BlackCat / ALPHV: Innovation, Betrayal, and the Collapse of a Ransomware Empire

Infosources™

August 19, 2025

BlackCat, also known as ALPHV, emerged in late 2021 as one of the most technically innovative ransomware groups, pioneering the use of Rust programming language for cross-platform attacks and building a professionalized Ransomware-as-a-Service model. Its operations leveraged capable affiliates and intrusion partners to target corporations, healthcare, and critical services worldwide. Yet its downfall was not driven solely by law enforcement, but by an unprecedented act of betrayal: in March 2024, the group carried out a $22 million exit scam against one of its own affiliates. This collapse exposed the fragility of trust within the ransomware economy and reshaped perceptions of stability in the RaaS ecosystem.

Origins and Innovation

BlackCat, also known as ALPHV, emerged in late 2021 and quickly distinguished itself from other ransomware groups. Its operators adopted Rust, a programming language rarely used in cybercrime at the time, which gave the malware cross-platform compatibility and greater flexibility for customization. This technical choice made it easier to adapt payloads across Windows and Linux systems, granting affiliates a broader operational range. Analysts widely assessed BlackCat as the successor to earlier, now-dismantled syndicates such as REvil and DarkSide, inheriting both code lineage and an experienced operator base. The group also adopted a competitive revenue-sharing model, offering affiliates lower commissions than rival programs, which helped it secure a strong network of partners in the crowded Ransomware-as-a-Service (RaaS) ecosystem.

Operational Milestones

Within months, BlackCat demonstrated its ability to execute high-profile and disruptive attacks. Targets included Moncler, Swissport, multiple hospitals, and international law firms — incidents that proved both the technical proficiency of its tools and the professionalism of its affiliates. The group gained further visibility in 2023 when it partnered with Scattered Spider, an intrusion set with strong social engineering capabilities. This alliance gave BlackCat access to some of the most significant ransomware incidents of the year, particularly in the gaming and hospitality sectors. The dual compromises of MGM Resorts and Caesars Entertainment highlighted the group's operational maturity and the strategic leverage of its extortion model. While Caesars chose to pay, MGM refused and suffered prolonged business disruption, demonstrating the high-stakes decisions victims face under ransomware pressure.

Law Enforcement Pressure

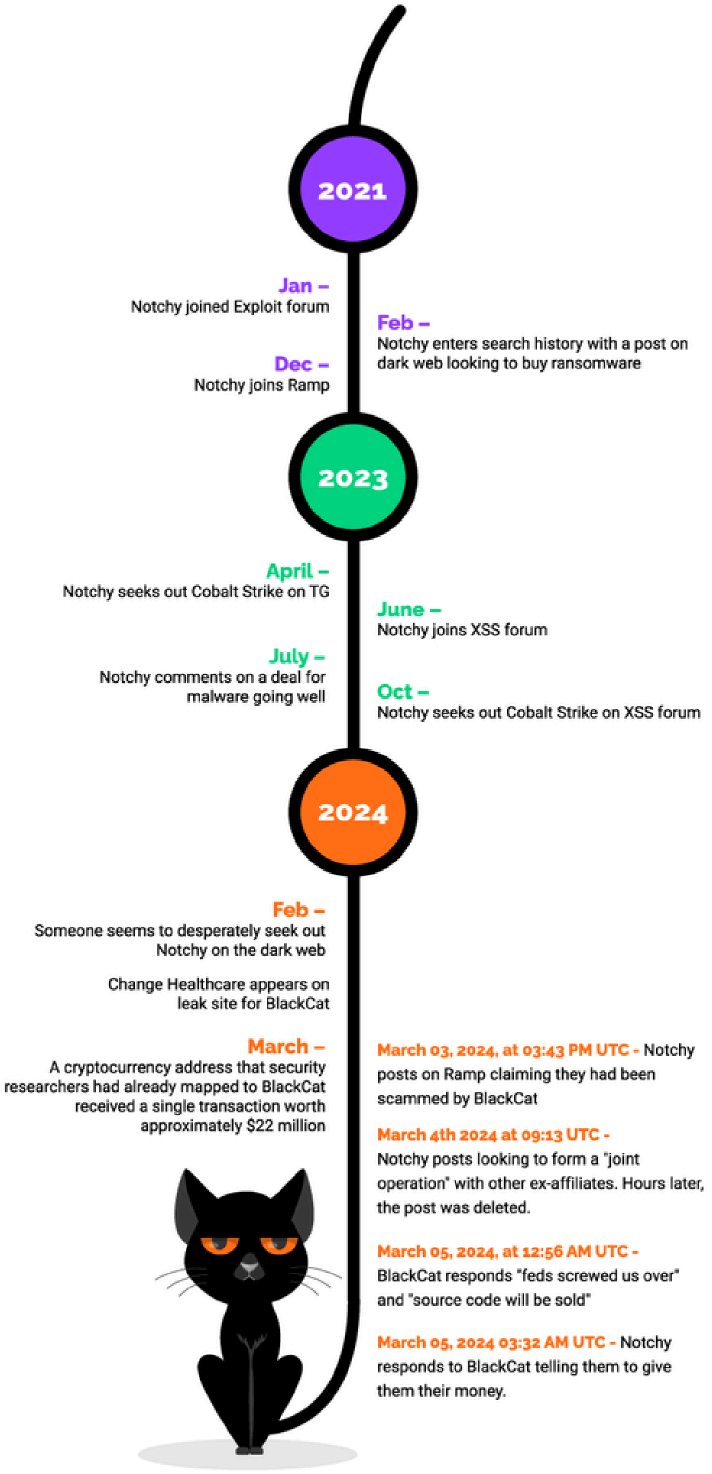
BlackCat's Operational resilience was sustained through a decentralized Tor/I2P architecture, but it rapid rise inevitably drew the attention of law enforcement. In December 2023, the FBI and Europol conducted a partial takedown of the group's infrastructure, seizing servers and releasing a decryption tool for victims. The disruption briefly stalled operations, but BlackCat quickly re-established its command-and-control network. In response to the crackdown, the operators escalated their tactics by removing earlier restrictions on sensitive sectors, effectively broadening their scope of potential targets. This move signaled resilience, but also desperation, as BlackCat demonstrated a willingness to defy law enforcement pressure by doubling down on its operations.

The Change Healthcare Affair

The defining event in BlackCat's trajectory occurred in early 2024. One of its affiliates, operating under the alias "Notchy," successfully compromised Change Healthcare and secured a $22 million ransom payment. Instead of following the established revenue-sharing model, the BlackCat core operators seized the entire payment, excluding the affiliate from any proceeds. This act of betrayal — unprecedented at such scale in the RaaS market — provoked immediate outrage. Notchy responded by publicly disclosing details of the operation on underground forums, exposing internal disputes and revealing how the syndicate had diverted funds. The incident fractured BlackCat's credibility and destabilized trust across the broader ransomware ecosystem.

Info

Notchy refers to a cybercriminal affiliate associated with the BlackCat ransomware group, who publicly claimed to have been cheated out of their share of a ransom payment after a cyberattack on Change Healthcare. This incident highlights the internal conflicts and trust issues within ransomware groups.



Jan – Notchy joined Exploit forum

Feb – Notchy enters search history with a post on dark web looking to buy ransomware

Dec – Notchy joins Ramp

April – Notchy seeks out Cobalt Strike on TG

June – Notchy joins XSS forum

July – Notchy comments on a deal for malware going well

Oct – Notchy seeks out Cobalt Strike on XSS forum

Feb – Someone seems to desperately seek out Notchy on the dark web

Change Healthcare appears on leak site for BlackCat

March – A cryptocurrency address that security researchers had already mapped to BlackCat received a single transaction worth approximately $22 million

March 03, 2024, at 03:43 PM UTC - Notchy posts on Ramp claiming they had been scammed by BlackCat

March 4th 2024 at 09:13 UTC - Notchy posts looking to form a "joint operation" with other ex-affiliates. Hours later, the post was deleted.

March 05, 2024, at 12:56 AM UTC - BlackCat responds "feds screwed us over" and "source code will be sold"

March 05, 2024 03:32 AM UTC - Notchy responds to BlackCat telling them to give them their money.

Exit Scam and Fallout

In March 2024, BlackCat officially announced the termination of its operations. The group laundered the stolen funds through cryptocurrency mixers and vanished, effectively conducting an exit scam against both its affiliates and the wider cybercriminal community. The fallout was immediate: forum discussions were dominated by anger, affiliates demanded stronger escrow mechanisms, and rival operators attempted to capitalize on the breach of trust. Within weeks, data stolen by BlackCat began resurfacing under a new collective branding, “RansomHub,” suggesting either a rebranding effort by the same operators or the opportunistic reuse of assets by competing actors.

Info

An exit scam is when a criminal group or organization — often in the cybercrime world — suddenly disappears with the money or assets of its partners, clients, or affiliates instead of fulfilling its obligations.

Strategic Impact

The collapse of BlackCat marked a watershed moment in the ransomware landscape. By betraying its own affiliates, the group undermined the trust model that sustained the RaaS economy. Affiliates began pressing for new safeguards, such as third-party escrow systems, to guarantee payouts and reduce dependency on operator goodwill. The episode also demonstrated the volatility of RaaS partnerships, where greed and mistrust can unravel even the most sophisticated operations. Despite its dissolution, most analysts assess that BlackCat's core operators remain active and are likely to reemerge under new branding. Their technical expertise, combined with the underground reputation they built before the exit scam, suggests they will attempt to rebuild influence in the evolving ransomware ecosystem.