FBI is Fighting Hybrid Cyberattacks

Terrorism, foreign intelligence threats and traditional crimes are coordinated with hackers.

Amanda Ziadeh

Thu, 03/01/2018 - 13:10

Illustration: Lightcome/iStock

In a world of advancing cyber threats and security vulnerabilities, the FBI finds itself facing a hybrid cybersecurity environment: traditional national security threats merging with computer hackers and predators.

“In terms of cybersecurity, most of the threats that we’re faced with today are much the same we’ve always seen,” said Paul Abbate, executive assistant director for the Criminal, Cyber, Response and Services in the FBI. He spoke at the AFCEA Cyber Security Summit on Feb. 27.

Abbate said the threats can still be placed into three buckets: terrorism, foreign

intelligence and traditional criminal threats. Now, cyber is used as a tool to commit these crimes from a different angle — almost anonymously — and enhancing what criminal nation-state actors are doing.

“It makes it harder to predict, detect, harder to make attribution as far as who’s doing it,” Abbate said.

In the terrorism bucket, organizations like the Islamic State group use the internet and cyber means to globally radicalize and recruit individuals for violence, which has resulted in crises around the world.

Foreign counterintelligence threats from foreign state adversaries like Russia, Iran, North Korea and China come at the U.S. for economic espionage, theft of state secrets, foreign influence of elections and so on.

“[Cyber] just adds to the dynamic of the challenges in terms of the work that we do to protect this country,” Abbate said.

And even with traditional criminal threats, business email compromise and ransomware crimes have grown significantly over the past couple years. In this bucket, Abbate said those are the more common threats the FBI faces, resulting in the greatest economic harm.

“What we’re seeing is a blended or hybrid threat, whereby the traditional criminal organizations and hackers are coming together, and nation-states and nation-state actors are attacking us in tandem, as a team,” Abbate said.

He provided a real-life example of this “hybrid” cybersecurity case the FBI faced not too long ago.

In 2015, a defendant named Ardit Ferizi was charged with providing information to support IS by hacking and stealing U.S military and federal personnel information. Through reporting by a private sector company, the FBI was able to detect a significant breach occurred, which included the exploitation of personally identifiable information.

The FBI tracked the hack back to Ferizi, who was based in Malaysia, and from there, connected him with an IS leader in Syria. With even further intelligence, the FBI learned IS leveraged Ferizi to commit this breach, steal the PII and transfer that information to IS. IS used social media to publicly broadcast a “kill list,” a

compilation of names for radicalized individuals to target.

“You have a foreign terrorist organization of the highest order coming together and leveraging the ordinary criminal hacker to move toward violence and terrorist attacks around the world,” Abbate said.

But by collaborating with the Defense Department, private sector partners and international partners like the Malaysian authorities, the FBI identified both individuals before any harm was done with the list. Ferizi was charged in the U.S., and the individual from IS was killed in Syria during a military strike.

Abbate also referred to the breach of Yahoo’s network, also a hybrid-type attack, which began in 2014. Russian Federal Security Service officers worked with criminal hackers to target Yahoo and steal more than 500 million user account information. These hackers, also using the breach for their own criminal purposes, gave the information to their Russian government handlers so it could be leveraged for foreign intelligence purposes to influence operations.

Ultimately, four defendants were indicted, including two FSB officers, for computer hacking, economic espionage and other criminal offenses. The indictments were announced to publicly attribute the criminal acts to the Russian government, “naming and shaming them,” as Abbate said.

Presenting clear consequences, as shown in both cases, is one way the FBI hopes to prevent criminals from committing these types of cyberattacks in the future.

“We need to send the message to our adversaries . . . to deter and prevent them from doing these things,” Abbate said.

However, there are a few areas the FBI is working to improve in, to stay on top of the changing cyber threat landscape. One is with cyber talent recruitment, engaging students early on and conducting on-the-job cyber training to enhance the talent already in the FBI. The other area is information sharing.

“We have to continue to work hard at that, all around, both within government and with the private sector and our international partners,” Abbate said. The FBI is constantly working with other agencies and organizations to detect, predict and fight cyber threats. Its primary platform for doing so is the National Cyber Investigative Joint Task Force, a multi-agency cyber center to coordinate and share

information for cyber threat investigations. It involves more than 20 agencies from across law enforcement, the intelligence community, DOD and state and local partners.

But to foster even more partnerships and opportunities for information sharing, Abbate urged the private sector to form relationships with local FBI field offices.

“We think that’s essential, and we think that’s going to prevent bad things from happening . . . to have that relationship and share intelligence in advance,” he said.

To best position the country to counter all cyber threats, this information sharing is a two-way street.

“In the event that something unfortunate occurs, or we’re faced with a crisis, we already have the relationship, the bond, and that puts us in the best position to address this together,” Abbate said.

View printer friendly version
Federal Cybersecurity
hackers
Defense Department
Islamic State
FBI