Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant

Published: 2023-12-18 · Archived: 2026-04-06 15:33:27 UTC

The Justice Department announced today a disruption campaign against the Blackcat ransomware group — also known as ALPHV or Noberus — that has targeted the computer networks of more than 1,000 victims and caused harm around the world since its inception, including networks that support U.S. critical infrastructure.

Over the past 18 months, ALPHV/Blackcat has emerged as the second most prolific ransomware-as-a-service variant in the world based on the hundreds of millions of dollars in ransoms paid by victims around the world. Due to the global scale of these crimes, multiple foreign law enforcement agencies are conducting parallel investigations.

The FBI developed a decryption tool that allowed FBI field offices across the country and law enforcement partners around the world to offer over 500 affected victims the capability to restore their systems. To date, the FBI has worked with dozens of victims in the United States and internationally to implement this solution, saving multiple victims from ransom demands totaling approximately $68 million. As detailed in a search warrant unsealed today in the Southern District of Florida, the FBI has also gained visibility into the Blackcat ransomware group's computer network as part of the investigation and has seized several websites that the group operated.

"In disrupting the BlackCat ransomware group, the Justice Department has once again hacked the hackers," said Deputy Attorney General Lisa O. Monaco. "With a decryption tool provided by the FBI to hundreds of ransomware victims worldwide, businesses and schools were able to reopen, and health care and emergency services were able to come back online. We will continue to prioritize disruptions and place victims at the center of our strategy to dismantle the ecosystem fueling cybercrime."

"The FBI continues to be unrelenting in bringing cybercriminals to justice and determined in its efforts to defeat and disrupt ransomware campaigns targeting critical infrastructure, the private sector, and beyond," said FBI Deputy Director Paul Abbate. "Helping victims of crime is the FBI's highest priority and is reflected here in the provision of tools to assist those victimized in decrypting compromised networks and systems. The FBI will continue to aggressively pursue these criminal actors wherever they attempt to hide and ensure they are brought to justice and held accountable under the law."

"At the Justice Department, we prioritize victim safety and security," said Acting Assistant Attorney General Nicole M. Argentieri of the Justice Department's Criminal Division. "In this case, agents and prosecutors worked tirelessly to restore victim networks, but these actions are not the culmination of our efforts, they are just the beginning. Criminal actors should be aware that the announcement today is just one part of this ongoing effort. Going forward, we will continue our investigation and pursue those behind Blackcat until they are brought to justice."

“Today’s announcement highlights the Justice Department’s ability to take on even the most sophisticated and prolific cybercriminals,” said U.S. Attorney Markenzy Lapointe for the Southern District of Florida. “As a result of our office’s tireless efforts, alongside FBI Miami, U.S. Secret Service, and our foreign law enforcement partners, we have provided Blackcat’s victims, in the Southern District of Florida and around the world, the opportunity to get back on their feet and to fortify their digital defenses. We will continue to focus on holding the people behind the Blackcat ransomware group accountable for their crimes.”

According to the unsealed warrant, Blackcat actors have compromised computer networks in the United States and worldwide. The disruptions caused by the ransomware variant have affected U.S. critical infrastructure – including government facilities, emergency services, defense industrial base companies, critical manufacturing, and healthcare and public health facilities – as well as other corporations, government entities, and schools. The loss amount globally is in the hundreds of millions and includes ransom payments, destruction and theft of proprietary data, and costs associated with incident response.

Blackcat uses a ransomware-as-a-service model in which developers are responsible for creating and updating ransomware and for maintaining the illicit internet infrastructure. Affiliates are responsible for identifying and attacking high-value victim institutions with the ransomware. After a victim pays, developers and affiliates share the ransom.

Blackcat actors employ a multiple extortion model of attack. Before encrypting the victim system, the affiliate will exfiltrate or steal sensitive data. The affiliate then seeks a ransom in exchange for decrypting the victim’s system and not publishing the stolen data. Blackcat actors attempt to target the most sensitive data in a victim’s system to increase the pressure to pay. Blackcat actors rely on a leak site available on the dark web to publicize their attacks. When a victim refuses to pay a ransom, these actors commonly retaliate by publishing stolen data to a leak website where it becomes publicly available.

The FBI Miami Field Office is leading the investigation.

Trial Attorneys Christen Gallagher and Jorge Gonzalez of the Criminal Division’s Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Kiran Bhat and Brooke Watson for the Southern District of Florida are handling the case.

The Justice Department also recognizes the critical cooperation of Germany’s Bundeskriminalamt and Zentrale Kriminalinspektion Göttingen, Denmark’s Special Crime Unit, and Europol. Significant assistance was provided by the U.S. Secret Service and the U.S. Attorney’s Office for the Eastern District of Virginia. The Justice Department’s Office of International Affairs and the Cyber Operations International Liaison also provided significant assistance. Additionally, the following foreign law enforcement authorities provided substantial assistance and support: the Australian Federal Police, the United Kingdom’s National Crime Agency and Eastern Region Special Operations Unit, Spain’s Policia Nacional, Switzerland’s Kantonspolizei Thurgau, and Austria’s Directorate State Protection and Intelligence Service.

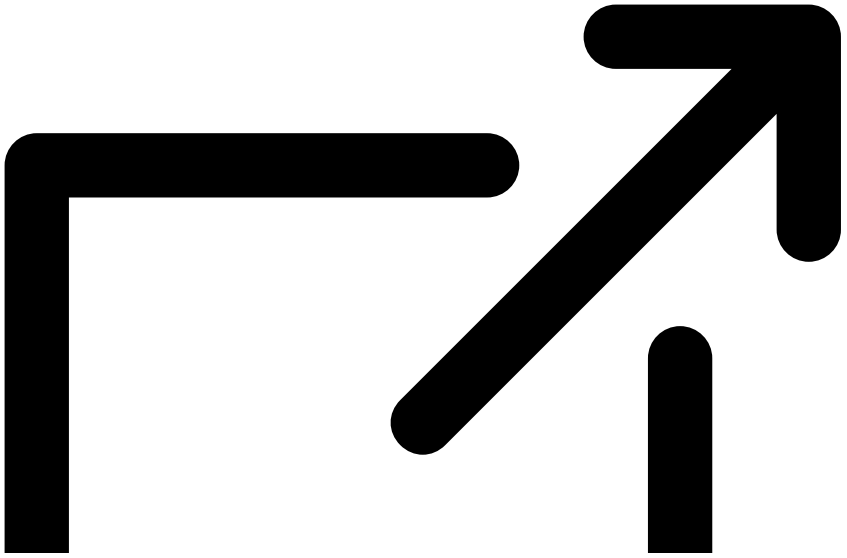
Victims of Blackcat ransomware are strongly encouraged to contact their local FBI field office at www.fbi.gov/contact-us/field-offices for further information and to determine what assistance may be available.

Blackcat affiliates have gained initial access to victim networks through a number of methods, including leveraging compromised user credentials to gain initial access to the victim system. More information about the malware, including technical information about indicators of compromise and recommendations to mitigate its effects, is available from the FBI at www.ic3.gov/Media/News/2022/220420.pdf.

Additional information regarding law enforcement's ongoing investigation into Blackcat is available at www.justice.gov/media/1329536/dl?inline.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program. Information can be submitted through the following Tor-based tip line (Tor browser required): he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion.

For more information about rewards for information on foreign malicious cyber activity against U.S. critical infrastructure, visit https://rfj.tips/SDT55f



.
