Bulgarian man pleads not guilty in US cybercrime case

December 22 2016, by Joe Mandak

A Bulgarian man pleaded not guilty Thursday to federal charges that he used sophisticated malware designed to steal banking credentials and other confidential information from infected computers of two western Pennsylvania companies and two California firms.

The U.S. Attorney's Office in Pittsburgh alleges Krasimir Nikolov, 44, of Varna, Bulgaria, gained access to online bank accounts by transmitting malware over Avalanche, a worldwide cybercrime network dismantled last month by federal and foreign authorities. Nikolov is one of at least five people arrested so far worldwide in the Avalanche investigation.

He appeared for arraignment Thursday on charges of conspiracy, unauthorized access of a computer to obtain financial information, and four counts of bank fraud. Although he speaks some English, he was aided by a translator. He also waived his right to a detention hearing, meaning he'll remain jailed until he stands trial.

Prosecutors allege in an indictment that Nikolov gained access to the online bank accounts of Nord-Lock Inc. in Carnegie and Protech Asphalt Maintenance of New Castle, as well as a golf equipment company in San Diego and a furniture company in Chula Vista, California.

They say he tried to transfer $378,500 from Nord-Lock's PNC Bank account to a bank in Bulgaria, but the company caught onto the scheme

and notified PNC Bank, which recalled the transfer so the company didn't lose any money. Similar attempts to transfer $243,000 from Protech's accounts, in February and April also failed, prosecutors allege.

The indictment also says Nikolov unsuccessfully attempted to transfer $118,000 from the accounts of Foresight Sports, the San Diego company, in May, and nearly $738,000 from California Furniture Collections' in Chula Vista from March to May.

In each instance, the companies' computers were infected when an employee clicked on a link or opened an attachment in an email that was designed to look like a legitimate business communication.

Defense attorney Stephen Begler said after the arraignment that it's "too early to determine what course we're going to take" in defending against the charges.

"I'm hoping they have the right guy for their sake," Begler said, referring to federal authorities. "They went all the way to Bulgaria to get him."

The Avalanche takedown was announced Dec. 1 in Europe before federal prosecutors in Pittsburgh revealed the ties to western Pennsylvania at an FBI news conference a few days later. Acting U.S. Attorney Soo Song said Avalanche participants like Nikolov infected at least 500,000 business and personal computers in nearly 190 countries and caused hundreds of millions of dollars in losses since 2010.

The European Union police agency said the sweep was "unprecedented in its scale" and included the seizure of 39 computer servers and hundreds of thousands of internet domains used by Avalanche. The takedown remained secret for months before it was revealed by law enforcement.

Nikolov was indicted under seal in October. The indictment was unsealed Dec. 13.