

TTPs Associated With a New Version of the...

securityscorecard.com/blog/ttps-associated-with-new-version-of-blackcat-ransomware



1. [Blog](#)

TTPs Associated With a New Version of the BlackCat Ransomware

Vlad Pasca, Senior Malware & Threat Analyst

Posted on September 6th, 2022

Executive summary

The BlackCat/ALPHV ransomware is a complex threat written in Rust that appeared in November 2021. In this post, we describe a real engagement that we recently handled by giving details about the tools, techniques, and procedures (TTPs) used by this threat actor. Firstly, the attacker targeted an unpatched Microsoft Exchange server and successfully dropped webshells on the machine. After getting initial access, the ransomware installed the MobaXterm software and then started to dump the credentials using Mimikatz or by creating an LSASS dump file with Process Hacker. The SoftPerfect Network scanner was used to perform network discovery. Before running the ransomware executable, the TA compressed the targeted files using WinRAR or 7zip and then exfiltrated them using rclone and MEGAsync.

Our Digital Forensics and Incident Response (DFIR) team was engaged in investigating a ransomware infection. We were able to determine that the ransomware involved is a new version of the BlackCat ransomware, based on the fact that the malware added new command line parameters that were not documented before.

As shown in Figure 1, the ransomware added a parameter called “--safeboot” that is used to reboot in Safe Mode. Whether the malware is running with the “--sleep-restart” parameter, the process sleeps for a specified number of seconds and then restarts the machine.

```
--log-file <LOG_FILE>
  Enable logging to specified file

--no-impers
  Do not spawn impersonated processes on Windows

--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

--prop-file <PROP_FILE>
  Propagate specified file

--propagated
  Run as propagated process

--safeboot
  Reboot in Safe Mode before running on Windows

--safeboot-instance
  Run as safeboot instance on Windows

--safeboot-network
  Reboot in Safe Mode with Networking before running on Windows

--sleep-restart <SLEEP_RESTART>
  Sleep for duration in seconds after successful run and then restart. (This is soft
  persistence, keeps process alive no longer then defined in --sleep-restart-duration, 24
  hours by default)

--sleep-restart-duration <SLEEP_RESTART_DURATION>
  Keep soft persistence alive for duration in seconds. (24 hours by default)

--sleep-restart-until <SLEEP_RESTART_UNTIL>
  Keep
  soft persistence alive until defined UTC time in millis. (Defaults to 24 hours
  since launch)

--ui
  Show user interface

-v, --verbose
  Log to console
```

Figure 1

A complete analysis of the BlackCat ransomware can be found [here](#).

By accessing the onion link specified in the ransom note called “RECOVER-<extension>-FILES.txt”, the victim is presented with multiple tabs that contain information such as the ransom amount in Bitcoin and Monero, the threat actor’s wallets addresses, a live chat, and a trial decrypt that can be used to decrypt a few files for free (see Figure 2).

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**.

Act quickly to get a **Discount!**

Decrypt App Price

You have **2 days, 10:23:42** until:

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

Discount Price: **\$450000**

Full Price: **\$60000**

Status

Awaiting payment of **\$450000** to one of the following wallets:



Bitcoin	[REDACTED]	\$517500 (?) = 25.184933 BTC
Monero	[REDACTED]	\$450000 = 3433.279927 XMR

< Instructions Data Breach Live-Chat Trial Decrypt >

I wish to pay with
Bitcoin

1. Create a Bitcoin Wallet.
2. Buy **25.184933 BTC** and deposit it to your Bitcoin Wallet.
3. Transfer **25.184933 BTC** to the following Bitcoin Address:
[REDACTED]
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**.

Figure 2

Initial access

According to our analysis, the entry point in the organization was an Exchange server that was vulnerable to Microsoft Exchange vulnerabilities. Multiple webshells have been identified on the impacted server.

Remote access tools

After gaining access to the internal network, the ransomware installed the legitimate tools MobaXterm and mottynew.exe (MobaXterm terminal).

Lateral Movement

As we already know from the malware analysis of the ransomware, BlackCat steals credentials from the victim's environment and incorporates them into its configuration ("credentials" field). Mimikatz was utilized to dump the credentials, and then the malware pivots from one machine to another via Remote Desktop Protocol (RDP).

An old version of the SoftPerfect Network scanner was used to perform network scanning in order to discover additional targets in the local network. Figure 3 reveals the interface of the network scanner:

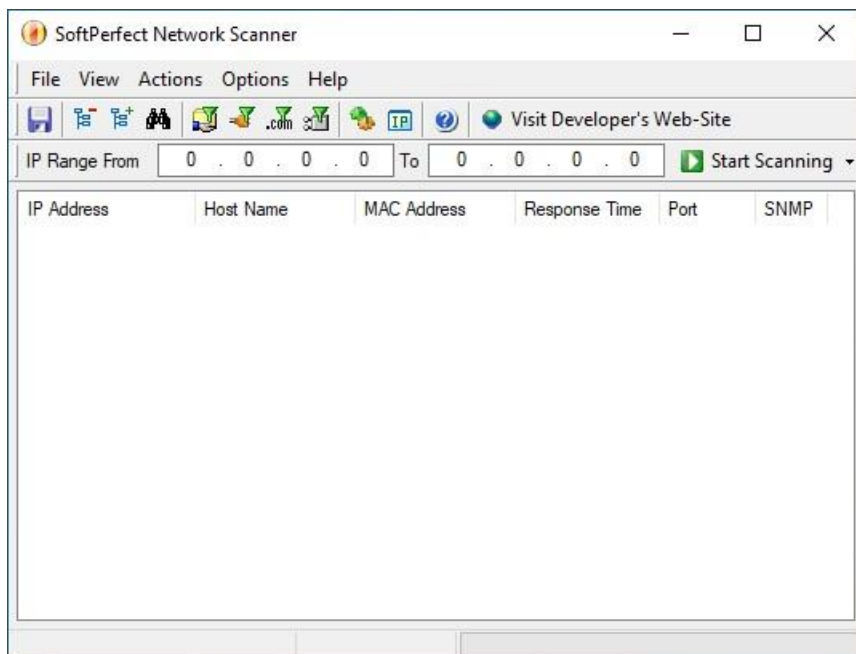


Figure 3

Data exfiltration

Once the threat actor decided which files to exfiltrate, the malware compressed them using WinRAR or 7zip. The ransomware installed a tool called rclone that is utilized to upload data to cloud storage providers. A second tool called MEGAsync is also installed by the process, which can upload data to the MEGA Cloud Storage.

We've also observed the ransomware installing tools such as FileZilla and WinSCP that could be used to perform data exfiltration.

Other tools installed

We've investigated and found out that the ransomware installed the cURL tool to download additional files. Process Hacker was also installed by the malware and could be used to dump the memory of the LSASS process. In the same directory with Process Hacker, the BlackCat ransomware dropped a copy of the PEView tool, which is a viewer for Portable Executable (PE) files.

Conclusion

BlackCat ransomware remains a serious threat because it targets Windows hosts, Linux hosts, and VMWare ESXi. The access token that the malware is running with makes the automated analysis impossible and increases the difficulty of the dynamic malware analysis.

The usage of legitimate tools to perform malicious activities increases the chance of not being detected by endpoint detection and response (EDR) or antivirus software.

About SecurityScorecard

SecurityScorecard offers a 360-degree approach to security prevention and response. For more information, request a demo. SecurityScorecard's threat research and intelligence could be the competitive advantage organizations need to stay ahead of today's fast-moving threat actors.

For more custom insights on a regular basis through our team's 100+ years of combined threat research and investigation experience, or more details on these findings and the other keywords that were provided, please [contact Ranell Gonzales](#) for a discussion of our Cyber Risk Intelligence (CRI) offering. If you have already suffered a breach, SecurityScorecard's Digital Forensics Solutions can empower your post-breach actions.

[Return to Blog](#)