Prosecutor's office paid bitcoin ransom in cyberattack

5 December 2016, by Joe Mandak

A state prosecutor's office in Pennsylvania was among hundreds of thousands of victims of a now-shuttered international cybercrime operation, paying nearly $1,400 in a bitcoin ransom to free up its infected computer network, authorities disclosed Monday.

Federal prosecutors said in court documents only that an unidentified state government entity had been victimized by the ring known as the Avalanche network. But the Allegheny County district attorney, Stephen Zappala Jr., confirmed to The Associated Press that it was his office.

The disabling of the Avalanche network by the European Union and U.S. authorities was announced last week in Europe. Federal documents unsealed in Pittsburgh on Monday provided additional details.

The Avalanche group had operated since at least 2010 and infected the computers of at least 500,000 computers worldwide, said Soo Song, acting U.S. Attorney in Pittsburgh.

"The takedown of Avalanche was unprecedented in its scope, scale, reach and level of cooperation among 40 countries," Song said.

Avalanche was a platform to distribute malware to people who wanted to buy it and use it to infect the computers of people and businesses.

In general, there were two broad types of malware. One was used to steal online banking information from computers so people known as "money mules" could transfer funds from those victims to overseas banks. The other was ransomware, which locks up a computer network until the victim agrees to pay a ransom.

The prosecutor's office was hit by ransomware in January 2015 when an employee clicked on a link embedded in phishing email, Zappala said.

Phishing is a process computer hackers use to try to get people to unwittingly install malware on their computer by clicking on what appears to be a legitimate internet link.

The employee "opened the link because it appeared to go back to a legitimate government agency," Zappala said. The link compromised the district attorney's computer system, which has since been upgraded to fend off similar attacks, he said.

The payment of a bitcoin ransom to free up the computer network was noted in federal court documents.

Zappala said his detectives traced the email to Australia but didn't identify the specific source and didn't alert other authorities. He said he's content to let federal authorities prosecute the case because "the penalties the federal government can impose are much more substantial than we can impose."

So far, infected computers have been found in 189 countries worldwide, Song said, and five people have been arrested. They're in custody on charges lodged by authorities in the countries where they're being held, though Song said they eventually could face federal charges and be tried in the United States. The identities of suspects have not yet been released.

Two unidentified Pennsylvania companies also were targets of the cybercrime operation, documents showed.

Money mules unsuccessfully attempted to steal more than $243,000 from a New Castle company using seven fraudulent wire transactions earlier this year, Song said. Unidentified people also transferred $387,500 from a Carnegie firm's bank account to one in Bulgaria in April, but the money was recovered.

Overseas officials, and specifically the Germans, began investigating Avalanche about four years ago. U.S. authorities were asked to get involved two years ago, Song said.

Pittsburgh is home to the National Cyber-Forensics and Training Alliance, a group consisting of the FBI and other law enforcement groups working with private businesses and academics, including computer experts at Carnegie Mellon University.