Two cybersecurity employees plead guilty to carrying out ransomware attacks

Two former employees at cybersecurity firms — one of whom was a ransomware negotiator — have pleaded guilty to carrying out a series of ransomware attacks in 2023. The Department of Justice announced the guilty pleas on Tuesday, saying 40-year-old Ryan Goldberg and 36-year-old Kevin Martin extorted $1.2 million in Bitcoin from a medical device company and targeted several others.

Goldberg, Martin, and an unnamed co-conspirator were indicted for the attacks in October, which involved using ALPHV / BlackCat ransomware to encrypt and steal data from their victims. As reported by the *Chicago Sun-Times*, Martin and the third conspirator worked as ransomware negotiators at Digital Mint, a cybercrime and incident response company, while Goldberg was an incident response manager at Sygnia Cybersecurity Services.

ALPHV / BlackCat is a hacker group that uses a ransomware-as-a-service model, with the developers who maintain the malware often taking a cut of stolen funds from the cybercriminals who use it to target victims. In 2023, the FBI developed a decryption tool designed to recover data from victims of ALPHV / BlackCat, which has been linked to high-profile attacks on companies like Bandai Namco, MGM Resorts, Reddit, and UnitedHealth Group.

The DOJ's indictment claims Goldberg, Martin, and the co-conspirator used the ransomware in an attempt to extort millions of dollars from victims throughout the US, including

a pharmaceutical company, a doctor’s office, an engineering company, and a drone manufacturer.

“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,” Assistant Attorney General A. Tysen Duva of the DOJ’s Criminal Division says in a statement. “The Department of Justice is committed to using all tools available to identify and arrest perpetrators of ransomware attacks wherever we have jurisdiction.”

Goldberg and Martin 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.” Their sentencing is scheduled for March 12th, 2026, where they’ll face up to 20 years in prison.

https://www.theverge.com/news/851467/cybersecurity-employees-plead-guilty-alphv-blackcat-ransomware