Two Americans Plead Guilty to Targeting Multiple U.S. Victims Using ALPHV BlackCat Ransomware

Published: 2025-12-30 · Archived: 2026-04-05 13:10:25 UTC

Yesterday, a federal district court in the Southern District of Florida accepted the guilty pleas of two men to conspiring to obstruct, delay or affect commerce through extortion in connection with ransomware attacks occurring in 2023.

“These defendants used their sophisticated cybersecurity training and experience to commit ransomware attacks — the very type of crime that they should have been working to stop,” said Assistant Attorney General A. Tysen Duva of the Justice Department’s Criminal Division. “Extortion via the internet victimizes innocent citizens every bit as much as taking money directly out of their pockets. The Department of Justice is committed to using all tools available to identify and arrest perpetrators of ransomware attacks wherever we have jurisdiction.”

“Ransomware is not just a foreign threat — it can come from inside our own borders,” said U.S. Attorney Jason A. Reding Quiñones for the Southern District of Florida. “Goldberg and Martin used trusted access and technical skill to extort American victims and profit from digital coercion. Their guilty pleas make clear that cybercriminals operating from within the United States will be found, prosecuted, and held to account.”

“Malware like ALPHV (BlackCat) ransomware is used by bad actors to steal, extort, and launder proceeds from victim businesses and organizations,” said Special Agent in Charge Brett Skiles of the FBI Miami Field Office. “The FBI remains committed to working alongside its law enforcement partners to disrupt and dismantle criminal enterprises involved in ransomware attacks and to hold accountable not only the perpetrators but also anyone who knowingly enables or profits from them. We will continue to leverage our intelligence, law enforcement tools, global presence, and partnerships to counter cybercriminals who seek to harm the American public through these insidious attacks. We strongly encourage businesses to exercise due diligence when engaging third parties for ransomware incident response, report suspicious or unethical behavior, and to expeditiously report any ransomware attack to the FBI and our law enforcement partners to safeguard their security and privacy.”

According to court documents, Ryan Goldberg, 40, of Georgia, Kevin Martin, 36, of Texas, and another co-conspirator successfully deployed the ransomware known as ALPHV BlackCat between April 2023 and December 2023 against multiple victims located throughout the United States. The three men agreed to pay the ALPHV BlackCat administrators a 20% share of any ransoms received in exchange for access to the ransomware and ALPHV BlackCat’s extortion platform. All three men worked in the cybersecurity industry — meaning that they had special skills and experience in securing computer systems against harm, including the type of harm they themselves were committing against the victims in this case. After successfully extorting one victim for approximately $1.2 million in Bitcoin, the men split their 80% share of this ransom three ways and laundered the funds through various means.

According to court documents, ALPHV BlackCat targeted the computer networks of more than 1,000 victims around the world. The group used a ransomware-as-a-service model in which developers were responsible for creating and updating ransomware and for maintaining the illicit internet infrastructure. Affiliates were responsible for identifying and attacking high-value victim institutions with the ransomware. After a victim paid, developers and affiliates shared the ransom.

Today's announcement follows the Justice Department's prior actions in December 2023 to disrupt ALPHV BlackCat ransomware, in which the FBI developed a decryption tool that allowed FBI field offices across the country and law enforcement partners around the world to offer hundreds of victims the capability of restoring their systems, saving victims approximately $99 million in ransom payments. At that time, the FBI also seized several websites operated by ALPHV BlackCat.

Goldberg and Martin each pleaded guilty to one count of conspiracy to obstruct, delay or affect commerce or the movement of any article or commodity in commerce by extortion in violation of 18 U.S.C. § 1951(a). The defendants are scheduled to be sentenced on March 12, 2026, and face a maximum penalty of 20 years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI Miami Field Office is leading the investigation, with assistance provided by the U.S. Secret Service.

Trial Attorneys Christen Gallagher and Jorge Gonzalez of the Justice Department's Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorneys Thomas Haggerty and Quinshawna Landon for the Southern District of Florida are prosecuting the case. Assistant U.S. Attorney Mitchell Hyman for the Southern District of Florida is handling asset forfeiture.

CCIPS investigates and prosecutes cybercrime in coordination with domestic and international law enforcement agencies, often with assistance from the private sector. Since 2020, CCIPS has secured the conviction of over 180 cybercriminals and court orders for the return of over $350 million in victim funds.

Significant assistance in this investigation was provided by Assistant U.S. Attorney Paul B. Morris for the Eastern District of Texas and Assistant U.S. Attorney Daniel W.A. Peach for the Middle District of Georgia. Additional assistance was provided by the Policía de Investigación of the Aeropuerto Internacional de la Ciudad de México.

Private sector organizations can report any suspicious activities and threats to the FBI's National Threat Operations Center by calling 1-800-CALL-FBI (225-5324), visiting www.tips.fbi.gov or contacting their local FBI field office.

If you are a victim of ransomware, contact your local FBI field office or file a report at ic3.gov.

If you have information about ALPHV BlackCat, their affiliates or activities, you may be eligible for a reward through the Department of State's Transnational Organized Crime Rewards program or [Rewards for Justice program]

. Information can be submitted through the following Tor-based tip line (Tor browser required):

he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion.
