BlackCat Ransomware: Tactics, Techniques & Mitigation Strategies

Archived: 2026-05-05 02:06:30 UTC

In February 2024, Change Healthcare, a subsidiary of UnitedHealth Group, faced every company's worst nightmare. Attackers struck swiftly, encrypted vital patient data, and demanded an eye-watering ransom of $22 million. Even after paying the ransom, Change Healthcare did not get its data back.

Behind this attack was BlackCat, also known as ALPHV, a ransomware group notorious for its ruthless efficiency, cunning affiliate tactics, and aggressive pursuit of high-value targets. Despite global crackdowns and arrests, ransomware poses the greatest cybersecurity threat in 2025. Underground forums continue to thrive, selling "access" and hiring "penetration testers".

In this article, you'll learn the latest intelligence on BlackCat ransomware – its evolution, extortion methods, notable attacks across industries, and the defensive strategies your organization can adopt today to detect, prevent, and respond to ransomware threats.

Images used by ALPHV in the beginning

Updated logo

Key Discoveries:

- BlackCat (ALPHV) surfaced in late 2021 and quickly became the second most prolific global ransomware strain, responsible for hundreds of millions in extorted payments.
- BlackCat operates as a Ransomware-as-a-Service (RaaS) with affiliates adopting whatever intrusion techniques yield results, including social engineering and malvertising.
- In just a few years, BlackCat's operators and affiliates have hit organizations from healthcare and hospitality to critical infrastructure, leaving a trail of encrypted systems and stolen data in their wake.
- BlackCat affiliates routinely engage in double extortion, stealing sensitive information and threatening to publish it if the ransom isn't paid. Some affiliates have even layered in DDoS attack threats to coerce payment.
- In 2024, the group grabbed headlines with one of the largest data breaches in history and even appeared to "shut down" amid internal turmoil, only to reemerge under a new guise.
- A similar Rust-based ransomware called "Cicada3301" appeared six months after, which cybersecurity analysts suspect is BlackCat 2.0 operating under a new name.

Advanced threat intelligence and detection solutions are helping organizations to identify and block BlackCat operations early. In an incident, strong offline backups and an incident response plan can reduce BlackCat's impact

What is BlackCat (ALPHV) Ransomware?

BlackCat operates as a Ransomware-as-a-Service (RaaS) model and is considered one of the most sophisticated RaaS operations. The Russian ransomware group emerged shortly after the BlackMatter/DarkSide shut down in 2021, suggesting a possible regrouping of veteran hackers under the ALPHV brand.

Security researchers unofficially called it BlackCat for using two logos: a black cat and a knife dripping with blood. ALPHV members later attempted to move away from romanticizing crime by changing the design of their logo, but the name BlackCat has stuck.

BlackCat started its activity in December 2021, when a campaign to attract new affiliates was advertised on underground forums. Not only was it led by experienced operators, but BlackCat's malware was written in the Rust programming language – one of the first significant ransomware families. Rust's efficiency and cross-platform capabilities enabled the developers to add custom features and hinder reverse engineering.

```
INTRO

Рады приветствовать Вас в нашей партнерской программе.
Мы  учли все преимущества и недостатки предыдущих партнерских программ и с гордостью хотим
предоставить вам ALPHV - новым поколением ransomware.
Весь софт написан с нуля, архитектурно заложена децентрализия всех веб-ресурсов. Для каждой новой
компании генерируется свой уникальный onion домен. Для каждого адверта обеспечен вход через свой
уникальный onion домен (привет локбит).
Собственный датацентр для размещения файлов утечек объемом более 100 ТБ.
С нами уже сотрудничают топовые рекавери компании, которые работали с дарками, ревил и т.д
Есть сапорт на чатах, который сидит 24 на 7, но при желании переговоры можете вести сами.

SECURITY

Мы всячески готовы к существованию в современных условиях, соответствуя всем требованиям к
безопасности инфраструктуры и адвертов. В партнерской программе архитектурно исключены все возможные
связи с форумами(привет ревил), заложены алгоритмы само удаления данных по истечению срока давности,
интегрирован встроенный миксер с настоящим разрывом цепочки(не путать с Wasabi, BitMix и
прочими),т.к. Вы получаете совершенно чистые монеты с иностранных бирж. Кошельки на которые были
отправлены Ваши монеты неизвестны для нашего бекенда. Инфраструктура раздроблена на т.н. ноды,
которые связанны между собой через целую сеть прокладок в пределах сети onion и находятся за NAT+FW.
Даже при получении полноценного cmdshell атакующий не сможет раскрыть реальный ip адрес сервера.
(привет конти)
```

Description of the affiliate program on an underground forum

Translation

arrow_drop_down

INTRO

Welcome to our affiliate program.
We've taken into account all the advantages and weaknesses of previous affiliate programs and are proud to

present to you ALPHV, a new generation of ransomware.
All the software has been developed from scratch, with decentralization of all web resources ensured architecturally. A unique onion domain is generated for every new campaign. Every affiliate has access through a unique onion domain (hello lockbit).
A proprietary data center for storing file leaks bigger than 100 TB.
Top recovery companies, which have worked with darkside, revil, etc. are already collaborating with us.
Chat support is available 24/7, but you can negotiate yourself if you'd like.

SECURITY

We are fully prepared for present-day conditions, complying with all infrastructure and affiliate security requirements. Our affiliate program architecturally rules out any connections with forums(hello revil), has algorithms for data self-deletion after a certain time, and has an integrated mixer with an actual break in the chain(not to be confused with Wasabi, BitMix, and others), as you get perfectly clean coins from foreign exchanges. Our backend does not know the wallets your coins are sent to. The infrastructure is divided into "nodes", which are interconnected via an entire network of intermediaries within the onion network and are located behind NAT+FW.
Even after receiving a full-on cmdshell, the attacker cannot reveal the real IP address of the server (hello conti)

ACCOUNT

If your account has not been active for two weeks, it will be locked, then deleted. Inorder to avoid that, we recommend notifying the admins about vacations, breaks, etc.

Rates are dynamic and depend on the size of a single payment for each company, namely:

- Up to $1.5M – 80%
- Up to $3.0M – 85%
- $3M and more – 90%

In this campaign, potential affiliates were offered a brand new kind of ransomware family developed "from scratch" in the Rust programming language, which is a popular cross-platform programming language for creating secure and effective applications. The use of Rust to create ransomware was a major event in the world of cybercrime.

```
SOFTWARE

Софт написан с нуля без использования каких либо шаблонов или утекших ранее исходных кодов других
ransomware. На выбор предлагается:
4 режима шифрования:
-Full - полное шифрование файла. Самое безопасное и самое медленное.
-Fast - шифрование первых N мегабайт. Не рекомендуется к использованию, самое небезопасное из
возможных решений, но самое быстрое.
-DotPattern  -  шифрование N мегабайт через M шаг. При неправильной настройке может работать хуже
Fast и по скорости и по криптостойкости.
-Auto. В зависмости от типа и размера файла, локер(как на windows так и на *nix / esxi) выбирает
наиболее оптимальную(в соотношении скорость / безопасность) стратегию обработки файлов.

-SmartPattern - шифрование N мегабайт с шагом в процентном соотношении. По умолчанию шифрует полосой
10 мегабайт каждые 10% файла начиная с заголовка. Самый оптимальный режим в соотношении скорость
\криптостойкость.
2 алгоритма шифрования:
-ChaCha20
-AES
В режиме auto софт определяет наличие аппаратной поддержки AES(существует во всех современных
процессорах) и использует его. В случае если поддержка AES отсутствует софт шифрует файлы ChaCha20.

Софт кроссплатформенный, т.е. если смонтировать диски Windows в Linux или наоборот - дешифратор
сможет расшифровать файлы.
Поддерживаемые ОС:
- Вся линейка Windows от 7 и выше (протестировано нами на 7, 8.1, 10, 11; 2008r2, 2012, 2016, 2019,
2022 ); XP и 2003 можно шифровать по SMB.
- ESXI (протестировано на 5.5, 6.5, 7.0.2u)
- Debian (протестировано на 7, 8, 9);
- Ubuntu (протестировано на 18.04, 20.04)
- ReadyNAS, Synology
```

Description of the BlackCat ransomware family

Translation

arrow_drop_down

SOFTWARE

The software has been developed from scratch without using any templates or leaked source codes of other ransomware. You can choose between:

4 encryption modes:

- Full – full file encryption. The most secure and the slowest.
- Fast – encryption of the first N megabytes. Not recommended, the least secure option, but the fastest.
- DotPattern – encryption of N megabytes with an M interval. May function worse than Fast in terms of both speed and encryption strength if configured incorrectly.
- Auto. Depending on the file type and size, the locker(both in windows and *nix / esxi) chooses the most optimal(in terms of the speed / security ratio) strategy for processing files.
- SmartPattern – encryption of N megabytes with a percentage interval. By default, it encrypts with 10-megabyte blocks with an interval of 10% of the file starting with the header. The most optimal mode in terms of the speed\encryption strength ratio.

2 encryption algorithms:

- ChaCha20
- AES

In auto mode, the software determines the presence of hardware support for AES(present in all modern processors) and uses it. If there is no AES support, the software encrypts files using ChaCha20.

The software is cross-platform, i.e., if you mount Windows disks in Linux or vice versa, the decryptor will be able to decrypt files.

Supported OSs

- The entire Windows line from Windows 7 and above (we tested it on 7, 8.1, 10, 11, 2008r2, 2012, 2016, 2019, 2022); XP and 2003 can be encrypted through 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

The new RaaS program took into account the hostile experience of their predecessors, namely the DarkSide, BlackMatter, and REvil affiliate programs. After their notorious attacks against major companies, these groups came under the spotlight of security researchers and law enforcers, who, together with samples, obtained access to victims' pages containing correspondence with threat actors, where they often interfered.

```
Так как в последнее время бинари утекают к аналитикам, а премиум VT позволяет скачать семплы и
получить ридми в чатах могут появлятся рандомные люди, которые могут срывать переговоры (привет
дарксайд), при запуске софта ОБЯЗАТЕЛЬНО использовать флаг  --access-token. Аргументы cmdline не
передаются к АВерам, что позволит сохранять секретность переписки с жертвой. По той же причине
каждый зашифрованный компьютер генерирует свой уникальный ID используемый для разделения чатов.

Имеется функция автоматического перекачивания файлов с сервиса MEGA, даете ссылку на файлы, они
автоматически перекачиваются на наши сервера.

Полное описание всего функционала вы можете получить в разделе FAQ.
```

Information about using access tokens

Translation

arrow_drop_down

Since binaries have been leaking to analysts lately, and VT premium lets you download samples and get readmes, random people may appear in chats and disrupt negotiations (hello darkside), when launching the software you MUST use the flag –access-token. cmdline arguments are not passed to AVs, which will ensure that your correspondence with the victim is confidential. For the same reason, every encrypted computer generates a unique ID used for dividing chats.

There is a feature for uploading files from the MEGA service, you provide a link to files and they are automatically uploaded to your servers.

The complete description of all features can be found in the FAQ section.

To avoid previous mistakes, the BlackCat authors fitted ransomware with a mandatory command line parameter containing an access token provided by the RaaS owners to their affiliates and their ransomware suite.

The ransomware uses the access token to determine the access key, which is added to a Tor link for the victim to access their page.

```
Attention!
Encrypt App requires "--access-token" launch parameter, example:

[redacted]_alpha_x86_32_windows_encrypt_app.exe --access-token [redacted]
```

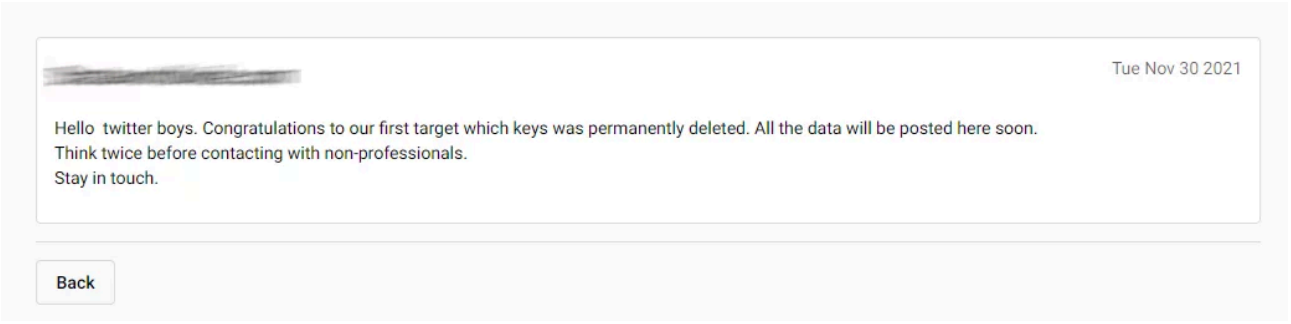
Contents of the help text file provided to RaaS affiliates

This link is saved in the ransom note, which is created as a text file in each catalog with encrypted files.

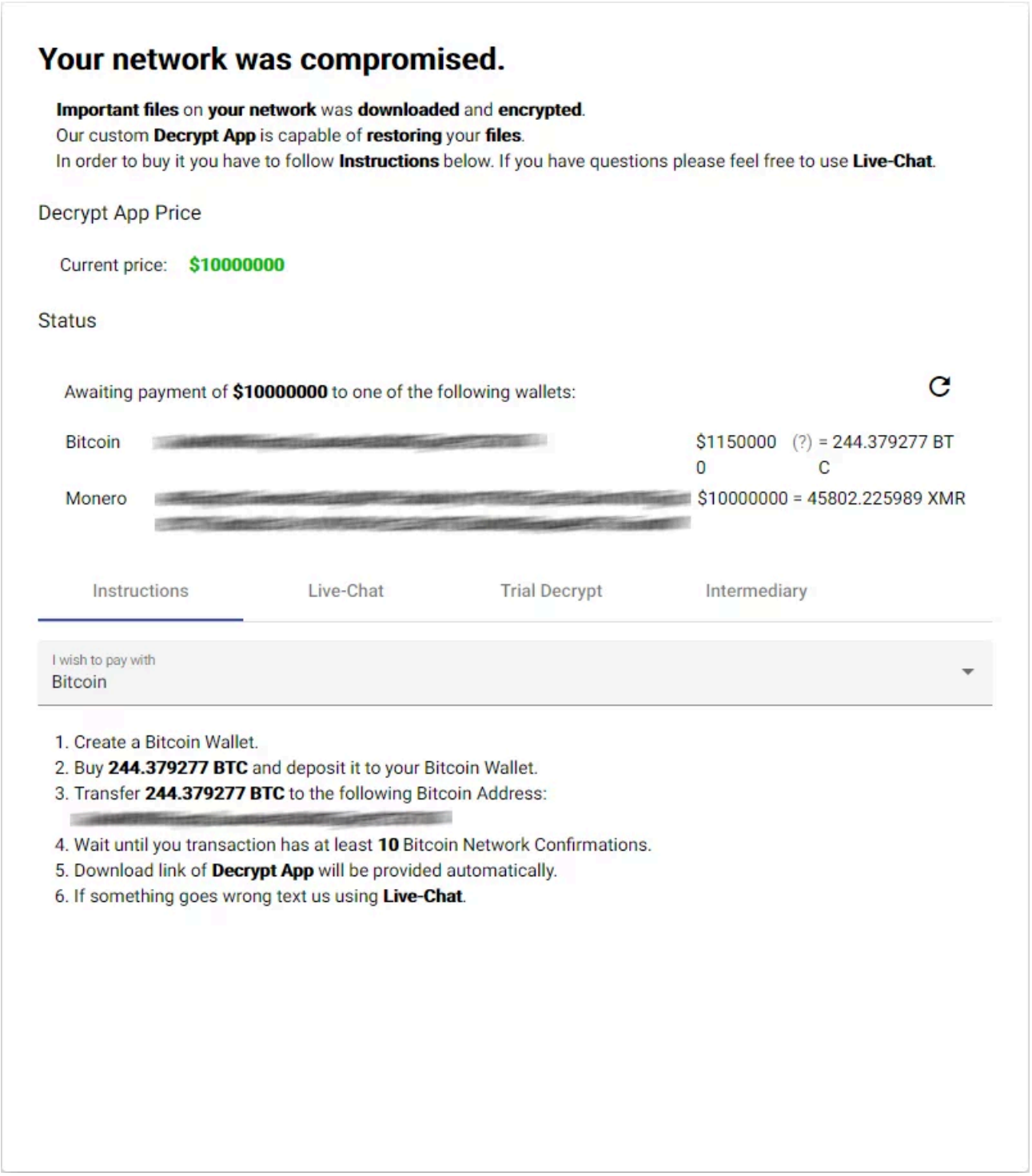
```
>> What happened?

Important files on your network was ENCRYPTED and now they have "[redacted]" 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:
- 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...

>> 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://[redacted].onion/?access-
key=[redacted]
```

Ransom note

When victims published information from their chats, BlackCat affiliates would punish them by increasing the ransom demands. At the start of their activity, the threat actors were even more radical; for instance, they deleted the victim’s encryption keys to intimidate future victims.



Information about deleting the encryption keys of a victim published by BlackCat operators



Victim's personal page

BlackCat Extortion Methods

Double/Triple Extortion and Leak Sites

A hallmark of BlackCat's operations is the use of double extortion and triple extortion techniques:

- The stolen information is published on BlackCat's Dedicated Leak Site (DLS).
- To mount pressure on the victim, BlackCat affiliates may threaten to send sensitive data to the victim's competitors, partners, customers, mass media, law enforcement, etc.
- BlackCat ransomware victims may receive threats of a DDoS attack launched against their infrastructure to extort higher payments, on top of data leaks.
- The gang prefers cryptocurrency (BTC or Monero) for payment , and negotiations are conducted via an encrypted chat hosted on a unique onion domain assigned to each victim.

U.S. authorities report that BlackCat targeted over 1,000 organizations worldwide in its first 18 months of activity. In 2022, **BlackCat launched "ALPHV Collections,**" a searchable leak platform on the open web (with a clearnet domain) that indexed victim data for anyone to browse. BlackCat's leaked data was indexed on the open web, making it easily accessible to the public and search engines.

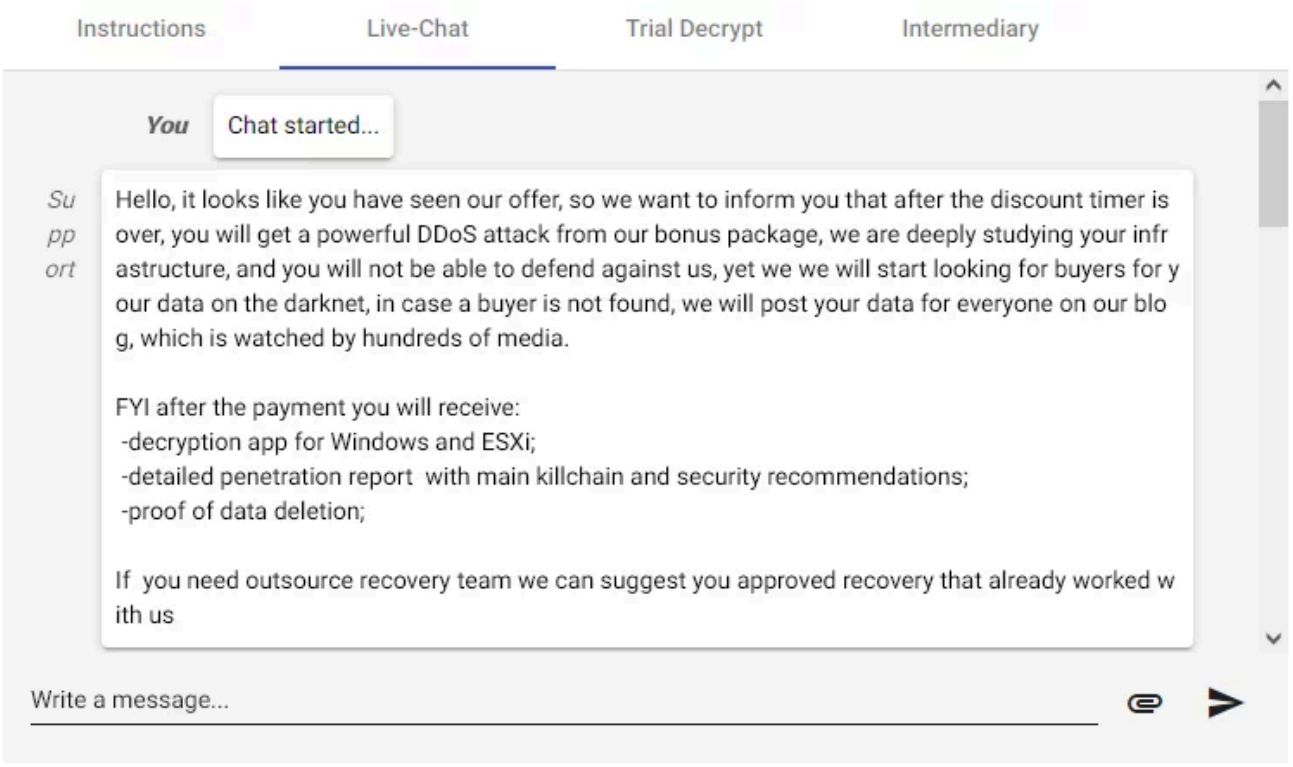
In some cases, the gang went further by leaking files on public websites, impersonating the victim's own domain (using lookalike/typosquatting URLs), a tactic intended to draw even more attention to the breach. BlackCat's leak site entries provide proof documents and a short, threatening description of the breach, openly shaming the victim.

A joint FBI/CISA alert noted that from December 2023 to February 2024, BlackCat's leak site listed nearly 70 new victims, with the healthcare sector the most commonly victimized. Additionally, our investigators have found that BlackCat operators increasingly allude to auctioning stolen data or selling it to competitors if the victim balks.

As published in Group-IB's Ransomware Readiness white paper, BlackCat was responsible for **427 known ransomware attacks in 2023**, where victim data was posted on leak sites, making it the second most active group that year (behind only LockBit's 1,079 incidents).

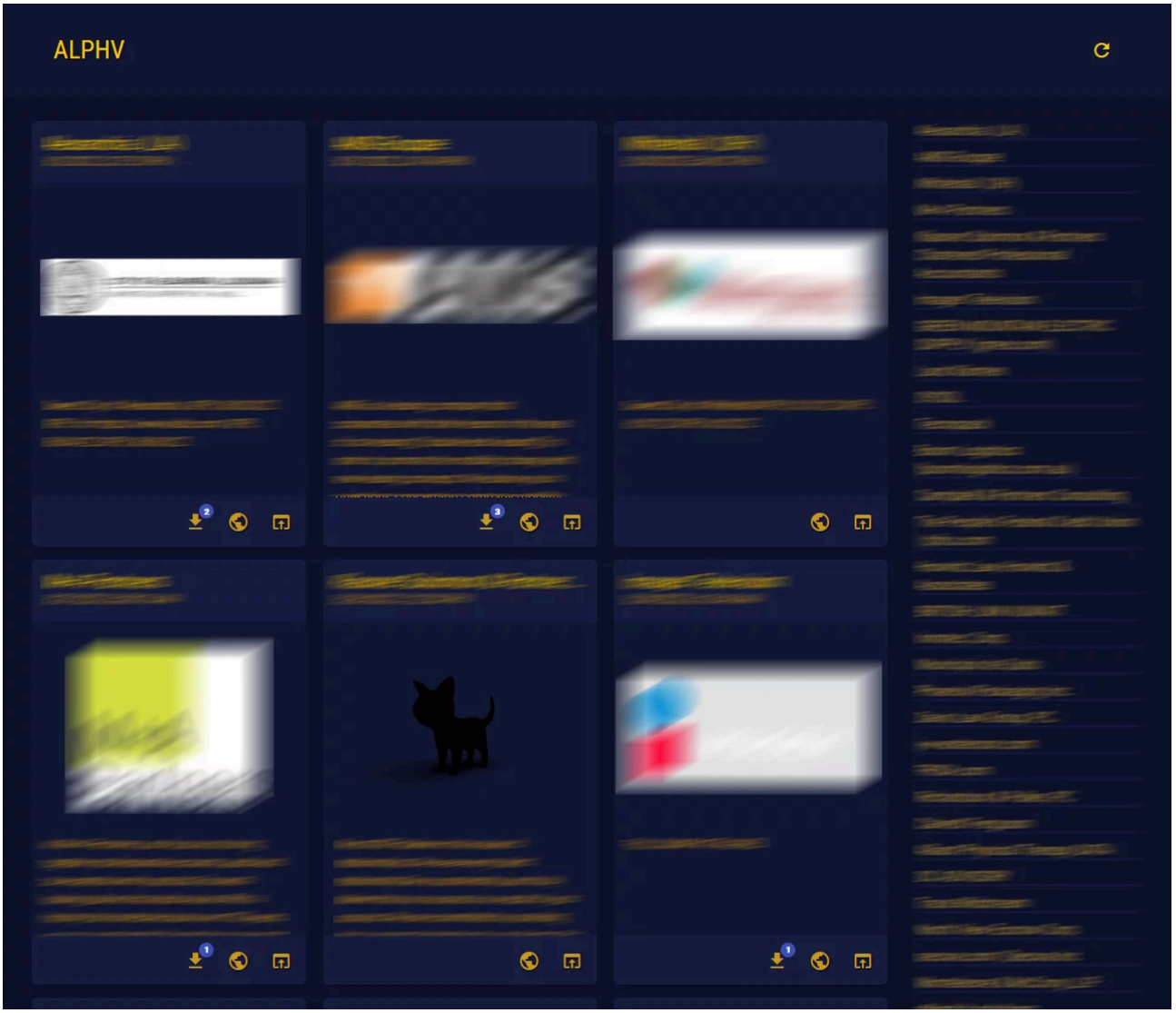
BlackCat had also unveiled a public data leak API on its site, allowing anyone to fetch updates about new victims and leaked files automatically. This helped to amplify the visibility of BlackCat's leaks when ransom negotiations faltered (e.g., after a high-profile victim like Estée Lauder refused to pay).

The FBI's December 2023 operation, notably, provided many victims with a free decryptor, undermining BlackCat's leverage. In response, BlackCat's admin raged on their blog and encouraged hitting more healthcare targets (viewed as more likely to pay quickly).



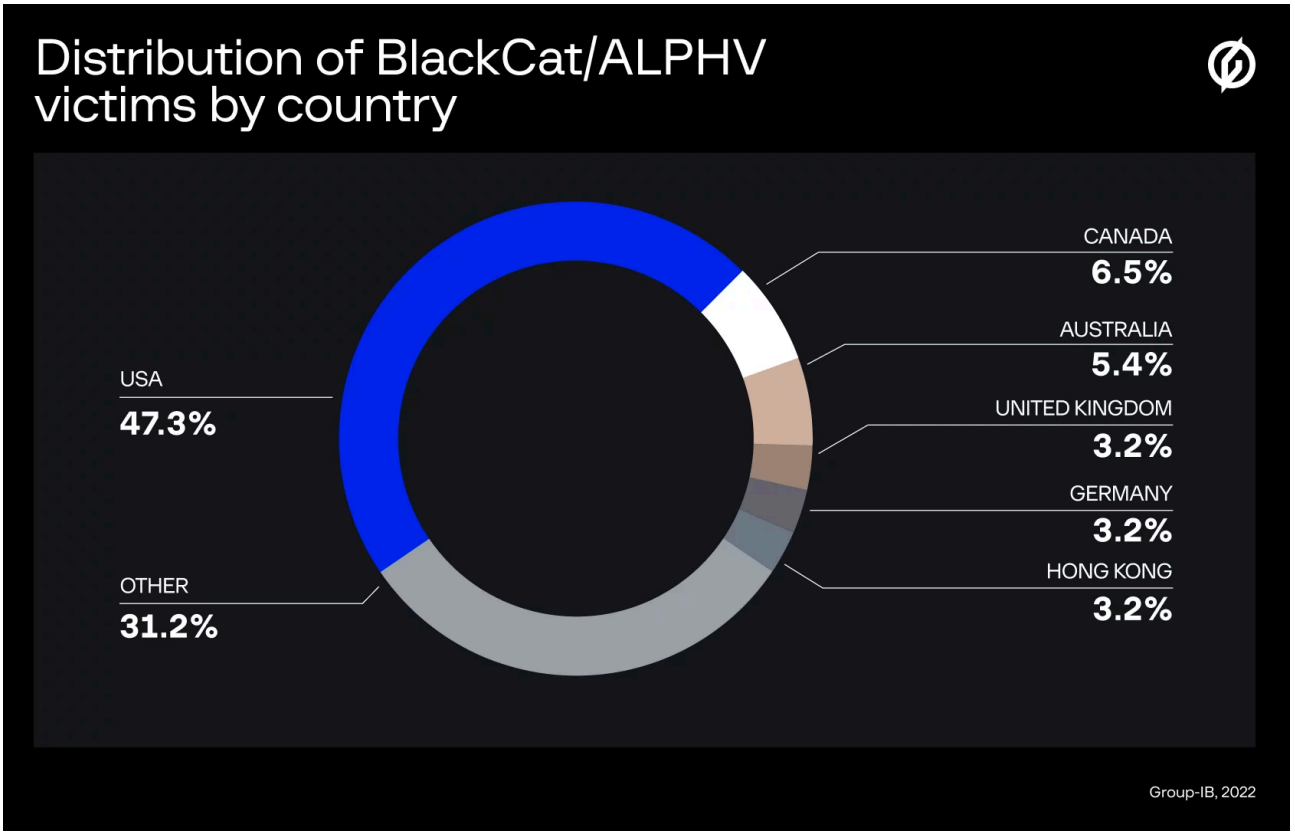
Chat with a victim

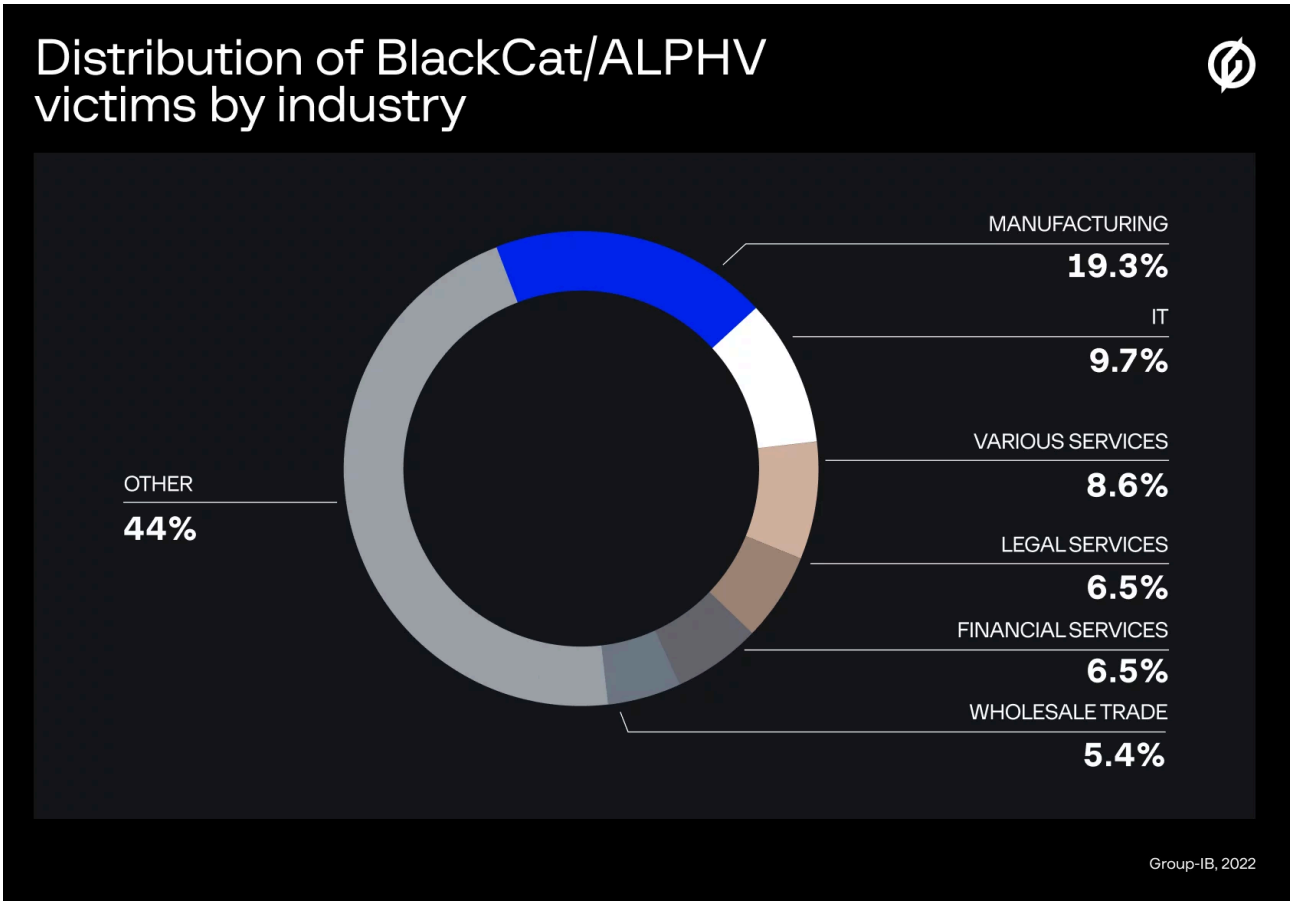
At the time of writing, the stolen documents of 93 affected companies that refused to pay a ransom were published on BlackCat's DLS. **We estimate that the overall number of BlackCat victims since December 2021 is about 140.**



In some cases, BlackCat affiliates have flipped the script entirely by forgoing encryption. For example, in February 2023, BlackCat claimed to have breached Reddit and stolen around 80 GB of data without deploying ransomware. They demanded $4.5 million and an end to Reddit's planned API pricing changes as "ransom," threatening to leak the stolen internal data.

This "data kidnapping" approach shows that if encrypting a target's systems is too difficult or not the goal, BlackCat will simply steal valuable data and use the fear of a leak as leverage, even if no ransomware is deployed.





BlackCat Ransomware Affiliates – Tactics, Techniques and Procedures

BlackCat affiliates were behind some of the most brazen social engineering attacks of 2023, including the high-profile breach of MGM Resorts. In another significant case, Caesars Entertainment was targeted by Scattered Spider, a group closely associated with ALPHV.

1. Gaining Access to the Network

Since a single affiliate program may involve different threat actors, techniques used for obtaining initial access may differ. Further, affiliates may use the services of initial access brokers, who sell access to companies' compromised infrastructures.

As part of investigating security incidents, we have seen the following techniques:

1. **Exploiting public-facing applications.**
   This technique gained popularity in 2021 among both affiliates and initial access brokers due to a lot of vulnerabilities being discovered that allowed arbitrary code execution in a variety of applications. In the case of BlackCat, the attackers exploited a set of vulnerabilities known as ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), which enabled them to place a web shell on a vulnerable Microsoft Exchange server and then conduct post-exploitation activities.
2. **Using remote access tools.**
   Access via publicly accessible terminal servers remains the most popular technique for gaining initial access and BlackCat affiliates used it in some cases. In addition to terminal servers, access to the target infrastructure could be gained via a VPN; many organizations still do not use multifactor authentication, which enables ransomware operators to easily use accounts whose data have been stolen using stealers, for example.
3. **Malvertising and cloning legitimate websites**Affiliates set up fake websites (or hijack real ones) to host trojanized software or credential stealers. They then run malicious ads or search engine poisoning to draw in victims looking for popular software cracks or tools.When an unwitting user downloads the payload, it installs a backdoor or keylogger that the attackers later use to pivot into the corporate network. This technique allows BlackCat to compromise companies with poor web filtering and might not fall for direct phishing.

2. Establishing Foothold

Having obtained initial access, the attackers copy a set of tools (in full or in part) to the compromised host and seek to ensure persistence and gain access to privileged accounts to be able to move across the network.

1. For additional capabilities to access the compromised network, the attackers could use tunnels built using ngrok or gost, or software such as TeamViewer or ScreenConnect.
2. Attackers also install backdoors or C2 beacons for persistent access. For example, they deploy a **Cobalt Strike Beacon** or CSharp-Streamer RAT.
3. In most incidents, **BlackCat affiliates relied on legitimate tools** to extract authentication data by dumping the **LSASS** (Local Security Authority Server Service) process. For instance, the threat actors used ProcDump and exploited the **MiniDump** feature of the legitimate library *comsvcs.dll*.

4. Some attackers went beyond LSASS and used various **NirSoft tools** to extract authentication data from the registry, web browsers, and other storage spaces.

3. Network Discovery

Having established a beachhead, BlackCat affiliates map out the victim's network. They need to identify what machines are present, how they're connected, and which ones hold vital data or critical services.

Attackers often start with classic network scanning commands and discovery tools:

1. **SoftPerfect Network Scanner scans the network**, a popular tool among ransomware groups.
2. **ADRecon** collects information about Active Directory, another standard tool among REvil and BlackMatter affiliates.
3. To collect data about available local and network drives, the **NS tool** is especially popular with affiliates that use terminal servers to gain initial access.

Key Assets Discovery, Network Propagation and Data Exfiltration

With enough privileges in the target IT infrastructure, the attackers start moving to key nodes, which will enable them to download the most important information and do away with backups.

1. BlackCat affiliates use **legitimate techniques** (such as **RDP**) and noisier ones (e.g., **Impacket:** wmiexec and smbexec in particular; and Cobalt Strike) to move across the network.
2. **PuTTY** is often used to gain access to the part of the infrastructure running on Linux.
3. Before being exfiltrated, **data is archived using 7-Zip and uploaded to the MEGA file** sharing service **using the Rclone utility**.
4. In some cases, **affiliates used ExMatter,** an exfiltration tool that was seen earlier in the arsenal of **BlackMatter affiliates.**

Deployment Preparation

BlackCat ransomware deployment is preceded by the erasure or encryption of available backup copies and collection of additional credentials that would allow the attackers to infect the Linux segment, in addition to Windows.

Despite the detectability of BlackCat samples not being high, some affiliates seek to disable antivirus software before moving on to the deployment stage.

BlackCat Ransomware Deployment

The propagation of BlackCat in the victim's IT infrastructure is achieved by either modifying group policies (which results in a scheduled task being created, on each host, that launches the malicious file) or using PsExec.

The ransomware is written in Rust. Many researchers rightfully consider BlackCat as one of the most sophisticated ransomware groups out there at the moment. BlackCat programs are feature-rich and offer flexible custom settings due to the use of various configuration data and command line arguments.

There are BlackCat versions for Windows (32bit) and Linux (32bit and 64bit). The 64bit Linux version primarily targets ESXi servers. In March 2022, a new version of BlackCat emerged, called ALPHV MORPH. On underground forums its authors proudly claimed that thanks to obfuscation, antivirus software is practically unable to detect it.

```
LOCKER
1. Вашему вниманию торжественно представляем - ALPHV MORPHV. Не вдаваясь в пикантные
подробности сообщаем, что раз в час происходит полная чистка бинаря. Помимо ре-крипта
вызовов, стрингов и прочего компилятор RUST позволяет насыщать каждый билд уникальным
рантайм мусором, что в конечном итоге дало фантастические результаты. На сегодняшний
день не палится не одним ав(не путать с edr! на sentinel'е не тестили), включая
дефендер с выключенным облаком - бинарь не удаляется даже после полного крипта машины.
Пока в тестовом режиме умышленно(!) доступно всем через Build->Obfuscated. В будущем
данный функционал будет доступен только адвертам со статусом +.
2. Мелкие фиксы в работе локера

p.s. AB для ESXI еще нет, а морф линукса у нас уже есть :) Да да, линукс также
морфится раз в час просто потому что можем.
```

Description of ALPHV MORPHV features on an underground forum

Translation

arrow_drop_down

LOCKER

1. We are proud to present ALPHV MORPH. Without going into the spicy details, we inform that the binary is completely cleared every hour. In addition to recrypting calls, stings, and other things, the RUST compiler makes it possible to enrich every build with unique runtime junk, which in the end yielded fantastic results. At the moment, no AV detects it(not to be confused with edr! we did not test it on sentinel), including defender with the cloud disabled – the binary is not deleted even after the machine is fully encrypted. In test mode so far, intentionally(!), it is available to everyone via Build->Obfuscated. In the future, this functionality will only be available to affiliates with the + status.
2. Minor fixes in the locker's operation.

p.s. There is no AV for ESXI yet, but we already have a linux polymorph 🙂 That's right, linux is also morphed every hour just because we can.

It has been mentioned before that launching BlackCat ransomware requires specifying the value of an access token in the command line parameter — **access-token**.

- In earlier versions, whether the token value is correct was not checked, while the access key is calculated using the entered token value; the program will be launched, and files will be encrypted, but accessing the victim's panel would be impossible.
- In the ALPHV MORPH version, the first 16 characters of the access token are used as a key to decrypt configuration data, which is why, if incorrect data is entered, the ransomware will not start.
- To bypass User Account Control (UAC), BlackCat escalates privileges using the ICMLuaUtil COM interface. Privileges can also be escalated using the Masquerade PEB method.

- BlackCat ransomware may attempt to authenticate using stolen credentials contained in configuration data.

When launched, **BlackCat allows symbolic links from a deleted item to local and remote items**:

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

Stops IIS by executing the following command:

iisreset.exe /stop

Deletes volume shadow copies:

vssadmin.exe Delete Shadows /all /quiet wmic.exe Shadowcopy Delete

Disables recovery in Windows boot menu:

bcdedit /set {default} bcdedit /set {default} recoveryenabled No

Clears Windows event logs:

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

In addition, the ransomware ends processes and stops services specified in the configuration.

It should be noted that **BlackCat for Windows can independently propagate itself** in the local area network as a network worm. To do so, the legitimate PsExec utility contained in the body of the ransomware is used together with stolen credentials specified in the configuration.

File encryption is multi-threaded. The AES 128 CTR or ChaCha20 algorithm can be used too encrypt file contents depending on the settings, with nonce vectors containing 8 or 12 null bytes respectively. In addition, various file encryption modes can be used; below are their brief descriptions.

```
USAGE:
    [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
```

Available command line parameters

Parameter	Description
-h, –help	Displays information about command line parameters.
-p, –paths …	Encrypts files at paths specified in this parameter.
-v, –verbose	Shows a report in the console.
–access-token	Specifies an access token (ACCESS_TOKEN). This is used to form an access key (ACCESS_KEY) that is used for creating a link for the victim to access their personal page. In the ALPHV MORPH versions, the first 16 characters of ACCESS_TOKEN are used as a key to decrypt (AES-128 CTR) the ransomware configuration data.
–bypass …	This parameter is not used.
–child	Launches the ransomware as a child process.
–drag-and-drop	Launches the ransomware in drag-and-drop mode.
–drop-drag-and-drop-target	Extracts a BAT file, to which objects that are to be encrypted can be dragged in drag-and-drop mode. The template for the BAT file is in the body of the ransomware in a compressed format (Deflate). In the ALPHV MORPH versions the template is additionally encrypted (AES128 CTR).
–extra-verbose	Shows a more detailed report.
–log-file	Outputs a report to a specified file.
–no-net	Ensure that files on available network resources are not encrypted.
–no-prop	Ensures that the ransomware does not self-propagate. For self-propagation, the PsExec utility is used together with credentials specified in the value of the configuration data parameter “credentials”. The PsExec utility is in the body of the ransomware in a compressed format (Deflate). In ALPHV MORPH it is also encrypted (AES128 CTR).
–no-prop-servers …	A list of servers excluded during self-propagation.
–no-vm-kill	Ensures that virtual machines are not stopped.
–no-vm-kill-names …	A list of names of virtual machines that are not stopped.
–no-vm-snapshot-kill	Ensures that virtual machine snapshots are not destroyed.
–no-wall	Ensures that the desktop wallpaper is not updated.

Parameter	Description
–propagated	Launches the ransomware in self-propagation (worm) mode.
–ui	Launch the ransomware with a graphical interface displaying the encryption progress.

BlackCat configuration data is contained in the body of the ransomware in the JSON format. In earlier BlackCat versions, the configuration data was in plain text, while in the latest versions (ALPHV MORPH), it is stored in an encrypted form (AES-128 CTR). For decryption, the first 16 characters of the access token are used as the key. If the characters are entered incorrectly, the ransomware will not be able to run due to a configuration data error.


```
{
  "config_id":"",
  "public_key":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApEgZ3mH3ZmyBRLGblHo85txXC3swHBu0HPRbI76lyNjmJ
  "extension":"d0mrj6x",
  "note_file_name":"RECOVER-${EXTENSION}-FILES.txt",
  "note_full_text":">> What happened?\n\nImportant files on your network was ENCRYPTED and now they have
  "note_short_text":"Important files on your network was DOWNLOADED and ENCRYPTED.\nSee \"${NOTE_FILE_NAM
  "default_file_mode":"Auto",
  "default_file_cipher":"Best",
  "credentials":[],
  "kill_services":["mepocs","memtas","veeam","svc$","backup","sql","vss","msexchange","sql$","mysql","mys
  "kill_processes":["agntsvc","dbeng50","dbsnmp","encsvc","excel","firefox","infopath","isqlplussvc","msa
  "exclude_directory_names":["system volume information","intel","$windows.~ws","application data","$recy
  "exclude_file_names":["desktop.ini","autorun.inf","ntldr","bootsect.bak","thumbs.db","boot.ini","ntuser
  "exclude_file_extensions":["themepack","nls","diagpkg","msi","lnk","exe","cab","scr","bat","drv","rtp",
  "exclude_file_path_wildcard":[],
  "enable_network_discovery":true,
  "enable_self_propagation":true,
  "enable_set_wallpaper":true,
  "enable_esxi_vm_kill":true,
  "enable_esxi_vm_snapshot_kill":true,
  "strict_include_paths":[],
  "esxi_vm_kill_exclude":[]
}
```


Formatted BlackCat configuration data

Parameter	Description
config_id	Configuration identifier
public_key	A Base64-encoded RSA public key in the DER format.
extension	Extension of encrypted files / victim identifier.
note_file_name	Name of a text file with a ransom note.
note_full_text	Template for a full ransom note text.
note_short_text	Template for a short ransom note text used for desktop wallpapers.

Parameter	Description
default_file_mode (DotPattern, HeadOnly, SmartPattern, AdvancedSmartPattern, Full, Auto)	Default file encryption mode. DotPattern – encryption with blocks with an interval. HeadOnly – encryption of the initial part. SmartPattern – encryption with blocks with an interval based on percentage of the file size. AdvancedSmartPattern – encryption with blocks with an interval based on the file size with advanced settings. Full – full encryption of file contents. Auto – automatic selection of the file encryption method based on the file type and size.
default_file_cipher (Best, Aes, ChaCha20)	Default file encryption algorithm. Best – if there is hardware support for AES (AES-NI), files are encrypted using AES-128 CTR, otherwise, using ChaCha20.
credentials	List of stolen credentials of the victim.
kill_services	List of services to be stopped.
kill_processes	List of substrings with names of processes to be ended.
exclude_directory_names	List of directory names excluded during encryption.
exclude_file_names	List of file names excluded during encryption.
exclude_file_extensions	List of file extensions excluded during encryption.
exclude_file_path_wildcard	List of file path wildcards excluded during encryption.
enable_network_discovery (true, false)	Encrypts files on available network resources.
enable_self_propagation (true, false)	Enables self-propagation in the network (worm mode). The PsExec utility and credentials specified in the value of the parameter “credentials” are used for the propagation process.
enable_set_wallpaper (true, false)	Sets an image with a message about files being encrypted as a wallpaper.
enable_esxi_vm_kill (true, false)	Stops virtual machines.
enable_esxi_vm_snapshot_kill (true, false)	Destroys virtual machine snapshots.
strict_include_paths	List of paths for encrypting files.
esxi_vm_kill_exclude	Whitelist of virtual machine names.

It must be noted that despite some of the group’s methods being sophisticated, **many tactics, techniques and procedures employed by BlackCat affiliates can be easily detected**, which indicates serious flaws in

organizations' security systems as well as a shortage of skilled security specialists.

Additional information

MITRE ATT&CK®

Tactic	Technique	Description
TA0001 Initial Access	T1190 Exploit Public-Facing Application	In a number of attacks, the threat actors used ProxyShell vulnerablilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207).
	T1133 External Remote Services	As an initial attack vector, insecure RDP and VPNs may be used.
	T1078 Valid Accounts	BlackCat affiliates may purchase access to their victim's network infrastructure on underground forums.
TA0002 Execution	T1106 Native API	BlackCat ransomware uses Native API.
	T1053 Scheduled Task/Job	When deploying ransomware in the victim's network infrastructure, BlackCat affiliates may exploit group policies, which results in a scheduled task being created (on each host) that launches the ransomware.
	T1059.001 Command and Scripting Interpreter: PowerShell	The attackers may use PowerShell scripts when deploying ransomware in the victim's network, disabling security tools, and encrypting files.
	T1059.003 Command and Scripting Interpreter: Windows Command Shell	For stopping IIS, deleting Volume Shadow Copies, disabling recovery, clearing Windows event logs, etc., the BlackCat ransomware uses the command shell to run appropriate commands.
	T1047 Windows Management Instrumentation	The attackers may use wmic to obtain information and run various commands, including to delete Volume Shadow Copies. They may also use the wmiexec module from Impacket to execute commands and move across the network.
	T1569.002 System Services: Service Execution	The BlackCat ranswomare for Windows can self-propagate in the local area network using the legitimate PsExec utility (contained in its body), which creates a temporary system service.

Tactic	Technique	Description
TA0003 Persistence	T1505 Server Software Component	Successfully exploiting ProxyShell vulnerabilities enabled the attackers to place a web shell on a vulnerable Microsoft Exchange server.
	T1078 Valid Accounts	Legitimate accounts obtained by the attackers can be used to ensure persistence in the compromised infrastructure.
TA0004 Privilege Escalation	T1078 Valid Accounts	To escalate privileges, BlackCat may use stolen legitimate accounts specified in the configuration data.
	T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control	To bypass UAC, BlackCat ransomware may escalate privileges using the ICMLuaUtil COM interface, as well as use the Masquerade PEB method.
	T1134.002 Access Token Manipulation: Create Process with Token	To escalate privileges, the BlackCat ransomware can launch its process using stolen authentication data and the function CreateProcessWithLogonW.
TA0005 Defense Evasion	T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control	The attackers may bypass UAC using the ICMLuaUtil COM interface, as well as use the Masquerade PEB method.
	T1140 Deobfuscate/Decode Files or Information	BlackCat decrypts configuration data as well as decrypts and unpacks the legitimate PsExec utility and an additional BAT file contained in the body of the ransomware.
	T1027 Obfuscated Files or Information	BlackCat ransomware uses obfuscation.
	T1562.001 Impair Defenses: Disable or Modify Tools	To prevent being detected, the attackers end processes and services related to security and antivirus software.
	T1497 Virtualization/Sandbox Evasion	To counter analysis (including in a sandbox), ALPHV MORPH checks the value of the command line parameter access-token. Its value must contain correct first 16 characters used to decrypt BlackCat configuration data.
	T1070.001 Indicator Removal on Host: Clear Windows Event Logs	By using wevtutil, BlackCat can clear all Windows event logs on a compromised host.

Tactic	Technique	Description
	T1036 Masquerading	The attackers use a SoftPerfect Network Scanner executable renamed to svchost.exe.
	T1112 Modify Registry	To propagate, BlackCat uses PsExec to modify the system registry parameter MaxMpxCt to increase the number of failed network requests for each client.
TA0006 Credential Access	T1003.001 OS Credential Dumping: LSASS Memory	To obtain authentication data, the attackers may dump the LSASS process using legitimate tools (procdump, comsvcs.dll).
	T1552 Unsecured Credentials	To obtain authentication data from the registry and files, the attackers may use NirSoft utilities.
	T1555 Credentials from Password Stores	To extract authentication data from web browsers and other storage spaces the attackers may use NirSoft utilities.
TA0007 Discovery	T1018 Remote System Discovery	To enumerate domain hosts, the attackers used the ADRecon tool.
	T1069.002 Permission Groups Discovery: Local Groups	To obtain information about local and domain user groups, the attackers used the ADRecon tool.
	T1069.002 Permission Groups Discovery: Local Groups	
	T1069.002 Permission Groups Discovery: Domain Groups	
	T1087.001 Account Discovery: Local Account	To obtain information about local and domain accounts, the attackers used the ADRecon tool.
	T1087.002 Account Discovery: Domain Account	
	T1482 Domain Trust Discovery	To obtain information about domain trust, the attackers used the ADRecon tool.
	T1046 Network Service Scanning	To scan the target network, the attackers use the open-source utility SoftPerfect Network Scanner.
	T1135 Network Share Discovery	To search for network shares, the attackers use the open-source utility SoftPerfect Network Scanner.

Tactic	Technique	Description
	T1016 System Network Configuration Discovery	For network reconnaissance, the attackers use the open-source utility SoftPerfect Network Scanner.
	T1082 System Information Discovery	BlackCat uses wmic to obtain the UUID of the compromised host.
	T1057 Process Discovery	BlackMatter enumerates all running processes to search for ones relating to security, backups, databases, email systems, office programs, etc.
	T1007 System Service Discovery	BlackCat enumerates system services to search for ones relating to security, backups, and databases.
	T1083 File and Directory Discovery	The attackers enumerate drives, directories, and files to search for sensitive information for exfiltration purposes.
TA0008 Lateral Movement	T1021.001 Remote Services: Remote Desktop Protocol	The attackers may use RDP to move across the network.
	T1021.002 Remote Services: SMB/Windows Admin Shares	After obtaining privileged authentication data, in order to spread over the local area network and access network resources, the attackers may use the PsExec utility, as well as the psexec, wmiexec and smbexec modules from Impacket.
	T1021.004 Remote Services: SSH	To access parts of the infrastructure running on Linux, the attackers use the PuTTY utility.
	T1570 Lateral Tool Transfer	Moving across the victim’s network and deploying ransomware involves copying related tools to the host. The BlackCat ransomware can self-propagate in the network by using the legitimate PsExec utility contained in its body.
TA0009 Collection	T1560.001 Archive Collected Data: Archive via Utility	Before being exfiltrated, data may be put in archives using 7-Zip.
	T1005 Data from Local System	The attackers collect information from the local system for exfiltration purposes.
	T1039 Data from Network Shared Drive	The attackers collect information from available network resources for exfiltration purposes.

Tactic	Technique	Description
	T1074 Data Staged	Before exfiltration, the attackers may put collected data in 7Zip archives.
	T1119 Automated collection	The attackers use ExMatter, a tool for automated collection of sensitive information.
TA0011 Command and Control	T1071 Application Layer Protocol	Remote access tools used by the attackers may use application layer protocols (HTTP, HTTPS, DNS).
	T1105 Ingress Tool Transfer	After gaining initial access, the attackers copy tools necessary for deployment to the compromised host.
	T1572 Protocol Tunneling	To access the compromised system, the attackers may use tunnels built using ngrok or gost.
	T1573 Encrypted Channel	To remotely access the compromised infrastructure, the attackers may use Cobalt Strike, TeamViewer and ScreenConnect, which perform asymmetric/symmetric encryption of the C&C server communication channel.
	T1219 Remote Access Software	To remotely access the compromised infrastructure, the attackers may use the legitimate tools TeamViewer and ScreenConnect.
TA0010 Exfiltration	T1041 Exfiltration Over C2 Channel	When the attackers use Cobalt Strike, the collected information may be sent via Cobalt Strike server communication channels.
	T1048.002 Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	The attackers may use the ExMatter exfiltration tool, which sends stolen data to SFTP and WebDav resources specified in the ExMatter configuration.
	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	The attackers use the Rclone synchronization utility to upload stolen data to the legitimate cloud storage service MEGA.
	T1020 Automated Exfiltration	After access has been gained, files from target hosts are automatically uploaded to the legitimate cloud storage service MEGA using the Rclone utility.
	T1030 Data Transfer Size Limits	To prevent exceeding the size limits of the data being sent and triggering security controls, the stolen data may be sent in fixed-size blocks.

Tactic	Technique	Description
TA0040 Impact	T1486Data Encrypted for Impact	BlackCat encrypts the contents of files in the local system as well as on available network resources.
	T1489 Service Stop	BlackCat stops security, backup, database, email and other services specified in the configuration.
	T1490 Inhibit System Recovery	BlackCat deletes Windows Volume Shadow Copies using vssadmin and wmic, disables recovery in the Windows boot menu using bccedit, and empties Recycle Bin. BlackCat can stop backup services. BlackCat can destroy virtual machine snapshots.
	T1485Data Destruction	If credentials for accessing a chat with the victim are leaked, BlackCat affiliates may delete encryption keys, which will render decrypting the files impossible.
	T1498 Network Denial of Service	If the victim refuses to pay a ransom, BlackCat may carry out DDoS attacks against the victim's infrastructure.

Notable BlackCat Attacks and Affected Industries

BlackCat/ALPHV targets large enterprises and institutions that use sensitive data or critical services. Below, we've highlighted a few high-profile incidents demonstrating the group's devastating impact and preferred targets.

Change Healthcare – Healthcare (Feb 2024)

Hospitals and health providers are seen as high-value targets (with lives and patient care at stake), which ransomware groups tend to exploit. In February 2024, BlackCat infiltrated Change Healthcare, causing system outages in claims processing and pharmacy services nationwide. BlackCat attackers stole data on 190 million individuals, including insurance member IDs, diagnoses, and Social Security numbers, making it the most significant healthcare breach in U.S. history and BlackCat's most notorious attack.

A $22 million ransom was paid to prevent the release of the stolen data. However, the BlackCat ransomware group performed an exit scam, pocketed the ransom payment, and didn't pay the affiliate who conducted the attack. The affiliate then worked with another ransomware group, RansomHub, which attempted to extort Change Healthcare further. No additional ransom payments were made, and the stolen data remains in the hands of cybercriminals.

In a 2023 incident that parallels the attack on Change Healthcare, BlackCat infiltrated a system used for radiation oncology, exfiltrating clinical photographs of breast cancer patients. When Lehigh Valley Health Network (LVHN) refused to pay the ransom, BlackCat escalated its tactics by publishing the nude images on its dark web

leak site, a new low in ransomware extortion strategies. In response, LVHN agreed to a $65 million class action settlement (one of the largest per-capita settlements in a healthcare data breach case).

MGM Resorts International – Hospitality/Gambling (Sep 2023)

In a highly publicized incident, BlackCat (in partnership with the social-engineering group Scattered Spider) attacked MGM, one of the largest casino resort operators. In a full compromise, BlackCat and Scattered Spider stole customer data, including names, SSNs, driver's licenses, and passport numbers.

The initial breach was achieved via a phone call to MGM's IT helpdesk, tricking an employee into revealing credentials. Once inside, the attackers deployed ransomware that forced MGM to shut down IT systems across all its Las Vegas properties as a containment measure.

MGM disclosed that the business impact was over $100 million in lost revenue and remediation costs. Interestingly, MGM refused to pay the ransom, attempting to recover on its own, which likely contributed to the prolonged outage.

Caesars Entertainment – Hospitality/Gambling (Sep 2023)

Just days before the MGM hack became public, Caesars Entertainment was hit by a similar attack. Caesars admitted in an SEC filing that hackers (believed to be the same BlackCat/Scattered Spider team) accessed its network via a third-party IT vendor compromise and stole customer data, including many loyalty program member records.

To avoid MGM's fate, Caesars paid the attackers $15 million of the demanded $30 million ransom. The quick payment apparently prevented the encryption of Caesars' systems—in contrast to MGM, Caesars experienced no major downtime. However, tens of millions of customer records were stolen. This pair of casino attacks raised alarm in corporate boardrooms worldwide about ransomware groups' potency of social engineering tactics.

Our incident response team, having handled hundreds of ransomware cases, finds it remarkable. "Companies are pouring hundreds of millions of dollars into sophisticated defenses—preventive security, threat detection, endpoint response, you name it. Yet attackers are still breaking in using the simplest methods imaginable: Click this link and enter your credentials. Sometimes the weakest link isn't technical – it's human."

Reddit – Technology/Social Media (Feb 2023)

As mentioned earlier in the article, BlackCat claimed responsibility for a breach of Reddit in 2023. In Reddit's case, an employee was phished, compromising internal documents and source code.

BlackCat attackers demanded $4.5 million and the rollback of Reddit's API pricing changes (a rare instance of a quasi-political demand). Reddit did not pay, and BlackCat leaked some of the stolen data on its site.

While the platform wasn't taken down (no ransomware deployed), the Reddit hack serves as a wake-up call for other companies to bolster their cybersecurity measures, train their employees regularly, and consider cybersecurity implications in their business decisions.

Estée Lauder – Consumer Goods (July 2023)

BlackCat infiltrated Estée Lauder, a global cosmetics company, in July 2023. In a curious twist, Estée Lauder was concurrently hit by the Clop ransomware via a supply-chain (MOVEit) vulnerability. Both BlackCat and Clop claimed responsibility for the breach. BlackCat's involvement included accessing the corporate network and exfiltrating data.

Group-IB investigators find the overlap of two major ransomware groups in one incident to be unusual and possibly coincidental. Furthermore, we observe a widening gap between cybersecurity measures and real digital maturity, where an organization can fall victim to multiple actors if multiple vulnerabilities exist.

Critical Infrastructure and Government

As further indication that no industry is off-limits, BlackCat/ALPHV ransomware and Conti hackers were said to have been behind the February 2022 cyberattacks that affected oil transport and storage companies across Europe. At the same time, large-scale cyberattacks have also targeted port facilities in Belgium, Germany, and the Netherlands.

IT systems were disrupted at SEA-Invest in Belgium and Evos in the Netherlands, and there are further reports that BlackCat ransomware has compromised systems at Oiltanking GmbH Group and Mabanaft Group in Germany. This wave of attacks is reminiscent of DarkSide's ransomware attack on Colonial Pipeline, a major U.S. fuel pipeline operator.

In another BlackCat attack, EPM (a Colombian energy supplier) was forced to halt operations after falling victim to the ransomware group. A DOJ 2023 press release later reported BlackCat had impacted networks that support U.S. government agencies and critical infrastructure, including sectors like transportation or manufacturing.

A pattern emerges: ALPHV's sting is felt across industries like healthcare, retail, hospitality, technology, and government. While not all incidents come to light, we believe that BlackCat affiliates are prowling for high-value (and lucrative) targets that can't afford downtime. The geographic reach is also broad, including the U.S., Europe, and Asia. That said, BlackCat and its affiliates are Russian-speaking and avoid attacking CIS (former Soviet) countries by code design, as is common with ransomware from that region.

The key takeaway from these incidents is that BlackCat attacks lead to multi-faceted crises: operational disruption, data breach notification, regulatory fines, customer lawsuits, and steep recovery costs. Many victims suffer extortion twice (paying ransom and dealing with data breach fallout).

BlackCat Ransomware Exit Scam and Rebranding

BlackCat's trajectory took a dramatic turn in March 2024 after the massive $22 million ransom payment from Change Healthcare. Shortly after the payoff, BlackCat closed its leak site and announced the sale of its RaaS source code for USD 5 million.

The gang announced that its infrastructure had been compromised by "the feds," even putting up a seizure message. In reality, this proved to be a ruse. In our Ransomware Readiness white paper, Group-IB threat intelligence analysts note that BlackCat pretended the FBI seized its site as cover for an exit scam.

Law enforcement actions around the same time (the U.S. DOJ reported seizing BlackCat servers in late 2023) may have contributed to pressure, but the catalyst for BlackCat's shutdown appears to have been greed—the administrators cashing out after their record-breaking ransom success. This betrayal caused BlackCat affiliates to migrate to other ransomware programs to continue their attacks.

A few months after BlackCat's so-called "goodbye," a suspiciously familiar ransomware operation surfaced. A new RaaS group calling itself **Cicada3301** began advertising on darknet forums and listing its first victims.

While some believe this may be a rebrand, it's difficult to say for sure whether Cicada3301 fully adopted the ALPHV/BlackCat ransomware codebase. It's more plausible that the group **borrowed specific functionalities**, such as anti-recovery commands, rather than integrating the full source code.

Though code-level similarities exist, distinct differences point to a partial reuse rather than a full clone. That said, **if anyone did get their hands on ALPHV's source**, Cicada3301 appears to be the most likely candidate.

Our researchers observed that Cicada3301's malware bore strong code-level similarities to BlackCat's. Both were written in Rust, targeted Windows/Linux/ESXi, and even shared particular functionality (e.g., using the same methods to halt VMs and clear logs).

Discover how Group-IB's threat intelligence analysts infiltrated the Cicada3301 Ransomware group in 2024.

Key observations: Compared to BlackCat's brazen attacks, Cicada3301 targets mostly smaller businesses via common attack vectors like exposed RDP (using stolen or weak credentials). Given the heat on BlackCat, this could be an attempt to stay under law enforcement's radar.

According to Group-IB's High-Tech Crime Trends 2025 report, BlackCat's exit scam (along with a similar scam by the NoEscape gang) undermined confidence among ransomware affiliates. Our analysts believe this could lead to affiliates being quicker to jump ship or demanding more decentralized control to avoid being left empty-handed.

We may also see new groups and extortion models rise to fill the vacuum. Indeed, within months of BlackCat's disappearance, multiple new RaaS brands (like Cicada3301 and others) were already on the scene. Organizations today must be vigilant as threat actors shift identities and tactics in response to mounting legal pressure.

Defensive Strategies Against BlackCat Ransomware

Below are key defensive recommendations and best practices informed by recent ransomware incidents and Group-IB's frontline cyber threat investigations:

1. Strengthen Authentication and Access Controls

Since BlackCat often gained entry via stolen or weak credentials, organizations should enforce multi-factor authentication (MFA) on all remote access and sensitive accounts.

- Use phishing-resistant MFA like hardware security keys (FIDO2/WebAuthn) or certificate-based authentication. Traditional OTP apps or push MFA can be compromised by SIM swapping or push fatigue

tactics that BlackCat affiliates use.

- Ensure that MFA is enabled for VPNs, RDP gateways, email, and administrative accounts.
- Passwords should never be reused across services. Implementing password managers and regularly rotating privileged credentials can help reduce the risk of credential dumps.
- Practice the principle of least privilege through an identity and access management system (IAM). Privileged access management (PAM) solutions create additional authentication barriers for admin access and isolate privileged sessions, making it harder for attackers to leap from an employee account to a domain admin account.

2. Improve User Awareness

Group-IB has identified several “persuasive” emails and text messages used by BlackCat with legitimate-sounding details (e.g., package delivery notices) to lure users. Given these cunning social engineering tactics, we recommend **prioritizing user awareness training** as your cybersecurity defense’s critical, human-centered layer.

- Conduct regular security awareness training covering phishing, spear-phishing, and phone-based scams.
- Teach staff how to verify unsolicited contacts claiming to be IT support, and to be wary of any message urging urgent action on their account.
- Simulate monthly phishing attacks to test employees – this can identify who might need extra training.
- Ensure there’s a 24/7 open channel for employees to report suspected phishing or strange IT requests.

3. Close Common Entry Points

BlackCat actively targets known vulnerabilities in external-facing systems, making patch management a key defensive strategy.

- Prioritize patching any vulnerabilities known to be exploited in the wild (CISA’s database of exploited vulnerabilities is a good guide).
- Mitigate Exchange bugs like ProxyShell, update remote desktop services, and apply fixes for any widely used software (VPNs, virtualization, etc.).
- If a system cannot be patched immediately, consider taking it offline or applying interim mitigation (like disabling an affected feature or adding WAF rules).
- Attack surface management solutions help prioritize remediation tasks with threat intelligence insights. Security teams can continuously scan the entire IPv4 space and beyond to identify all Internet-facing assets, including shadow IT, forgotten infrastructure, and misconfigurations that may expose an internal asset to the open web.
- Use network segmentation to separate critical servers (databases, domain controllers, and backups) from the user network.

4. Detect and Respond to Intrusions Quickly

Deploy advanced Endpoint Detection and Response (EDR) tools on servers and workstations.

- EDR can catch suspicious behavior, such as credential dumping, unusual PowerShell execution, or a ransomware binary trying to mass-encrypt files. Advanced EDR solutions can even halt encryption in

progress.

- Ensure that logging is enabled and centralized. Windows Event Logs (especially Security logs, Sysmon logs), firewall logs, VPN access logs, and DNS logs should feed into a SIEM or monitoring system where alerts can be generated.
- Use fraud protection behavioral analytics to flag anomalies, such as an account logging in at odd hours, an admin tool running on a non-admin machine, or a workstation suddenly initiating connections to dozens of other PCs or to an IP in a foreign country.
- Conduct regular incident response drills (tabletop exercises and live simulations) for a ransomware scenario. The speed of BlackCat's encryption (often minutes to an hour for an enterprise) means every second counts once an attack is detected. Ensure your team knows how to isolate an infected machine quickly, disconnect from the VPN or domain to stop propagation, and activate backups.
- Group-IB recommends exercising your security program against behaviors mapped to frameworks like MITRE ATT&CK to validate that your controls can detect or prevent those techniques.

5. Protect and Isolate Backups

Follow the 3-2-1 backup rule by keeping at least three copies of critical data, on two different media, with one copy offline and offsite.

- Ransomware cannot access offline (immutable) backups. You can use disk or cloud backup services that offer immutability (write-once-read-many storage).
- Ensure backup admin interfaces are not exposed to the general network and that MFA is required to access them. Segment backup systems from the domain if possible (so domain admin creds alone can't delete backups).
- Implement delayed deletion for cloud backups (so that if an attacker tries to delete them, they remain recoverable for a period).
- Secure backup credentials. BlackCat ransomware analysis shows that attackers have tools to extract backup software passwords, so use strong, unique credentials for backup systems and monitor login attempts to those consoles.
- If using Windows Shadow Copies, you can monitor or lock the VSS admin functions to prevent unauthorized deletion. In the event of an incident, having intact backups that ransomware groups couldn't encrypt will reduce the temptation to pay a ransom.

6. Incident Response and External Support

If, despite all efforts, your organization ends up in an attacker's crosshairs, ensure you have a strong Incident Response (IR) plan ready.

- Your incident response plan must clearly define steps for technical containment (like network isolation and immediate password resets), internal and external communications, legal protocols, and interactions with law enforcement.
- Maintain an incident response retainer with cybersecurity firms where dedicated IR specialists can assist in comprehensive analysis, containment, and remediation to restore operations fast.

For an accurate assessment of your organization's current readiness, Group-IB's Cybersecurity Ultimate Assessment Guide helps you evaluate your security posture, uncover vulnerabilities, and take decisive actions to strengthen defenses against emerging threats.

How Group-IB Helps Organizations Stay Ahead of Ransomware

As ransomware groups continue to innovate, Group-IB has helped organizations create a resilient and secure environment through strategic threat intelligence and expert incident response.

Here's how our approach works to defend against and outrun threats like BlackCat:

1. **Early warning:** Group-IB Threat Intelligence Platform (with over 850 threat actor profiles) helps you to understand ransomware trends and anticipate attacks by monitoring dark web forums, leak sites, and malware developments. You'll receive actionable insights into attacker behaviors to strengthen your defenses against emerging ransomware tactics.
2. **24/7 threat monitoring and detection:** For real-time defense, our Managed Extended Detection and Response (XDR) is built with threat hunting and intel to monitor your endpoints, network, and cloud. We can detect early signs of ransomware, like unusual admin activities, and isolate affected systems, evicting adversaries before they detonate ransomware. To guarantee peace of mind, an expert Compromise Assessment can identify hidden threats and cybersecurity gaps that could lead to incidents in the future.
3. **Reduce potential attack surface:** Our external Attack Surface Management solution scans and assesses external-facing assets for weaknesses. It will highlight exposed RDP ports, out-of-date VPN appliances, or forgotten websites that could serve as entry points.
4. **Secure email gateways:** Many ransomware attacks start with a phishing email. You can block phishing attempts before they reach employees with Business Email Protection, which recognizes phishing domains or malware attachments.
5. **Restore business continuity:** In the event of an attack, the Group-IB Incident Response team can jump in to identify the intrusion vector, secure the network, and help restore systems. Our goal is to minimize downtime and data loss. This includes negotiating with threat actors, coordinating with law enforcement, and leveraging available decryption tools or keys.

No single tool or strategy can stop a sophisticated RaaS group like BlackCat, but a layered defense can raise the cost and difficulty of attack to the point where the adversary might turn tail, or move on to an easier target.

Recognized by Gartner as a Representative Vendor in the Market Guide for Security Threat Intelligence Products and Services, Group-IB offers the industry's most complete and detailed insights into threat actors and their activities. We continuously update our tools and methodologies to integrate new detection analytics for malware variants, or tracking the emergence of BlackCat rebrands like Cicada3301.

With the latest intelligence, robust security controls, and expert response capabilities, businesses can defend themselves and significantly reduce the risk of falling victim. Explore Group-IB's solutions for ransomware protection to give your organization a decisive advantage.

FAQs

What is BlackCat ransomware?

BlackCat ransomware (also known as ALPHV) is a sophisticated Ransomware-as-a-Service (RaaS) operation that targets enterprises with double extortion tactics by encrypting data and threatening to leak it unless a ransom is paid.

How does BlackCat ransomware spread?

BlackCat spreads through stolen credentials, phishing emails, VPN exploits, and Remote Desktop Protocol (RDP) attacks. It often uses social engineering or known vulnerabilities to gain initial access.

What industries are most targeted by BlackCat?

BlackCat ransomware attacks target industries where downtime or data breaches cause significant harm or financial loss, especially healthcare, hospitality, technology, energy, and critical infrastructure.

What encryption techniques does BlackCat use?

BlackCat uses strong AES and RSA encryption methods, customizing its payload to maximize impact across Windows, Linux, and ESXi systems during a ransomware attack.

How does BlackCat evade detection and security measures?

To evade threat detection, BlackCat disables security tools, clears logs, abuses legitimate admin tools, and operates stealthily using customized scripts and malware built in Rust.
