPT they e In or	2 Struct	
Ligoropa 1 Ligoropa 1 Ligoro	Hex 3E 3E 2 3F 0D 0 69 6C 6 77 6F 7 45 44 2 68 61 7 78 74 6 64 65 7	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E 72 20	68 61 0A 49 20 6F 20 77 6E 64 73 69 74 6F	20mp 3 74 6D 6E 61 20 6F 20	20 68 70 6F 20 79 73 20 6E 6F 6E 2E 72 65	Dump 4 61 70 72 74 6F 75 45 4E 77 20 0D 0A 63 6F	70 65 61 66 72 20 43 52 74 68 49 66 76 65	Dump 5 6 6E 6 7 4 2 0 6E 6 2 59 5 3 65 7 2 2 20 6 5 72 2	5 64 0 66 5 74 0 54 9 20 0 65 F 72 0 79	ASCII >> What happ ?Importa iles on your work was ENC ED and now 1 have xtension der to recou	pened ant f r net CRYPT they e In or wer y	2 Struct	
Dump 1           ddress         H           16676F0         3           1667700         3           1667710         6           1667730         4           1667740         6           1667750         7           1667750         7           1667760         6           1667760         6           1667760         6           1667770         6	Hex 3E 3E 2 3F 0D 0 69 6C 6 77 6F 7 45 44 2 68 61 7 78 74 6 64 65 7 6F 75 7	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E 72 20 72 20	68 61 0A 49 20 6F 20 77 6E 64 73 69 74 6F 66 69	20mp 3 74 6D 6E 61 20 6F 20 6C	20 68 70 6F 20 79 73 20 6E 6F 6E 2E 72 65 65 73	Dump 4 61 70 72 74 6F 75 45 4E 77 20 0D 0A 63 6E 20 79	43 76 76 74 76 76 76 76 76 75 76 76 75 75 76 75 75 75 75 75 75 75 75 75 75 75 75 75	Dump 5 6 6E 6 74 2 6 59 5 8 65 7 2 2 20 6 5 72 2 5 20 6	5 64 0 66 5 74 0 54 9 20 0 65 F 72 0 79 E 65	ASCII >> What happ ?Importa iles on your work was ENC ED and now 1 have xtension) der to reco our files yo	pened ant f r net CRYPT they e In or vver y ou ne	2 Struct	
Dump 1           Idress         H           16676F0         3           1667700         3           1667710         6           1667730         7           1667740         6           1667750         7           1667770         6           1667760         6           1667770         6           1667760         6           1667770         6           1667780         6           1667780         6	Hex 3E 3E 2 3F 0D 0 69 6C 6 77 6F 7 45 44 2 68 61 7 78 74 6 64 65 7 65 64 2	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E 72 20 72 20 72 20 20 74	68 61 0A 49 20 6F 20 77 6E 64 73 69 74 6F 66 69 6F 20	74 6D 6E 61 20 6F 20 6C 66	20 68 70 6F 20 79 73 20 6E 6F 6E 2E 72 65 65 73 6F 6C	61 70 72 74 6F 75 45 4E 77 20 0D 0A 63 6F 20 79 6C 6F	70 65 61 66 72 20 43 52 74 68 49 66 76 65 77 20	Dump 5 6 6E 6 74 2 6 6E 6 2 59 5 8 65 7 20 6 5 72 2 5 20 6 0 69 6	5 64 0 66 5 74 0 54 9 20 0 65 iF 72 0 79 iE 65 iE 73	ASCII ASCII ASCII ASCIN Nork was ENC ED and now 1 have xtension der to recov our files yy ed to follow	pened ant f r net CRYPT they e In or vver y ou ne w ins	2 struct	
Dump 1           ddress         H           166760         3           1667700         3           1667700         3           1667700         4           1667740         6           1667760         6           1667760         6           1667760         6           1667760         6           1667760         6           1667770         6           1667780         6           1667790         7	Hex           3E         3E         3E         3F         0D         0         69         6C         67         76         7         6F         45         44         2         68         61         7         78         74         6         65         75         76         7         6F         75         7         6F         75         7         6F         75         6         7         7         6         7         6         7         6         7         6         7         4         2         7         7         7         4         7         2         7         7         4         7         2         7         7         4         7         2         7         7         4         7         2         7         7         4         7         2         7         7         4         7         7         4         7         7         7         4         7         7         4         7         7         4         7         7         4         7         7         4         7         7         4         7         7         4         7         7         3         4	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E 72 20 72 20 72 20 72 20 72 20 74 75 63	68 61 0A 49 20 6F 20 77 6E 64 73 69 74 6F 66 69 6F 20 74 69	74 6D 6E 61 20 6F 20 6C 66 6F	20 68 70 6F 20 79 73 20 6E 6F 6E 2E 73 6F 6C 73	Dump 4 61 70 72 74 6F 75 45 4E 77 20 0D 0A 63 6F 20 79 6C 6E 20 62	70 65 61 66 72 20 43 52 74 68 49 66 6F 75 77 20 6F 75 77 20 65 60	Dump 5 6 6E 6 7 4 2 6 6E 6 2 59 5 3 65 7 2 2 0 6 5 20 6 5 20 6 6 69 6 6 6F 7	5 64 0 66 5 74 0 54 9 20 0 65 iF 72 0 79 iE 65 iE 73 7 2E	ASCII ASCII ASCII ASCINT A	pened ant f r net CRYPT they e In or ver y rou ne w ins elow.	Struct	
Dump 1           ddress         H           1667700         3           1667700         3           1667700         6           1667710         6           1667730         4           1667740         6           1667750         7           1667760         6           1667760         6           1667770         6           1667780         6           1667790         7           1667780         6           1667790         7	Hex 3E 3E 2 3F 0D (69 6C 6 69 6C 6 67 6F 7 68 61 7 68 61 7 64 65 7 64 65 7 65 64 2 74 72 7 00 0A (0 00 0A)	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E 72 20 20 74 20 72 20 74 20 75 63 0D 0A	68 61 0A 49 20 6F 20 77 6E 64 73 69 74 69 66 69 74 69 3E 3E	74 6D 6E 61 20 6F 20 6C 66 6F 20 6C 66 6F 20	20 68 70 6F 20 79 73 20 6E 6F 72 65 73 65 73 65 73 65 73 65 65 73 65	61 70 72 74 6F 75 45 45 77 20 0D 0A 63 6F 20 79 6C 6F 20 62 20 62 20 62 20 62	70 65 61 66 72 20 43 55 74 66 74 66 76 65 67 77 20 65 65 69 74	Dump 5 6 6E 6 7 4 2 9 6E 6 2 59 5 8 65 7 2 2 0 6 5 72 2 5 20 6 6 20 6 6 20 6 6 20 6 6 20 6 7 2 2 6 20 6 6 20 6 7 4 0 7 0 0 7 4 0 7 4 0 7 4 0 7 7 4 0 7 0 0 7 7 0 0 7 7 0 0 7 0 0 0 0	5 64 0 66 5 74 0 54 9 20 0 65 F 72 0 65 F 72 0 65 F 72 0 65 F 73 7 2E 6 65	ASCII ASCII ASCII ASCINT A	pened ant f r net CRYPT they e In or ver y vou ne w ins elow. itive	2 struct	
Dump 1           ddress         H           166760         3           1667700         3           1667700         3           1667700         3           1667700         4           1667730         4           1667740         5           1667760         6           1667760         6           1667780         7           1667780         7           1667780         7           1667780         6           1667780         7           1667780         6           1667780         7           1667780         6           1667780         7           1667780         7           1667780         7           1667780         7	Hex 3E 3E 2 3F 0D (69 6C 6 77 6F 7 45 44 2 68 61 7 78 74 6 64 65 7 6F 75 7 6F 75 7 65 64 2 74 72 7 00 0A (6 20 44 6 20 5 20	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E 72 20 72 20 20 74 75 63 0D 0A 61 74	68 61 0A 49 20 6F 20 77 6E 64 73 69 74 69 6F 20 74 69 3E 3E 61 00	74 6D 6E 61 20 6F 20 6C 66 6F 20 0A	20 68 70 6F 20 79 73 20 6E 6F 6E 2E 72 65 65 73 6F 65 73 65 6F 73 65 65 73 65 00 0A	61 70 72 74 6F 75 45 4E 77 20 0D 0A 63 6F 20 79 6C 6F 20 62 6E 73 53 65	70 65 61 66 72 20 43 52 74 68 76 65 77 20 65 65 69 74 65 77	Dump 5 6 6E 6 74 2 6 5 6 6 5 7 8 65 7 2 20 6 6 72 2 5 20 6 6 69 6 6 69 7 8 69 7 8 69 7	5 64 0 66 5 74 0 54 9 20 0 65 F 72 0 65 F 72 0 65 F 72 0 65 F 73 F 72 6 65 4 69	ASCII ASCII ASCII ASCINT A	pened ant f r net CRYPT they e In or ver y ou ne w ins elow. itive nsiti	2 struct	
Dump 1           ddress         H           1667700         3           1667700         3           1667700         6           1667710         6           1667730         4           1667740         6           1667750         7           1667760         6           1667760         6           1667770         6           1667780         6           1667790         7           1667780         6           1667790         7	Hex 3E 3E 2 3F 0D (69 6C 6 77 6F 7 45 44 2 68 61 7 78 74 6 64 65 7 6F 75 7 6F 75 7 65 64 2 74 72 7 00 0A (6 20 44 6 20 5 20	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E 72 20 72 20 20 74 75 63 0D 0A 61 74	68 61 0A 49 20 6F 20 77 6E 64 73 69 74 69 6F 20 74 69 3E 3E 61 00	74 6D 6E 61 20 6F 20 6C 66 6F 20 0A	20 68 70 6F 20 79 73 20 6E 6F 6E 2E 72 65 65 73 6F 65 73 65 6F 73 65 65 73 65 00 0A	61 70 72 74 6F 75 45 4E 77 20 0D 0A 63 6F 20 79 6C 6F 20 62 6E 73 53 65	70 65 61 66 72 20 43 52 74 68 76 65 77 20 65 65 69 74 65 77	Dump 5 6 6E 6 74 2 6 5 6 6 5 7 8 65 7 2 20 6 6 72 2 5 20 6 6 69 6 6 69 7 8 69 7 8 69 7	5 64 0 66 5 74 0 54 9 20 0 65 F 72 0 65 F 72 0 65 F 72 0 65 F 73 F 72 6 65 4 69	ASCII ASCII ASCII ASCINT A	pened ant f r net CRYPT they e In or ver y ou ne w ins elow. itive nsiti	2 Struct	
Dump 1           ddress         H           166760         3           1667700         3           1667700         3           1667700         3           1667700         4           1667730         4           1667740         5           1667760         6           1667760         6           1667780         7           1667780         7           1667780         7           1667780         6           1667780         7           1667780         6           1667780         7           1667780         6           1667780         7           1667780         7           1667780         7           1667780         7	Hex 3E 3E 2 3F 0D (69 6C 6 69 6C 6 77 6F 7 45 44 2 68 61 7 78 74 6 64 65 7 6F 75 7 65 64 2 74 72 7 00 0A (6 20 44 6 20 5 20 5	ump 2 20 57 0A 0D 65 73 72 68 20 61 76 65 65 6E 72 20 72 20 20 74 75 63 0D 0A 61 74	68 61 0A 49 20 6F 20 77 6E 64 73 69 74 69 6F 20 74 69 3E 3E 61 00	74 6D 6E 61 20 6F 20 6C 66 6F 20 0A	20 68 70 6F 20 79 73 20 6E 6F 6E 2E 72 65 65 73 6F 65 73 65 6F 73 65 65 73 65 00 0A	61 70 72 74 6F 75 45 4E 77 20 0D 0A 63 6F 20 79 6C 6F 20 62 6E 73 53 65	70 65 61 66 72 20 43 52 74 68 76 65 77 20 65 65 69 74 65 77	Dump 5 6 6E 6 74 2 6 5 6 6 5 7 2 2 6 65 7 2 2 6 6 7 6 7 4 6 9 7 3 6 9 7	5 64 0 66 5 74 0 54 9 20 0 65 F 72 0 65 F 72 0 65 F 72 0 65 F 73 F 72 6 65 4 69	ASCII ASCII ASCII ASCINT A	pened ant f r net CRYPT they e In or ver y ou ne w ins elow. itive nsiti	2 struct	

### Image 18: Dropping ransom note

As for encryption procedures, the ransomware employs the AES method, generating a unique private key for each execution. This private key will then be RSA encrypted using the public key in the configurations and be embedded alongside the encrypted file.

Image 19: AES Configuration in JSON format

00	00	00	00	00	00	00	00	20	5	11	FU	20		00	TD	
/B	22	/6	65	12	13	69	6F	6E	22	3A	30	2C	22	6D	6F	{"version":0,"mo
64	65	22	3A	22	46	75	6C	6C	22	2C	22	63	69	70	68	de":"Full","ciph
65	72	22	3A	22	41	65	73	22	2C	22	70	72	69	76	61	er":"Aes","priva
74	65	5F	6B	65	79	22	3A	5B	31	31	39	2C	31	33	38	te_key": [119,138
2C	31	30	35	2C	32	35	30	2C	32	35	34	2C	32	31	39	,105,250,254,219
																,180,214,28,21,2
																14,64,6,181,164,
32	33	30	5D	2C	22	64	61	74	61	5F	73	69	7 <b>A</b>	65	22	230],"data_size"
3A	33	32	37	36	33	2C	22	63	68	75	6E	6B	5F	73	69	:32763,"chunk_si
																ze":25362816,"fi
6E	69	73	68	65	64	22	3A	74	72	75	65	7D	AB	AB	AB	nished":true}«««

The encrypted file can be identified by a unique 4-byte border that is added to the head and tail of the file. This is essential for the ransomware as it uses this to identify the configuration file that was embedded. The ransomware also creates checkpoint files, which is speculated to be used if the initial encryption process was interrupted or corrupted then it would recreate from this checkpoint. After each successful encryption, the malware will drop a ransom note.

	Image 20:	Unique	4-bvte	border	identifiers
--	-----------	--------	--------	--------	-------------

7FD0H:	64	62	64	20	69	0E	20	74	68	65	20	60	69	PC.	62	UD	aea in the life.
7FE0h:	0A	64	6F	63	73	2F	6C	69	63	65	6E	73	65	2E	68	74	.docs/license.ht
7FF0h:	6D	6C	5F	6C	69	62	2E	0D	0A	0D	0A	19	47	<b>B</b> 7	6E	76	ml_libG·nv
8000h:	46	46	E7	13	<b>B</b> 4	EF	2F	<b>B</b> 4	D3	80	F2	F0	12	A5	DB	4C	FFç.´ï/´Ó€òð.¥ÛL
8010h:	6E	26	C1	1A	E5	0D	6A	27	86	2E	3A	58	FA	FC	CA	11	n&Á.å.j't.:XúüÊ.
8020h:	76	30	97	98	A5	5F	90	AD	EF	DB	59	8A	C6	97	4B	43	v0—~¥ïÛYŠÆ—KC
8030h:	1E	47	FE	8B	<b>B</b> 9	DD	23	06	94	36	E5	CA	23	4B	16	81	.Gþ<¹Ý#."6åÊ#K
8040h:	DF	A4	<b>B</b> 3	3C	38	48	97	<b>B</b> 8	D2	46	51	0D	A9	EF	6D	<b>B</b> 6	ߤ³<8H— ÒFQ.©ïm¶
8050h:	72	2A	8A	19	68	3B	0B	C6	C6	5C	A3	D6	42	88	0F	8F	r*Š.h;.ÆÆ\£ÖB^
8060h:	8E	06	D2	1B	94	00	C8	9C	08	2F	52	EB	0D	96	A8	50	Ž.Ò.″.Èœ./Rë"P
8070h:	BB	45	0E	BD	<b>B</b> 9	92	50	D3	DO	A9	B6	82	A1	7A	9C	E8	»E.½1'PÓĐ©¶,;zœè
8080h:	93	76	EC	71	3C	AC	F2	56	24	7D	9B	8E	67	<b>B</b> 5	05	EC	"vìq<¬òV\$}›Žgµ.ì
8090h:	19	61	06	63	A5	99	29	85	42	D9	F6	EE	16	D2	85	58	.a.c¥™)BÙöî.ÒX
80A0h:	87	4F	6D	17	35	C2	61	05	07	5C	E0	8C	<b>E</b> 5	71	F1	53	‡Om.5Âa∖àŒåqñS
80B0h:	5C	A6	DF	2F	D4	99	7C	99	1F	F5	FD	BA	55	E1	7E	31	\¦ß/Ô™ ™.õý°Uá~1
80C0h:	F3	FF	68	F0	AA	96	D7	50	81	11	F8	27	2E	52	3D	33	óÿhðª-×Pø'.R=3
80D0h:	18	AF	2D	9A	24	E6	2F	73	EA	6C	01	8C	C8	73	15	6D	š\$æ/sêl.ŒÈs.m
80E0h:																	r{d~ZBŸ£ûê-;ä.aË
80F0h:	90	DD	0A	C1	EA	AE	31	DC	AF	C1	EA	6E	5D	5F	41	00	.Ý.Áê®1Ü Áên]_A.
8100h:																	G·n

#### Image 21: AES Encryption

	0039DD30	66:0F6F72 50	<pre>movdqa xmm6, xmmword ptr ds:[edx+50]</pre>
	0039DD35	66:0F6F7A 60	<pre>movdqa xmm7, xmmword ptr ds:[edx+60]</pre>
	0039DD3A	66:0FEFC1	pxor xmm0, xmm1
•	0039DD3E	66:0FEFD9	pxor xmm3, xmm1
	0039DD42	66:0FEFE1	pxor xmm4, xmm1
	0039DD46	66:0FEFE9	pxor xmm5,xmm1
•	0039DD4A	66:0FEFF1	pxor xmm6,xmm1
	0039DD4E	66:0FEFF9	pxor xmm7, xmm1
	0039DD52	66:0F7F0424	movdqa xmmword ptr ss:[esp],xmm0
	0039DD57	66:0F6F42 10	<pre>movdqa xmm0, xmmword ptr ds:[edx+10]</pre>
	0039DD5C	66:0F6F1424	<pre>movdqa xmm2,xmmword ptr ss:[esp]</pre>
	0039DD61	66:0FEFC1	pxor xmm0, xmm1
	0039DD65	66:0FEF4A 70	<pre>pxor xmm1, xmmword ptr ds:[edx+70]</pre>
	0039DD6A	66:0F7F4424 10	<pre>movdqa xmmword ptr ss:[esp+10],xmm0</pre>
	0039DD70	66:0F6F41 10	<pre>movdqa xmm0,xmmword ptr ds:[ecx+10]</pre>
	0039DD75	66:0F38DCD0	aesenc xmm2, xmm0
•	0039DD7A	66:0F38DCD8	aesenc xmm3, xmm0
•	0039DD7F	66:0F38DCE0	aesenc xmm4, xmm0
	0039DD84	66:0F38DCE8	aesenc xmm5, xmm0
•	0039DD89	66:0F38DCF0	aesenc xmm6,xmm0
•	0039DD8E	66:0F38DCF8	aesenc xmm7, xmm0
	0039DD93	66:0F38DCC8	aesenc xmm1, xmm0
۰	0039DD98	66:0F7F1424	<pre>movdqa xmmword ptr ss:[esp],xmm2</pre>
	0039DD9D	66:0F6F5424 10	<pre>movdqa xmm2,xmmword ptr ss:[esp+10]</pre>
•	0039DDA3	66:0F38DCD0	aesenc xmm2, xmm0
	0039DDA8	66:0F6F41 20	<pre>movdqa xmm0, xmmword ptr ds:[ecx+20]</pre>
•	0039DDAD	66:0F7F5424 10	<pre>movdqa xmmword ptr ss:[esp+10],xmm2</pre>
	0039DDB3	66:0F6F1424	<pre>movdqa xmm2,xmmword ptr ss:[esp]</pre>
•	0039DDB8	66:0F38DCD8	aesenc xmm3, xmm0
	0039DDBD	66:0F38DCE0	aesenc xmm4, xmm0
	0039DDC2	66:0F38DCE8	aesenc xmm5, xmm0
	0039DDC7	66:0F38DCF0	aesenc xmm6, xmm0
	0039DDCC	66:0F38DCF8	aesenc xmm7, xmm0
	0039DDD1	66:0F38DCC8	aesenc xmm1,xmm0
	0000 0	CC 0-300	

### Image 22: Ransomware note

File Edit Format View Help	
>> What happened?	
Important files on your network was ENCRYPTED and now they have " " extension. In order to recover your files you need to follow instructions below.	
>> Sensitive Data	
Sensitive data on your network was DONNLOADED. If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.	
Data includes: - NDA	
Employees personal data, CVs, DL, SSN. - Complete network map including credentials for local and remote services. - Private financial information including: clients data, bills, budgets, annual reports, bank statements.	
<ul> <li>Anufacturing documents including: clater(s data, blick, budgets, annual reports, bank statements.</li> <li>And matrix documents including: datagrams, schemas, drawings in solidworks format</li> <li>And more</li> </ul>	
Samples are available on your personal web page linked below.	
>> CAUTION	
DO NOT MODIFY ENCRYPTED FILES YOURSELF.	
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA. YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.	
>> What should I do next?	
1) Download and install Tor Browser from: https://torproject.org/	
<ol> <li>Navigate to: http://ybozogb2p6y51bxoivei3sanxqpqvbf7jfr3ygwtbmpache2dziz3fad.onion/?access-key=</li> </ol>	

### Indicator of compromise (IOCs) identified

RECOVER-<extension>-FILES.txt checkpoint<-filename>.<extension> RECOVER-<extension>-FILES.txt.png \\.\pipe\\_\_rust\_anonymous\_pipe1\_.<process\_id>.<generated\_number> {3E5FC7F9-9A51-4367-9063-A120244FBEC7

### Commands executed

wmic csproduct get UUID
iisreset.exe /stop
reg add
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
/v MaxMpxCt /d 65535 /t REG\_DWORD
vssadmin.exe Delete Shadows /all /quiet
arp -a
wmic.exe Shadowcopy Delete
wevutil.exe el
weutil.exe cl
net use <device\_name> /user <username> <password> /persistent:no

### Contact EY team



### Jeffrey Tan

Associate Partner, Technology Consulting Ernst & Young Advisory Pte. Ltd. jeffery.tan@sg.ey.com



### Goh Siong Por

Senior Manager - Technology Consulting Ernst & Young Advisory Pte. Ltd. siong.por.goh@sg.ey.com



### EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2024 Ernst & Young Advisory Pte. Ltd. All Rights Reserved.

APAC no. 12003510

ED None

UEN 198905395E

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com