US disrupts hacking schemes that stole millions

2 June 2014, by Joe Mandak

A band of hackers implanted viruses on hundreds of thousands of computers around the world, secretly seized customer bank information and stole more than $100 million from businesses and consumers, the Justice Department said Monday in announcing charges against the Russian man accused of masterminding the effort.

In unveiling the criminal case, federal authorities said they disrupted European-based cyber threats that were sophisticated, lucrative and global.

In one scheme, the criminals infected computers with malicious software that captured bank account numbers and passwords, then used that information to secretly divert millions of dollars from victims' bank accounts to themselves. In another, they locked hacking victims out of their own computers, secretly encrypted personal files on the machines and returned control to the users only when ransom payments of several hundred dollars were made.

"The criminals effectively held for ransom every private email, business plan, child's science project, or family photograph— every single important and personal file stored on the victim's computer," Leslie Caldwell, the head of the Justice Department's criminal division, said at a news conference.

Working with officials in more than 10 other countries, the FBI and other agencies recently seized computer servers that were central to the crimes, which affected hundreds of thousands of computers.

The FBI called the alleged ringleader, 30-year-old Evgeniy Bogachev, one of the most prolific cyber criminals in the world and issued a "Wanted" poster that lists his online monikers and describes him as a boating enthusiast. He faces criminal charges in Pittsburgh, where he was named in a 14-count indictment, and in Nebraska, where a criminal complaint was filed. He has not been arrested, but Deputy Attorney General James Cole said U.S. authorities were in contact with Russia to try to bring him into custody.

Officials say the case is another stark reminder of the evolving cybercrime threat, though it's unrelated to the recently unsealed cyber-espionage indictment of five Chinese military hackers accused of stealing trade secrets from American firms. Both sets of hackers relied on similar tactics—including sending emails to unsuspecting victims that installed malware—but the Chinese defendants were government officials who sought information that could bring Chinese companies a competitive advantage.

Bogachev's operation, prosecutors say, consisted of criminals in Russia, Ukraine and the United Kingdom who were assigned different roles within the conspiracy. The group is accused in the development of both "Gameover Zeus"—a network of infected computers that intercepted customer bank account numbers and passwords that victims typed in— and "Cryptolocker," malicious software that hijacked victims' computers and demands ransom payments. Computer users who don't pay the fee generally lose their files for good.

The victims of the different schemes included an American Indian tribe in Washington state; an insurance company and a firm that runs assisted living centers in Pennsylvania; a local police department in Massachusetts; a pest control company in North Carolina; and a restaurant operator in Florida.

The Pittsburgh indictment unsealed Monday also accuses Bogachev's group of trying to siphon hundreds of thousands of dollars from the bank accounts of Haysite Reinforced Plastics of Erie, in northwestern Pennsylvania, on a single day in 2011. According to the indictment, two of the transfers went through—one for about $198,000 and

one for about $175,000—but multiple other attempted transfers did not.

Officials with Haysite did not immediately return phone calls for comment Monday. The accounts were with Pittsburgh-based PNC Bank, which declined to comment.

A Florida bank lost nearly $7 million through an unauthorized wire transfer. The Swansea, Massachusetts, police department, on the other hand, lost $750 when it paid a ransom demanded by the malicious software that infected its computers.

Last week, a federal judge in Pittsburgh granted a temporary restraining order against Bogachev and the others, demanding that they cease such activities. That order was unsealed along with the charges Monday.

___

Mandak reported from Pittsburgh.