This post is also available in: 日本語 (Japanese)

Executive Summary

BlackCat (aka ALPHV) is a ransomware family that surfaced in mid-November 2021 and quickly gained notoriety for its sophistication and innovation. Operating a ransomware-as-a-service (RaaS) business model, BlackCat was observed soliciting for affiliates in known cybercrime forums, offering to allow affiliates to leverage the ransomware and keep 80-90% of the ransom payment. The remainder would be paid to the BlackCat author.

BlackCat has taken an aggressive approach to naming and shaming victims, listing more than a dozen on their leak site in a little over a month. The largest number of the group's victims so far are U.S. organizations, but BlackCat and its affiliates have also attacked organizations in Europe, the Philippines and other locations. Victims include organizations in the following sectors: construction and engineering, retail, transportation, commercial services, insurance, machinery, professional services, telecommunication, auto components and pharmaceuticals.

Use of BlackCat ransomware has grown quickly for a variety of reasons (for comparison, AvosLocker had only listed a handful of victims publicly within two months of becoming known). Effective marketing to affiliates is a likely factor – in addition to offering an enticing share of ransom payments, the group has solicited affiliates by posting ads on forums such as Ransomware Anonymous Market Place (RAMP).

The malware itself is written in Russian and coded in the Rust programming language. Though this is not the first piece of malware to use Rust, it is one of the first, if not the first, piece of ransomware to use it. By leveraging this programming language, the malware authors are able to easily compile it against various operating system architectures. Given its

numerous native options, Rust is highly customizable, which facilitates the ability to pivot and individualize attacks.

The threat actors leveraging BlackCat, often referred to as the "BlackCat gang," utilize numerous tactics that are becoming increasingly commonplace in the ransomware space. Notably, they use multiple extortion techniques in some cases, including the siphoning of victim data before ransomware deployment, threats to release data if the ransom is not paid and distributed denial-of-service (DDoS) attacks.

Palo Alto Networks detects and prevents BlackCat ransomware with the following products and services: Cortex XDR and Next-Generation Firewalls (including cloud-delivered security subscriptions such as WildFire).

Due to the surge of this malicious activity, we've created this threat assessment for overall awareness. Full visualization of the techniques observed, relevant courses of action and IOCs can be viewed in the Unit 42 ATOM viewer.

Types of Attacks Covered	Ransomware, DDoS
Ransomware Families Discussed	BlackCat
Related Unit 42 Topics	Cybercrime, Conti, LockBit 2.0, Hive, Avos

Table of Contents

BlackCat Ransomware Overview

Soliciting via known cybercrime forums, BlackCat is seeking affiliates to deploy its ransomware. Affiliates keep an 80-90% share of the ransom payment, with the remainder going to the BlackCat author. These affiliates are interviewed and vetted before being accepted into the RaaS group. Once the affiliate is confirmed, they are given unique access to a Tor-based control panel that hosts the affiliate's access.

Written in the Russian language, the control panel gives the affiliate updates and announcements about deploying and operating the ransomware as well as troubleshooting tips to help the affiliate be more successful in their campaigns. Along with the control panel, a name and shame blog is also hosted, targeting victims who have either ignored or refused to pay the ransom. This site has been regularly updated with new victims since the initial discovery of the group.

As shown in Figure 1 below, many RaaS operators use the double-extortion technique of exfiltrating data prior to encryption, which provides them greater leverage in negotiating ransom funds. As of December 2021, BlackCat has the seventh largest number of victims listed on their leak site among ransomware groups tracked by Unit 42 – impressive considering that this group has only been publicly known since November 2021. While Conti (ranked second) has been around in various guises for almost two years, it is surrounded at the top of the chart by emerging families. LockBit 2.0 and Hive both have at least six months' head start on BlackCat, but this highlights a worrying trend that newcomers (or reformed groups) can attack many victims in a short space of time.

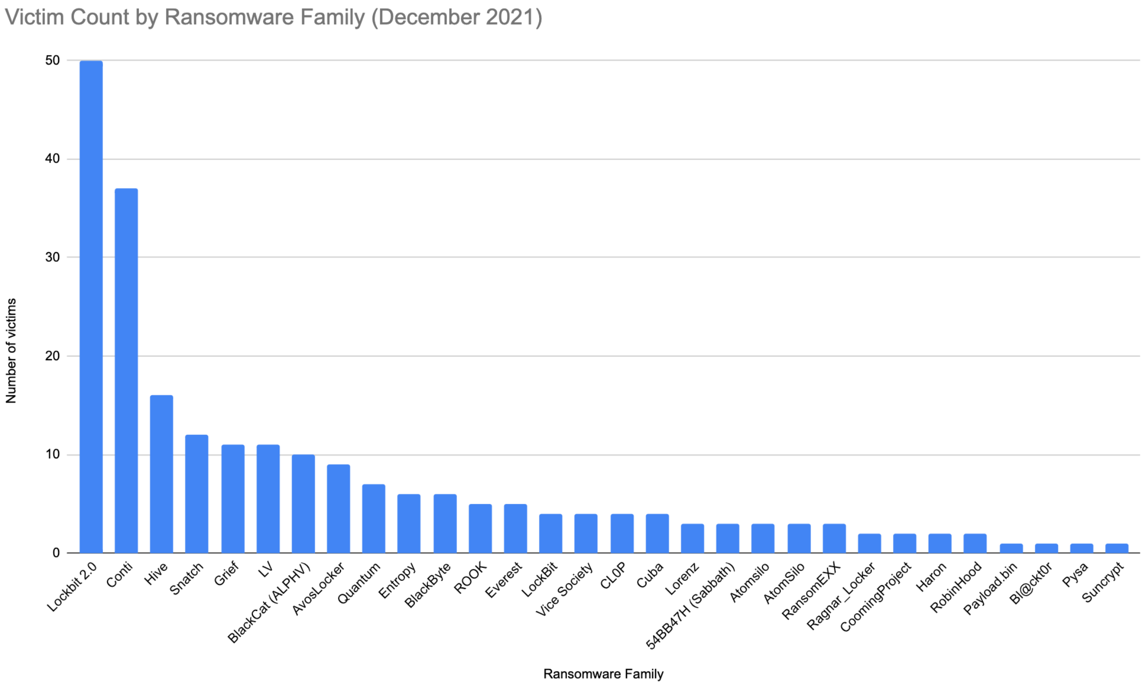


Figure 1. Leak site/name and shame blog statistics, December 2021.
Using the leak site information, we can understand the location and types of victims affected by BlackCat attacks. Victims include organizations in the following sectors: construction and engineering, retail, transportation, commercial services, insurance, machinery, professional services, telecommunication, auto components and pharmaceuticals. Figure 2 breaks down the victims by country. However, the so-far sporadic spread of the attacks may indicate a somewhat opportunistic approach, as with most contemporary ransomware families.

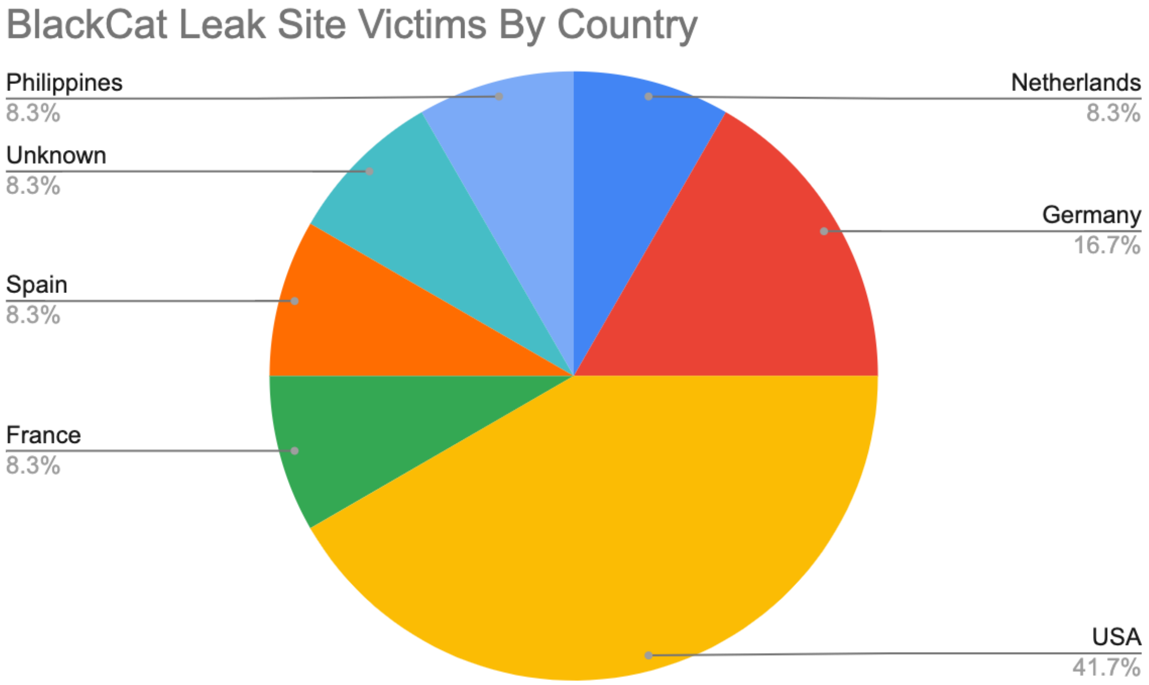
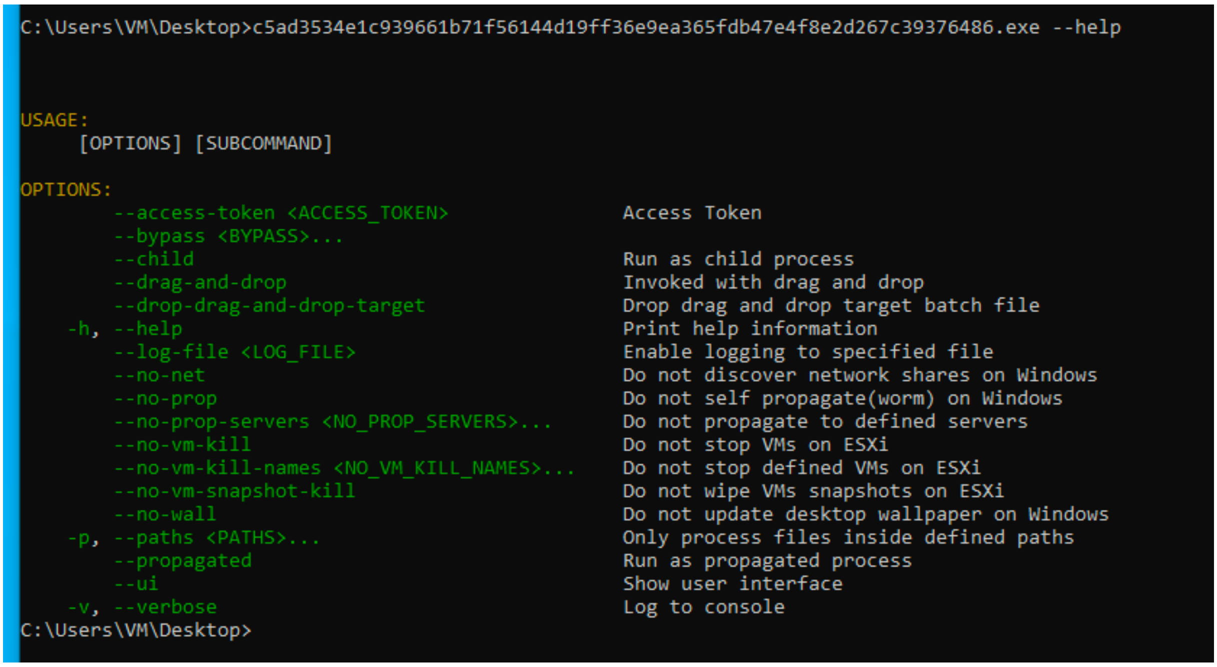


Figure 2. BlackCat leak site victims by country.

Technical Details

BlackCat is positioned to pivot to individualized, customized attacks due to the numerous options available when coding in Rust (Figure 3). Rust programming has gained momentum due to its fast and high performance, powerful web application development, low overhead for embedded programming, and memory management resolution. Rust also facilitates the BlackCat author due to its efficiency regarding algorithms that power the encryption capability of the ransomware. Because of its efficiency and adaptability, BlackCat has been seen targeting both Windows and Linux systems.



```
C:\Users\VM\Desktop>c5ad3534e1c939661b71f56144d19ff36e9ea365fdb47e4f8e2d267c39376486.exe --help


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
    -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
C:\Users\VM\Desktop>
```

Figure 3. BlackCat execution options.

In an effort to maintain longevity, the use of the `--access-token` flag is required to execute the ransomware, which can make it harder to analyze in sandboxed environments.

BlackCat Config

While analyzing the ransomware configurations, we observed numerous evasion tactics deployed. These evasion techniques are used in an effort to impair or disable system defenses as well as to stop certain applications that may lock files open on disk, causing problems when trying to encrypt them. BlackCat attempts to kill several processes and services to hinder or prevent security solutions and backups. The process list checked is as follows:

```
agntsvc, dbeng50, dbsnmp, encsvc, excel, firefox, infopath,
isqlplussvc, msaccess, mspub, mydesktopqos, mydesktopservice,
notepad, ocautoupds, ocomm, ocssd, onenote, oracle, outlook,
powerpnt, sqbcoreservice, sql, steam, synctime, tbirdconfig,
thebat, thunderbird, visio, winword, wordpad, xfssvccon,
*sql*, bedbh, vxmon, benetns, bengien, pvlsvr, beserver,
raw_agent_svc, vsnapvss, CagService, QBIDPService, QBDBMgrN,
QBCFMonitorService, SAP, TeamViewer_Service, TeamViewer,
tv_w32, tv_x64, CVMountd, cvd, cvfwd, CVODS, saphostexec,
saposcol, sapstartsrv, avagent, avscc, DellSystemDetect,
EnterpriseClient, VeeamNFSSvc, VeeamTransportSvc,
VeeamDeploymentSvc
```

The services running on the compromised system are checked against the following list:

```
mepocs, memtas, veeam, svc$, backup, sql, vss, msexchange,
sql$, mysql, mysql$, sophos, MSExchange, MSExchange$,
WSBExchange, PDVFSService, BackupExecVSSProvider,
BackupExecAgentAccelerator, BackupExecAgentBrowser,
BackupExecDiveciMediaService, BackupExecJobEngine,
BackupExecManagementService, BackupExecRPCService, GxBlr,
GxVss, GxClMgrS, GxCVD, GxCIMgr, GXMMM, GxVssHWProv, GxFWD,
SAPService, SAP, SAP$, SAPD$, SAPHostControl, SAPHostExec,
QBCFMonitorService, QBDBMgrN, QBIDPService, AcronisAgent,
VeeamNFSSvc, VeeamDeploymentService, VeeamTransportSvc,
MVArmor, MVarmor64, VSNAPVSS, AcrSch2Svc
```

In an effort to maintain persistence, the BlackCat ransomware excludes key system and application folders – as well as key components – from encryption so as not to render the system and ransomware inoperative. The folders excluded are as follows:

```
system volume information, intel, $windows.~ws, application
data, $recycle.bin, mozilla, $windows.~bt, public, msocache,
windows, default, all users, tor browser, programdata, boot,
config.msi, google, perflogs, appdata, windows.old
```

Excluded file names are as follows:

```
desktop.ini, autorun.inf, ntldr, bootsect.bak, thumbs.db,
boot.ini, ntuser.dat, iconcache.db, bootfont.bin, ntuser.ini,
ntuser.dat.log
```

Any file with an extension matching the following list will also be avoided:

```
themepack, nls, diagpkg, msi, lnk, exe, cab, scr, bat, drv,
rtp, msp, prf, msc, ico, key, ocx, diagcab, diagcfg, pdb, wpx,
hlp, icns, rom, dll, msstyles, mod, ps1, ics, hta, bin, cmd,
ani, 386, lock, cur, idx, sys, com, deskthemepack, shs, ldf,
theme, mpa, nomedia, spl, cpl, adv, icl, msu
```

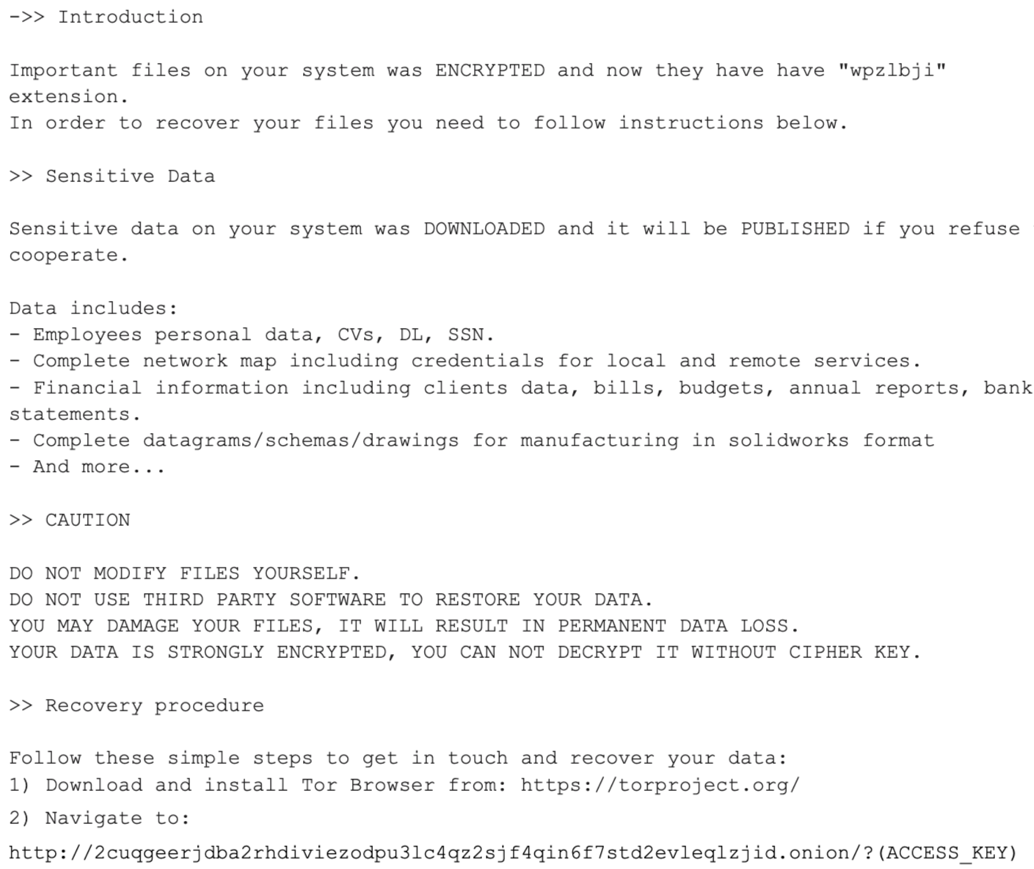
Hardcoded credentials stored within the BlackCat ransomware config lend credence to the likelihood that specific victims are being targeted. The credentials also allow BlackCat to move laterally within the victim's system and/or network, often with administrative privileges. Credential access permits the ransomware to deploy additional tools that further propagate the attack. These observations have also been confirmed by Symantec.

Associated Tools

BlackCat has been observed using multiple – often legitimate – tools throughout their attacks, such as Mimikatz, LaZagne and WebBrowserPassView to recover stored passwords, as well as GO Simple Tunnel (GOST) and MEGAsync to exfiltrate data. Additionally, anti-forensics tools like fileshredder, an application to securely delete unwanted files beyond recovery, have also been leveraged during some BlackCat ransomware attacks investigated by Unit 42.

Post-compromise Activities

Once candidate systems have been identified for encryption by the threat actors, the ransomware deployment occurs and all viable files will be encrypted. This process often involves renaming files to include another or a different file extension, such as `wpzlbji`, in the example shown in Figure 4. As is commonplace with other ransomware strains, BlackCat ransomware will drop ransom notes on the compromised system(s) to inform the victim of what has happened and how to go about getting their data restored. Text files with the name `RECOVER-[RANDOM]-FILES.txt` (where `[RANDOM]` refers to the aforementioned file extension name) will be found on the compromised system containing information and instructions such as those in the example below:

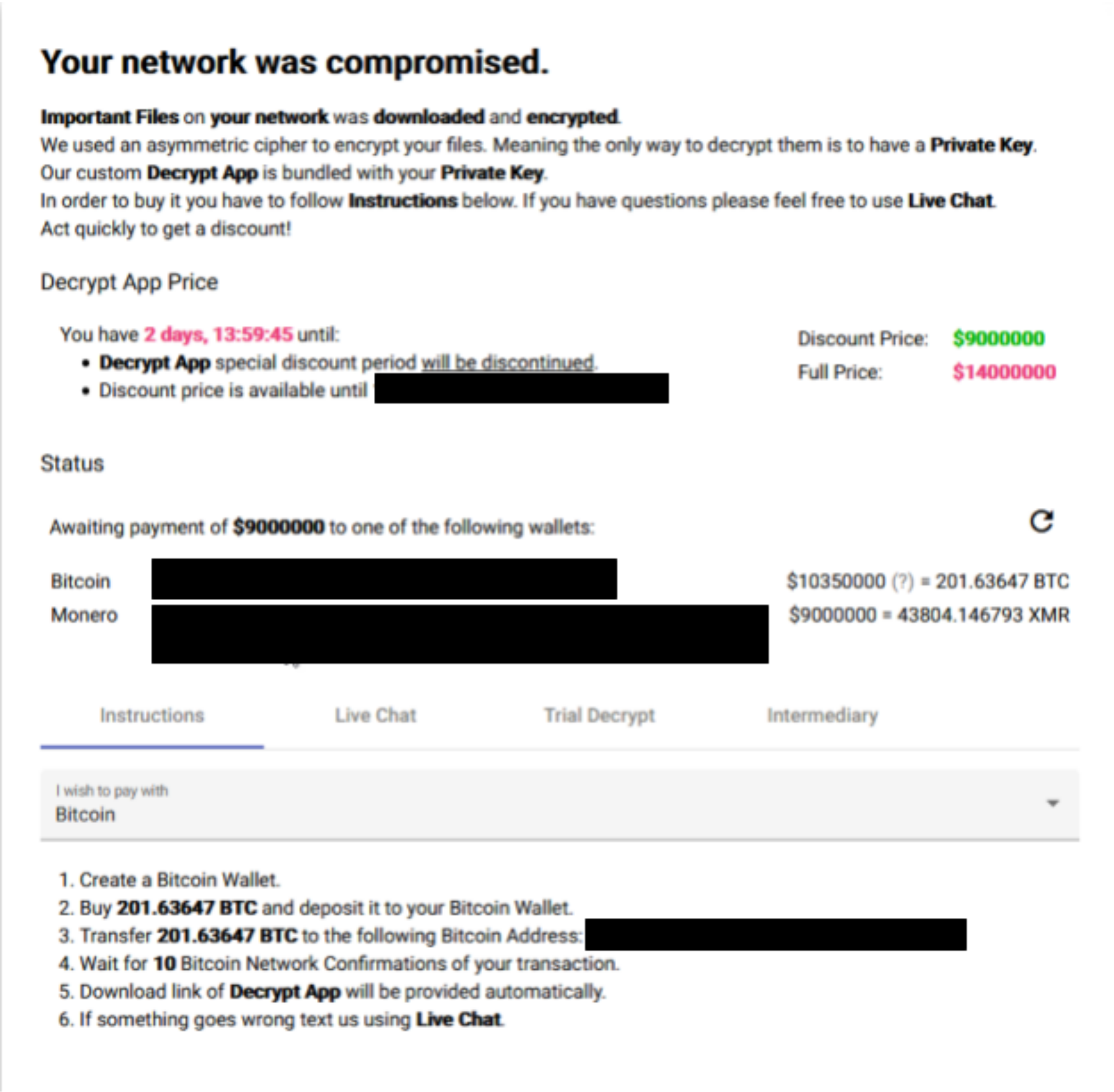


```
->> Introduction

Important files on your system was ENCRYPTED and now they have have "wpzlbji"
extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to
cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank
statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

>> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to:
http://2cuqgeerjdba2rhdiviezodpu3lc4qz2sjf4qin6f7std2evleqlzjid.onion/?(ACCESS_KEY)
```

Figure 4. An example of a BlackCat ransom note dropped on a compromised system. BlackCat utilizes a unique onion domain with a victim-specific access key for the victim to use to learn more about the attack, their data, and what the threat actors want the victim to do next. The following example URL highlights the notation used by BlackCat ransomware:

```
http://2cuqgeerjdba2rhdiviezodpu3lc4qz2sjf4qin6f7std2evleqlzjid[.]onion/?access-key=${ACCESS_KEY}","note_short_text":"Important
```

Once the victim navigates to the onion site provided, they will see something similar to Figure 5 below. This site reiterates the problem and that the actor's Decrypt App private key is the only way to get their data back. The portal also provides chat facilities, the ransom amounts – which can differ depending on when the payment is sent – how to pay, and a way to test that the decryption works.



Your network was compromised.

Important Files on **your network** was **downloaded** and **encrypted**.
We used an asymmetric cipher to encrypt your files. Meaning the only way to decrypt them is to have a **Private Key**.
Our custom **Decrypt App** is bundled with your **Private Key**.
In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live Chat**.
Act quickly to get a discount!

Decrypt App Price

You have 2 days, 13:59:45 until:

- **Decrypt App** special discount period will be discontinued.
- Discount price is available until [redacted]

Discount Price:	$9000000
Full Price:	$14000000

Status

Awaiting payment of **$9000000** to one of the following wallets:

Bitcoin	[redacted]	$10350000 (?) = 201.63647 BTC
Monero	[redacted]	$9000000 = 43804.146793 XMR

I wish to pay with
Bitcoin

1. Create a Bitcoin Wallet.
2. Buy **201.63647 BTC** and deposit it to your Bitcoin Wallet.
3. Transfer **201.63647 BTC** to the following Bitcoin Address: [redacted]
4. Wait for **10** Bitcoin Network Confirmations of your transaction.
5. Download link of **Decrypt App** will be provided automatically.
6. If something goes wrong text us using **Live Chat**.

Figure 5. Example onion site information for BlackCat victims.

Unit 42 has observed BlackCat affiliates asking for ransom amounts of up to $14 million, though they offered to discount this demand to $9 million if paid before the established time. Interestingly, the ransom demand gives the victim the option to pay not only in Bitcoin (the most common option) but also in Monero.

In some cases, BlackCat operators use the chat to threaten the victim, claiming they will perform a DDoS attack on the victims' infrastructure if the ransom is not paid. When it appears in addition to the use of a leak site, this practice is known as triple extortion, a tactic that was observed being used by groups like Avaddon and Suncrypt in the past.

One unique feature of BlackCat ransomware is that negotiation chats can only be accessed by those holding an access token key or ransom note – the group has made efforts to avoid third-party snooping.

Courses of Action

This section documents the relevant tactics, techniques and procedures (TTPs) used by BlackCat ransomware and operators, mapping them directly to the Palo Alto Networks product(s) and service(s) protecting against them. It also further instructs customers on how to ensure their devices are appropriately configured.

Product / Service	***Course of Action***
Discovery	
The below courses of action mitigate the following techniques: *Process Discovery [T1057], File and Directory Discovery [T1083]*	
CORTEX XDR PREVENT	*Configure Behavioral Threat Protection under the Malware Security Profile*
Lateral Movement	
The below courses of action mitigate the following techniques: *Lateral Tool Transfer [T1570]*	
THREAT PREVENTION†	*Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'*
	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories and threats
	Ensure a secure antivirus profile is applied to all relevant security policies
Command and Control	
The below courses of action mitigate the following techniques: *Multi-hop Proxy [T1090.003]*	
THREAT PREVENTION†	*Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use*
	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories and threats
	Ensure a secure anti-spyware profile is applied to all security policies permitting traffic to the internet
	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
	Ensure DNS sinkholing is configured on all anti-spyware profiles in use

	Ensure a secure antivirus profile is applied to all relevant security policies
ADVANCED URL FILTERING†	*Ensure that URL Filtering uses the action of “block” or “override” on the URL categories*
	Ensure secure URL filtering is enabled for all security policies allowing traffic to the internet
	Ensure that Advanced URL Filtering is used
	Ensure that access to every URL is logged
	Ensure all HTTP Header Logging options are enabled
CORTEX XSOAR	*Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators*
	Deploy XSOAR Playbook - Palo Alto Networks - Hunting And Threat Detection
NEXT-GENERATION FIREWALLS	*Ensure 'SSL Forward Proxy Policy' for traffic destined to the internet is configured*
	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS
	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources exists
	Ensure that the Certificate used for Decryption is Trusted
Exfiltration	
The below courses of action mitigate the following techniques: *Exfiltration to Cloud Storage [T1567.002]*	
URL FILTERING†	*Ensure secure URL filtering is enabled for all security policies allowing traffic to the internet*
	Ensure all HTTP Header Logging options are enabled
	Ensure that URL Filtering uses the action of ‘block’ or ‘override’ on the URL categories

	Ensure that access to every URL is logged
	Ensure that Advanced URL Filtering is used
Impact	
The below courses of action mitigate the following techniques: *Data Encrypted for Impact [T1486], Service Stop [T1489], Inhibit System Recovery [T1490]*	
CORTEX XSOAR	*Deploy XSOAR Playbook - Ransomware Manual for incident response.*
	Deploy XSOAR Playbook - Palo Alto Networks Endpoint Malware Investigation

Table 1. Courses of Action for BlackCat ransomware.

†These capabilities are part of the NGFW security subscriptions service

Conclusion

BlackCat is an innovative and sophisticated ransomware family that is rapidly forming a reputation for its highly customized and individualized attacks. By leveraging the Rust programming language, the malware authors are able to easily compile it against various operating system architectures, which facilitates the group's ability to pivot from one victim to the next. As seen with other ransomware families, BlackCat operates with a RaaS model and utilizes multiple extortion techniques, then publishes a leak site to further pressure victims into paying the ransom.

Palo Alto Networks detects and prevents BlackCat ransomware in the following ways:

- WildFire: All known samples are identified as malware.
- Cortex XDR with:
  - Indicators for BlackCat.
  - Anti-Ransomware Module to detect BlackCat encryption behaviors on Windows.
  - Local Analysis detection for BlackCat binaries on Windows.
  - BTP rule prevents Ransomware activity on Linux.
- Next-Generation Firewalls: DNS Signatures detect the known command and control (C2) domains, which are also categorized as malware in URL Filtering.

Indicators of compromise and BlackCat-associated TTPs can be found in the BlackCat ATOM.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Additional Resources

- Noberus: Technical Analysis Shows Sophistication of New Rust-Based Ransomware
- Highlights from the 2021 Unit 42 Ransomware Threat Report