LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ransomware Takedown Adds Fuel To Gov't Disclosure Push

By **Ben Kochman**

Law360 (February 1, 2023, 8:36 PM EST) -- The FBI's unprecedented dismantling of an international cybercrime crew — saving ransomware victims from being extorted out of more than $130 million — is expected to boost the agency's effort to hear about a greater share of cyberattacks.

During last week's announcement that the bureau and foreign law enforcement partners seized servers and websites belonging to an international ransomware group known as Hive, bureau director Christopher Wray reiterated his pitch for victims to tell law enforcement when they believe they've been hacked.

Only about 20% of Hive's victims across the globe reported potential issues to government authorities, Wray said. And despite the bureau and its partners still identifying Hive victims who didn't report the episodes — while providing more than 300 decryption keys that could be used to unlock frozen networks — Wray warned that targets of future attacks should not rely on the same thing happening to them.

"Here, fortunately, we were still able to identify and help many victims who didn't report in, but that is not always the case," Wray said during a press conference announcing the takedown. "When victims report attacks to us, we can help them — and others, too."

The U.S. government's effort to convince hacking victims to disclose episodes, either voluntarily or through various breach disclosure laws, is nothing new. But the Hive takedown could convince attack victims that the benefits of tipping off law enforcement are real rather than merely theoretical, cybersecurity attorneys say.

"There are few things more valuable to victim organizations than being able to quickly get its hands on a decryption key that gets its systems back up and running and prevents a significant disruption of operations," said Alex Iftimie, a privacy and data security partner at Morrison Foerster LLP.

The FBI's efforts in the case "speak to a direct value to victims of coming forward and cooperating with the FBI in the context of a ransomware attack," Iftimie added.

Federal officials have for years claimed that around three-fourths of all cyberattacks hitting U.S. entities are believed to be never reported. Despite recent reports that revenue from ransomware attacks sunk significantly in 2022, as less than 40% of victims reported making extortion payments, the threat of cyberattacks remains at or near the top of the companies' list of concerns.

With international law enforcement yet to arrest an alleged member of the Hive syndicate, one immediate possibility is that its members could reconstitute themselves under a different name.

"This is fantastic news in the world of ransomware and should reassure victim companies that law enforcement is very proactive and should be contacted because they can be a helpful partner," said Erez Liebermann, a member of the data strategy and security group at Debevoise & Plimpton LLP. "But the bad news is that the ransomware actors are like a multiheaded hydra: when you cut one off, more will come, and more are already there."

Still, last week's revelation that FBI agents penetrated Hive's computer networks in July 2022 and placed the group under surveillance for months — in what Deputy Attorney General Lisa Monaco called a "21st century cyber stakeout" — is likely to force the group to work harder to hide its activity, potentially leading it to make more mistakes, added Liebermann, a former federal cybercrime prosecutor.

The only way to slow down cybercrime long term, according to current and former federal officials, is to raise the costs of carrying out attacks, while making a life of ransomware crime less lucrative.

"These malicious actors are in it for the money, so if they are not getting as big of a return on their investment, they are going to look somewhere else," said Jennie Wang VonCannon, another former federal cybercrime prosecutor who is now a partner in the cybersecurity and privacy practice at Crowell & Moring LLP.

FBI officials say the investigation into Hive continues and that the bureau is engaged in so-called joint sequence operations, which include going after Hive's infrastructure, seizing its cryptocurrency and pursuing people who work with the group.

The idea that law enforcement may have internally identified some Hive members, even if they have not disclosed that information publicly, could make some people in the Hive crew concerned about whether they are being monitored by international law enforcement, limiting their future opportunities for work or travel, said Morrison Foerster's Iftimie.

"Many of the people who might think that this is a costless criminal activity might think twice about joining the next criminal group that constitutes itself," said the former federal prosecutor and U.S. Department of Justice national security official.

The FBI's announcement could also help combat feelings of helplessness expressed by some organizations that feel like the odds are stacked against them, given reports that cybercriminals have been paid staggering sums in recent years while continuing to evolve their tactics in an extended cat-and-mouse game with authorities.

"When I talk to people about ransomware attacks and cyber breaches, I sometimes get the general sense that people feel like they can't do anything about it," said VonCannon. The Hive takedown, however, sends a "clear message that law enforcement is taking the threat of ransomware seriously and that they have been working to disrupt those malicious actors all along," she added.

--Additional reporting by Stewart Bishop. Editing by Jay Jackson Jr. and Lakshna Mehta.