

BlackCat (ALPHV) ransomware levels up for stealth, speed and exfiltration

securityintelligence.com/posts/blackcat-ransomware-levels-up-stealth-speed-exfiltration/



[Threat Intelligence](#) May 30, 2023

By [IBM Security X-Force Team](#) 9 min read

This blog was made possible through contributions from Kat Metrick, Kevin Henson, [Agnes Ramos-Beauchamp](#), Thanassis [Diogos](#), Diego Matos Martins and Joseph Spero.

[BlackCat ransomware](#), which was among the top ransomware families observed by IBM Security X-Force in 2022, according to the [2023 X-Force Threat Intelligence Index](#), continues to wreak havoc across organizations globally this year. BlackCat (a.k.a. ALPHV) ransomware affiliates' more recent attacks include targeting organizations in the [healthcare](#), [government](#), [education](#), [manufacturing](#) and [hospitality](#) sectors. Reportedly, several of these incidents resulted in the group's publishing of sensitive data to their leak site including financial and medical information stolen from the victim organizations.

Ransomware groups like BlackCat that are able to shift their tooling and tradecraft to make their operations faster and stealthier have a better chance of extending their [lifespan](#). X-Force has observed BlackCat affiliates continue to hone their operations in order to increase the likelihood of successful impact, namely data theft and encryption. Attackers automated the data exfiltration portion of the operation using ExMatter, a custom malware capable of 'melting' (self-deletion). In addition, the BlackCat group recently released a new version of their ransomware, dubbed Sphynx, with upgraded capabilities meant to thwart defensive measures.

While evolving tactics to delay or prevent detection and evade analysis present renewed challenges, knowing which tactics, techniques and procedures attackers are most likely to employ can help defenders seeking to disrupt and defeat ransomware attacks. This blog provides details around the aforementioned recently deployed tactics by BlackCat and other ransomware groups and how organizations can best protect themselves by knowing what to look for in their environments.

BlackCat's rise

BlackCat has become known as a highly formidable and innovative ransomware operation since its debut in November 2021. BlackCat has consistently been [listed](#) among the [top ten most active ransomware groups](#) by multiple research entities and was linked in an April 2022 [FBI advisory](#) to now-defunct BlackMatter/DarkSide ransomware. In 2022, BlackCat affiliates were linked to attempted extortion of entities globally across multiple sectors including [education](#), [government](#), and [energy](#).

Additionally, BlackCat switched to the [Rust programming language](#) in 2022, likely due to the customization opportunities afforded by the language, and as a means to hamper efforts to detect and analyze the malware. A year and a half since it entered the ransomware crime circuit, the BlackCat group shows no signs of winding down.

Continuous evolution

During the last six months, X-Force observed multiple intrusions by BlackCat affiliates that demonstrated continuous enhancement of their tooling and tradecraft. BlackCat affiliates continue to abuse the functionality of Group Policy Objects, both to deploy tools and to interfere with security measures. Attackers displaying a nuanced understanding of Active Directory can abuse GPOs to great effect for swift mass malware deployment. For example, threat actors may attempt to increase the speed of their operations by changing default Group Policy refresh times, likely to shorten the window of time between changes taking effect and defenders being able to respond.

As BlackCat generally attempts to carry out a double extortion scheme, attackers also deployed tools for both data encryption and theft. X-Force observed attackers leveraging ExMatter, a .NET data exfiltration tool that was introduced in 2021 and received a substantial update in August 2022. ExMatter is exclusively used by one BlackCat ransomware affiliate cluster, tracked by Microsoft as DEV-0504. IBM X-Force has observed evidence that multiple terabytes of data had been exfiltrated from a victim environment to threat actor controlled infrastructure. Stolen data is frequently posted publicly on the group's official leak site in an attempt to apply pressure on extortion victims.

Lastly, X-Force observed and analyzed a new version of BlackCat being deployed dubbed Sphynx. This version was first announced in February 2023 and introduced a number of updated capabilities that strengthen the group's efforts to evade detection.

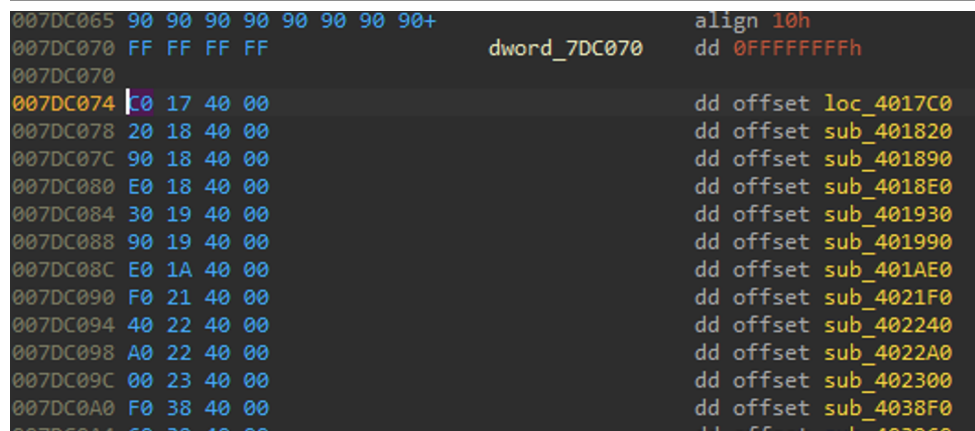
Sphynx differs from the previous variants in notable ways. For example, the command line arguments have been reworked. Previous variants utilized the `--access-token` parameter in order to execute. The updated ransomware removes that parameter and adds a set of more complex arguments. This makes it harder to detect since defenders do not have standard commands to hunt.

Additionally, the configuration data is not JSON formatted, but raw structures. Updated samples contain junk code and thousands of encrypted strings which hinder static analysis. An announcement by the BlackCat group suggests the motives for updating the ransomware, indicating that BlackCat ransomware "has been completely rewritten from scratch" and that "The main priority of this update was to optimize detection by AV/EDR."

BlackCat Sphynx loader

The exemplar sample is an obfuscated loader, that upon execution, decrypts thousands of strings and its payload. The string decryption functions are found in an array and executed from the bottom function to the top.

String function array



```
007DC065 90 90 90 90 90 90 90 90+ align 10h
007DC070 FF FF FF FF dword_7DC070 dd 0FFFFFFFh
007DC070
007DC074 C0 17 40 00 dd offset loc_4017C0
007DC078 20 18 40 00 dd offset sub_401820
007DC07C 90 18 40 00 dd offset sub_401890
007DC080 E0 18 40 00 dd offset sub_4018E0
007DC084 30 19 40 00 dd offset sub_401930
007DC088 90 19 40 00 dd offset sub_401990
007DC08C E0 1A 40 00 dd offset sub_401AE0
007DC090 F0 21 40 00 dd offset sub_4021F0
007DC094 40 22 40 00 dd offset sub_402240
007DC098 A0 22 40 00 dd offset sub_4022A0
007DC09C 00 23 40 00 dd offset sub_402300
007DC0A0 F0 38 40 00 dd offset sub_4038F0
007DC0A4 C0 30 40 00 dd offset sub_403060
```

Figure 1: String decryption functions

The decrypted strings reveal project paths that hint at this component's purpose. Notably, the following strings suggest that this component is a loader.

```
bin/loader/src/lib.rs
bin/loader/src/setup.rs
bin/loader/src/payload.rs
bin/loader/src/loader.rs
```

Scroll to view full table

While decrypting strings, the loader decrypts the payload as follows:

- The payload is XORed with a one-byte key. The result is still AES encrypted.
- The loader obtains the last 16 bytes of the XORed payload and uses it in the AES-128 cipher. The AES cipher is believed to be based on code from the following repository:

<https://github.com/RustCrypto/block-ciphers/blob/master/aes/>

- After being AES decrypted, the resulting binary is XORed with a 16-byte key.
- The result is found in memory marked by the string "payload" and followed by a DWORD that represents the size of the payload.

Payload XOR function

```

1 int first_stage_XOR_sub_401990()
2 {
3     char v0; // d1
4     int v2; // [esp+0h] [ebp-4h]
5
6     v2 = 0;
7     byte_22DE8DA ^= 0x76u;
8     while ( 1 )
9     {
10        byte_22DE8DA = 68 - byte_22DE8DA;
11        if ( v2 >= &payload_size )
12            break;
13        v0 = byte_22DE8DA;
14        payload[v2] ^= 0x98u;
15        byte_22DE8DA = -49 - v0;
16        ++v2;
17    }
18    return v2;
19 }

```

Figure 2: Payload XOR function (key: 0x98)

Payload marker

Hex	ASCII
70 61 79 6C 6F 61 64 C0 00 00 00 00 5A A7 03 00	payload.....Z\$. .
00 00 00 4D 5A 90 00 03 00 00 00 04 00 00 00 FF	...MZ.....y
FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00	ÿ.....@...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80
00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD°..'!'.L
21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61	!This program c
6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44	nnot be run in
4E 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00	OS mode...\$. .
00000 (User Data) 5 00 00 4C 01 0A 00 94 CF 2A 64 00	...PE..L....I*d.

Figure 3: Payload marker "payload"

The payload is executed in memory with command line arguments similar to the following.

```
195ToGOF -oAC -AUC -X99odn4 -pdTvb -ewi -vyJtKOOTxBdQ7QI9
```

Scroll to view full table

BlackCat Sphynx

Upon execution, the Sphynx version of BlackCat conducts the following activity:

- Gets a list of volumes to traverse using `GetVolumePathNamesForVolumeNameW()` API function.
- Mounts unmounted volumes using the `SetVolumeMountPointW()` API function.

- Conducts network discovery activities to discover additional systems.
- Creates named pipe: `\\.\pipe__rust_anonymous_pipe1__.<processid>.<random_num>` with pipe mode set to `PIPE_REJECT_REMOTE_CLIENTS`. The output of commands such as the `vssadmin.exe Delete Shadows /all /quiet` is sent to the pipe.
- Creates multiple child processes of itself with command line arguments as shown below:

```
2UmS -wGI3yV_X8t5Cck3 -MEX -B0 -IK -_Lec0 -7 -j_LXnE -vwro -XG6511Pvnxdc cdia -JRibtTPA8zwlP -
uNoFTcFoS37GYiB0dUh5UC5RvUyp_DI -Y6TW9vflA_j -oNPMCKXQnhP -
Y0YEr06KkeJzSTKI_YblvGdaAF6yJY915vCyjylaLvO6_aBDLNh3LafNstQBAy7B7Q8hkyQ5rAg5_FyvAk -MIO2mzZh4LFAuYto -
PWOUxbGNvW5zFMNR0SdoxbWvX8JhFtE8WF2OSDwhKI8KzIwF7UD18tyOvYeEZ6N6jAMix0IDWQY5PAu80LIPWISgWRqST8QRvSMIbSv
-dwdbcxb0xc00LXlm1_qkq9Avx5KhcY8CwS9Qno55wBINTEsB6CM1T
```

Scroll to view full table

Gets a list of shadow copies using the following WMI COM Object functions.

- `CoCreateInstance()` — called with CLSID `{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}` (`WbemAdministrativeLocator`) and IID `{dc12a687-737f-11cf-884d-00aa004b2e24}` (`IWbemClassObject`) to create a `IWbemLocator` interface object.
 - `CoCreateInstance()` — called with CLSID `{674B6698-EE92-11D0-AD71-00C04FD8FDFD}` (`WbemContext`) and IID `{44aca674-e8fc-11d0-a07c-00c04fb68820}` (`IWbemContext`) to create a `IWbemContext` interface object.
 - `WbemAdministrativeLocator:IWbemLocator:ConnectServer()` – Connects to the “**ROOT\CIMV2**” namespace.
 - `IWbemServices:ExecQuery()` — Executes “`SELECT * FROM Win32_ShadowCopy`” to retrieve shadow copies.
- Deletes volume shadow copies by executing `vssadmin.exe Delete Shadows /all /quiet`.
 - Executes the query “`SELECT DS_cn, DS_dnsHostName, DS_userAccountControl FROM DS_computer`” using WMI COM object functions. This command retrieves information about an active directory environment.
 - Creates a ransom note with a name consisting of alphanumeric characters (ex: `0diX0Z.txt`). The note is created in every directory that contains encrypted files.

```
Data on Your network was exfiltrated and encrypted.

Modifying encrypted files will result in permanent data loss!

Get in touch with us ASAP to get an offer:
1. Download and install Tor Browser from https://www.torproject.org/
2. Access User Panel at http://{ONION_SITE}.onion/?access-key={ACCESS_KEY}
   THIS IS YOUR PRIVATE USER PANEL ADDRESS, DO NOT SHARE IT WITH ANYONE!

See also:
Visit our Blog: http://alphvmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion
Social Media: https://twitter.com/search?q=%23alphv
```

Figure 4: Sample ransom note

- Encrypts files with AES or ChaCha20 ciphers and appends a seven-character file extension consisting of characters [a-z] (ex: `.wpzlbji`).
- If the `-v` command line argument is provided, log messages are printed to the console.

```
04:12:44 [ERROR] IO error in winapi call Access is denied. (os error 5)
04:12:44 [INFO] "\\?\Volume{fdb4821e-c578-4f21-8dd6-9375f6a61c4}\\", \"A:\\\"
04:12:44 [ERROR] SetVolumeMountPointW Access is denied. (0x80070005)
04:12:44 [INFO] "\\?\Volume{29d03762-1bd3-4a37-b35f-2d37a6bd44cc}\\", \"B:\\\"
04:12:44 [ERROR] SetVolumeMountPointW Access is denied. (0x80070005)
04:12:44 [WARN] Starting network discovery
04:12:44 [INFO] Starting IPC server at:
04:12:44 [INFO] Enum WMI
04:12:44 [INFO] Enum NetMan
04:12:44 [INFO] Enum ARP Table
04:12:44 [INFO] Pass #1
04:12:44 [INFO] Starting local discovery
04:12:45 [ERROR] Can't delete Shadow Copies with WMI: 0x80041014
04:12:45 [ERROR] Fallback to: vssadmin.exe and wmic.exe methods.
04:12:47 [ERROR] Enum WMI: HRESULT Call failed with: 0x80041017
04:12:52 [ERROR] Host dead? Can't connect to: 224.0.0.251 (224.0.0.251:445)
04:12:52 [ERROR] Host dead? Can't connect to: 239.255.255.250 (239.255.255.250:445)
04:12:53 [ERROR] Host dead? Can't connect to: 224.0.0.252 (224.0.0.252:445)
04:12:53 [ERROR] Host dead? Can't connect to: 224.0.0.22 (224.0.0.22:445)
04:12:53 [ERROR] Host dead? Can't connect to: 224.0.0.22 (224.0.0.22:445)
04:12:53 [ERROR] Host dead? Can't connect to: 192.168.1.255 (192.168.1.255:445)
04:12:53 [ERROR] Host dead? Can't connect to: 239.255.255.250 (239.255.255.250:445)
04:12:53 [ERROR] ReadDir(0s [ code: 21, kind: Uncategorized, message: "The device is not ready." ])
```

Figure 5: Log messages printed during execution

BlackCat toolkit

While conducting string analysis on decrypted strings, the following notable strings were revealed:

```
core::ipc
core::module::client
core::module::client::command
core::module::exec
core::module::server
core::module::server::windows
core::module::server::windows::elevate
core::module::server::windows::network
core::module::toolkit
core::program
kernel::core::hook
kernel::core::ipc
kernel::core::server
kernel::core::stats
bin/core/src/program.rs
bin/core/src/module/toolkit/mod.rs
bin/core/src/module/server/windows/network.rs
bin/core/src/module/exec/mod.rs
bin/core/src/module/server/mod.rs
bin/core/src/ipc.rs
bin/core/src/module/client/mod.rs
bin/core/src/module/client/command.rs
bin/core/src/module/server/windows/mod.rs
bin/core/src/module/server/windows/elevate.rs
```

Scroll to view full table

The paths suggest that the BlackCat ransomware sample contains more than just ransomware functionality but can function as a “toolkit.” An additional string suggests that tooling is based on tools from [Impacket](#).

Launch embedded python module, contains impacket examples such as [smbexec, psexec, atexec, secretsdump and etc...]

Scroll to view full table

If the -h command line is provided along with the proper validation arguments, the following usage statement is printed to the console.

Commands:

```
server      (Default) Start local Server and discover resources automatically
client, -c  Connect to local Server instance
exec, -e    Start Remote Server
toolkit, -t Various Tools
help        Print this message or the help of the given subcommand(s)
```

Options:

```
-p, --path <PATH>          Path to resource to be processed
-f, --paths-file <PATHS_FILE> Load paths from file, one or many
-R, --disable-recursion    If Resource is a directory and this option is defined, only direct children of that directory will be processed
-N, --disable-network      Disable automatic network discovery
-E, --disable-self-propagation Disable network self propagation
-s, --suspend              Initialize and wait for incoming client connections
-w, --watch <WATCH>       After finishing, server will remain active and periodically repeat discovery pass for <WATCH> hours
-v, --verbose              Print log to console instead of detaching the process
-X, --self-destruct        Self destruct when finished
-h, --help                 Print help (see more with '-help')
```

Scroll to view full table

Stages of a BlackCat ransomware attack

X-Force observed the following MITRE ATT&CK tactics and techniques across one or more recent cases associated with BlackCat ransomware.

Initial access

While evidence of the initial access vector is not always available, earliest indication of compromise was likely threat actor use of [valid credentials](#). Credentials are frequently obtained through infections with common stealer malware, such as [Raccoon](#) and [Vidar](#) information stealers.

Discovery, credential access and privilege escalation

Once inside the network, BlackCat attackers used PowerShell and the command prompt to gather information about user accounts, permissions, and domain computers. Attackers used PowerShell code associated with 'PowerSploit', a publicly available PowerShell post-exploitation framework, for credential theft through Kerberoasting, and were able to obtain domain administrator credentials.

Defense evasion, persistence and lateral movement

Attackers used Remote Desktop Protocol (RDP) to move internally within the network, including authenticating to Domain Controllers using credentials for accounts with administrative privileges. Once authenticated, attackers were able to make modifications that expanded and solidified their reach within the network.

At this stage, attackers modified the default domain Group Policy Object (GPO) to fulfill two main objectives:

- Disable security controls/antivirus: Attackers changed security policy settings to turn off system monitoring, protection, and notifications, and disabled Microsoft Defender.
- Deploy and execute ExMatter and BlackCat: Attackers edited default domain GPO settings to spread and execute the attacker's data exfiltration and ransomware tools. The malware executables were placed in the Domain Controller SYSVOL directory, causing the files to be spread to every other Domain Controller and correspondingly to all joined computers. The same GPO also created two scheduled tasks for persistent execution of the associated malware payload.

Exfiltration and impact:

BlackCat attackers exfiltrated data from target networks using ExMatter before executing the ransomware. ExMatter exfiltrates stolen data to attacker infrastructure using Secure File Transfer Protocol (port 22) and WebDAV (port 80). ExMatter has been observed transferring files directly to threat actor controlled infrastructure, rather than staging or archiving the data before exfiltration.

When it has finished exfiltrating data, Exmatter starts one of the following processes to remove any trace of itself:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -C "Stop-Process -Id <PID>; Start-Sleep 3; Set-Content -Path '<ORIGINAL FILE PATH>' -Value 0"
```

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden -C $path = '<ORIGINAL FILE PATH>';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;
```

This command "melts" the original executable into three bytes:

```
30 0D 0A
```

For additional behaviors and IOCs related to ExMatter, please see IBM X-Force's [ExMatter Malware Profile](#).

In cases where BlackCat attackers were successful, operations resulted in encryption of target systems. In addition to impacting Windows systems, BlackCat affiliates have been observed leveraging the Linux version of the BlackCat ransomware: the payload was deployed to ESXi hosts running virtual machines using WinSCP, after which attackers accessed the hosts using PuTTY to run the ransomware. For additional behaviors and IOCs related to BlackCat, please see IBM X-Force's [BlackCat Malware Profile](#).

Know your adversary

X-Force assesses that actors associated with BlackCat and other ransomware groups are likely to try to increase the speed and stealth of their operations using novel means to accomplish different stages of their attacks. Continuous advancements in BlackCat ransomware associated tradecraft, as well as the design of BlackCat and ExMatter malware, underscore adversary understanding of target systems and defender processes — as well as potential points where these can be leveraged for attacker advantage.

The following recommendations can assist with detecting two of the more notable techniques highlighted in this blog:

Malicious use of GPOs: Group Policy Objects form a powerful management tool used to apply and enforce security policy settings to Active Directory clients. Group policies may apply to all Domain objects thus any account authorized to create or edit group policies is automatically enforced to affect the security state of the complete Active Directory domain.

It is recommended that every administrative interface is thoroughly monitored and granularly configured with proper access controls. Furthermore, it is suggested that only few (two to three) accounts handle the GPO administration from dedicated and secure administrative hosts. Forensic tools such as ADTimeline and ADEExport can also assist in revealing specific malicious GPO modification events as well as the domain controller they were performed on.

Deployment of exfiltration tools (such as ExMatter): Organizations may control the software execution within client systems based on attributes, such as executable file path, hash, and publisher. For most organizations, an allow list can be used to enforce consistency and enable alerting when there is an anomaly detected. This will allow execution of authorized software only and prevent malicious software or

threat actor tools from executing without explicit exception rules.

For additional behaviors and IOCs related to Exmatter, please see X-Force's [Exmatter Malware Profile](#).

Additional recommendations can be found in X-Force's [Definitive Guide to Ransomware](#).

[Schedule a consultation](#) with an X-Force team member to learn more.

This blog was updated on June 13, 2023 to reflect a correction made to X-Force's analysis of ExMatter. A previous version stated that this malware establishes persistence by installing itself as a service, however this malware does not exhibit persistence behavior.

[IBM Security X-Force Team](#)



Cost of a Data Breach Report 2023

Get new insights on the threats you face

Read the report →