Everything You Need To Know About BlackCat (AlphaV)

By Aaron Sandeen

Published: 2022-09-08 · Archived: 2026-04-05 18:29:08 UTC

Source: Nils Jacobi via Alamy Stock Photo

Did you know that the BlackCat ransomware group has successfully breached more than 60 organizations in a couple of months? Government, healthcare, or public utilities — the group has made it abundantly clear that everyone is a target and will demand ransoms that can reach into the millions. Our own research shows that the BlackCat cybergroup favors exploiting vulnerabilities found in Windows operating systems, Exchange servers, and Secure Mobile Access products. Let's break down their tactics and ways to defend against their attacks.

Who Is BlackCat?

BlackCat (also known as AlphaV, AlphaVM, ALPHV, ALPHV-ng, or Noberus) is a relative newcomer to the ransomware scene but quickly gained notoriety during its first active months. Discovered in November 2021, the group was feared for its sophistication. Experts and researchers believe the group may be associated with other advanced-persistent threat (APT) groups like Conti, DarkSide, Revil, and BlackMatter.

BlackCat: The Brief

BlackCat has been observed to have the knowledge to exploit these five vulnerabilities: CVE-2016-0099 (High), CVE-2019-7481 (High), CVE-2021-31207 (High), CVE-2021-34473 (Critical), and CVE-2021-34523 (Critical). CVE-2021-34473 and CVE-2021-34523, are both critical vulnerabilities found in Microsoft Exchange Server and require immediate remediation.

Although CVE-2021-31207, CVE-2021-34473, and CVE-2021-34523 have high severity scores, they should still take priority in patching efforts for their potential use in vulnerability chaining attacks and have multiple known threat actor associations.

CVE-2019-7481 is a SQL injection vulnerability that affected SonicWall SMA100 version 9.0.0.3 and earlier. As this version is no longer supported by the vendor, an immediate version upgrade is advised.

How BlackCat Operates

BlackCat's entry into an organization's network begins by leveraging stolen access credentials. At the pace security breaches occur, it is difficult to gauge how many credentials are stolen or leaked to the public every year, but about 20,000 (or 50%) of security incidents in 2021 were initiated by stolen credentials.

After initial access is made, BlackCat or similar ransomware groups silently collect information, mapping the entire network and manipulating accounts for deeper access. Vendor-specific ransomware is then created based on the intelligence gathered during the initial phase of the attack, and security/backup systems are disabled or made to appear to be functioning as expected. The final step is to execute the ransomware and drop ransom notes on their unsuspecting victims.

Notable Characteristics

What sets BlackCat apart from other ransomware groups is its ability to create highly tailored executables for the intended target that contribute to its reputation for sophisticated attack patterns across environments.

BlackCat develops its tools with the Rust programming language, which brings greater stability and integration possibilities. By taking advantage of command-line-driven and human-operated code, BlackCat brings a higher level of configuration.

Its ransomware can then encrypt victims' data with four types of encryption methods. The code can be deployed across different platforms, including Linux- and Windows-based systems.

BlackCat also engages in the practice of selling its services to others, or commonly known as ransomware-as-a-service. Although BlackCat is the first known group to develop its ransomware with the Rust programming language, its use is now becoming common in threat circles. The group is further known for its speedy data encryption, which gives victims a smaller window and fewer chances of preventing prolonged damage and disruption to their services. The group's public leak site makes it simple for users to search their database of stolen information by victim name, password, and document type.

How Organizations Can Prevent a BlackCat Attack

The ransomware group is quickly becoming the preferred ransomware-as-a-service provider for many threat

actors today. Although the true extent of BlackCat's havoc may never fully be known, more than 60 incidents involving the group have pushed the FBI to release an advisory warning of the group's potential danger.

Keeping this information in mind, here are some actions businesses and organizations can take to protect themselves from a ransomware attack.

- Patch vulnerabilities that are known to be exploited by the group, like the ones listed at the top of this article. Make sure unused network ports are properly protected.
- Deploy multifactor authentication for all users, require consistent identity verification, and routinely refresh passwords.
- Regularly perform attack surface management scans to identify exposures within organization assets like servers, applications, and cloud-connected deployments.
- Consider a professional penetration test of company networks to find unknown exposures.
- Maintain separate backup data to avoid contamination in the event of a ransomware attack.

Although the threat landscape evolves and BlackCat's methods adapt over time, organizations have a responsibility to consistently monitor their networks and patch vulnerabilities accordingly. Many vulnerabilities, like CVE-2016-0099 (found in Microsoft Windows), have been known for years and yet are still exploited today. When it comes to ransomware groups, give them an inch, and they will take a mile.

About the Author

CEO & Co-Founder, Securin

Aaron Sandeen is the CEO and co-founder of Securin (formerly Cyber Security Works), a Department of Homeland Security-sponsored company focused on helping leaders proactively increase their resilience against

ever-evolving security threats on-premises and in the cloud. Aaron leads Securin in providing intelligent and actionable security insights at every layer of company operations.
