Foreign National Pleads Guilty to Role in Cybercrime Schemes Involving Tens of Millions of Dollars in Losses

Press Release

Thursday, February 15, 2024

For Immediate Release
Office of Public Affairs

A Ukrainian national pleaded guilty today to his role in two separate and wide-ranging malware schemes involving tens of millions of dollars in losses.

“Vyacheslav Igorevich Penchukov was a leader of two prolific malware groups that infected thousands of computers with malicious software. These criminal groups stole millions of dollars from their victims and even attacked a major hospital with ransomware, leaving it unable to provide critical care to patients for over two weeks,” said Acting Assistant Attorney General Nicole M. Argentieri of the Justice Department’s Criminal Division. “Before his arrest and extradition to the United States, the defendant was a fugitive on the FBI’s most wanted list for nearly a decade. Today’s guilty pleas should serve as a clear warning: the Justice Department will never stop in its pursuit of cybercriminals.”

According to court documents, Vyacheslav Igorevich Penchukov, also known as Vyacheslav Igoravich Andreev and Tank, 37, of Donetsk, helped lead a wide-ranging racketeering enterprise and conspiracy that infected thousands of business computers with malicious software known as “Zeus” beginning in May 2009. After installing “Zeus” without authorization on victims’ computers, the enterprise then used the malicious software to capture bank account information, passwords, personal identification numbers, and similar information necessary to log into online banking accounts. Penchukov and his co-conspirators then falsely represented to banks that they were employees of the victims and authorized to make transfers of funds from the victims’ bank accounts, causing the banks to make unauthorized transfers of funds from the victims’

accounts, resulting in millions of dollars in losses to the victims. The enterprise used residents of the United States and elsewhere as “money mules” to receive wired funds from victims’ bank accounts into their own bank accounts, who then withdrew and wired funds overseas to accounts controlled by Penchukov’s co-conspirators.

Penchukov was charged with these offenses in the District of Nebraska. Given the severity of the charges in the case and the harm posed to American victims, Penchukov was added to the FBI’s Cyber Most Wanted List.

“The U.S. Attorney’s Office for the District of Nebraska, in concert with the U.S. Attorney’s Office for the Eastern District of North Carolina and Justice Department’s Computer Crime and Intellectual Property Section, successfully coordinated the prosecution and plea of Penchukov,” said U.S. Attorney Susan T. Lehr for the District of Nebraska. “This case demonstrates that cybercrime can affect anyone, no matter where they are. It also demonstrates that no matter where the cybercriminals are, the department can and will bring them to justice.”

Despite being added to the FBI’s Cyber Most Wanted List, Penchukov returned to criminal activity by helping lead a conspiracy that infected victim computers with IcedID or Bokbot, a new malware, from at least November 2018 through February 2021. IcedID was a sophisticated form of malicious software that collected and transmitted personal information from victims, including credentials for banking accounts. Penchukov and his co-conspirators used this information to steal from IcedID’s victims. IcedID also provided access to infected computers for other forms of malicious software, including ransomware. One such victim of this ransomware attack was the University of Vermont Medical Center, causing the loss of over $30 million from this victim alone, and left the medical center unable to provide many critical patient services for over two weeks, creating a risk of death or serious bodily injury to patients. Penchukov was charged with these offenses in the Eastern District of North Carolina.

“Malware like IcedID bleeds billions from the American economy and puts our critical infrastructure and national security at risk,” said U.S. Attorney Michael Easley for the Eastern District of North Carolina. “The Justice Department and FBI Cyber Squad won’t stand by and watch it happen, and won’t quit coming for the world’s most wanted cybercriminals, no matter where they are in the world. This operation removed a key player from one of the world’s most notorious cybercriminal rings. Extradition is real. Anyone who infects American computers had better be prepared to answer to an American judge.”

“Core to the FBI’s cyber strategy is our willingness to play the long game and take players off the field. Vyacheslav Penchukov was a prolific criminal for over a decade and his criminal activities caused millions in damages,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “The FBI would like to thank our partners in both public and private sectors, and domestically and globally, for helping us bring Penchukov to justice.”

Penchukov was arrested in Switzerland in 2022 and extradited to the United States in 2023.

Penchukov pleaded guilty to one count of conspiracy to commit a racketeer influenced and corrupt organizations (RICO) act offense for his leadership role in the “Zeus” enterprise. Penchukov (as Andreev) also pleaded guilty to one count of conspiracy to commit wire fraud for his leadership role in the IcedID malware group. He is scheduled to be sentenced on May 9 and faces a maximum penalty of 20 years in prison for each count. A federal judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI Omaha and Charlotte Field Offices are investigating the case.

Assistant Deputy Chief William A. Hall Jr. and Senior Counsels Frank Lin and Ryan K.J. Dickey of the Criminal Division’s Computer Crime and Intellectual Property Section, Assistant U.S. Attorney John E. Higgins for the District of Nebraska, and Assistant U.S. Attorney Brad DeVoe for the Eastern District of North Carolina are prosecuting the case.

The Justice Department’s Office of International Affairs worked with the Swiss Federal Office of Justice to secure the arrest and extradition of Penchukov.

Updated February 15, 2024

Topic

Cybercrime

Press Release Number: 23-183