Moldovan phishing scheme took $3.5M from drilling accounts

October 14 2015, byJoe Mandak

A man from the eastern European country of Moldova ran an email phishing scheme that enabled him and others to steal banking information from U.S. companies, including $3.5 million taken from the accounts of a western Pennsylvania drilling firm, federal prosecutors said.

Some of the emails claimed to be from medical providers and coaxed the recipients to open them by claiming they had tested positive for cancer, court records show.

Andrey Ghinkul, 30, was charged in a sealed criminal complaint Aug. 28, when he was also arrested in Cyprus. The charges were announced by U.S. Attorney David Hickton in Pittsburgh late Tuesday.

Ghinkul remained in custody in Cyprus on Wednesday. He does not have a U.S. defense attorney and his counsel in Cyprus could not be immediately identified. A hearing to extradite him to the United States is set for next week.

U.S. victims of the Bugat malware that infected computers of those who opened the phishing emails lost about $10 million, the FBI said. The charges were filed in Pittsburgh partly because the greatest threats involved a bank and a school district in western Pennsylvania.

Hickton's office and the FBI cybercrime squad in Pittsburgh also have been on the cutting edge of computer-based crimes in recent years.

In the Ghinkul case, prosecutors say, an employee of Penneco Oil Company Inc., in Delmont, opened an email that attacked the computer and enabled Ghinkul and others to steal keystroke and other information that enabled them to attempt bank transfers.

The hackers moved nearly $2.2 million from a Penneco account to a bank in Krasnodar, Russia, in August 2012 and $1.35 million from a Penneco account to a bank in Minsk, Belarus, in September 2012. Another attempted transfer of about $76,000 to a Philadelphia bank account that same month failed, the indictment said.

Penneco's senior vice president, D. Marc Jacobs, said the company learned of the problem after an employee's email system went haywire in May 2012. The company's computer consultant urged them to contact the FBI, which seized the computer and began investigating, Jacobs said.

The company's bank First Commonwealth, based in Indiana, Pennsylvania, "worked to completely restore our funds almost immediately," Jacobs said. "So we're not out money. We're whole."

The bank did not immediately return a call seeking comment Wednesday.

The other western Pennsylvania victim was the Sharon City School District, where the hackers tried and failed to transfer $999,000 from one of its bank accounts to an account in Kiev, Ukraine, in December 2011, the indictment said.

Among other cases, Hickton and the FBI have worked to charge five Chinese army intelligence officers with stealing trade secrets from companies including U.S. Steel and Alcoa and a Russian-based ring that has used identity-theft software to steal $100 million from bank accounts worldwide.