BlackCat (AKA ALPHV)

Executive Summary
BlackCat is a relatively new ransomware variant, known to be in operation since November 2021. It is exceptionally capable and is believed to be operated by individuals with significant experience as cyber criminals, who have extensive relationships with other significant players throughout the cybercriminal ecosystem. BlackCat is known to have targeted the healthcare and public health (HPH) sector and is expected to continue. The HPH should take this threat seriously and apply appropriate defensive and mitigative actions towards protecting their infrastructure from compromise.

Report
BlackCat (also known as Noberus or ALPHV) is a ransomware variant offered as part of one of the most sophisticated Ransomware-as-a-service (RaaS) operations in the global cybercriminal ecosystem. BlackCat has been used in operations since November 2021. They are believed to be a successor to the REvil, Darkside and BlackMatter operators and have connections to FIN7 AKA Carbon Spider as well as FIN12. BlackCat is noteworthy because its features make it technically sophisticated as compared to other RaaS variants, allowing for the ability to target a wide range of corporate environments. BlackCat was one of the first major ransomware variants to be developed in the rust programming language, has a highly-customizable feature set, and relies heavily on internally-developed capabilities, which are constantly developed and have upgrades. The many advanced technical features include being entirely command-line driven, human-operated and adaptable malware which has the ability to use several different encryption routines, self-propagate, and render hypervisors ineffective to frustrate analysis. This has made BlackCat one of the more adaptable ransomware operations in the world.

Like all ransomware-as-a-service (RaaS) operations, the BlackCat operators recruit affiliates to perform corporate breaches and encrypt devices, while retaining code maintenance and development responsibilities for themselves. As previously noted, their ransomware code is highly customizable, and the executable includes a JSON configuration that allows that customization. This includes extensions, ransom note details, encryption, services targeted for termination and whitelisted folders/files/extensions.

Encryption
According to their own RaaS advertisements, BlackCat ransomware can be configured to use several different encryption modes:

- **Full file encryption** – the strongest but slowest encryption method.
- **Fast encryption** – the opposite of full – sacrifices strength for speed as it only encrypts the first N megabytes.
- **DotPattern encryption** – favors speed but is still somewhat strong encryption by encrypting N megabytes through M step.
- **SmartPattern encryption** – the most optimal mode in terms of speed/strength ratio; encrypts N megabytes in percentage steps (default: 10 megabytes every 10% of the file starting from the header).
  - **Auto** – The encryption speed/strength can change depending on the type and size of the file, the choice will be optimized for both speed and security.
BlackCat has two encryption algorithms – ChaCha20 and AES. In auto mode (see above), it will default to AES unless there is no support for it in the local processor, in which case the malware encrypts files with ChaCha20.

**Functionality Summary**

Some of BlackCat’s primary functions can be seen in its command line parameters (Figure 1). Further details and explanation of its command line parameters can be found in Appendix B.

BlackCat can be configured with domain credentials to distribute its ransomware.
- The executable will extract PSExec (Sysinternals) to the %Temp% folder and use it to distribute and execute the encryptor to remote Windows machines

BlackCat can terminate processes and Windows services that can protect against encryption. This includes but is not limited to:
- Shadow copies
- Commercial backup software
- Microsoft Exchange
- Database servers
- Microsoft Office Applications

BlackCat can also clear the Recycle Bit, connect to a Microsoft cluster and scan for network devices. It also uses the Windows Restart Manager API to close processes or shut down Windows services keeping a file open during encryption.
Some victims have had unique Tor sites for negotiations and data leaks. BlackCat uses the following Tor site: https://alphvmmm27o3abo3r2mlmrpdmzle3rykajqc5xsj7j7ejksbpa36ad.onion[.]ly

BlackCat uses a tool called Exmatter for data exfiltration. Some of Exmatter’s details can be found here. It also received some significant updates in August of 2022, the details of which can be found here.

Since that update, it limits the type of exfiltrated files to: PDF, DOC, DOCX, XLS, PNG, JPG, JPEG, TXT, BMP, RDP, SQL, MSG, PST, ZIP, RTF, IPT, and DWG.

Exmatter also possesses the ability to create a report for exfiltrated files as well as corrupt them. Additionally, it has a self-destruct option if deployed and executed to a non-valid environment.

**Targeting**

It is believed that BlackCat is capable of targeting the following operating systems:

- Windows, from 7 to 11, as well as Server 2008r2, 2012, 2016, 2019, 2022 (XP and 2003 can be encrypted over Server Message Block)
- ESXI (at least versions 5.5, 6.5, 7.0.2u)
- Debian (at least versions 7,8 and 9)
- Ubuntu (at least versions 18.04 and 20.04)
- ReadyNAS
- Synology

BlackCat has been known to target pharmaceutical companies as well as pharmaceutical manufacturers, as well as several other non-healthcare enterprises.

**Analyst Comment**

There are a number of recommendations for protecting against and mitigating impact from a BlackCat attack. First, HC3 continues to see the following four categories of attack vectors frequently associated with ransomware operators:

- Phishing
- Compromise of known vulnerabilities
- Compromise of remote-access technologies, especially VPNs and RDP
- Distributed attacks, especially supply chain and Managed Service Provider compromise

The FBI has provided mitigations, which include:

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides
HC3: Analyst Note
December 12, 2022   TLP:CLEAR   Report: 202212121500

- Review antivirus logs for indications they were unexpectedly turned off
- Implement network segmentation
- Require administrator credentials to install software
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud)
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released
- Use multifactor authentication where possible
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind
- Install and regularly update antivirus and anti-malware software on all hosts

FBI’s full list of mitigations can be found here. If you are compromised by ransomware, the FBI advises you contact your local FBI field office, which can be found here. Ransomware mitigation recommendations from the Department of Homeland Security can be found here.

Samples of indicators of compromise and Yara rules can be found below.

IOCs:
- https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware
- https://otx.alienvault.com/pulse/62960d2bab11f2124cb4962e

Yara Rules:

References
BlackCat — In a Shifting Threat Landscape, It Helps to Land on Your Feet: Tech Dive https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive

Fat Cats: An analysis of the BlackCat ransomware affiliate program https://blog.group-ib.com/blackcat

A Deep Dive Into ALPHV/BlackCat Ransomware https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware


Leading Ransomware Variants Q3 2022
Noberus Ransomware: Darkside and BlackMatter Successor Continues to Evolve its Tactics

Analyzing Exmatter: A Ransomware Data Exfiltration Tool

Emotet botnet now pushes Quantum and BlackCat ransomware

BlackCat ransomware claims attack on European gas pipeline

BlackCat ransomware could be about to get a whole lot nastier

BlackCat Ransomware Group Deploys Brute Ratel Pen Testing Kit

BlackCat ransomware attacks not merely a byproduct of bad luck

BlackCat (aka ALPHV) Ransomware is Increasing Stakes up to $2.5M in Demands

Ransomware gang creates site for employees to search for their stolen data #ALPHV #BlackCat

Prolific Ransomware Affiliate Groups Deploy BlackCat

Microsoft: Exchange servers hacked to deploy BlackCat ransomware

The many lives of BlackCat ransomware
BlackCat — In a Shifting Threat Landscape, It Helps to Land on Your Feet: Tech Dive
https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive

Novel BlackCat Ransomware Tactic Speeds Up Encryption Process
https://duo.com/decipher/novel-blackcat-ransomware-tactic-speeds-up-encryption-process

FBI: BlackCat ransomware breached at least 60 entities worldwide

FBI: BlackCat/ALPHV Ransomware Indicators of Compromise

An Investigation of the BlackCat Ransomware via Trend Micro Vision One

BlackCat Purveyor Shows Ransomware Operators Have 9 Lives
https://www.darkreading.com/attacks-breaches/blackcat-purveyor-shows-ransomware-operators-have-nine-lives

BlackCat Ransomware Targets Industrial Companies
https://www.securityweek.com/blackcat-ransomware-targets-industrial-companies

A Bad Luck BlackCat
https://securelist.com/a-bad-luck-blackcat/106254/

A look at the ransomware threat landscape. BlackMatter affiliate connected to BlackCat. EXOTIC LILY provides initial access for ransomware actors.
https://thecyberwire.com/podcasts/research-briefing/109/notes

From BlackMatter to BlackCat: Analyzing two attacks from one affiliate
http://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html

Cybereason vs. BlackCat Ransomware
https://www.cybereason.com/blog/cybereason-vs-blackcat-ransomware

LockBit, BlackCat, Swissport, Oh My! Ransomware Activity Stays Strong
https://threatpost.com/lockbit-blackcat-swissport-ransomware-activity/178261/

BlackCat (ALPHV) ransomware linked to BlackMatter, DarkSide gangs

An ALPHV (BlackCat) representative discusses the group’s plans for a ransomware ‘meta-universe’
Threat Assessment: BlackCat Ransomware
https://unit42.paloaltonetworks.com/blackcat-ransomware/

Who Wrote the ALPHV/BlackCat Ransomware Strain?
https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/

Actor username01 (aka alphv, ransom) runs ALPHV aka ALPHV-ng, BlackCat ransomware-as-a-service affiliate program
https://titan.intel471.com/report/inforep/aff92438c62c32c3a6a4835d7a62a94c

Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware

ALPHV BlackCat - This year's most sophisticated ransomware

ALPHV (BlackCat) is the first professional ransomware gang to use Rust
https://therecord.media/alphv-blackcat-is-the-first-professional-ransomware-gang-to-use-rust/

Ransomware Group Debuts Searchable Victim Data
https://krebsonsecurity.com/2022/06/ransomware-group-debuts-searchable-victim-data/

Appendix A: MITRE ATTACK MAPPING (Courtesy of Group-IB)

<table>
<thead>
<tr>
<th>TACTIC</th>
<th>TECHNIQUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA0001 Initial Access</td>
<td>T1190 Exploit Public-Facing Application</td>
<td>In a number of attacks, the threat actors used ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207).</td>
</tr>
<tr>
<td>TA0002 Execution</td>
<td>T1113 External Remote Services</td>
<td>As an initial attack vector, insecure RDP and VPNs may be used.</td>
</tr>
<tr>
<td></td>
<td>T1078 Valid Accounts</td>
<td>BlackCat affiliates may purchase access to their victim’s network infrastructure on underground forums.</td>
</tr>
<tr>
<td>TA0003 Persistence</td>
<td>T1053 Scheduled Task/Job</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>T1059.001 Command and Scripting Interpreter: PowerShell</td>
<td>The attackers may use PowerShell scripts when deploying ransomware in the victim’s network, disabling security tools, and encrypting files.</td>
</tr>
<tr>
<td></td>
<td>T1059.003 Command and Scripting Interpreter: Windows Command Shell</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>T1047 Windows Management Instrumentation</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>T1569.002 System Services: Service Execution</td>
<td>The BlackCat ransomware 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.</td>
</tr>
<tr>
<td>TA0004 Privilege Escalation</td>
<td>T1505 Server Software Component</td>
<td>Successfully exploiting ProxyShell vulnerabilities enabled the attackers to place a web shell on a vulnerable Microsoft Exchange server.</td>
</tr>
<tr>
<td></td>
<td>T1078 Valid Accounts</td>
<td>Legitimate accounts obtained by the attackers can be used to ensure persistence in the compromised infrastructure.</td>
</tr>
<tr>
<td></td>
<td>T1078 Valid Accounts</td>
<td>To escalate privileges, BlackCat may use stolen legitimate accounts specified in the configuration data.</td>
</tr>
<tr>
<td></td>
<td>T1548.002 Abuse Elevation Control Mechanism: Bypass User Account</td>
<td>To bypass UAC, BlackCat ransomware may escalate privileges using the ICMLuaUtil COM interface, as well as use the Masquerade PEB method.</td>
</tr>
</tbody>
</table>
Before exfiltration, the attackers may put collected data in 7Zip archives. The attackers collect information from the local system for exfiltration purposes. PsExec utility contained in its body. The host. The BlackCat ransomware can self-propagate in the network by using the legitimate wmiexec and smbexec modules from Impacket. After obtaining privileged authentication data, in order to spread over the local area network and deploy ransomware involves copying related tools to access network resources, the attackers may use the PsExec utility, as well as the psexec, wmiexec and smbexec modules from Impacket. By using wevtutil, BlackCat can clear all Windows event logs on a compromised host. The attackers use a SoftPerfect Network Scanner executable renamed to svchost.exe. To access parts of the infrastructure running on Linux, the attackers use the PuTTY utility. The attackers may use RDP to move across the network. 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. 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.
HC3: Analyst Note

December 12, 2022   TLP:CLEAR   Report: 202212121500

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.

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.

TA0040 Impact
T1486 Data 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.

T1485 Data 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.

Appendix B: Available Command-Line Parameters (Courtesy of Group-IB)

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Displays information about command line parameters.</td>
</tr>
<tr>
<td>-p, --paths ...</td>
<td>Encrypts files at paths specified in this parameter.</td>
</tr>
<tr>
<td>-v, --verbose</td>
<td>Shows a report in the console.</td>
</tr>
<tr>
<td>--access-token</td>
<td>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.</td>
</tr>
<tr>
<td>--bypass ...</td>
<td>This parameter is not used.</td>
</tr>
<tr>
<td>--child</td>
<td>Launches the ransomware as a child process.</td>
</tr>
<tr>
<td>--drag-and-drop</td>
<td>Launches the ransomware in drag-and-drop mode.</td>
</tr>
<tr>
<td>--drop-drag-and-drop-target</td>
<td>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).</td>
</tr>
<tr>
<td>--extra-verbose</td>
<td>Shows a more detailed report.</td>
</tr>
<tr>
<td>--log-file</td>
<td>Outputs a report to a specified file.</td>
</tr>
<tr>
<td>--no-net</td>
<td>Ensure that files on available network resources are not encrypted.</td>
</tr>
</tbody>
</table>
**HC3: Analyst Note**  
December 12, 2022   TLP:CLEAR   Report: 202212121500

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--no-prop</td>
<td>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 &quot;credentials&quot;. The PsExec utility is in the body of the ransomware in a compressed format (Deflate). In ALPHV MORPH it is also encrypted (AES128 CTR).</td>
</tr>
<tr>
<td>--no-prop-servers</td>
<td>A list of servers excluded during self-propagation.</td>
</tr>
<tr>
<td>--no-vm-kill</td>
<td>Ensures that virtual machines are not stopped.</td>
</tr>
<tr>
<td>--no-vm-kill-names</td>
<td>A list of names of virtual machines that are not stopped.</td>
</tr>
<tr>
<td>--no-vm-snapshot-kill</td>
<td>Ensures that virtual machine snapshots are not destroyed.</td>
</tr>
<tr>
<td>--no-wall</td>
<td>Ensures that the desktop wallpaper is not updated.</td>
</tr>
<tr>
<td>--propagated</td>
<td>Launches the ransomware in self-propagation (worm) mode.</td>
</tr>
<tr>
<td>--ui</td>
<td>Launch the ransomware with a graphical interface displaying the encryption progress.</td>
</tr>
</tbody>
</table>

**Contact Information**

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback