

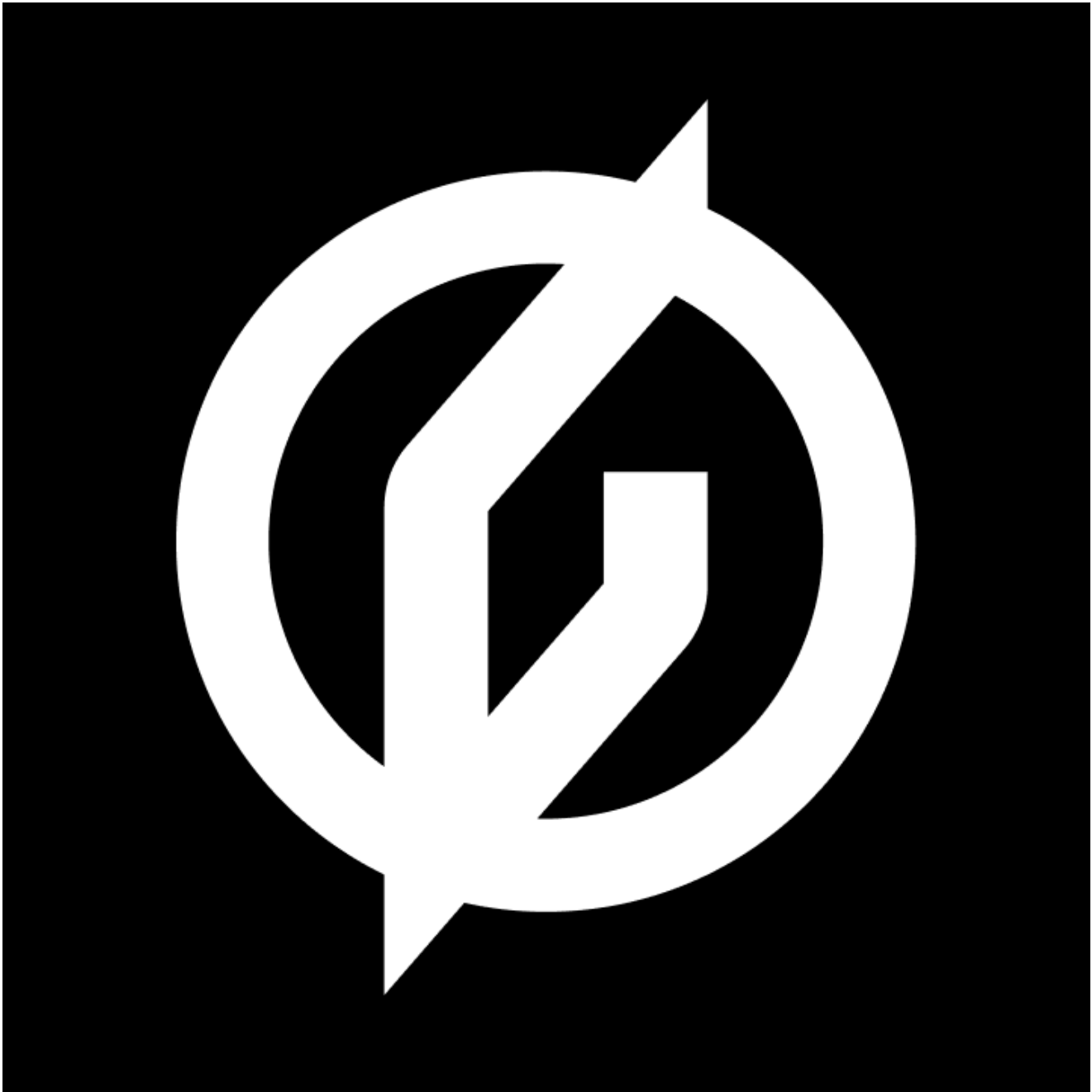
Fat Cats

[i blog.group-ib.com/blackcat](https://blog.group-ib.com/blackcat)



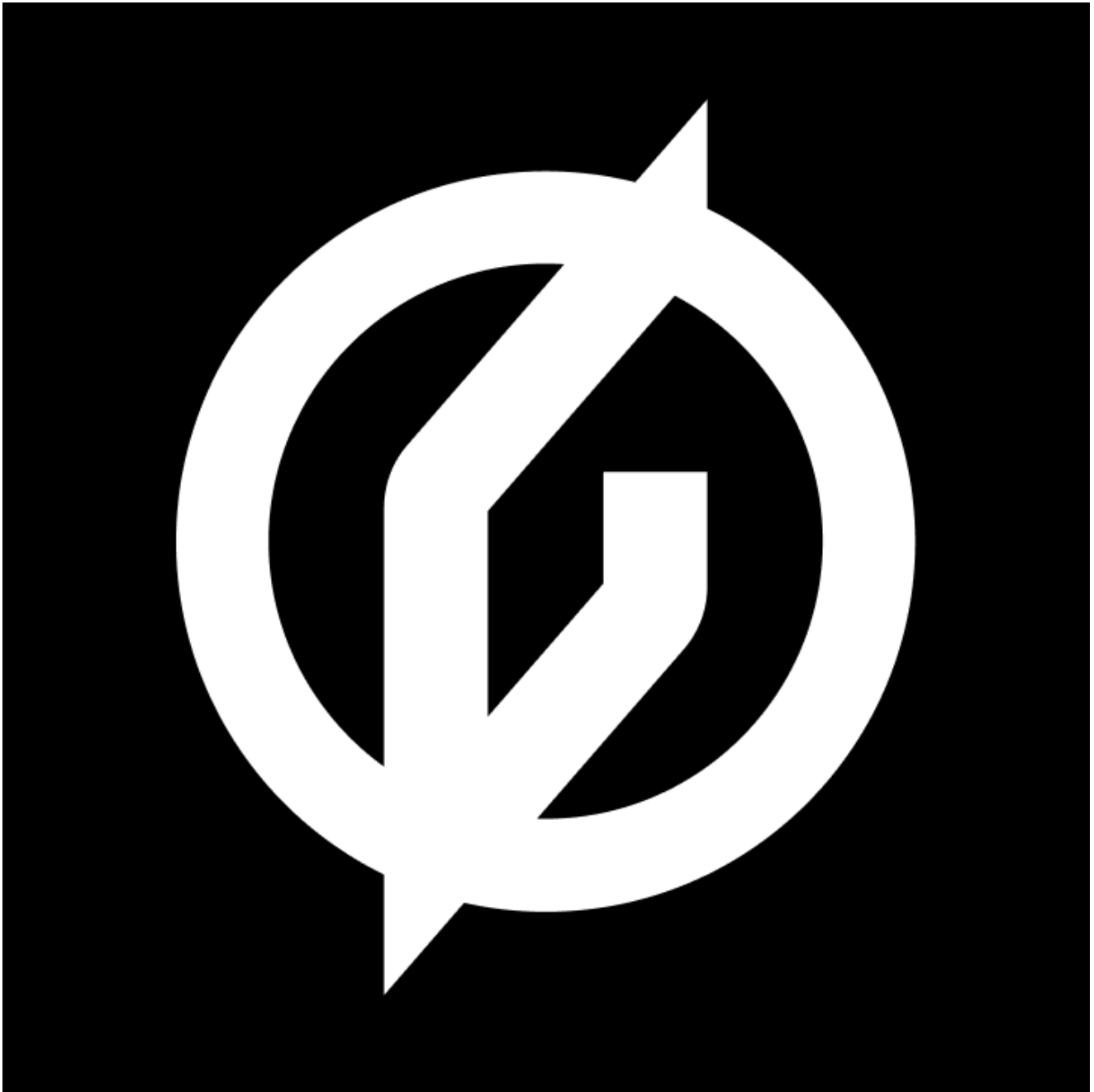
29.06.2022

An analysis of the BlackCat ransomware affiliate program



Andrey Zhdanov

Chief malware analyst and threat hunter at Digital Forensics and Incident Response Team,
Group-IB



Oleg Skulkin

Head of Digital Forensics and Incident Response Team, Group-IB

In the popular Soviet TV series **The Meeting Place Cannot Be Changed**, a Moscow Criminal Investigation Department detective infiltrates a criminal group called “Black Cat”. The image of this elusive and brutal gang, which left their calling card — a picture of a black cat — on crime scenes, is a composite. After the Second World War, there were several gangs in Moscow that engaged in robberies and committed murders. Criminals that remained at large hiding from the police often switched from a disrupted gang to another or created new groups.

We often see something similar among cyber criminals. Despite numerous arrests of people involved in ransomware activity as well as the shutdown of some affiliate programs, ransomware remains threat No. 1. Ransomware attacks continue to be conducted around the world, with underground forums teeming with posts about selling “access” and hiring “penetration testers”.

There is no doubt in the security community that the former members of **DarkSide**, **BlackMatter**, and **REvil** have formed the core of **ALPHV**, a more mature (due to their experience) and sophisticated affiliate program. Security researchers unofficially call it **BlackCat** for its use of 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.

Despite its short history, the group has conducted about **140** attacks worldwide over the course of six months and has set a new direction for the development of extortion-related crime. Many affiliate programs, such as **Hive**, started mimicking and adopting the methods and approaches of **BlackCat**. This blog post describes the details of this affiliate program and analyzes what exactly affiliates do after obtaining access to the networks of their victims.

INTRO from ALPHV

ALPHV started its activity in December 2021, when a campaign to attract new affiliates started to be advertised on underground forums:

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 децентрализация 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 рекаверы 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 связаны 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)

ACCOUNT

При отсутствии активности в течении двух недель Ваш аккаунт будет заморожен, а в последствии удален. Что бы избежать этого рекомендуем оповещать администрацию о возможных отпусках, паузах и прочим.

Рейт динамическим и зависит от суммы единичной выплаты по каждой компании, а именно:

- до 1.5M\$ - 80%
- до 3.0M\$ - 85%
- от 3.0M\$ - 90%

После достижения отметки в 1.5M\$ по сумме всех выплат на аккаунте вам будут доступны услуги хостинга файлов утечек компаний, прозвона и DDoS'a абсолютно бесплатно.

Description of the affiliate program on an underground forum

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 зависимости 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

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

It was clear from the very beginning of the new RaaS program that its creators were not new to the criminal business and took into account the negative 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' personal 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 появляться случайные люди, которые могут срывать переговоры (привет дарксайду), при запуске софта ОБЯЗАТЕЛЬНО использовать флаг `--access-token`. Аргументы cmdline не передаются к AVерам, 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

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**, which is provided by the RaaS owners to their affiliates together with their ransomware suite.

The ransomware uses the access token to calculate 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:

```
alpha_x86_32_windows_encrypt_app.exe --access-token
```

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 " " 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://.onion/?access-key=>

Ransom note

When victims publish information from their chats, BlackCat affiliates punish them by increasing ransom demands, for example. 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.

Tue Nov 30 2021

Hello twitter boys. Congratulations to our first target which keys was permanently deleted. All the data will be posted here soon.
Think twice before contacting with non-professionals.
Stay in touch.

[Back](#)

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

Your network was compromised.

Important files on **your network** was **downloaded** and **encrypted**.

Our custom **Decrypt App** is capable of **restoring** your **files**.

In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live-Chat**.

Decrypt App Price

Current price: **\$10000000**

Status

Awaiting payment of **\$10000000** to one of the following wallets:



Bitcoin		\$1150000 (?) = 244.379277 BT 0 C
Monero		\$10000000 = 45802.225989 XMR

Instructions

Live-Chat

Trial Decrypt

Intermediary

I wish to pay with
Bitcoin

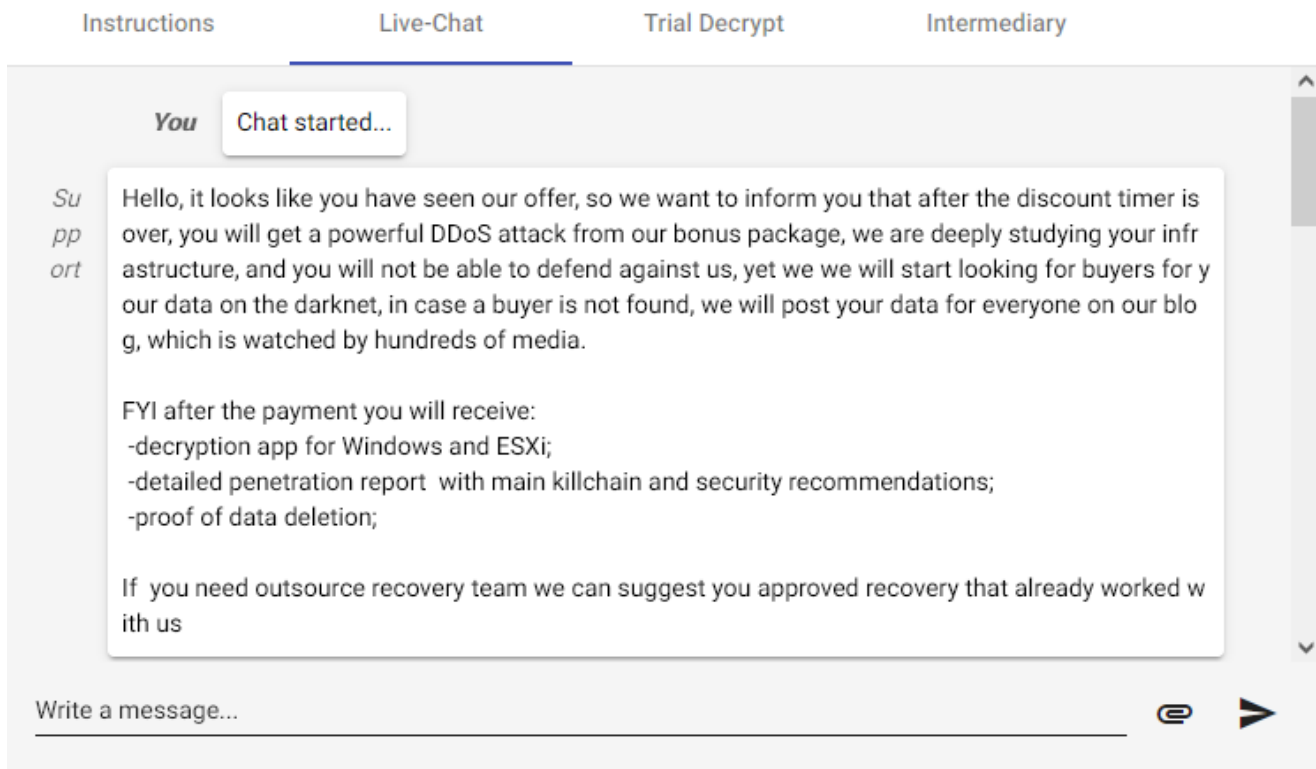
1. Create a Bitcoin Wallet.
2. Buy **244.379277 BTC** and deposit it to your Bitcoin Wallet.
3. Transfer **244.379277 BTC** to the following Bitcoin Address:
4. Wait until you transaction has at least **10** Bitcoin Network Confirmations.
5. Download link of **Decrypt App** will be provided automatically.
6. If something goes wrong text us using **Live-Chat**.

Victim's personal page

Extortion

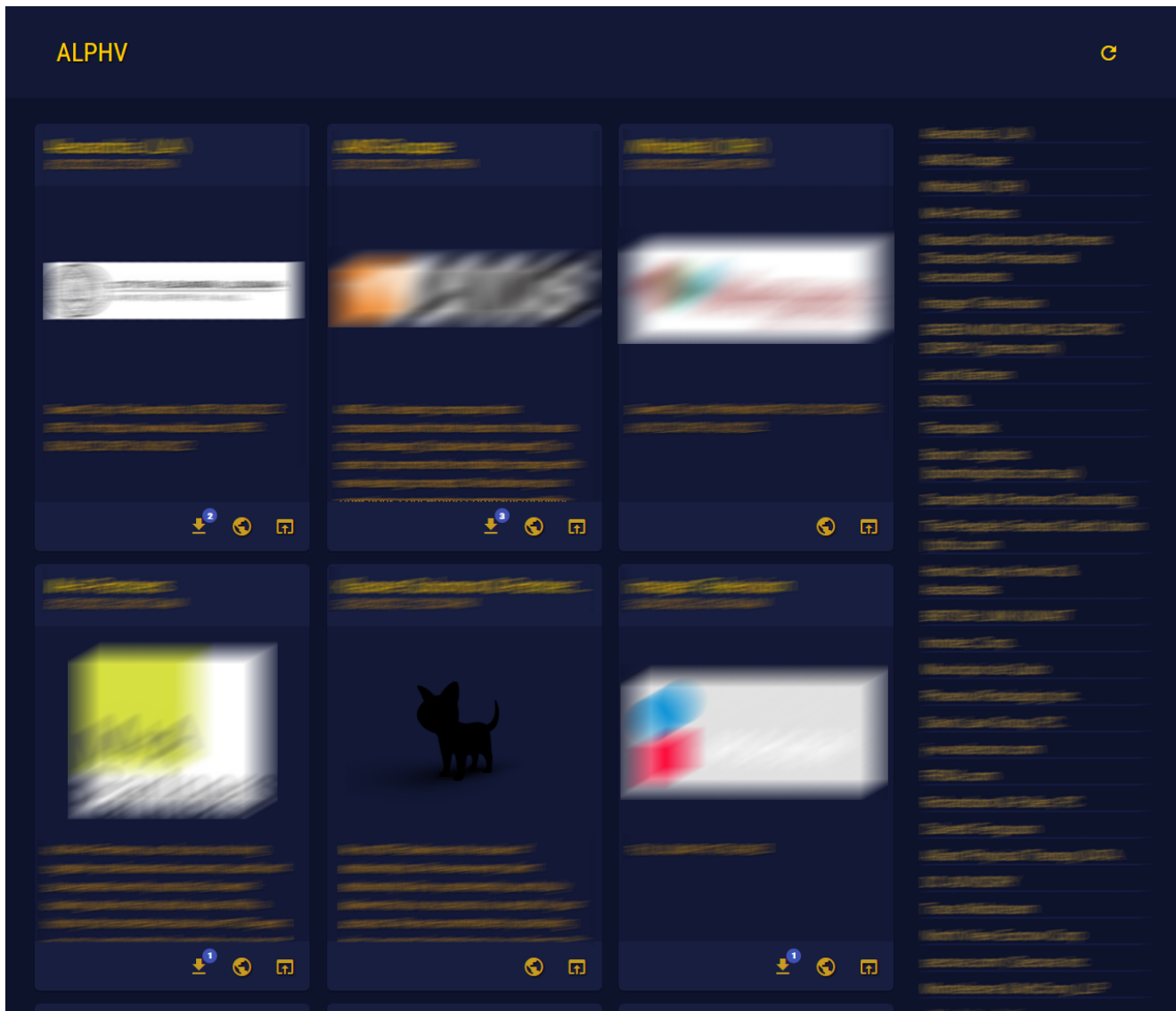
BlackCat affiliates use the double and triple extortion techniques. Firstly, the stolen information is published on BlackCat's dedicated leak site (DLS). Secondly, to mount pressure on the victim, BlackCat affiliates may threaten to send sensitive data to the victim's

competitors, partners, or customers, mass media, law enforcement, etc. Thirdly, the victim may receive threats of a DDoS attack being launched against their infrastructure.



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**.



BlackCat's DLS

The tactics, techniques and procedures of BlackCat ransomware affiliates

To reconstruct the lifecycle of a BlackCat attack, we use the Unified Ransomware Kill Chain described in [Incident Response Techniques for Ransomware Attacks](#).

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.

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.

To have additional capabilities to access the compromised network, the attackers could use tunnels (built using **ngrok** or **gost**) or legitimate software (such as **TeamViewer** or **ScreenConnect**).

In some cases, affiliates used **Cobalt Strike**, a framework that many are already used to seeing when investigating ransomware attacks.

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**.

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

Network Discovery

Affiliates seldom used innovative methods at the data collection stage, relying on classic tools. For instance, to scan the network, the attackers used **SoftPerfect Network Scanner**, which is another tool many ransomware groups use extensively.

To collect information about Active Directory, the attackers used **ADRecon**, a tool that is popular among REvil and BlackMatter affiliates.

In addition, the **NS** tool was used to collect data about available local and network drives. The tool was especially popular with those affiliates that used 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.

To move across the network, affiliates may use both perfectly legitimate techniques (such as **RDP**) and noisier ones (e.g., **Impacket: wmiexec** and **smbexec** in particular; and **Cobalt Strike**).

PuTTY is often used to gain access to the part of the infrastructure running on Linux.

Before being exfiltrated, data is put into archives using **7-Zip**, then uploaded to the **MEGA** file sharing service using the **Rclone** utility. In addition, in some cases affiliates used **ExMatter**, an exfiltration tool that has earlier been seen in the arsenal of **BlackMatter** affiliate program members.

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.

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. AV 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

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 reencrypting 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 is not checked in any way, 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. In addition, privileges can 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 to 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

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": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApegZ3mH3ZmyBRLGb1Ho85txXC3swHBu0HPRbI761yNjmJI",
  "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_NAME}\",",
  "default_file_mode": "Auto",
  "default_file_cipher": "Best",
  "credentials": [],
  "kill_services": ["mepocs", "memtas", "veeam", "svc$", "backup", "sql", "vss", "msexchange", "sql$", "mysql", "mysq",
  "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

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

Ransomware Uncovered

2021/2022

The well-known complete guide to the latest tactics, techniques, and procedures of ransomware operators based on MITRE ATT&CK®

[Download the report](#)