US turns to rewards in hunt for overseas cyber criminals

March 19 2015, byEric Tucker

This image provided by the FBI shows the FBI's wanted poster of Evgeniy Bogachev. The FBI considers Bogachev one of the world's most prolific and brilliant cyber criminals, slapping his photos -- bald, beefy-faced and smiling faintly -- on "Wanted" fliers posted online. The Russian would be an ideal target

for prosecution -- if only the Justice Department could find him. Unable to bring him into custody in the nine months since his indictment, the government has turned to a time-honored technique long used for more conventional crime: putting a bounty on Bogachev's head. (AP Photo/FBI)

The FBI considers Evgeniy Bogachev one of the world's most prolific and brilliant cyber criminals, slapping his photos—bald, beefy-faced and smiling faintly—on "Wanted" fliers posted online. The Russian would be an ideal target for prosecution—if only the Justice Department could find him.

Unable to bring him into custody in the 10 months since his indictment, the government has turned to a time-honored technique long used for more conventional crime: putting a bounty on Bogachev's head.

It's too soon to say whether the $3 million reward for information leading to his arrest—the first of its kind offered under a special State Department program—will ever pay off. But federal officials say they intend to use the strategy in additional cyber cases involving international hackers whose whereabouts are either unknown to the U.S. government or who are holed up in nations that have little or no diplomatic relations with the United States.

"We've really not done something like this" in cyber cases, Robert Anderson, an FBI executive assistant director, said in announcing the reward. "All of a sudden, somebody's putting an 'x' on somebody, saying, 'Bring him to justice, you get $3 million.'"

The reward is also a reminder of how many accused masterminds of cyberattacks on U.S. targets remain out of reach for federal law enforcement.

Five Chinese military officials were indicted last spring on charges of siphoning away corporate secrets from the networks of major American business. Federal officials say they're committed to bringing them to justice, but they won't speak publicly about what they're doing to nab them. Experts are skeptical that the military officials will ever see the inside of a courtroom.

Roman Zolotarev, charged in Nevada with masterminding a massive underworld marketplace of credit card fraud and identity theft, also is not in federal custody even as multiple lower-level members of the operation, called Carder.Su, have been convicted.

The U.S. has not publicly identified individuals involved in the Sony Pictures Entertainment hacking but has linked it to the North Korean government.

Some defense lawyers for more peripheral players charged in cybercrimes have seized on the absence of accused ringleaders, highlighting a potential vulnerability in the government's cases. The argument was raised in the 2013 trial of David Ray Camez, who was convicted and sentenced to 20 years in prison for his involvement in the Carder.Su organization.

"And they talk about all these people that created Carder.su, the real people, the bad guys in this case, where are they at?" Camez's lawyer, Chris Rasmussen, told the jury. "They don't have any of these Russians here. There's no Russians in this courtroom. Where are they?"

There's generally limited recourse against hackers committing crimes from countries like Russia and China, where the U.S. lacks formal extradition treaties and where foreign governments may be reluctant to turn them over for prosecution. Justice Department officials say they're hopeful that as more countries are harmed by international cybercrime,

there will be fewer sanctuaries for such criminals. Sometimes the best hope is for criminals to become careless over time and travel to countries where they're exposed to arrest.

"It can be a long, cold winter in Russia. A lot of these people have a lot of money. It's pretty tempting to travel somewhere warmer," Assistant Attorney General Leslie Caldwell, chief of the Justice Department's criminal division, said in an interview.

There are isolated examples of that happening, though not as many as the U.S. would like.

Roman Seleznev, the son of a Russian lawmaker, was arrested last July after he traveled to the Maldives and is awaiting trial in Seattle on charges that he hacked computers at American businesses and led a marketplace for stolen credit cards that raked in millions of dollars.

Vladimir Drinkman was arrested in Amsterdam in 2012 and extradited to New Jersey last month to face charges in a massive computer hacking scheme involving the theft of credit and debit card numbers from businesses including JC Penney and 7-Eleven.

Bogachev was indicted in Pittsburgh last year, accused of running two schemes that authorities say caused widespread financial losses. One, Cryptolocker, was a ransom-demanding virus that infected hundreds of thousands of computers. Another, Gameover Zeus, involved malicious software that intercepted customer bank account numbers and passwords that victims typed in. Both have been dismantled.

The FBI hasn't revealed much about the 31-year-old Bogachev, but the agency says he's believed to be in Russia and may travel by boat to locations along the Black Sea.

The $3 million reward is offered under a 2-year-old State Department program that so far has paid out more than $20 million and has posted rewards for people suspected of wildlife trafficking and international smuggling. This is the first reward offered under the program for this type of cybercrime.

Shawn Henry, a retired executive assistant director of the FBI and president of CrowdStrike Services, a security technology company, said it's challenging to find suspects in cyber cases, and a reward can attract tips. But other tactics, such as negotiations among governments, also are needed to deter attacks, he said.

"Time will tell whether this is a successful tactic or not," Henry said. "It's a strategy, and it's certainly not the sole strategy."