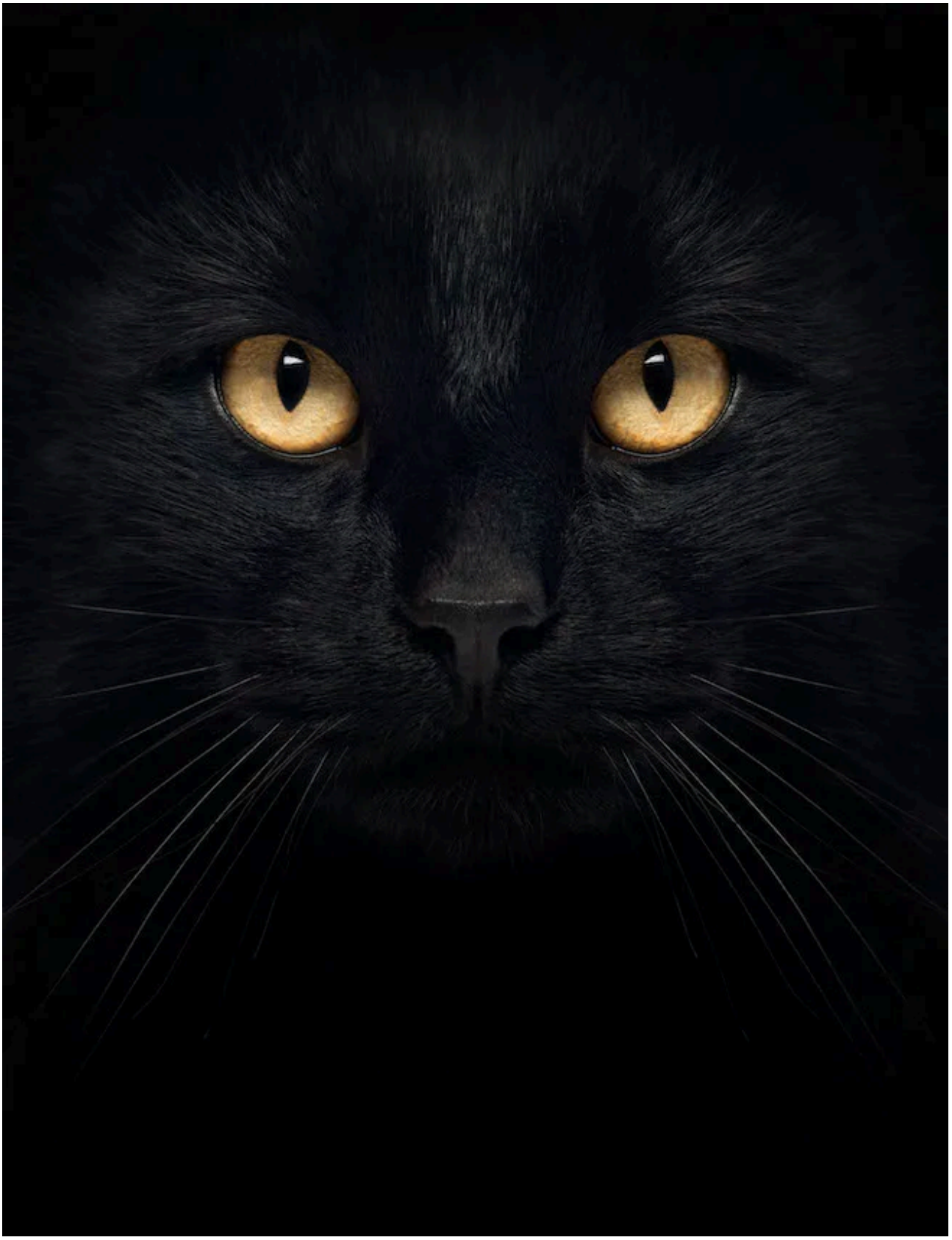
BlackCat Purveyor Shows Ransomware Operators Have 9 Lives

By Robert Lemos

Published: 2022-04-07 · Archived: 2026-04-05 17:55:26 UTC



Source: Life on white via Alamy Stock Photo

A ransomware group boasting its members come from now-shuttered groups BlackMatter and REvil has emerged from the shadows to launch a new ransomware-as-a-service, already attacking an enterprise resource planning

(ERP) service provider and an industrial firm, new research shows.

The group, known as ALPHV, and its BlackCat malware have already infected "numerous corporate victims," endpoint security firm Kaspersky said in an initial analysis posted on April 7. The operators of the new group advertise themselves as the strongest option to replace BlackMatter and REvil following international takedowns of those ransomware groups and their infrastructures. Kaspersky researchers have detected signs that at least some of the members likely had roles in a previous group, BlackMatter.

The exact division of activities between the new group, its affiliates, and other cybercriminal services is unclear, says Kurt Baumgartner, principal security researcher at Kaspersky.

"In all likelihood, the overall set of global BlackCat incidents is performed by a mix of both the group maintaining the code and service, and affiliates performing their own work," he says. "Some of that work can be broken down further, too, into access brokers and penetration efforts performed by the individual groups."

The analysis — and the strong hint that at least some of the operators may have been part of BlackMatter — shows that taking down ransomware groups' infrastructure does not stop them from again setting up shop.

In the case of ALPHV, Kaspersky researchers discovered that the group used a private tool, dubbed Fendr, that has only been used by BlackMatter in the past. ALPHV used the tool to exfiltrate data from corporate victims in December 2021 and January 2022 before deploying ransomware, in a popular tactic known as double extortion.

"Our telemetry suggests that at least some members of the new BlackCat group have links to the BlackMatter group, because they modified and reused a custom exfiltration tool we call Fendr and which has only been observed in BlackMatter activity," Kaspersky stated in the threat brief. "This use of a modified Fendr, also known as ExMatter, represents a new data point connecting BlackCat with past BlackMatter activity."

Malware Coders Take a Shine to Rust

The group is one of the few that has written their tools in the popular, but still uncommon, programming language Rust, which allows them to quickly compile tools for multiple platforms, Kaspersky stated in its blog post. Rust allows the group to release one version for Windows and Linux, because of cross-compilation, and has significant security checks to reduce the incident of vulnerabilities.

"Rust is a cross-compilation language, so a number of BlackCat Linux samples quickly appeared in the wild shortly after their Windows counterparts," the researchers stated in the analysis. Other security firms have seen an increase in Linux malware in the past year.

Kaspersky has detected BlackCat activity against a Middle Eastern provider of enterprise resource planning (ERP) services, with the attackers attempting to steal credentials as well as encrypt the drives. A second attack — against an oil, gas, mining, and construction company in South America — included the use of the Fendr exfiltration tool.

REvil and BlackMatter Redux?

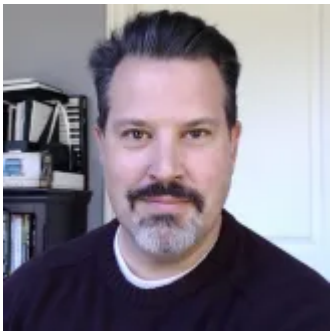
Divining the composition of the current group is a complex task, because ALPHAV is a collection of developers, RaaS services, affiliates, negotiators, and cash-out support, says Baumgartner. Could the ALPHAV group just be an affiliate who created their own organization and decide to use the REvil and BlackMatter brands for name recognition?

"It's possible, and certainly, 'they' — ALPHAV — claim to be composed of multiple parts of various past ransomware schemes including REvil and BlackMatter, but at the same time, they are completely unreliable sources with bad agendas of their own," he says. "I will say that it's clear for at least a portion of the BlackCat activity, there is a definitive lineage back to BlackMatter activity."

While both REvil and BlackMatter have been linked to the Russian actors, Baumgartner could not say whether ALPHV is itself made up of Russian nationals. Previous research has connected both to other groups such as DarkSide and LockBit 2.0.

Kaspersky has been the focus of a debate over whether the firm's software could pose a threat to national security. In 2017, Russian cyber-espionage operators stole classified cyberattack and defense tools from the home computer of a National Security Agency contractor by exploiting Kaspersky's security software. The US government has since banned the software, but the issue has resurfaced with Russia's invasion of Ukraine. According to a report in The Wall Street Journal, the Biden administration is debating whether to sanction the firm.

About the Author



Contributing Writer

Veteran technology journalist of more than 20 years. Former research engineer. Written for more than two dozen publications, including CNET News.com, Dark Reading, MIT's Technology Review, Popular Science, and Wired News. Five awards for journalism, including Best Deadline Journalism (Online) in 2003 for coverage of the Blaster worm. Crunches numbers on various trends using Python and R. Recent reports include analyses of the shortage in cybersecurity workers and annual vulnerability trends.
