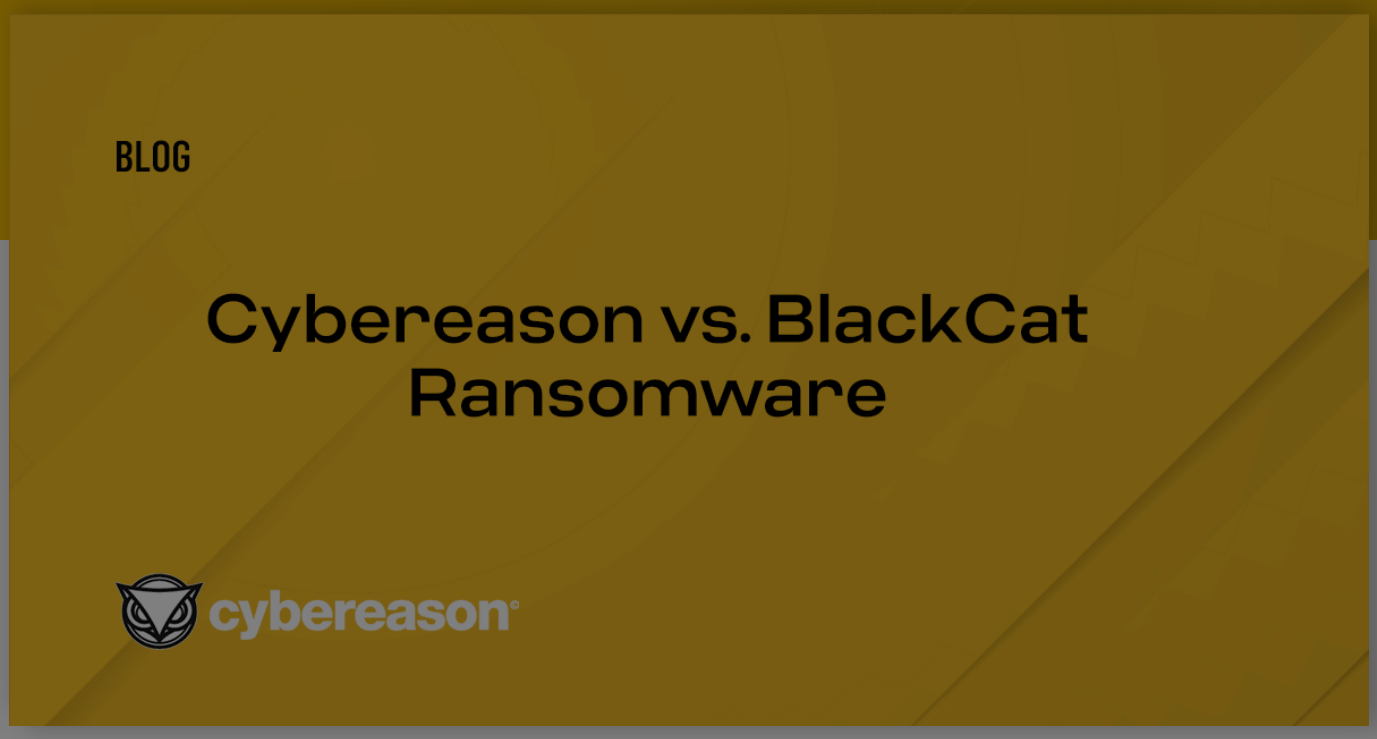
BLOG



Cybereason vs. BlackCat Ransomware

WRITTEN BY Cybereason Nocturnus

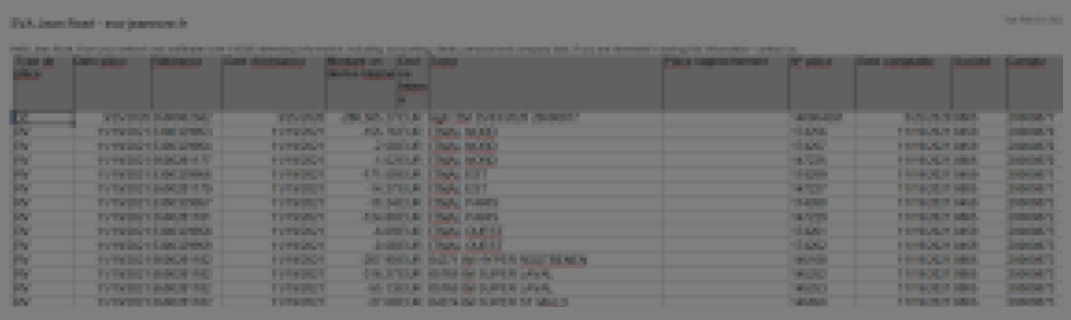
Since its first emergence in November 2021, the Cybereason Nocturnus team has been tracking the BlackCat Ransomware (aka ALPHV), which has been called "2021's most sophisticated ransomware".

BlackCat ransomware gained notoriety quickly leaving a trail of destruction behind it, among its recent victims are German oil companies, an Italian luxury fashion brand and a Swiss Aviation company.

Since its recent emergence, BlackCat has attacked various industries, including telecommunication, commercial services, insurance, retail, machinery, pharmaceuticals, transportation, and construction industries. Among the affected regions are Germany, France, Spain, the Philippines, and the Netherlands, with the most victims being located in the US.

The ransomware was given the name “BlackCat” due to the favicon of a black cat being used on every victim's Tor payment site. The operators of BlackCat have been using the names “alphv” and “ransom” in Cybercrime forums (ramp_v2, exploit.in) in order to recruit affiliates.

The operators of the ransomware appear to be from Russian speaking regions. Like many others, BlackCat uses a RaaS model (Ransomware-as-a-service). Affiliates of BlackCat are offered between 80-90% of the ransom payment, and once approved, are given access to a control panel that manages access:



Leaked document from BlackCat Leaks website

One of the unique elements of the BlackCat ransomware is that it is written in Rust, which is not a common coding language for malware and ransomware. *“Rust is a multi-paradigm, general-purpose programming language designed for performance and safety."*

Because of Rust’s emphasis on performance, the process of encryption is very fast, and in addition, Rust is cross-platform, which makes it easier to create variants for both Windows and Linux.

The operators of BlackCat confirmed that they are affiliates of DarkSide/BlackMatter ransomware gang. They claim to be apolitical in regards to geopolitical relations and to refrain from attacking medical institutions and hospitals.

The group has adopted the popular double extortion

Webinars

Resources

Videos

News

All Posts

- **Sophisticated Ransomware:** BlackCat has been called "2021's most sophisticated ransomware
- **High Severity**: The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
- **Developed in Rust**: BlackCat was developed in rust which is unusual for ransomware.
- **Triple Extortion**: The BlackCat operators used double extortion and sometimes triple extortion to make victims pay the ransom
- **Shared Infrastructure with LockBit**: BlackCat has shared infrastructure, and used similar tools and naming conventions as the LockBit ransomware.
- **Detected and Prevented**: The Cybereason XDR Platform fully detects and prevents the Lorenz ransomware.

TECHNICAL ANALYSIS

BREAKING DOWN BLACKCAT RANSOMWARE

The BlackCat ransomware has both Windows and Linux variants. The ransomware includes multiple execution flags which grant its operators control over operations like whether to stop executions of virtual machines or if the ransomware should change the desktop wallpaper or not:

```
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
```

BlackCat help menu

In order to execute properly, BlackCat must be executed with the "--access-token" flag, although the value of the string that is passed on to it can be any string.

exploit)

- Adjusting access token token privileges

Next, BlackCat checks the UUID (universally unique identifier) of the machine by running a WMI command, which is used later for the recovery URL in the ransom note:

- *wmic csproduct get UUID*

BlackCat enables local and remote *symbolic links* on the infected machine. A symbolic link is a type of file that contains a reference to another file. This is probably done to make sure that the ransomware is able to follow shortcuts on the machine in order to find the original file to encrypt:

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

BlackCat also attempts to stop Internet services on the infected machine using the iisreset.exe:

- *iisreset.exe /stop*

The ransomware changes the number of outstanding requests that can be maintained. An outstanding request is a request that is still waiting for a response. These are used when performing SMB requests, the change is probably done to raise the number of possible PsExec requests the machine could make so the ransomware may spread:

- *reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f*

Then, it deletes the shadow copies from the infected machine using both “vssadmin” and “wmic”:

- *vssadmin.exe delete shadows /all /quiet*
- wmic shaodwcopy delete

BlackCat Execution as seen in the Cybereason XDR Platform

BlackCat enumerates all local disk partitions on the infected machine, and any hidden partition that is found is mounted in order to make it possible to encrypt more files.

The ransomware also attempts to propagate through the

clears the machine's event log, by running the following commands:

- *bcdedit /set {default} recoveryenabled No*
- *cmd.exe /c for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"*

In order to maximize the number of encrypted files, BlackCat attempts to kill several processes and services on the machine in order to decrease the number of locked files that are not accessible due to another program (full list in appendix). In addition, BlackCat's configuration includes a list of directories to be excluded from encryption. (see appendix):

BlackCat Configuration

To encrypt the files, BlackCat may use AES or ChaCha20 for encryption, based on the configuration. It drops a ransom note titled : "*RECOVER-[encrypted file extension]- FILES.txt*" in each folder and in the end, the ransomware changes the desktops wallpaper:

Wallpaper after BlackCat change

BlackCat ransom note

LINUX VARIANT SPECIFIC COMMANDS

The Linux variant was observed executing commands in order to delete VMware ESXi snapshots. The ransomware generates a list of running virtual machines:

- *esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list*

Each virtual machine is then terminates using the command:

- *awk -F "\"*,\"*" '{system("esxcli vm process kill --type=force --world-id="$1)}'*

Finally all snapshots of the virtual machines are deleted:

- *for i in `vim-cmd vmsvc/getallvms| awk '{print$1}'`;do vim-cmd vmsvc/snapshot.removeall $i & done*

The launcher contains the following PDB path:

- *"D:\my\Documents\Visual Studio 2019\setup\obj\Release\setup.pdb"*.

When searching for files that share the PDB, we encountered several additional malware with the same name that have remarkable similarities to the BlackCat launcher. When examining the code and Infrastructure of these malware, we see overlaps between BlackCat infrastructure and LockBit infrastructure.

BLACKCAT LAUNCHER

The launcher downloads the BlackCat executable from the C2 and executes it using the "--access-token" argument, which is required in order to run BlackCat:

BlackCat Launcher code

Additionally, the tool collects basic profiling information about the infected machine and uploads it to the C2. The information collected is:

- A screen capture
- Username
- OS name
- OS language
- Timezone
- Windows UUID
- Keyboard language
- Installed users
- Installed software
- Drives

LOCKBIT PROFILER TOOL

The Nocturnus team discovered striking similarities with the BlackCat launcher and a profiler associated with LockBit ransomware. The profiler variants which are linked to LockBit use almost the same code as the BlackCat launcher, except for slight variations.

see connections and similarities in the IP addresses, URI structure, and file names:

BlackCat and LockBot infrastructure comparison

All the IP addresses that are used by the BlackCat launcher and LockBit profiler, share the URI paths “files” and “upload”. In addition, BlackCat and LockBit samples sometimes share file names. For example, we observed BlackCat samples with the name:

- “*test_**4mmc**_x86_32_windows_encrypt_app.exe*” and LockBit samples with the name “**4mmc.exe**”

Another example of shared file names is a LockBit sample named “*screensaver.exe*”, which is also the default name used for the BlackCat executable that is downloaded using the launcher:

“Screensaver.exe” used in BlackCat Launcher

This connection between some of the tools and infrastructure between BlackCat ransomware and LockBit ransomware might indicate sharing of code and tools between cybercriminals, or there could be individuals that worked for both ransomware operators:

BlackCat and LockBit Infrastructure map

CYBEREASON DETECTION AND PREVENTION

The Cybereason XDR Platform is able to prevent the execution of the BlackCat Ransomware using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and next-gen antivirus (NGAV) capabilities.

Additionally, when the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and generates a MalOp for it:

Cybereason Detects and Blocks BlackCat Ransomware

- **Enable Anti-Malware Feature on Cybereason NGAV**: Set Cybereason Anti-Malware mode to Prevent and set the detection mode to Moderate and above - more information for Cybereason customers can be found here
- **Keep Systems Fully Patched**: Make sure your systems are patched in order to mitigate vulnerabilities
- **Regularly Backup Files to a Remote Server**: Restoring your files from a backup is the fastest way to regain access to your data
- **Use Security Solutions**: Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

MITRE ATT&CK BREAKDOWN

Reconnaissance	Execution	Privilege Escalation	Discovery	Lateral Movement	Collection	Impact
Gather Victim Host Information	Command-line interface	Signed Binary Proxy Execution	Process Discovery	Lateral Tool Transfer	Data from Local System	Data Encrypted for Impact
		Access Token Manipulation	System Service Discovery			Service Stop
		Exploitation for Privilege Escalation	File and Directory Discovery			Inhibit System Recovery

APPENDIX

Process to kill list:

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 ,

Services to kill 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 , GxClMgr , GXMMM , GxVssHWProv , GxFWD , SAPService , SAP , SAP$, SAPD$, SAPHostControl , SAPHostExec , QBCFMonitorService , QBDBMgrN , QBIDPService , AcronisAgent , VeeamNFSSvc , VeeamDeploymentService , VeeamTransportSvc , MVArmor , MVarmor64 , VSNAPVSS , AcrSch2Svc

ABOUT THE RESEARCHERS

Tom Fakterman

Tom Fakterman, Cyber Security Analyst with the Cybereason Nocturnus Research Team, specializes in protecting critical networks and incident response. Tom has experience in researching malware, computer forensics and developing scripts and tools for automated cyber investigations.

Ohav Peri

Ohav Peri, cyber security analyst with the Cybereason Nocturnus Research Team, focusing on malware analysis and defense platforms research. Ohav began his career as a security researcher and software engineer in the intelligence corps of the military forces.

SHARE

ABOUT THE AUTHOR

reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus →

Related Posts

THREAT ANALYSIS REPORT: Ragnar Locker Ransomware Targeting the Energy Sector

Ragnar Locker is a ransomware family with security evasion capabilities which is targeting the energy sector and recently claimed to have breached DESFA, a Greek pipeline company...

Cybereason vs. Black Basta Ransomware

In just two months, Black Basta has added nearly 50 victims to their list, making them one of the more prominent ransomware gangs. The attackers infiltrate and move laterally throughout the network in a fully-developed RansomOps attack. The Cybereason Nocturnus Team assesses the threat level as HIGH SEVERITY given the destructive potential of the attacks...