Cybercrimes present unique challenges for investigators

November 12 2017, by Kate Brumback

This July 21, 2012, file photo shows signage at the corporate headquarters of Equifax Inc. in Atlanta. Attacks launched by cybercriminals wreak havoc and cause disruption as more of everyday life moves online. The U.S. attorney's office in Atlanta has worked hand-in-hand with the local FBI office to prosecute a number of high-profile cybercrime cases. They're currently investigating the breach at Atlanta-based Equifax, which exposed the personal information of 145 million Americans. (AP Photo/Mike Stewart, File)

The federal investigators looking into the breach that exposed personal information maintained by the Equifax credit report company are used

to dealing with high-profile hacks and the challenges they present.

The U.S. attorney's office and FBI in Atlanta have prosecuted developers and promoters of the SpyEye and Citadel malware toolkits, used to infect computers and steal banking information. They've helped prosecute a hack into Scottrade and ETrade that was part of an identity theft scheme, and aided the international effort that in July shut down AlphaBay, the world's largest online criminal marketplace.

The U.S. Attorney's office has confirmed that, along with the FBI, it is investigating the breach at Atlanta-based Equifax, which the company said lasted from mid-May to July and exposed the data of 145 million Americans. Neither agency would discuss Equifax, but the leaders of their cybercrime teams shared insights about the difficulties of cybercrime cases.

"They are challenging, and the success stories are rare," said prosecutor Steven Grimberg, who leads the Atlanta U.S. attorney's office cybercrime unit, created last year to fight the growing threat. For every conviction there may be 10 times as many that don't end successfully, he said.

Atlanta has become a hub for cybercrime prosecution in large part because of a proactive and aggressive local FBI team, and because U.S. attorneys have committed the necessary resources in recent years, Grimberg said.

___

WHO'S BEHIND THE KEYBOARD?

Identifying who's responsible is a key difficulty: Cybercriminals use aliases and operate on the dark web, in corners of the internet reached

using special software, where access is invite-only.

Investigators have infiltrated some of these online forums and can sometimes engage cybercriminals there, said FBI Supervisory Special Agent Chad Hunt, who oversees one of FBI Atlanta's cyber investigation squads. Once they obtain some information, they can use search warrants to get other data, such as business records or credit card transactions, to match the online alias to a real person.

Even extremely sophisticated cybercriminals sometimes slip up or collaborate with someone who's less careful, Hunt said.

"If we're looking at somebody for a while, eventually they'll make a mistake," he said. "So even if they are using high-quality encryption, eventually they'll do something stupid."

___

UNCOOPERATIVE FOREIGN GOVERNMENTS

Even when a cybercriminal's identity is pinpointed, arrests can take time. Many operate in countries that won't extradite to the U.S. But the FBI continues monitoring these suspects and can catch them if they travel, said Assistant Special Agent in Charge Ricardo Grave de Peralta, who oversees the Atlanta office's cyber investigation squads.

"A lot of these people are in places that aren't so great and they like to go on vacation, and we're happy to meet them in a third location and perhaps bring them to a second vacation here in the United States, all expenses paid," he said with a smile.

Even with friendly foreign governments, extraditions can take time: Often, the merits of a case are essentially litigated in the process, so that

authorities in the other country are satisfied the incriminating evidence is solid, Grimberg said.

___

DEALS AND COOPERATION

Once confronted with evidence against them, some cybercriminals decide to plead guilty and work with prosecutors instead of going to trial.

Their language skills, technical expertise and ability to communicate on online forums and sites open exclusively to cybercriminals make their cooperation invaluable, sometimes leading directly to new prosecutions, Grimberg said.

The government is committed to being as transparent as possible about that cooperation, especially when people get lighter sentences as a result, Grimberg said, but details are often sealed because cooperators fear repercussions.

___

MEANINGFUL SENTENCES

Prosecutors said the SpyEye malware caused close to $1 billion and Citadel more than $500 million in harm to individuals and financial institutions worldwide.

Because the scope of harm can be huge, federal sentencing guidelines often allow for a life-in-prison sentence.

Prosecutors ask for sentences tough enough to send a warning to others, and to discourage the person from returning to cybercrime when they get

out. But because cybercriminals are frequently young, have no criminal history and the crimes aren't violent, prosecutors rarely ask for life, Grimberg said.

One hacker involved in SpyEye's development got nine-plus years in prison while another got 15 when sentenced last year, and a Citadel developer got five in July. They weren't ordered to reimburse victims.

That highlights another challenge: Despite financial losses, prosecutors frequently ask judges to find that it is impractical or overly cumbersome to impose restitution. Tracing the affected IP addresses to identify possible victims would be difficult, Grimberg said, and U.S. authorities can't force them to pay once they return to their home countries.

___

WORKING WITH THE PRIVATE SECTOR

Investigators and prosecutors in Atlanta work to establish relationships with companies before anything bad happens, which can make them more comfortable if there is a problem. But companies may hesitate to contact law enforcement because they worry about reputational damage, actions from civil authorities, lawsuits, and the exposure of trade secrets or sensitive information.

The former head of Equifax told members of Congress last month that the company was cooperating with the FBI and state agencies, but Equifax has suffered at least some of these consequences after failing to repair a known security weakness for months this year. Digital burglars had access to the company's computer systems for 11 weeks before Equifax discovered the hack July 29. The company then waited until Sept. 7 before issuing a public alert, saying they hadn't understood until then just how much information had been stolen.