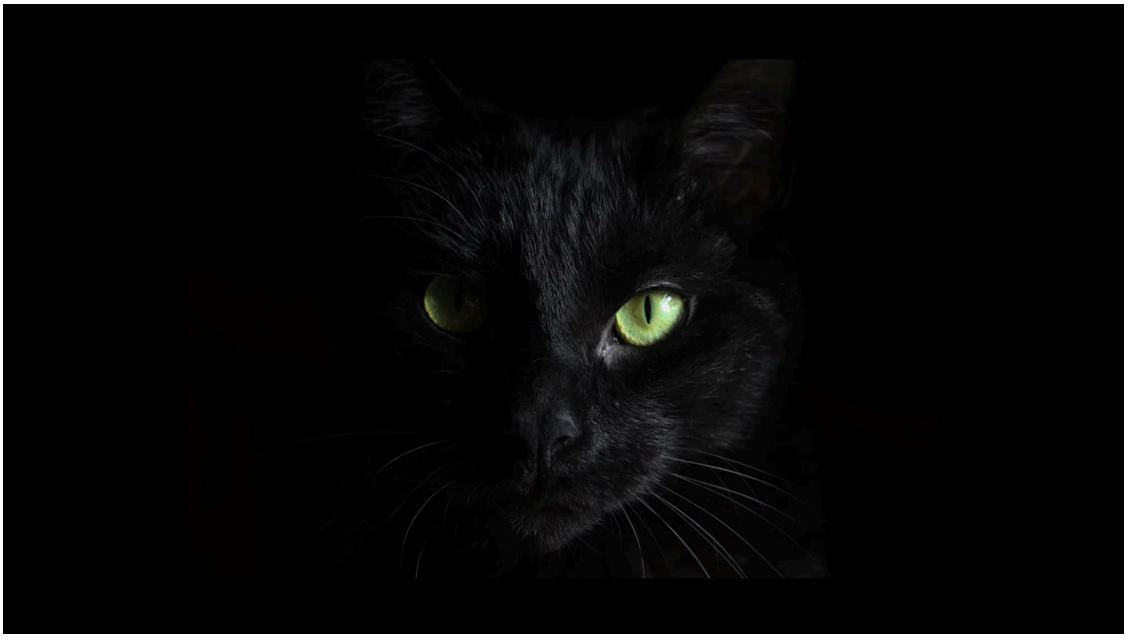
ALPHV BlackCat - This year's most sophisticated ransomware

By Lawrence Abrams

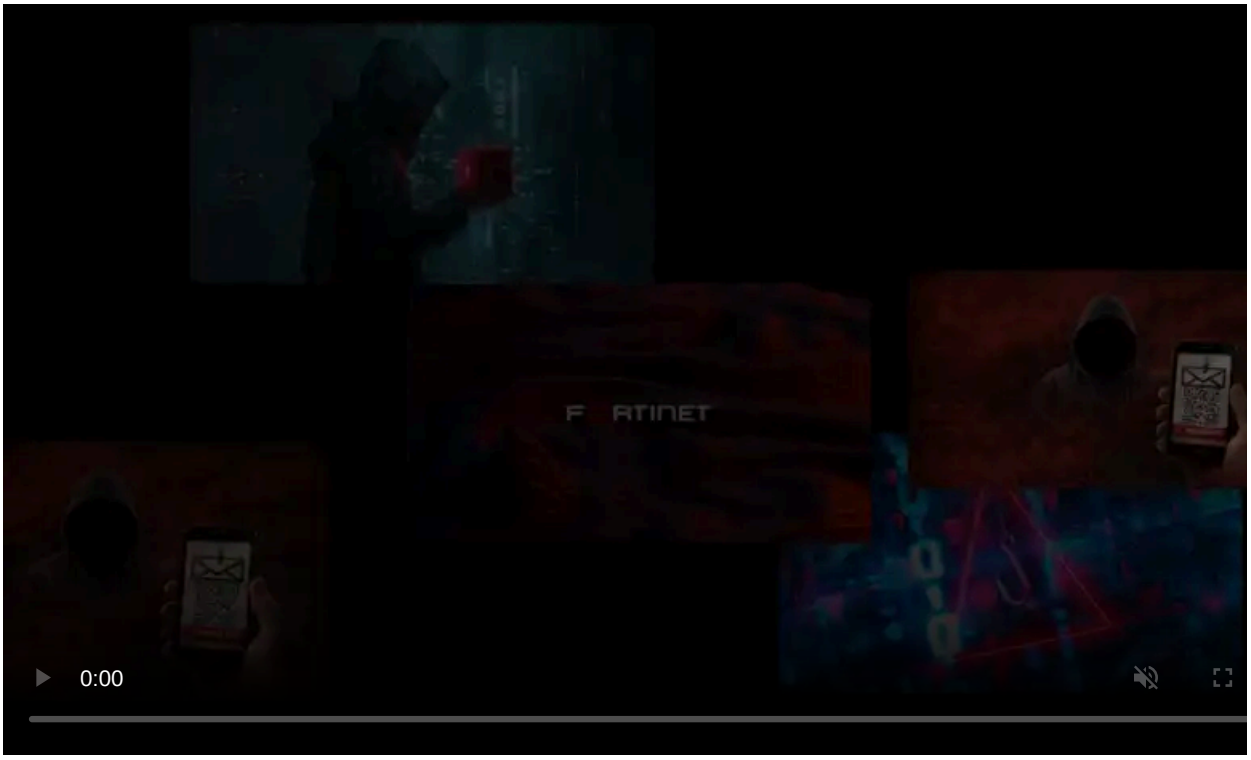
Published: 2021-12-09 · Archived: 2026-04-06 02:08:45 UTC

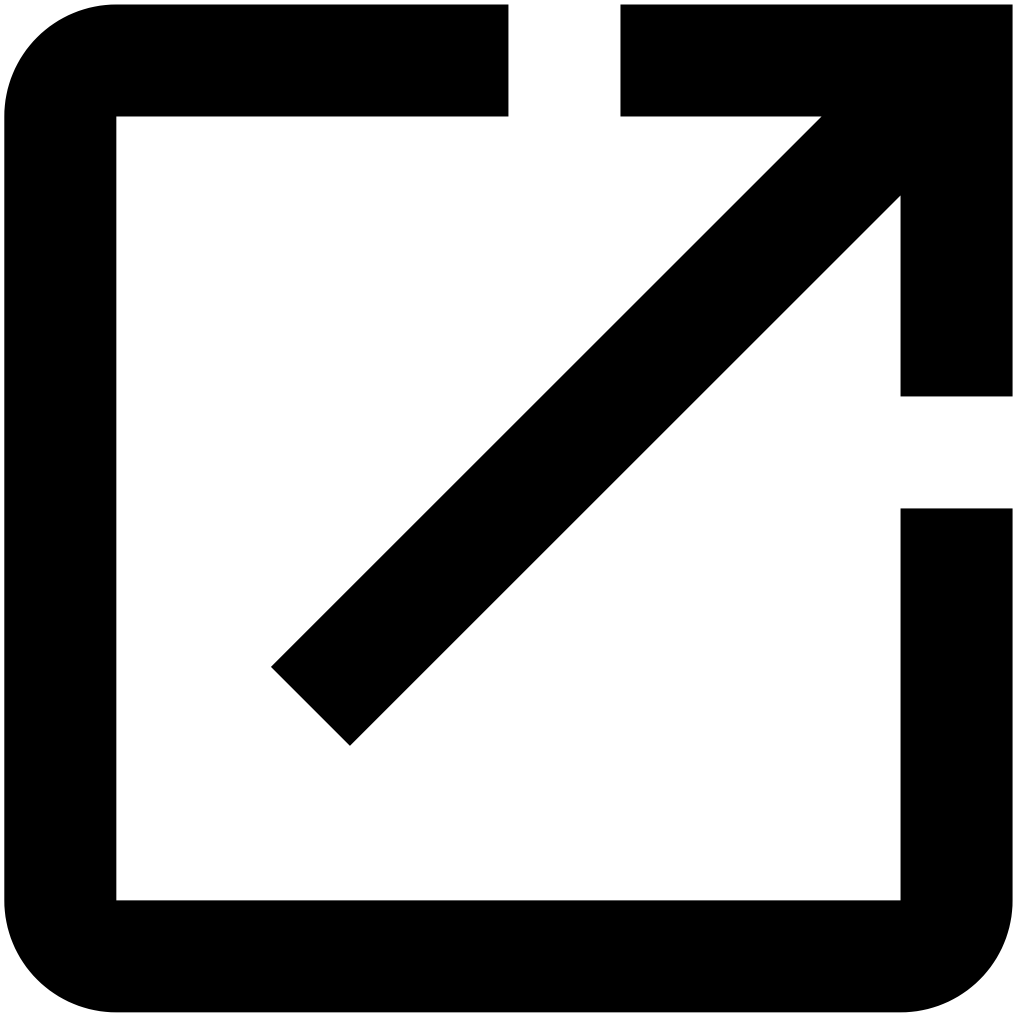


The new ALPHV ransomware operation, aka BlackCat, launched last month and could be the most sophisticated ransomware of the year, with a highly-customizable feature set allowing for attacks on a wide range of corporate environments.

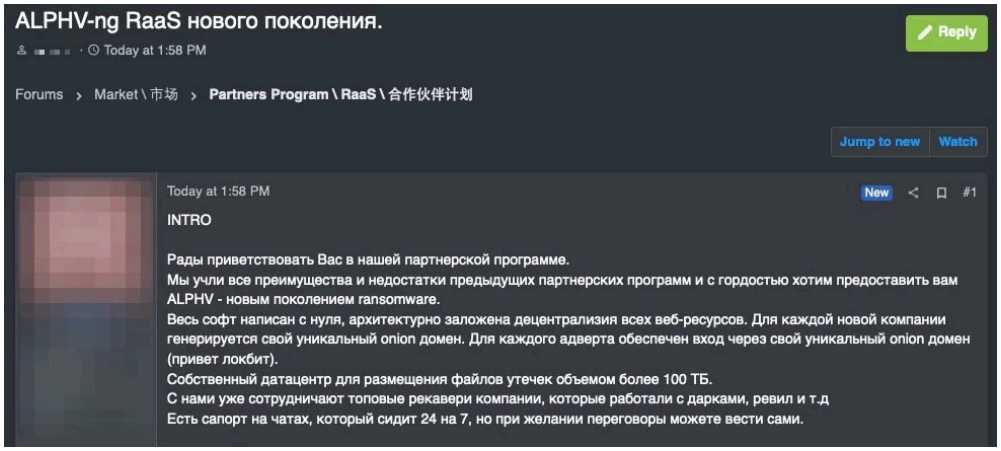
The ransomware executable is written in Rust, which is not typical for malware developers but is slowly increasing in popularity due to its high performance and memory safety.

MalwareHunterTeam found the new ransomware and told BleepingComputer that the first ID Ransomware submission for the new operation was on November 21st.


F RTINET
0:00

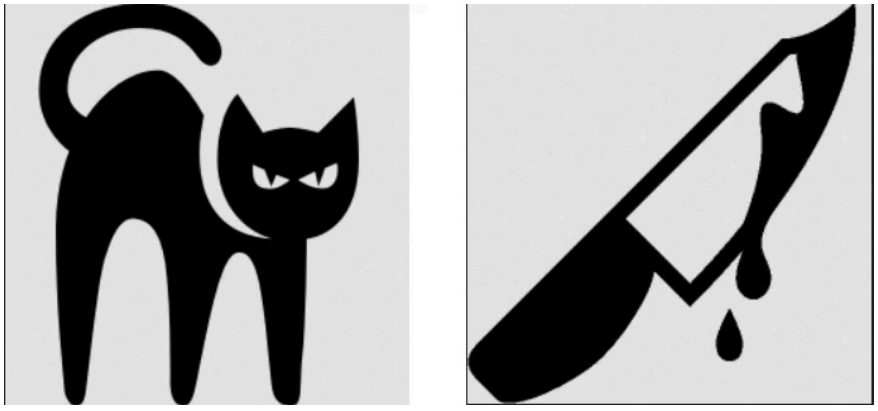


The ransomware is named by the developers as ALPHV and is being promoted on Russian-speaking hacking forums.



ALPHV RaaS promoted on Russian-speaking hacking forum
Source: Twitter

MalwareHunterTeam named the ransomware BlackCat due to the same favicon of a black cat being used on every victim's Tor payment site, while the data leak site uses a bloody dagger, shown below.



Favicons used on Tor payment and data leak sites

Like all ransomware-as-a-service (RaaS) operations, the ALPHV BlackCat operators recruit affiliates to perform corporate breaches and encrypt devices.

In return, affiliates will earn varying revenue shares based on the size of a ransom payment. For example, for ransom payments up to $1.5 million, the affiliate earns 80%, 85% for up to $3 million, and 90% of payments over $3 million.

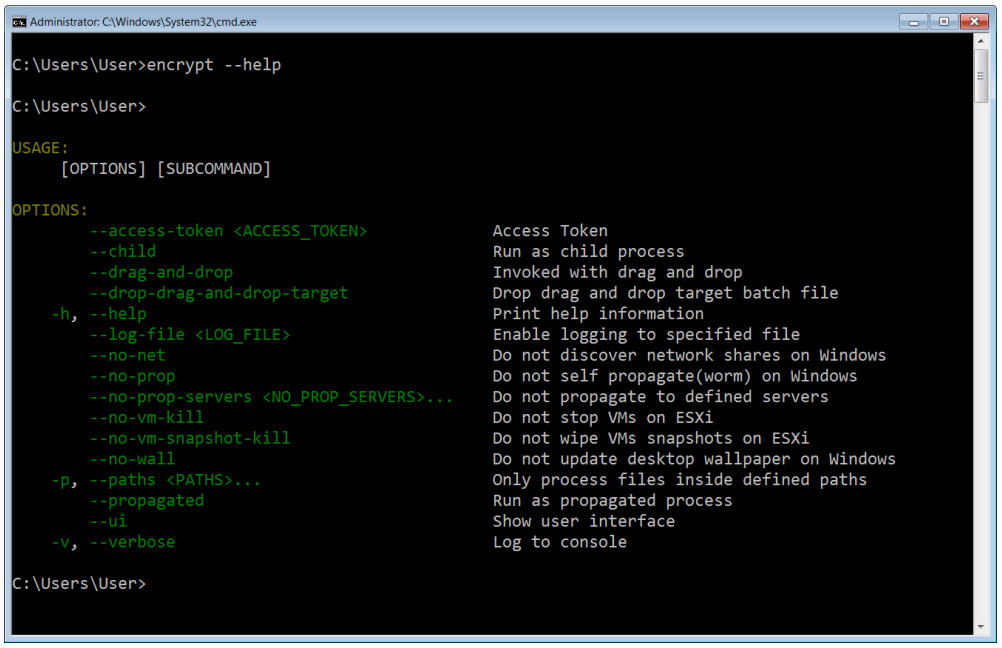
To illustrate the type of money an affiliate can earn from these RaaS programs, CNA reportedly paid a $40 million ransom to the Russian hacking group Evil Corp. Under ALPHV's revenue share, this would equate to $36 million paid to the affiliate.

Exploring the features of the ALPHV BlackCat ransomware

The ALPHV BlackCat ransomware includes numerous advanced features that let it stand out from other ransomware operations. In this section, we will take a look at the ransomware and how it operates, and demonstrate a test encryption from a sample shared with BleepingComputer.

The ransomware is entirely command-line driven, human-operated, and highly configurable, with the ability to use different encryption routines, spread between computers, kill virtual machines and ESXi VMs, and automatically wipe ESXi snapshots to prevent recovery.

These configurable options can be found using the `--help` command-line argument, shown below.



ALPHV BlackCat ransomware command-line arguments

Source: BleepingComputer

Each ALPHV ransomware executable includes a JSON configuration that allows customization of extensions, ransom notes, how data will be encrypted, excluded folders/files/extensions, and the services and processes to be automatically terminated.

According to the threat actor, the ransomware can be configured to use four different encryption modes, as described in their "recruitment" post on a dark web hacking forum.

The software is written from scratch without using any templates or previously leaked source codes of other ransomware.
The choice is offered:
4 encryption modes:
-Full - full file encryption. The safest and slowest.
-Fast - encryption of the first N megabytes. Not recommended for use, the most unsafe possible solution, but the fastest.
-DotPattern - encryption of N megabytes through M step. If configured incorrectly, Fast can work worse both in speed and in cryptographic strength.
-Auto. Depending on the type and size of the file, the locker (both on windows and * nix / esxi) chooses the most optimal (in terms of speed / security) strategy for processing files.

-SmartPattern - encryption of N megabytes in percentage steps. By default, it encrypts 10 megabytes every 10% of the file starting from the header. The most optimal mode in the ratio of speed / cryptographic strength.
2 encryption algorithms:
-ChaCha20
-AES
In auto mode, the software detects the presence of AES hardware support (exists in all modern processors) and uses it. If there is no AES support, the software encrypts files ChaCha20.

ALPHV BlackCat can also be configured with domain credentials that can be used to spread the ransomware and encrypt other devices on the network. The executable will then extract PSExec to the %Temp% folder and use it to copy the ransomware to other devices on the network and execute it to encrypt the remote Windows machine.

When launching the ransomware, the affiliate can use a console-based user interface that allows them to monitor the progression of the attack. In the image below, you can see this interface displayed while BleepingComputer encrypted a test device using a modified executable to append the .bleepin extension.

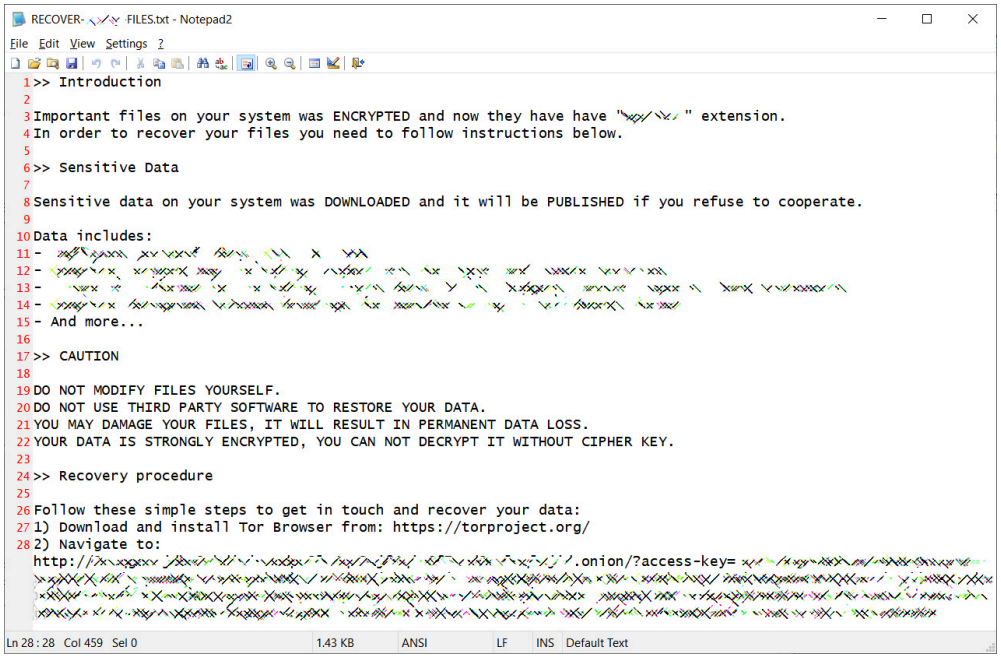
Encrypting a test computer
Source: BleepingComputer

In the sample tested by BleepingComputer, the ransomware will terminate processes and Windows services that could prevent files from being encrypted. These terminated processes include Veeam, backup software, database servers, Microsoft Exchange, Office applications, mail clients, and the Steam process not to leave gamers out.

Other actions taken during this "setup" process include the clearing of Recycle Bin, deleting Shadow Volume Copies, scanning for other network devices, and connecting to a Microsoft cluster if one exists.

ALPHV BlackCat also uses the Windows Restart Manager API to close processes or shut down Windows services keeping a file open during encryption.

Usually, when encrypting a device, the ransomware will use a random name extension, which is appended to all files and included in the ransom note. Ransom notes are named in the format '**RECOVER-[extension]-FILES.txt**', which in our example above is RECOVER-bleepin-FILES.txt.



ALPHV BlackCat ranson note

Source: BleepingComputer

Ransom notes are preconfigured by the affiliate performing the attack and are different for each victim. Some ransom notes include the types of data stolen and a link to a Tor data leak site where the victims can preview stolen data.

Each victim also has a unique Tor site and sometimes a unique data leak site, allowing the affiliate to conduct their own negotiations.

Finally, BlackCat claims to be cross-platform with support for multiple operating systems.

> Cross-platform software, i.e. if you mount Windows disks in Linux or vice versa, the decryptor will be able to decrypt the files. - ALPHV operator.

Operating systems that the threat actors allegedly tested their ransomware on are included below:

- All line of Windows from 7 and higher (tested on 7, 8.1, 10, 11; 2008r2, 2012, 2016, 2019, 2022); XP and 2003 can be encrypted over SMB.
- ESXI (tested on 5.5, 6.5, 7.0.2u)
- Debian (tested on 7, 8, 9);
- Ubuntu (tested on 18.04, 20.04)
- ReadyNAS, Synology

Ransomware expert and ID Ransomware creator Michael Gillespie has analyzed the encryption routine used by the ransomware and, unfortunately, was not able to find any weaknesses that could allow free decryption.

Access-token feature makes negotiations secret

A long-standing problem affecting both victims and ransomware operations is that samples commonly get leaked through malware analysis sites, allowing full access to the negotiation chat between a ransomware gang and their victim.

In some cases, this has led to unrelated parties commenting in the chat and disrupting negotiations.

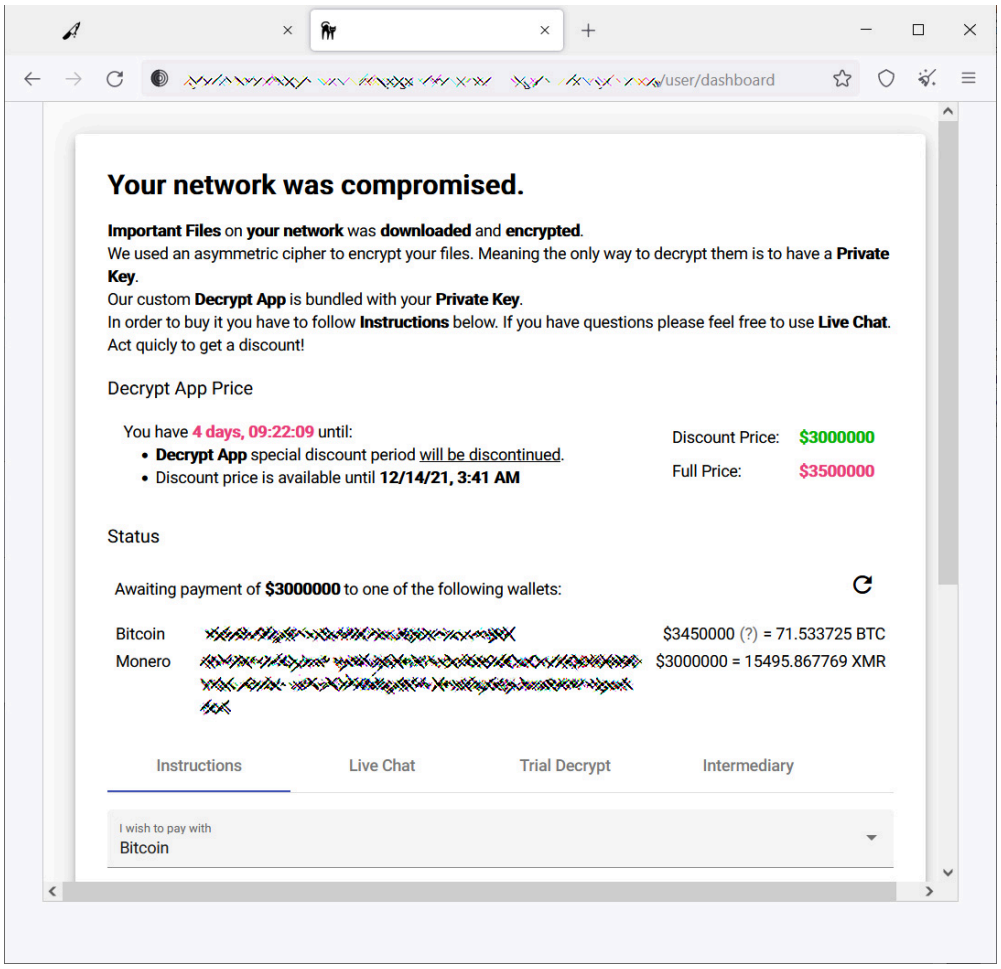
To prevent this from happening, the ALPHV BlackCat ransomware developers introduced an `--access-token=[access_token]` command-line argument that must be used when launching the encryptor.

This access token is used to create the access key needed to enter a negotiation chat on the ransomware gang's Tor payment site. As this token is not included in the malware sample, even if it is uploaded to a malware analysis site, researchers will not use it to access a negotiation site without the ransom note from the actual attack.

Ransoms range from $400k to millions of dollars

BleepingComputer is aware of multiple victims targeted by this ransomware since November from numerous countries, including the USA, Australia, and India.

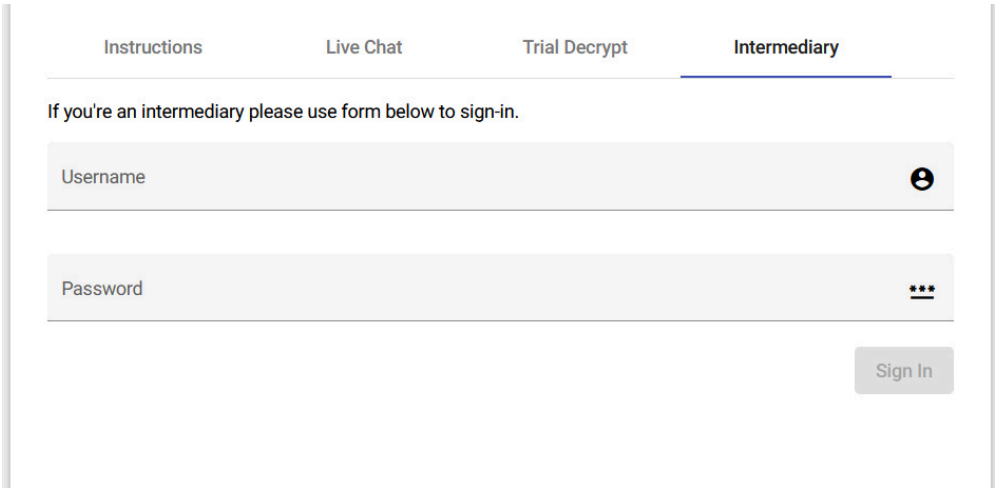
Ransom demands range between $400,000 to $3 million payable in Bitcoin or Monero. However, if victims pay in bitcoin there is an additional 15% fee added to the ransom.



ALPHV Tor Payment Site
Source: BleepingComputer

However, as Monero is considered a privacy coin and frowned upon by the US government, it is not as easily accessible to victims.

Unlike other ransomware operations who have been threatening to wipe or publish data if negotiation firms are hired, ALPHV is catering to ransomware negotiators with a "Intermediary" login page to conduct private negotiations.



Ransomware negotiation login page
Source: BleepingComputer

Like other newer ransomware gangs, ALPHV uses a triple-extortion tactic where they steal data before encrypting devices and threat to publish the data if a ransom is not paid. BleepingComputer has seen multiple data leaks sites for this operation where screenshots of data have been published.

As an additional extortion method, the threat actors threaten to DDoS victims until they pay a ransom.

Overall, this is a highly sophisticated ransomware with the threat actors clearly considering all aspects of attacks.

With the BlackMatter and REvil ransomware operations shutting down under pressure from law enforcement, it has left a large void waiting for another threat actor to fill.

It is very likely that ALPHV BlackCat is the one that has a good chance of filling it.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
