Russian National Arrested for Conspiracy to Introduce Malware into a Nevada Company's Computer Network

Press Release

Tuesday, August 25, 2020

For Immediate Release
Office of Public Affairs

Before Attempting to Flee the United States, Defendant Allegedly Plotted with Co-Conspirators to Pay $1 Million to Company Employee to Surreptitiously Insert Malware

A Russian national made his initial appearance in federal court Monday for his role in a conspiracy to recruit an employee of a company to introduce malicious software into the company's computer network, extract data from the network, and extort ransom money from the company.

Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division, U.S. Attorney Nicholas A. Trutanich of the District of Nevada and Special Agent in Charge Aaron C. Rouse of the FBI's Las Vegas Field Office made the announcement.

Egor Igorevich Kriuchkov, 27, a citizen of Russia, was charged in a complaint with one count of conspiracy to intentionally cause damage to a protected computer. He was arrested on Aug. 22, 2020, in Los Angeles and had his initial appearance before U.S. Magistrate Judge Alexander F. MacKinnon in U.S. District Court in Los Angeles, California, who ordered Kriuchkov detained pending trial.

According to the complaint and statements made in court, from about July 15, 2020 to about Aug. 22, 2020, Kriuchkov conspired with associates to recruit an employee of a company to introduce malware – i.e., malicious software programs designed to damage or do other unwanted actions on a computer system – into the company's computer network. The malware would supposedly provide Kriuchkov and his co-

conspirators with access to the company's system. After the malware was introduced, Kriuchkov and his co-conspirators would extract data from the network and then threaten to make the information public, unless the company paid their ransom demand.

Kriuchkov entered the United States using his Russian passport and a tourist visa. He contacted and met with the employee numerous times to discuss the conspiracy. Kriuchkov promised to pay the employee $1 million after the malware was introduced. In furtherance of the conspiracy, Kriuchkov provided the employee with a burner phone, and instructed him to leave the burner phone in airplane mode until after the money was transferred.

After being contacted by the FBI, Kriuchkov drove overnight from Reno, Nevada, to Los Angeles. Kriuchkov asked an acquaintance to purchase an airline ticket for him in an attempt to fly out of the country.

The charges and allegations contained in a complaint are merely accusations. The defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

The investigation was led by the FBI's Las Vegas Field Office with assistance from the FBI's Los Angeles Field Office; the FBI's Sacramento Field Office; the Washoe County Sheriff's Office; and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). Assistant U.S. Attorney Richard Casper and C.S. Heath, Senior Counsel of CCIPS, are prosecuting the case.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

Updated August 25, 2020

Topic

Cybercrime

Press Release Number: 20-819