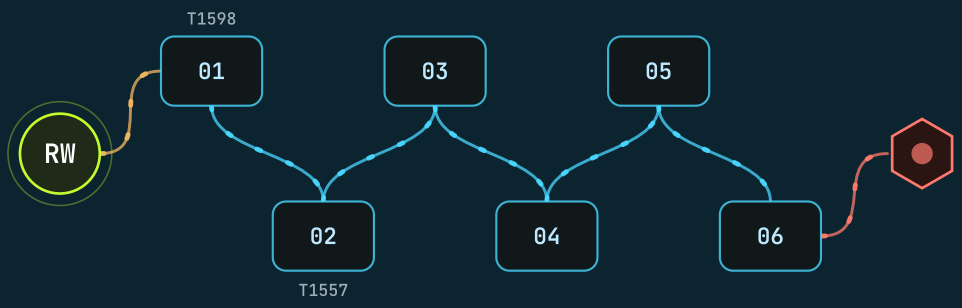


INTELLIGENCE BRIEF

ALPHV BlackCat Stays Dark as Its Change Healthcare Breach Reaches 192.7 Million

ALPHV BlackCat has posted no victims since its March 2024 exit scam, but Change Healthcare now counts 192.7 million people and three US insiders were sentenced in 2026. Require MFA on remote access and vet your vendors.

EDITION
Fall/Winter 2026/2027 Edition
RW-05 · Ransomware group

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a Glance

STATUS

DORMANT

The last ALPHV leak-site post the ransomware.live tracker holds is March 3, 2024, no revival or rebrand turned up in the sources checked, and RansomHub, which held the Change Healthcare data, also went dark on April 1, 2025. [15]

HEADLINE NUMBERS

192.7M

people in the Change Healthcare breach, per its final estimate on the HHS portal [4]

$395.3M

ransom payments reported to FinCEN for ALPHV/BlackCat, 2022 to 2024, the highest of any variant [7]

$22M

ransom UnitedHealth's CEO told Congress he decided to pay [4]

70 months

prison sentence announced July 9, 2026 for a ransomware negotiator tied to BlackCat [2]

KEY FACTS

REPORTED STATUS

Dormant: last leak-site post tracked on March 3, 2024, after an exit scam in which, by its affiliate's account, ALPHV kept the reported $22 million payment [15]

INITIAL ACCESS

Affiliates posed as IT or help desk staff by phone and text to get credentials, and used the Evilginx2 adversary-in-the-middle tool to capture MFA codes and session cookies [8]

PLATFORMS

Encryptor rewritten in the February 2023 Sphynx update to hit Windows, Linux and VMware instances [8]

MONEY

About $395.3 million in payments reported in US bank filings for 2022 to 2024 across 353 incidents, the highest total of any ransomware variant [7]

BIGGEST CASE

Change Healthcare, detected February 21, 2024: 192.7 million people in Change Healthcare's final estimate [4]

PROSECUTIONS

Three US insiders sentenced in 2026: four years each for two of them, announced April 30, and 70 months for the third on July 9 [2]

02 What Happened

ALPHV, also called BlackCat, was a ransomware-as-a-service operation active from 2021 until its operators ran an exit scam in March 2024, and the Justice Department says its affiliates targeted more than 1,000 victims. Its best-known case is Change Healthcare, where an affiliate used compromised credentials on a Citrix portal with no MFA in February 2024 and the breach was later put at 192.7 million people. The brand has stayed dark since, but the affiliates, the help desk playbook and the lessons have not gone away.

- In December 2023 the FBI infiltrated ALPHV's servers; the Justice Department now says its decryption tool saved victims about $99 million, while ALPHV regained its sites, removed limits on whom affiliates could attack, and CISA found healthcare the most commonly victimized sector among nearly 70 leaked victims in the following weeks.
- Change Healthcare detected the attack on February 21, 2024. UnitedHealth's CEO told Congress on May 1, 2024 that a threat actor got in on February 12 with compromised credentials on a Citrix portal that lacked MFA, that he decided to pay the $22 million ransom, and that the payment did not stop the stolen data being used for further extortion.
- ALPHV ran an exit scam in March 2024: the affiliate known as Notchy said on March 3 that ALPHV kept the payment while the data was still with the affiliate, and ALPHV then showed a fake FBI seizure notice that researchers noted was copied from the December 2023 raid (Krebs on Security, March 5, 2024).
- The stolen data went to RansomHub, which demanded a second payment; Change Healthcare's account is that no second payment was made, and RansomHub itself went dark on April 1, 2025.
- FinCEN's December 2025 analysis of Bank Secrecy Act data credits ALPHV/BlackCat with about $395.3 million in reported payments for 2022 to 2024 across 353 incidents, the largest total of any ransomware variant.

- In 2026 the Justice Department sentenced three US cybersecurity professionals tied to ALPHV attacks: two of them to four years each, announced April 30, and a former ransomware negotiator to 70 months on July 9, with the Justice Department saying he passed clients' negotiating positions to BlackCat attackers.

03 How It Works

01 Call the help desk or use a login

MITRE ATT&CK T1598

Affiliates researched a company, then phoned or texted employees posing as IT or help desk staff to obtain credentials; at Change Healthcare the way in was a Citrix remote access portal without MFA, reached with compromised credentials.

02 Capture MFA and build admin access

MITRE ATT&CK T1557

They used the Evilginx2 adversary-in-the-middle tool to take MFA codes and session cookies, created an aadmin account, and generated Kerberos tokens for domain access.

03 Install remote tools and tunnel

AnyDesk, Mega sync and Splashtop were installed ahead of data theft, Plink and Ngrok tunneled traffic, and affiliates claimed Brute Ratel and Cobalt Strike beacons.

04 Disable defenses, steal the data

Affiliates used POORTRY and STONESTOP to terminate security processes, cleared logs, and moved data out through Mega.nz or Dropbox before encryption; some skipped encryption and extorted on stolen data alone.

05 Encrypt Windows, Linux and ESXi

The Sphynx update of February 2023 rewrote the encryptor to cover Windows, Linux and VMware instances, and the ransom note is dropped as RECOVER-(seven-digit extension) FILES.txt.

06 Extort through chat and leaks

Victims received victim-specific emails and links to a live-chat portal, and affiliates offered unsolicited vulnerability reports as an incentive to pay.

04 Who Is at Risk

Healthcare organizations, health insurers and any organization that depends on a single clearinghouse or an outsourced help desk carry the most exposure, because ALPHV affiliates attacked help desks and, after December 2023, healthcare in particular. The brand is dormant, but Microsoft and CISA documented Scattered Spider using ALPHV ransomware in 2023, and the same social engineering persists.

- Hospitals, physician practices and health plans: CISA found healthcare the most commonly victimized sector among ALPHV's nearly 70 leaked victims after December 2023, and the Justice Department cited a doctor's office whose patient data was leaked.
- Any provider that depends on a clearinghouse or billing vendor: Change Healthcare's clearinghouse services were declared fully restored on November 19, 2024, nine months after the attack, and UnitedHealth lent providers more than $9 billion.
- Any organization with a remote access portal, VPN or Citrix gateway that lacks MFA, or a help desk that resets passwords on a phone call.
- Organizations that hire outside ransomware negotiators or incident responders: the Justice Department said a negotiator passed clients' bargaining positions to BlackCat, and CyberScoop reported that five clients of his firm paid ransoms totaling $75.3 million between April and September 2023.

Sectors in scope: healthcare and health insurance, medical devices, physician practices.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 Two US insiders were sentenced. Ryan Goldberg and Kevin Martin pleaded guilty in December 2025 and the Justice Department announced on April 30, 2026 that each received four years for deploying ALPHV BlackCat ransomware in 2023 in exchange for a 20 percent share to ALPHV; the original edition expected sentencing on March 12, 2026.

SOURCE 1

02 A third insider was sentenced. Angelo Martino, a ransomware negotiator who pleaded guilty on April 14, 2026, received 70 months on July 9, 2026; the Justice Department says he was paid by BlackCat attackers for his employer's clients' confidential negotiating positions, about $10 million in his assets were seized, and a restitution hearing was set for September 17, 2026. CyberScoop reports he worked at DigitalMint.

SOURCE 2

03 The Change Healthcare count nearly doubled. Change Healthcare's final estimate, reflected on the HHS breach portal on August 6, 2025, is 192.7 million individuals, against the 100 million the original edition used (190 million was reported in January 2025).

SOURCE 4

04 UnitedHealth's costs are far above the $872 million quoted. Its 2024 annual report shows $2.2 billion of direct response costs and $867 million of business disruption impacts for 2024, and its 2025 annual report shows a $799 million reserve increase in the fourth quarter of 2025 against provider loans and other customer balances.

SOURCE 5

05 The $22 million payment is confirmed. UnitedHealth's CEO told a House subcommittee on May 1, 2024 that he decided to pay, so the original edition's 'neither confirmed nor denied' is out of date.

SOURCE 4

06 RansomHub is gone too. Halcyon records RansomHub as inactive since April 1, 2025, so the 'newer ransomware operation' that held the Change Healthcare data no longer exists, and Change Healthcare's account is that no second payment was made.

SOURCE 11

07 The Nebraska attorney general's December 2024 lawsuit survived a motion to dismiss, reported on November 17, 2025, so a state court will hear claims that Change Healthcare failed to follow reasonable security practices; no OCR finding, penalty or class-action settlement turned up in the sources checked.

SOURCE 4

08 No ALPHV revival was found. The last ALPHV leak-site post in the ransomware.live tracker is March 3, 2024 and no source checked documents a successor brand, so the original edition's expected fourth-generation operation remains a forecast, not an event.

SOURCE 15

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Require phishing-resistant MFA (FIDO2/WebAuthn or PKI-based) on every remote access path: VPN, Citrix and similar gateways, email and all administrative accounts.**

Change Healthcare's entry was a Citrix portal without MFA, and ALPHV affiliates used Evilginx2 to defeat ordinary MFA codes.

02 **Make the help desk verify identity before any password or MFA reset, with a call back to a known number and a manager approval for privileged accounts.**

CISA documents ALPHV affiliates posing as IT or help desk staff by phone and text, and help desk impersonation is still the core of Scattered Spider's playbook.

03 **Inventory every internet-facing remote access portal and every account that can reach it, and lock down or remove any without MFA this week.**

The affiliate had roughly nine days inside Change Healthcare between first access and the ransomware, so a control that blocks the first login is the cheapest defense.

04 **Map your clearinghouse, billing and e-prescribing dependencies, line up an alternate path, and rehearse a multi-week outage with manual claims and a cash-flow bridge.**

Change Healthcare's clearinghouse services were declared fully restored nine months after the attack, and UnitedHealth lent providers more than $9 billion to keep them running.

05 **Keep offline, immutable backups of servers and virtual machines, and test a full restore each quarter.**

ALPHV's encryptor covered Windows, Linux and VMware instances, and a backup on the same network is not a backup.

06 **Run EDR with tamper protection and a 24/7 alert owner, and alert on remote tools such as AnyDesk and Splashtop, tunnels such as Plink and Ngrok, and large uploads to Mega or Dropbox.**

CISA lists those as the steps before ransomware, which is the window in which a SOC can stop an attack; Z7 Solutions™ provides 24/7 monitoring for mid-size organizations, school districts and public agencies.

07 **Vet outside ransomware negotiators and incident-response firms like any vendor that sees your crisis decisions, with background checks, confidentiality and conflict-of-interest terms, and limits on who can see your bargaining position.**

The Justice Department says a negotiator was paid by BlackCat attackers for clients' negotiating positions, and he was sentenced to 70 months.

08 **Decide your ransom policy with counsel before an incident, including a sanctions check, and assume paid data can still be sold or used for a second demand.**

Change Healthcare paid $22 million and the stolen data still reached RansomHub, which demanded more.

07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

FILE	`Ransom note and encrypted-file naming of the form RECOVER-(seven-digit extension) FILES.txt` [8]
BEHAVIOR	New account named aadmin followed by Kerberos token generation for domain access [8]
BEHAVIOR	Phone calls or text messages to staff from callers posing as IT or help desk, followed by logins from the targeted employee's account [8]
BEHAVIOR	Evilginx2 phishing infrastructure used to capture MFA codes, passwords and session cookies [8]
BEHAVIOR	AnyDesk, Mega sync or Splashtop installed on hosts shortly before large uploads to Mega.nz or Dropbox [8]
BEHAVIOR	Victim-specific email addresses used to notify victims of the initial compromise [8]

08 Sources

[1] **Two Americans Who Attacked Multiple US Victims Using ALPHV BlackCat Ransomware Sentenced** U.S. Department of Justice · April 30, 2026. https://www.justice.gov/opa/pr/two-americans-who-attacked-multiple-us-victims-using-alphv-blackcat-ransomware-sentenced

[2] **Florida Ransomware Negotiator Who Extorted and Attacked Multiple US Victims Sentenced to Prison** U.S. Department of Justice · July 9, 2026 (updated July 10, 2026). https://www.justice.gov/opa/pr/florida-ransomware-negotiator-who-extorted-and-attacked-multiple-us-victims-sentenced-prison

[3] **DigitalMint ransomware negotiator Angelo Martino sentenced** CyberScoop · July 9, 2026. https://cyberscoop.com/digitalmint-ransomware-negotiator-angelo-martino-sentenced/

[4] **Change Healthcare responding to cyberattack (running timeline of notices, testimony, OCR portal updates and litigation)** HIPAA Journal · latest entry November 17, 2025. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/

[5] **UnitedHealth Group Form 10-K for fiscal year 2024** UnitedHealth Group (SEC filing) · filed February 27, 2025. https://www.sec.gov/Archives/edgar/data/731766/000073176625000063/unh-20241231.htm

[6] **UnitedHealth Group Form 10-K for fiscal year 2025** UnitedHealth Group (SEC filing) · filed March 2, 2026. https://www.sec.gov/Archives/edgar/data/731766/000073176626000062/unh-20251231.htm

[7] **Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024** FinCEN (US Treasury) · December 2025. https://www.fincen.gov/system/files/2025-12/FTA-Ransomware.pdf

[8] **#StopRansomware: ALPHV Blackcat (AA23-353A)** FBI, CISA and HHS · December 19, 2023; updated February 27, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

[9] **FBI disrupts BlackCat ransomware operation, creates decryption tool** BleepingComputer · December 19, 2023. https://www.bleepingcomputer.com/news/security/fbi-disrupts-blackcat-ransomware-operation-creates-decryption-tool/

[10] **BlackCat Ransomware Group Implodes After Apparent $22M Ransom Payment by Change Healthcare** Krebs on Security · March 5, 2024. https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/

[11] **Threat group profile: RansomHub** Halcyon · updated September 22, 2025. https://www.halcyon.ai/threat-group/ransomhub

[12] **The State of Ransomware, Q2 2026** Check Point Research · August 13, 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q2-2026/

[13] **Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction** Microsoft Threat Intelligence · October 25, 2023. https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/

[14] **MGM Resorts International Form 8-K, Item 7.01 cybersecurity update** MGM Resorts International (SEC filing) · October 5, 2023. https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

[15] **ALPHV and RansomHub victim records (public API, Z7 review of first and last posts)** ransomware.live · retrieved October 13, 2026. https://api.ransomware.live/v2/groupvictims/alphv

[16] **Change Healthcare cyberattack updates (hospital survey results, March 15, 2024)** American Hospital Association · page accessed October 13, 2026. https://www.aha.org/change-healthcare-cyberattack-updates

[17] **#StopRansomware: Scattered Spider (AA23-320A)** FBI, CISA and international partners · November 16, 2023; updated July 29, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

NEXT STEP

What does this mean for your security?

Bring your questions about ALPHV BlackCat, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

Qilin still tops most ransomware counts
More from the edition · z7solutions.com/z7-cyber/qilin/

Qilin still hits hospitals and infrastructure
More from the edition · z7solutions.com/z7-cyber/qilin-part-2/

LockBit 5.0 returns after Operation Cronos
More from the edition · z7solutions.com/z7-cyber/lockbit/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A SECURITY CONVERSATION Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.