

BlackCat ransomware technical analysis

Additional reading



About BlackCat ransomware

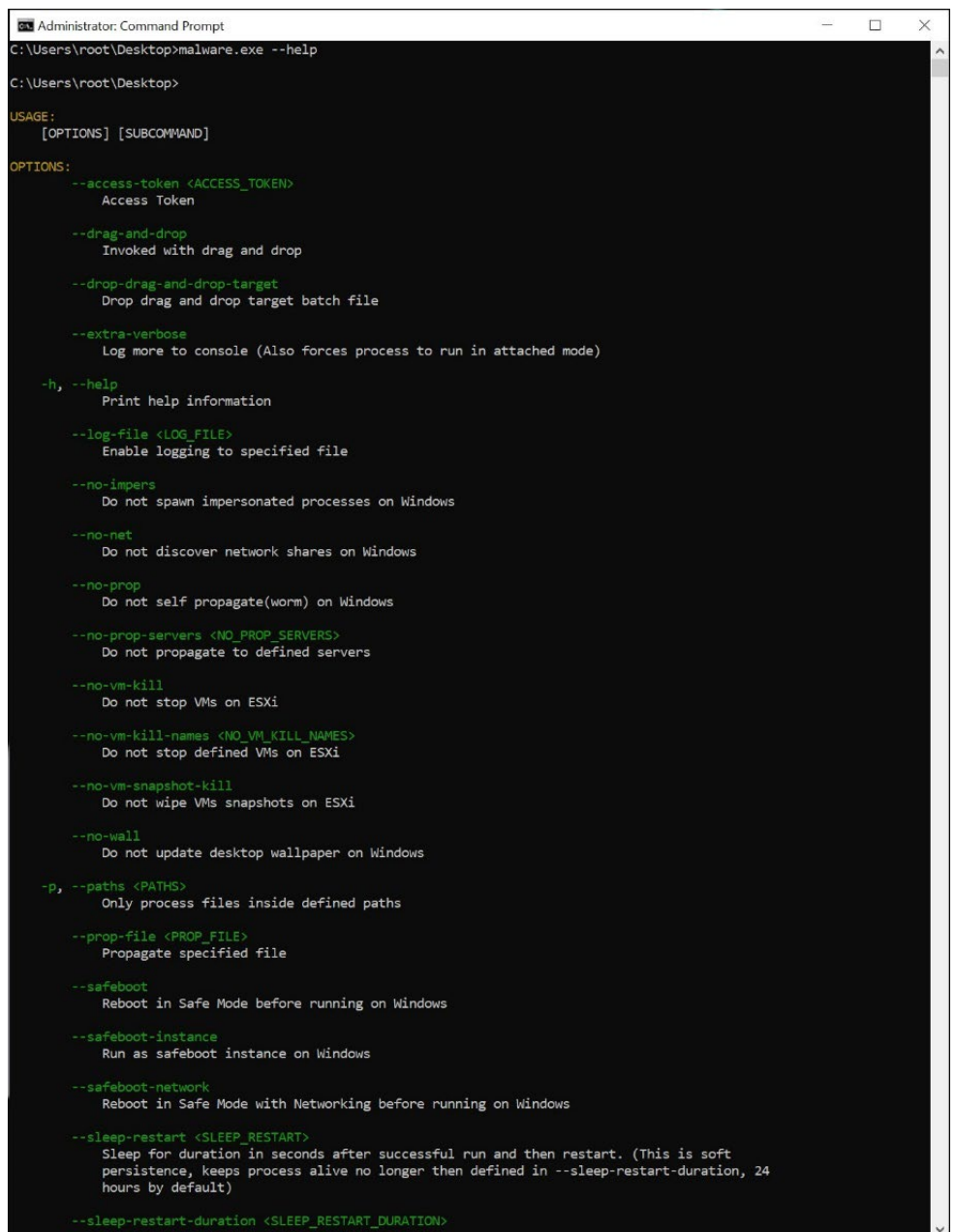


The BlackCat ransomware, also known as ALPHV, is a potent strain of malware that targets and encrypts critical data on an infected system, subsequently demanding a ransom payment for decryption. It typically propagates through phishing campaigns, malicious downloads or exploit kits. By leveraging advanced 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



```
Administrator: Command Prompt
C:\Users\root\Desktop>malware.exe --help
C:\Users\root\Desktop>

USAGE:
  [OPTIONS] [SUBCOMMAND]

OPTIONS:
  --access-token <ACCESS_TOKEN>
    Access Token

  --drag-and-drop
    Invoked with drag and drop

  --drop-drag-and-drop-target
    Drop drag and drop target batch file

  --extra-verbose
    Log more to console (Also forces process to run in attached mode)

  -h, --help
    Print help information

  --log-file <LOG_FILE>
    Enable logging to specified file

  --no-impers
    Do not spawn impersonated processes on Windows

  --no-net
    Do not discover network shares on Windows

  --no-prop
    Do not self propagate(worm) on Windows

  --no-prop-servers <NO_PROP_SERVERS>
    Do not propagate to defined servers

  --no-vm-kill
    Do not stop VMs on ESXi

  --no-vm-kill-names <NO_VM_KILL_NAMES>
    Do not stop defined VMs on ESXi

  --no-vm-snapshot-kill
    Do not wipe VMs snapshots on ESXi

  --no-wall
    Do not update desktop wallpaper on Windows

  -p, --paths <PATHS>
    Only process files inside defined paths

  --prop-file <PROP_FILE>
    Propagate specified file

  --safeboot
    Reboot in Safe Mode before running on Windows

  --safeboot-instance
    Run as safeboot instance on Windows

  --safeboot-network
    Reboot in Safe Mode with Networking before running on Windows

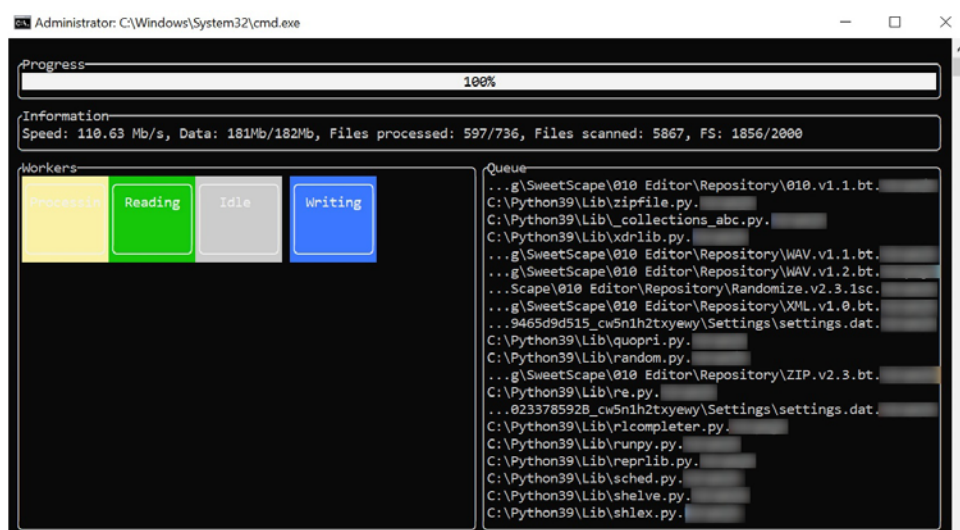
  --sleep-restart <SLEEP_RESTART>
    Sleep for duration in seconds after successful run and then restart. (This is soft
    persistence, keeps process alive no longer then defined in --sleep-restart-duration, 24
    hours by default)

  --sleep-restart-duration <SLEEP_RESTART_DURATION>
```

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.

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

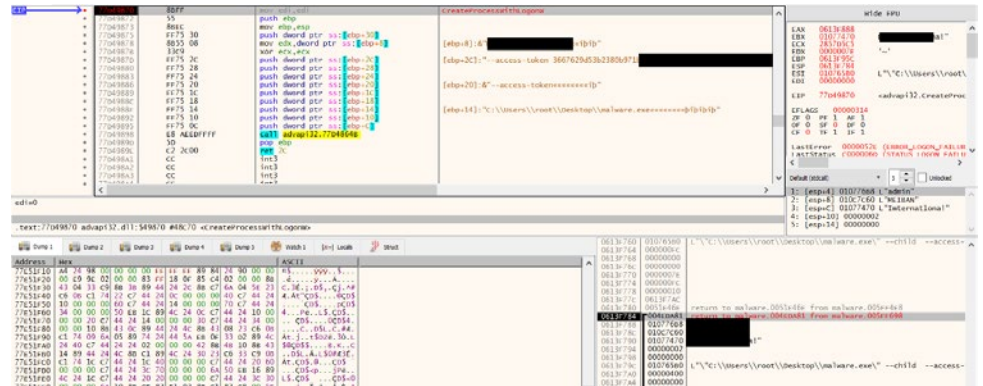


Image 7: Deleting all Shadow Copy backups

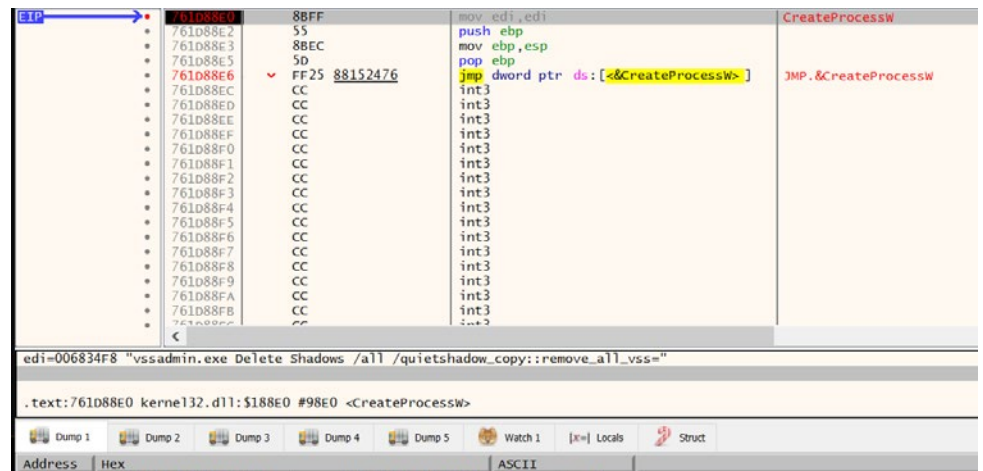
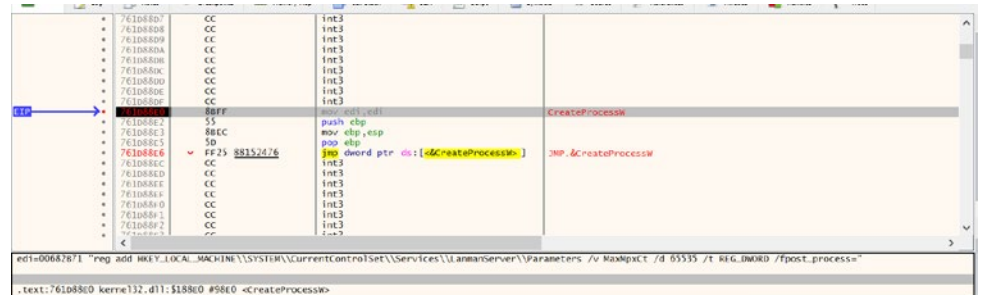


Image 8: Updating a registry key



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

```

766E04CF  CC          int3
EIP → 766E04D0  8BFF      mov     edi,edi          OpenSCManagerW
766E04D2  55        push    ebp
766E04D3  8BEC     mov     ebp,esp
766E04D5  5D        pop     ebp
766E04D6  FF25 14F67276  jmp     dword ptr ds:[<&OpenSCManagerW>]  JMP ,&OpenSCManagerW
766E04DC  CC          int3
766E04DD  CC          int3
766E04DE  CC          int3
766E04DF  CC          int3

```

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

```

766F5E97  CC          int3
EIP → 766F5C02  8BFF      mov     edi,edi          EnumDependentServicesW
766F5C04  55        push    ebp
766F5C05  8BEC     mov     ebp,esp
766F5C06  5D        pop     ebp
766F5C07  FF25 0De57276  jmp     dword ptr ds:[<&numDependentServiceW>]  JMP ,&numDependentServicesW
766F5C0C  CC          int3
766F5C0D  CC          int3
766F5C0E  CC          int3
766F5C0F  CC          int3
766F5C10  CC          int3

```

Image 11: Stopping the service with ControlService Function 0x01 (Service_Control_Stop)

```

765B54A0  6A 10      push    10          ControlService
765B54A2  68 A0406076  push    sechost.766040A0
765B54A7  E8 F81F0100  call   sechost.765C74A4
765B54AC  8365 FC 00  and     dword ptr ss:[ebp-4],0
765B54B0  FF75 10    push   dword ptr ss:[ebp+10]
765B54B3  FF75 0C    push   dword ptr ss:[ebp+C]

```

.text:765B54A0 sechost.d11:\$154A0 #148A0 <ControlService>

Table 1: Services targeted threads

Services targeted		
acronisagent	gxcvd	mvarmor64
acrsch2svc	gx fwd	mysql
backup	gxmmm	mysql\$
backupexecagentaccelerator	gxvss	pdfvsservice
backupexecagentbrowser	gxvsshwprov	qbcfmonitorservice
backupexecdivicemediaservice	mepocs	qbdbmgrn
backupexecjobengine	memtas	qbidservice
backupexecmanagementservice	msexchange	sap
backupexecrpcservice	msexchange\$	sap\$
backupexecvssprovider	mvarmor	sapd\$
gxblr	mvarmor64	saphostcontrol
gxclmgrs	mysql	saphostexec
gxcimgr	mysql\$	sophos

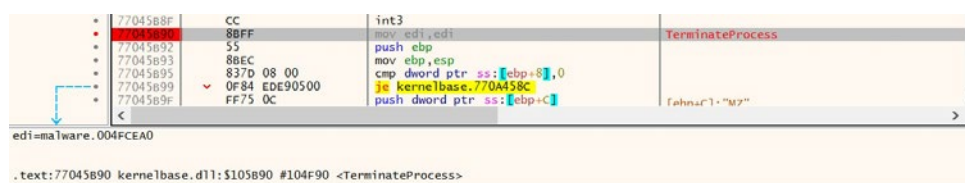
Image 12: Gathering a snapshot of all current processes



Image 13: Selecting a process via OpenProcess function

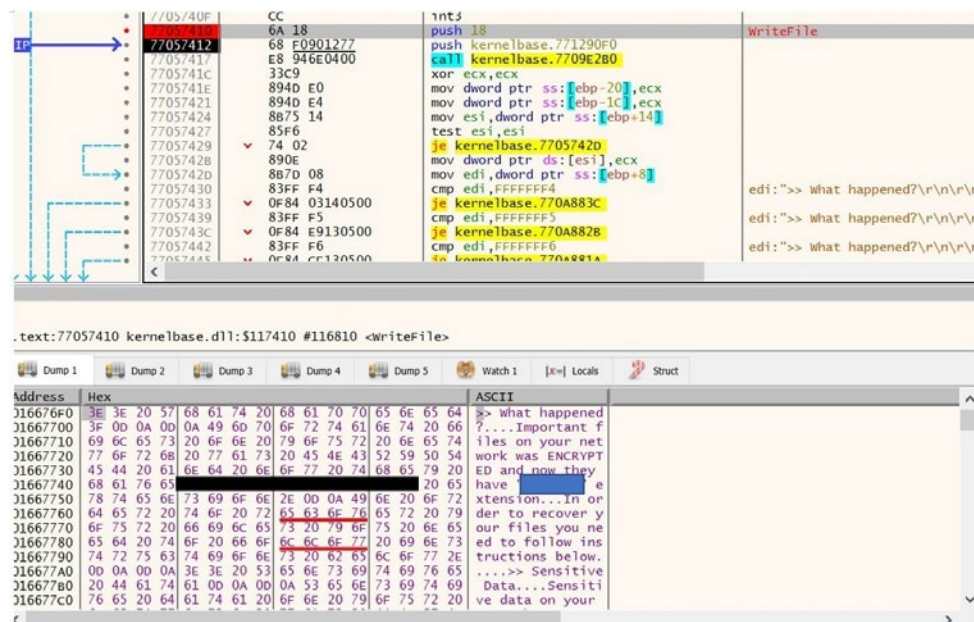


Image 14: Terminating the function selected with TerminateProcess function



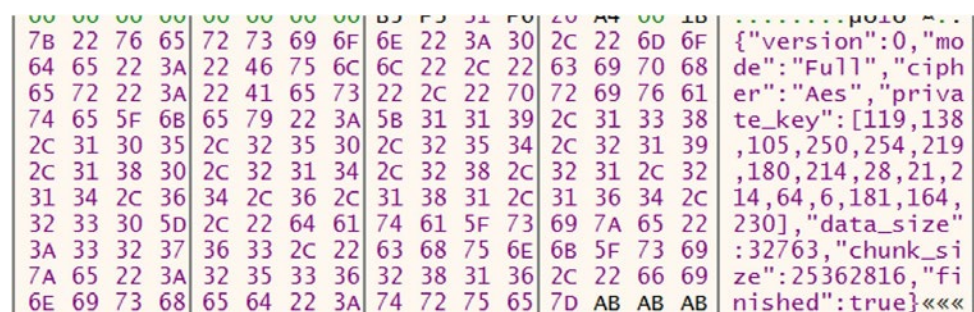
The ransomware traverses every directory within the system and drops its ransom note.

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



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-byte border identifiers

```

7FD0h: 64 65 64 20 69 6E 20 74 68 65 20 66 69 6C 65 0D ded in the file.
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 B7 6E 76 ml_lib.....G.nv
8000h: 46 46 E7 13 B4 EF 2F B4 D3 80 F2 F0 12 A5 DB 4C FFç.'i/ÓÉðð.ÿÜL
8010h: 6E 26 C1 1A E5 0D 6A 27 86 2E 3A 58 FA FC CA 11 n&Å.ã.j'†.:XúÛË.
8020h: 76 30 97 98 A5 5F 90 AD EF DB 59 8A C6 97 4B 43 v0-~¥. -iÜYŠÆ-KC
8030h: 1E 47 FE 8B B9 DD 23 06 94 36 E5 CA 23 4B 16 81 .Gp<'Y#. "6âÉ#K..
8040h: DF A4 B3 3C 38 48 97 B8 D2 46 51 0D A9 EF 6D B6 ß³<8H-_0FQ_@im¶
8050h: 72 2A 8A 19 68 3B 0B C6 C6 5C A3 D6 42 88 0F 8F r*Š.h; .ÆÆ\FÖB^..
8060h: 8E 06 D2 1B 94 00 C8 9C 08 2F 52 EB 0D 96 A8 50 Ž.Ö."."Èæ./Rë.-"P
8070h: BB 45 0E BD B9 92 50 D3 D0 A9 B6 82 A1 7A 9C E8 »E.½'1'PÓÐ@¶,;zæè
8080h: 93 76 EC 71 3C AC F2 56 24 7D 9B 8E 67 B5 05 EC "viq<-òV$}>Žgu.ì
8090h: 19 61 06 63 A5 99 29 85 42 D9 F6 EE 16 D2 85 58 .a.c¥™)...BUöî.Ö...X
80A0h: 87 4F 6D 17 35 C2 61 05 07 5C E0 8C E5 71 F1 53 ‡0m.5Åa.. \àÆãqñŠ
80B0h: 5C A6 DF 2F D4 99 7C 99 1F F5 FD BA 55 E1 7E 31 \|β/Ô™|™.öý°Uá~1
80C0h: F3 FF 68 F0 AA 96 D7 50 81 11 F8 27 2E 52 3D 33 óyhãª-×P..ø'.R=3
80D0h: 18 AF 2D 9A 24 E6 2F 73 EA 6C 01 8C C8 73 15 6D .-š$æ/sêl.ÆÈs.m
80E0h: 72 7B 64 98 5A 42 9F A3 FB EA 96 A1 E4 12 61 CB r{d~ZBÿËÛê-jä.aÉ
80F0h: 90 DD 0A C1 EA AE 31 DC AF C1 EA 6E 5D 5F 41 00 .Y.Áê@1Ü-Áên]_A.
8100h: 00 01 00 19 47 B7 6E ....G.n

```

Image 21: AES Encryption

```

• 0039DD30 66:0F6F72 50 movdqa xmm6,xmmword ptr ds:[edx+50]
• 0039DD35 66:0F6F7A 60 movdqa xmm7,xmmword ptr ds:[edx+60]
• 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 movdqa xmm0,xmmword ptr ds:[edx+10]
• 0039DD5C 66:0F6F1424 movdqa xmm2,xmmword ptr ss:[esp]
• 0039DD61 66:0FEFC1 pxor xmm0,xmm1
• 0039DD65 66:0FEF4A 70 pxor xmm1,xmmword ptr ds:[edx+70]
• 0039DD6A 66:0F7F4424 10 movdqa xmmword ptr ss:[esp+10],xmm0
• 0039DD70 66:0F6F41 10 movdqa xmm0,xmmword ptr ds:[ecx+10]
• 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
• 0039DD98 66:0F7F1424 movdqa xmmword ptr ss:[esp],xmm2
• 0039DD9D 66:0F6F5424 10 movdqa xmm2,xmmword ptr ss:[esp+10]
• 0039DDA3 66:0F38DCD0 aesenc xmm2,xmm0
• 0039DDA8 66:0F6F41 20 movdqa xmm0,xmmword ptr ds:[ecx+20]
• 0039DDAD 66:0F7F5424 10 movdqa xmmword ptr ss:[esp+10],xmm2
• 0039DDB3 66:0F6F1424 movdqa xmm2,xmmword ptr ss:[esp]
• 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

```

Image 22: Ransomware note



```
RECOVER FILES.txt - Notepad
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 DOWNLOADED.
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.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

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/
2) Navigate to: http://ybozogb2pdy5lboivei3sanxqpqvbf7jfr3ygtbmpache2dziz3fad.onion/?access-key=
```

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