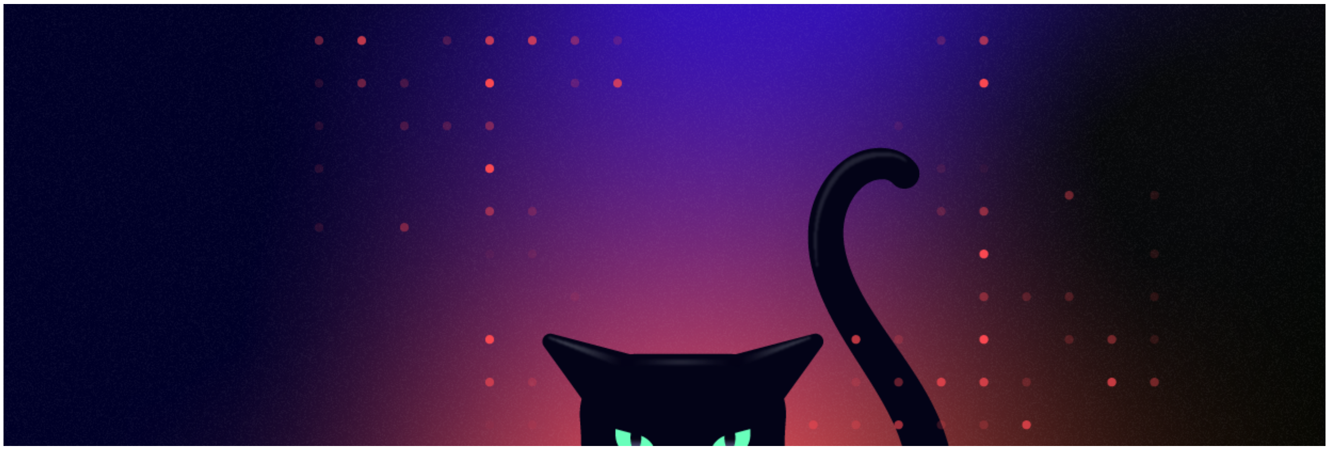
BlackCat Ransomware (ALPHV)

varonis.com/blog/alphv-blackcat-ransomware



Inside Out Security Blog / Threat Research

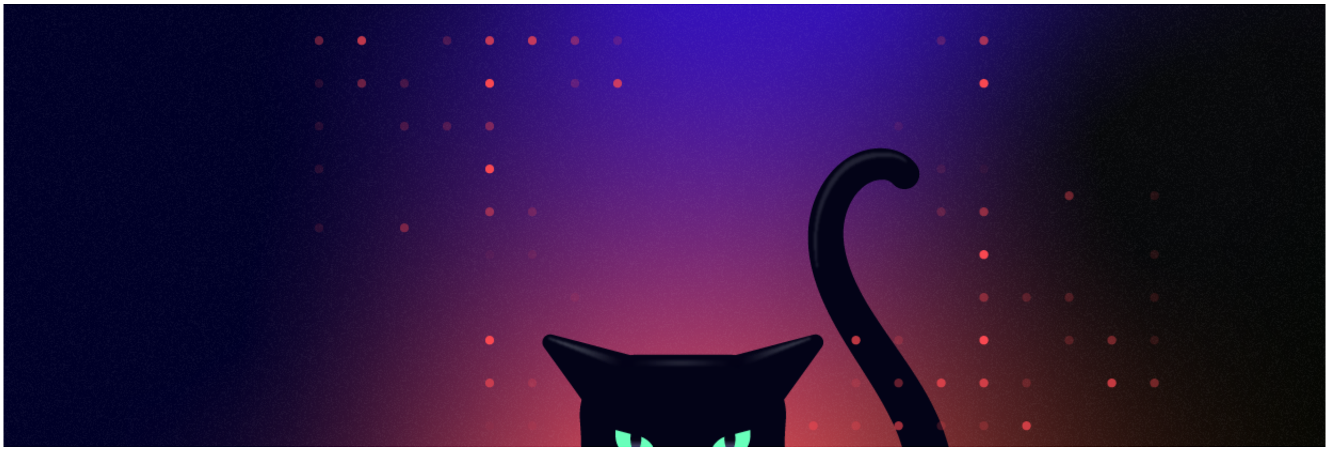
Jason Hill

|

9 min read

|

Last updated January 26, 2022



Following news that members of the infamous ‘big-game hunter’ ransomware group REvil have been arrested by Russian law enforcement, effectively dismantling the group and their operations, it is likely that the group’s affiliates will migrate to other ransomware-as-a-service (RaaS) providers.

Varonis Threat Labs has observed one such RaaS provider, ALPHV (aka BlackCat ransomware), gaining traction since late 2021, actively recruiting new affiliates and targeting organizations across multiple sectors worldwide.

Here are some of the key takeaways:

- The group is actively recruiting ex-REvil, BlackMatter, and DarkSide operators
- Increased activity since November 2021
- Lucrative affiliate pay-outs (up to 90%)
- Rust-based ransomware executable (fast, cross-platform, heavily customized per victim)
- AES encryption by default

- Built-in privilege escalation (UAC bypass, Masquerade_PEB, CVE-2016-0099)
- Can propagate to remote hosts via PsExec
- Deletes shadow copies using VSS Admin
- Stops VMware ESXi virtual machines and deletes snapshot

The group’s leak site, active since early December 2021, has named over twenty victim organizations as of late January 2022, though the total number of victims, including those that have paid a ransom to avoid exposure, is likely greater.

This article seeks to provide an overview of this emerging ransomware threat, detailing both the Linux and Windows variants of their encryption tool.

Background

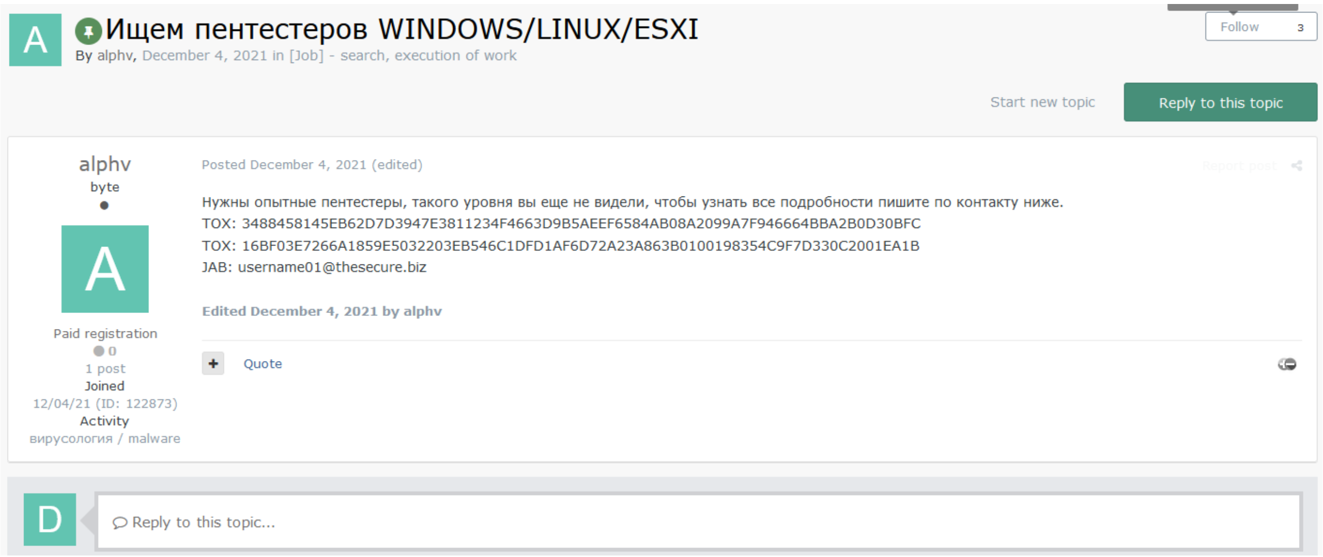
First observed in November 2021, ALPHV, also known as ALPHV-ng, BlackCat, and Noberus, is a ransomware-as-a-service (RaaS) threat that targets organizations across multiple sectors worldwide using the triple-extortion tactic.

Building upon the common double-extortion tactic in which sensitive data is stolen prior to encryption and the victim threatened with its public release, triple-extortion adds the threat of a distributed denial-of-service (DDoS) attack if the ransomware group's demands aren't met.

Demonstrating prior experience in this threat space, such as the use of proven big-game hunter tactics, techniques, and procedures (TTP) and the apparent recent success, this threat was likely created by a former ransomware group member rather than a new-comer.

Going further, some cybercrime forum users have commented that ALPHV may even be an evolution or rebranding of BlackMatter, itself a 'spin-off' or successor of REvil and DarkSide.

Previously advertised on Russian-language cybercrime forums (Figure 1), affiliates are enticed to join the group with returns of up to ninety percent of any ransom collected.



Ищем пентестеров WINDOWS/LINUX/ESXI

By alphv, December 4, 2021 in [Job] - search, execution of work

alphv
byte
Paid registration
0
1 post
Joined
12/04/21 (ID: 122873)
Activity
вирусология / malware

Posted December 4, 2021 (edited)

Нужны опытные пентестеры, такого уровня вы еще не видели, чтобы узнать все подробности пишите по контакту ниже.
TOX: 3488458145EB62D7D3947E3811234F4663D9B5AEEF6584AB08A2099A7F946664BBA2B0D30BFC
TOX: 16BF03E7266A1859E5032203EB546C1DFD1AF6D72A23A863B0100198354C9F7D330C2001EA1B
JAB: username01@thesecure.biz

Edited December 4, 2021 by alphv

Figure 1 – ALPHV 'Looking for WINDOWS/LINUX/ESX pentesters'

Working with these new affiliates, the initial intrusion of a victim network will likely use tried-and-tested techniques. For example, the exploitation of common vulnerabilities in network infrastructure devices such as VPN gateways and credential misuse via exposed remote desktop protocol (RDP) hosts.

Subsequently, those conducting ALPHV attacks have been observed as using PowerShell to modify Windows Defender security settings throughout the victim network as well as launching the ransomware binary, an interactive process, on multiple hosts using PsExec.

Ransomware

Having gained initial access to a victim network, the group will undoubtedly conduct reconnaissance and lateral movement phases in which sensitive and valuable data will be identified for exfiltration and later encryption.

Utilizing their own ransomware executable, created afresh rather than being based on some existing threat, the threat actor will build a victim-specific threat that takes into account elements such as encryption performance, perhaps electing to only encrypt parts of large files, as well as embedded victim credentials to allow automated propagation of the ransomware payload to other servers.

Unlike many other ransomware threats, ALPHV was developed using Rust, a programming language known for its fast performance and cross-platform capabilities, leading to both Linux and Windows variants being observed throughout December 2021 and January 2022.

Whilst many suggest that ALPHV could be the first 'in-the-wild' ransomware threat using this language, a Rust ransomware proof-of-concept was published on GitHub in June 2020 albeit there is nothing to suggest that the two are in any way related.

Notably, the use of Rust, amongst other modern languages including Golang and Nim, appears to be a growing trend amongst cybercrime threat actors over the past year or two.

In addition to creating new cross-platform and high-performance threats, some threat actors have also taken to rewriting their older threats likely to evade detection and thwart analysis, as seen with the updated 'Buer' downloader dubbed 'RustyBuer'.

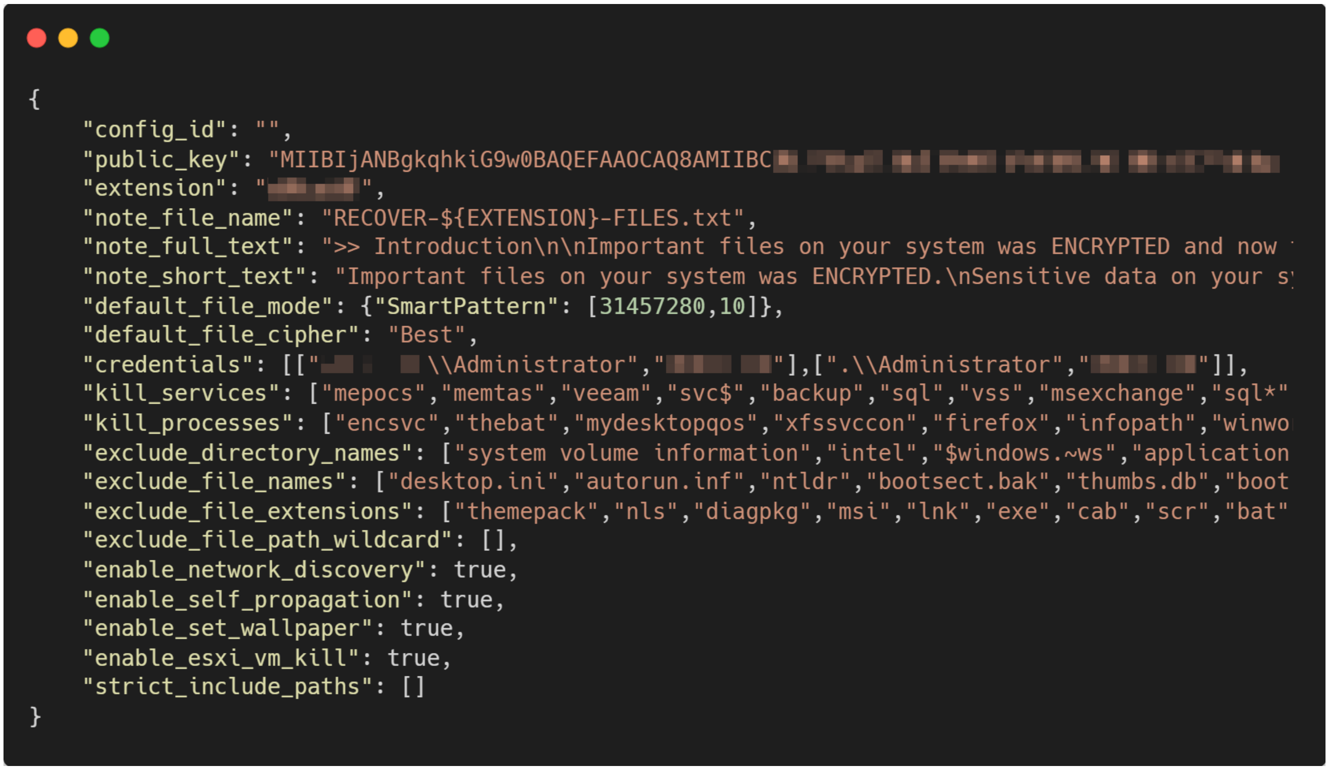
Analysis of ALPHV samples collected recently indicates that the development process likely took place during early-to-mid November 2021 given the release history of Rust 'crates' (programming libraries) used.

Specifically, recently observed ALPHV samples utilize 'Zeroize' version 1.4.3 which was not released until November 4, 2021, whilst also using public key cryptography versions that were superseded by versions released on November 16 and 17, 2021.

Whilst many of the Rust crates used are somewhat obvious, such as the use of command-line interface and encryption libraries, the use of Zeroize, a library that securely clears secrets from memory, appears to be a deliberate attempt to prevent encryption secrets from being recovered from a compromised host.

Configuration

Each victim-specific ALPHV ransomware binary has an embedded JSON data structure (Figure 2) that contains a tailored configuration taking into account the threat actor's knowledge of the victim network.



```
{
    "config_id": "",
    "public_key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC[redacted]
    "extension": "[redacted]",
    "note_file_name": "RECOVER-${EXTENSION}-FILES.txt",
    "note_full_text": ">> Introduction\n\nImportant files on your system was ENCRYPTED and now
    "note_short_text": "Important files on your system was ENCRYPTED.\nSensitive data on your s
    "default_file_mode": {"SmartPattern": [31457280,10]},
    "default_file_cipher": "Best",
    "credentials": [["[redacted]\\Administrator","[redacted]"],[".\\Administrator","[redacted]"]],
    "kill_services": ["mepocs","memtas","veeam","svc$","backup","sql","vss","msexchange","sql*"
    "kill_processes": ["encsvc","thebat","mydesktopqos","xfssvccon","firefox","infopath","winwo
    "exclude_directory_names": ["system volume information","intel","$windows.~ws","application
    "exclude_file_names": ["desktop.ini","autorun.inf","ntldr","bootsect.bak","thumbs.db","boot
    "exclude_file_extensions": ["themepack","nls","diagpkg","msi","lnk","exe","cab","scr","bat"
    "exclude_file_path_wildcard": [],
    "enable_network_discovery": true,
    "enable_self_propagation": true,
    "enable_set_wallpaper": true,
    "enable_esxi_vm_kill": true,
    "strict_include_paths": []
}
```

Figure 2 – Example embedded JSON data structure

Recently observed samples include configurations with a common set of options (Table 1) some of which apply to both variants and others that are operating system specific.

Configuration Option	Description
config_id	Not set in recently observed samples.
public_key	Victim-specific RSA public key used to secure the encryption key.
extension	Victim-specific extension appended to encrypted files, a seemingly randomly generated string of seven lowercase alphanumeric characters (Regular Expression: **[a-z0-9]{7}**).
note_file_name	Ransom note filename, set to '*RECOVER-${EXTENSION}-FILES.txt*' in recently observed samples.
note_full_text	Ransom note text, consistent across recently observed samples with a victim-specific Tor onion address used for negotiations.
note_short_text	Windows desktop wallpaper text directing the victim to the ransom note, consistent across recently observed samples.

default_file_mode	Typically set to ‘Auto’ although two ‘SmartPattern’ values have been observed that result in a specified number of megabytes of each file being encrypted in steps of ten: • map[SmartPattern:[1.048576e+07 10]] • map[SmartPattern:[3.145728e+07 10]] These values would be set for performance reasons on specific victim hosts such as when dealing with very large files.
default_file_cipher	Set to ‘Best’ in all recently observed samples, attempts to use AES encryption first and falls back to ChaCha20.
credentials	Victim-specific, and likely used for propagation. Both domain and local administrator credentials have been observed in some samples.
kill_services	Typical list of common Windows services related to applications, backup utilities, security solutions and servers with some victim-specific services observed in recent samples.
kill_processes	Typical list of common Windows processes related to applications, backup utilities, security solutions and servers with victim-specific processes observed in recent samples.
exclude_directory_names	Typical list of Windows system directories to ensure that the host remains stable post-encryption (allowing the ransom note to be accessed).
exclude_file_names	Typical list of Windows system files to ensure the host remains stable post-encryption (allowing the ransom note to be accessed).
exclude_file_extensions	Typical list of Windows system file extensions to ensure the host remains stable post-encryption (allowing the ransom note to be accessed).
exclude_file_path_wildcard	Not set in recently observed samples, excludes specified file paths from the encryption process on a per-host/victim basis.
enable_network_discovery	Boolean value, set to ‘true’ in recently observed samples and enabling network discovery via NetBIOS/SMB in search of other hosts to encrypt.

enable_self_propagation	Boolean value, mixed configurations observed in recent samples suggest this is configured on a per-host/victim basis.
enable_set_wallpaper	Boolean value, set to ‘true’ in recently observed samples resulting in the Windows desktop wallpaper displaying ‘note_short_text’.
enable_esxi_vm_kill	Boolean value, determines if VMware ESXi virtual machines will be terminated.
enable_esxi_vm_snapshot_kill	Boolean value, determines if VMware ESXi virtual machine snapshots will be removed (configuration option only present in recently observed Linux samples).
strict_include_paths	Not set in recently observed samples, results in the encryption process only processing files within the specified paths.
esxi_vm_kill_exclude	Boolean value, excludes specific VMware ESXi virtual machines from the termination process

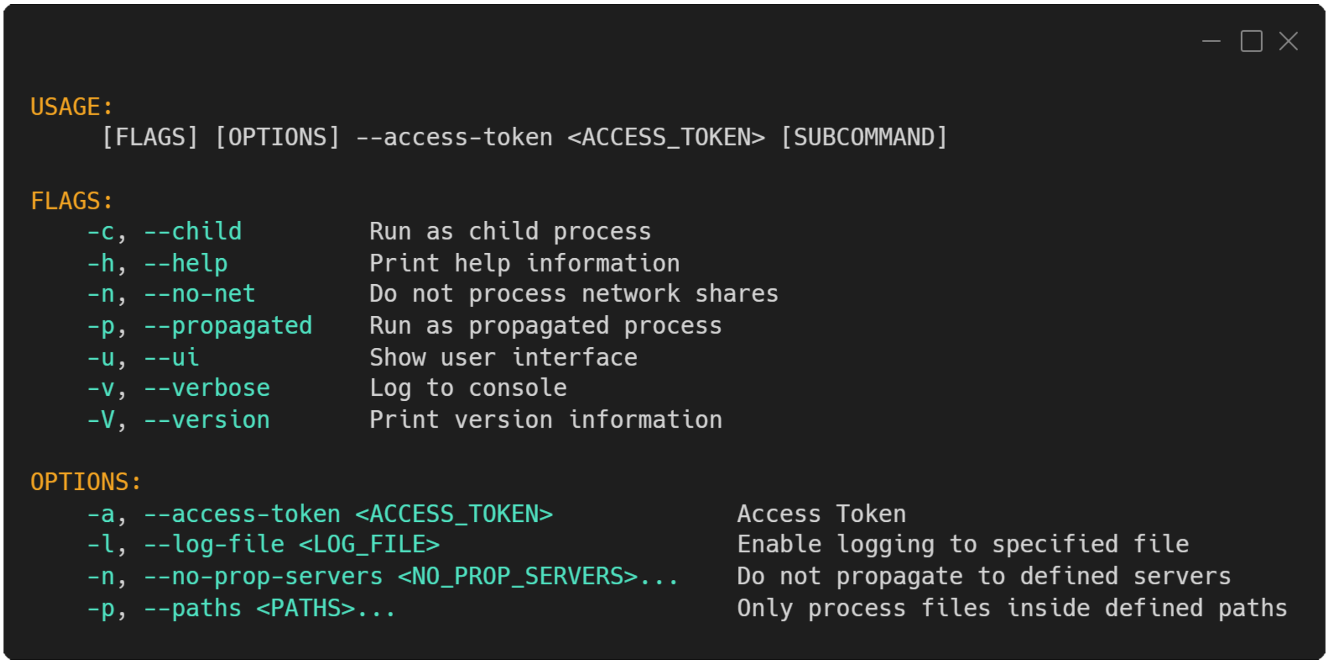
Table 1 – ALPHV Configuration Options

Although many options appear within the embedded configurations of both samples, it appears that the ransomware will ignore those that don’t apply to the host, for example, recently observed Windows samples include references to VMware ESXi, a platform supported by the Linux variant, whilst recently observed Linux samples retain references to Windows directories, files, and file extensions.

Based on the command-line options available to both variants, many of the embedded configuration options can likely be overridden at execution.

Command-line Interface

Launching the ransomware with the ‘--help’ parameter conveniently shows available options (Figure 3) and provides an insight into its capabilities.

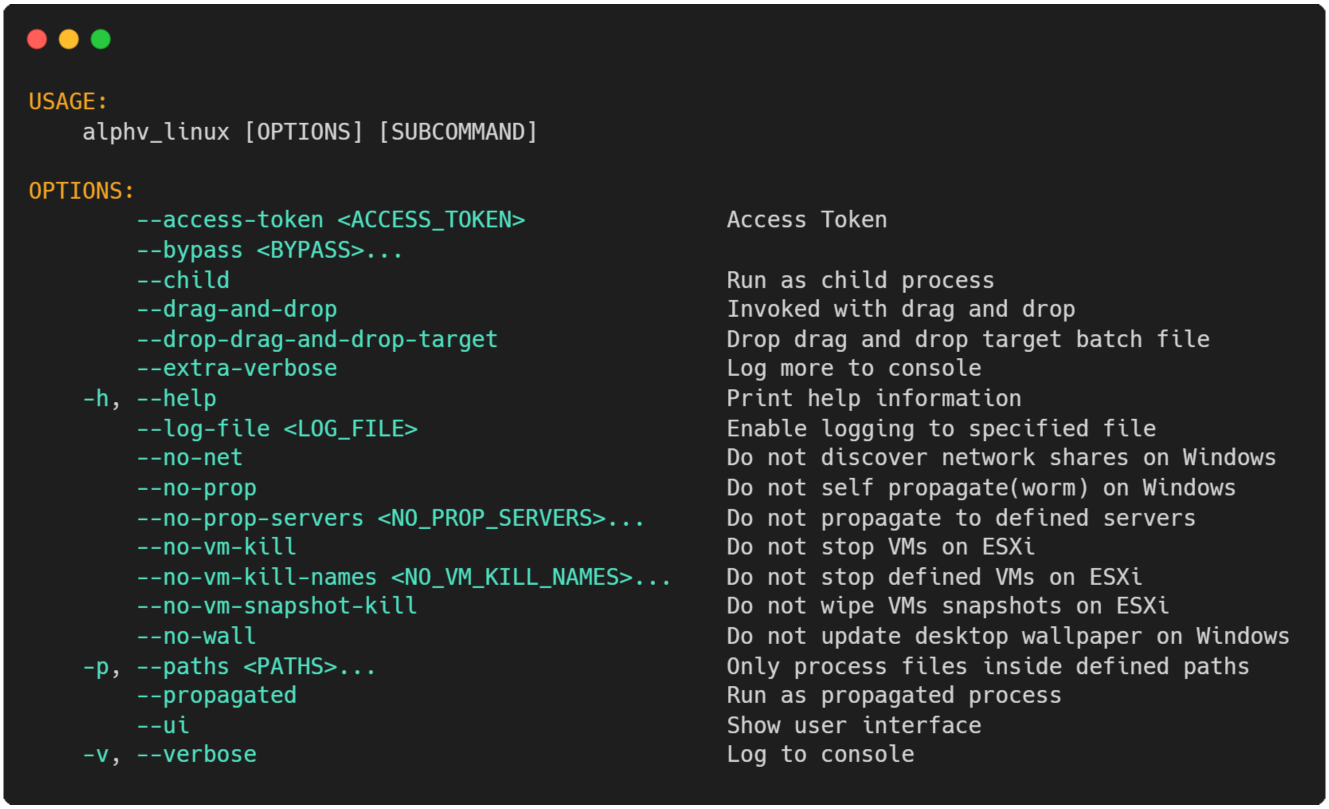


```
USAGE:
     [FLAGS] [OPTIONS] --access-token <ACCESS_TOKEN> [SUBCOMMAND]

FLAGS:
    -c, --child          Run as child process
    -h, --help           Print help information
    -n, --no-net         Do not process network shares
    -p, --propagated     Run as propagated process
    -u, --ui             Show user interface
    -v, --verbose        Log to console
    -V, --version        Print version information

OPTIONS:
    -a, --access-token <ACCESS_TOKEN>            Access Token
    -l, --log-file <LOG_FILE>                    Enable logging to specified file
    -n, --no-prop-servers <NO_PROP_SERVERS>...   Do not propagate to defined servers
    -p, --paths <PATHS>...                       Only process files inside defined paths
```

Figure 3 – ALPHV ‘Core’ Options (Windows variant)

Differences in the options displayed may indicate an earlier version or victim/Windows-specific variant, with many options allowing the threat actor to override any embedded configuration.

In addition to these core capabilities, analysis of a recent Linux variant provides insight (Figure 4) into support for VMware ESXi hosts including the ability to stop virtual machines and, if enabled, wipe virtual machine snapshots to thwart recovery efforts.



```
USAGE:
    alphv_linux [OPTIONS] [SUBCOMMAND]

OPTIONS:
        --access-token <ACCESS_TOKEN>              Access Token
        --bypass <BYPASS>...
        --child                                    Run as child process
        --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
    -h, --help                                     Print help information
        --log-file <LOG_FILE>                      Enable logging to specified file
        --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
        --propagated                               Run as propagated process
        --ui                                       Show user interface
    -v, --verbose                                  Log to console
```

Figure 4 – ALPHV 'ESXi' Options (Linux variant)

Once initially launched, both the Linux and Windows variants include a multi-threaded worker pool that spawns a 'file worker pool' comprised of four workers that are used to open and modify each target file, replacing the original content with encrypted data.

Windows Variant

Having initialized its core features, including the creation of the file worker pool, privilege escalation capabilities can be executed by the Windows variant under certain conditions.

Given that the manual execution of the ransomware element occurs post-intrusion, after the reconnaissance and data exfiltration stages, it is expected that the threat actor would already have elevated privileges.

Regardless, the following privilege escalation capabilities appear to be embedded within the ransomware and will likely increase the chance of success when propagated to other Windows hosts:

- 'Masquerade_PEB', previously released as a proof-of-concept script [6] and used to give a PowerShell process the appearance of another process that in turn could allow elevated operations.
- User Account Control (UAC) bypass via an elevated COM interface, in this case abusing the Microsoft Connection Manager Admin API Helper for Setup COM object (cmstplua.dll):

  %SYSTEM32%\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}

  CVE-2016-0099, a Secondary Logon Service exploit via the 'CreateProcessWithLogonW' API.

Additionally, the Windows variant performs a number of processes prior to the encryption phase that differs from common ransomware threats, namely:

> Acquiring the host universally unique identifier (UUID) using the Windows Management Interface command-line utility (WMIC) that, along with the 'access token' value, generates an 'access-key' to allow access to the victim-specific Tor site:
>
> **wmic csproduct get UUID**
>
> Enabling both 'remote to local' and 'remote to remote' symbolic links using the file system utility (fsutil) to allow the creation of links that redirects to some other file or directory:

- **fsutil behavior set SymlinkEvaluation R2L:1**
- **fsutil behavior set SymlinkEvaluation R2R:1**

> Setting the number of network requests the Server Service can make to the maximum, avoiding any remote file access issues when the encryption process executes, by updating the configuration in the Windows registry:

```
reg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
/v MaxMpxCt /d 65535 /t REG_DWORD /f
```

- Enumerating all local disk partitions and, if any hidden partitions are found, mounting these to allow additional data to be encrypted, potentially rendering recovery partitions useless.
- Propagation, if enabled, likely uses credentials contained within the embedded configuration and makes use of PsExec, a Microsoft Windows Sysinternals utility, to execute the ransomware on a remote host:

```
psexec.exe -accepteula \\<TARGET_HOST> -u <USERNAME> -p <PASSWORD> -s -d -f
-c <ALPHV_EXECUTABLE> [FLAGS] [OPTIONS] --access-token <ACCESS_TOKEN>
[SUBCOMMAND]
```

In addition to suppressing the display of the PsExec license dialog (**-accepteula**), the propagated ransomware process will be executed using the SYSTEM account (**-s**) in a non-interactive session (**-d**), negating the need to wait for the remote process to complete, with the ransomware executable being copied to the remote host (**-c**) and overwriting any existing file (**-f**).
Notably, the legitimate PsExec executable is embedded within the Windows variant and is dropped in the victim's **%TEMP%** directory.

As expected, common Windows ransomware traits are also performed:

Deletion of shadow copies using the Volume Shadow Copy Service (VSS) administrative utility (vssadmin) to thwart recovery efforts:

```
vssadmin.exe delete shadows /all /quiet
```

Terminating the processes and/or services specified within the configuration to minimize the number of locked (open) files as well as potentially disabling backup utilities and security software to evade detection.

Emptying the Recycle Bin.

Defaulting to AES encryption, signified by the 'best' configuration option, the process can fallback or be overridden to use ChaCha20.

After a file has been encrypted, the pre-configured seven-character alphanumeric file extension is appended to the filename, a value that appears to differ between victims.

Following the encryption phase, a number of final tasks are performed:

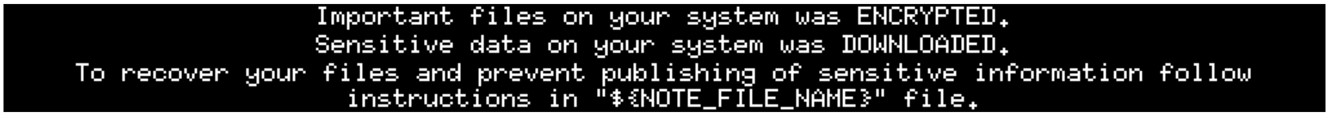
Network discovery, using NetBIOS and SMB, likely in preparation for propagation, seemingly including the use of native address resolution protocol (ARP) command to gather the IP and MAC addresses from the ARP table (a list of hosts known to the victim host):

```
arp -a
```

Creating the predefined ransom note in each folder containing encrypted files as well as an image containing the short ransom note on the Desktop of all users:

- **RECOVER-<ENCRYPTED_FILE_EXTENSION>-FILES.txt**
- **%USERPROFILE%\Desktop\RECOVER-<ENCRYPTED_FILE_EXTENSION>-FILES.txt.png**

- Setting the desktop wallpaper (Figure 5) to the dropped PNG image file for each user through a Windows registry key update:
- **HKEY_USERS\<SID>\Control Panel\Desktop\WallPaper = "C:\\Users\\<USERNAME>\\Desktop\\RECOVER-<ENCRYPTED_FILE_EXTENSION>-FILES.txt.png"**



```
Important files on your system was ENCRYPTED.
Sensitive data on your system was DOWNLOADED.
To recover your files and prevent publishing of sensitive information follow
instructions in "${NOTE_FILE_NAME}" file.
```

Figure 5 – Desktop wallpaper post-encryption

- Repeating the shadow copy deletion process using vssadmin.
- Using the Windows Event Log utility (wevtutil) to list and then clear all event logs:

```
for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\""
```

VMware ESXi Behaviour

Assuming the ESXi options are not disabled, the VMware ESXi command-line interface utility (esxcli) is called and generates a comma-separated list of all running virtual machines:

```
esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list
```

The output of this command is subsequently ‘piped’ to AWK, a text-processing utility, to parse the result and launch the ESXI command-line interface utility to force terminate each virtual machine:

```
awk -F "\"*,\"*" '{system("esxcli vm process kill --type=force --world-id="$1)}'
```

Utilizing the VMware Virtual Infrastructure Management utility (vimcmd), another list of virtual machines is gathered and parsed, the results of which are passed back to vimcmd with the ‘snapshot.removeall’ command that results in any, and all, snapshots being deleted:

```
for i in `vim-cmd vmsvc/getallvms| awk '{print$1}'`;do vim-cmd
vmsvc/snapshot.removeall $i & done
```

Victimology

As is common with big-game hunter ransomware threats, victims are typically large organizations from which bigger ransoms can be extorted with reports suggesting that demands have ranged from US$400K up to $3M payable in cryptocurrency.

Whilst the true number of victims is unknown, over twenty organizations have been named on the group’s Tor ‘leak site’, across a variety of sectors and countries including:

- Australia, Bahamas, France, Germany, Italy, Netherlands, Philippines, Spain, United Kingdom, and the United States.
- Business services, construction, energy, fashion, finance, logistics, manufacturing, pharmaceutical, retail, and technology.

Indicators of Compromise (IOC)

Linux Processes

The following legitimate, albeit suspicious, processes were spawned by the Linux/VMware ESXi variant:

- **esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list | awk -F "\"*,\"*" '{system("esxcli vm process kill --type=force --world-id="$1)}'**
- **for i in `vim-cmd vmsvc/getallvms| awk '{print$1}'`;do vim-cmd vmsvc/snapshot.removeall $i & done**

Windows Processes

The following legitimate, albeit suspicious, processes were spawned by the Windows variant:

- **arp -a**
- **%SYSTEM32%\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}**
- **for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\""**
- **fsutil behavior set SymlinkEvaluation R2L:1**
- **fsutil behavior set SymlinkEvaluation R2R:1**

- **psexec.exe -accepteula \\<TARGET_HOST> -u <USERNAME> -p <PASSWORD> -s -d -f -c <ALPHV_EXECUTABLE> [FLAGS] [OPTIONS] --access-token <ACCESS_TOKEN> [SUBCOMMAND]**
- **reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f**
- **wmic csproduct get UUID**

Linux Ransomware Executables (SHA256)

Given that each sample is victim-specific, the following are provided for research rather than detection purposes:

- **3a08e3bfec2db5dbece359ac9662e65361a8625a0122e68b56cd5ef3aedf8ce1**
- **5121f08cf8614a65d7a86c2f462c0694c132e2877a7f54ab7fcefd7ee5235a42**
- **9802a1e8fb425ac3a7c0a7fca5a17cfcb7f3f5f0962deb29e3982f0bece95e26**
- **e7060538ee4b48b0b975c8928c617f218703dab7aa7814ce97481596f2a78556**

- **f7a038f9b91c40e9d67f4168997d7d8c12c2d27cd9e36c413dd021796a24e083**

  f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6

Windows Ransomware Executables (SHA256)

Given that each sample is victim-specific, the following are provided for research rather than detection purposes:

- **0c6f444c6940a3688ffc6f8b9d5774c032e3551ebbccb64e4280ae7fc1fac479**
- **13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31**

- **15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed**
- **1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e**
- **2587001d6599f0ec03534ea823aab0febb75e83f657fadc3a662338cc08646b0**
- **28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169**
- **2cf54942e8cf0ef6296deaa7975618dadff0c32535295d3f0d5f577552229ffc**

- **38834b796ed025563774167716a477e9217d45e47def20facb027325f2a790d1**
- **3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83**
- **4e18f9293a6a72d5d42dad179b532407f45663098f959ea552ae43dbb9725cbf**
- **59868f4b346bd401e067380cac69080709c86e06fae219bfb5bc17605a71ab3f**
- **5bdc0fb5cfbd42de726aacc40eddca034b5fa4afcc88ddfb40a3d9ae18672898**

- **658e07739ad0137bceb910a351ce3fe4913f6fcc3f63e6ff2eb726e45f29e582**
- **7154fdb1ef9044da59fcfdbdd1ed9abc1a594cacb41a0aeddb5cd9fdaeea5ea8**
- **722f1c1527b2c788746fec4dd1af70b0c703644336909735f8f23f6ef265784b**
- **731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161**
- **7b2449bb8be1b37a9d580c2592a67a759a3116fe640041d0f36dc93ca3db4487**

- **7e363b5f1ba373782261713fa99e8bbc35ddda97e48799c4eb28f17989da8d8e**
- **9f6876762614e407d0ee6005f165dd4bbd12cb21986abc4a3a5c7dc6271fcdc3**
- **aae77d41eba652683f3ae114fadec279d5759052d2d774f149f3055bf40c4c14**
- **b588823eb5c65f36d067d496881d9c704d3ba57100c273656a56a43215f35442**
- **bd337d4e83ab1c2cacb43e4569f977d188f1bb7c7a077026304bf186d49d4117**

- **be8c5d07ab6e39db28c40db20a32f47a97b7ec9f26c9003f9101a154a5a98486**
- **c3e5d4e62ae4eca2bfca22f8f3c8cbec12757f78107e91e85404611548e06e40**
- **c5ad3534e1c939661b71f56144d19ff36e9ea365fdb47e4f8e2d267c39376486**
- **c8b3b67ea4d7625f8b37ba59eed5c9406b3ef04b7a19b97e5dd5dab1bd59f283**
- **cda37b13d1fdee1b4262b5a6146a35d8fc88fa572e55437a47a950037cc65d40**

- **cefea76dfdbb48cfe1a3db2c8df34e898e29bec9b2c13e79ef40655c637833ae**
- **d767524e1bbb8d50129485ffa667eb1d379c745c30d4588672636998c20f857f**
- **f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb**

Jason Hill

Jason is a Security Researcher within the Varonis Research Team and has a penchant for all things threat intelligence. Equally happy analyzing nefarious files or investigating badness, Jason is driven by the desire to make the cyberworld a safer place.