Russian National Pleads Guilty to Trickbot Malware Conspiracy

Press Release

Thursday, November 30, 2023

For Immediate Release
Office of Public Affairs

A Russian national pleaded guilty today to his role in developing and deploying the malicious software known as Trickbot, which was used to launch cyber-attacks against American hospitals and other businesses.

According to court documents and public reporting, Vladimir Dunaev, 40, of Amur Blast, provided specialized services and technical abilities in furtherance of the Trickbot scheme. Trickbot, which was taken down in 2022, was a suite of malware tools designed to steal money and facilitate the installation of ransomware. Hospitals, schools, and businesses were among the millions of Trickbot victims who suffered tens of millions of dollars in losses. While active, Trickbot malware, which acted as an initial intrusion vector into victim computer systems, was used to support various ransomware variants.

“Dunaev’s guilty plea and our collaboration with South Korea that made his extradition possible are a prime example of what we can accomplish together with our foreign partners,” said Acting Assistant Attorney General Nicole M. Argentieri of the Justice Department’s Criminal Division. “Cybercriminals should know that countries around the world stand ready to bring them to justice and hold them accountable for their crimes.”

Dunaev developed browser modifications and malicious tools that aided in credential harvesting and datamining from infected computers, facilitated and enhanced the remote access used by Trickbot actors, and created a program code to prevent the Trickbot malware from being detected by legitimate security software. During Dunaev’s participation in the scheme, 10 victims in the Northern District of Ohio, including Avon schools and a North Canton real-estate company, were defrauded of more than $3.4 million via ransomware deployed by Trickbot.

“As set forth in the plea agreement, Vladimir Dunaev misused his special skills as a computer programmer to develop the Trickbot suite of malware,” said U.S. Attorney Rebecca C. Lutzko for the Northern District of Ohio. “Dunaev and his codefendants hid behind their keyboards, first to create Trickbot, then using it to infect millions of computers worldwide — including those used by hospitals, schools, and businesses — invading privacy and causing untold disruption and financial damage. The Justice Department and our office have prioritized investigating and prosecuting cybercrime, and today’s guilty plea demonstrates our willingness to reach across the globe to bring cybercriminals to justice. We will continue to work closely with our partners, foreign and domestic, and use all resources at our disposal to stop similar behavior.”

“Combating bad actors in cyberspace is a team sport, and we are proud of the collaboration and coordination at the international level that went into today’s plea,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “The FBI will pursue criminals who target the American people with malware no matter where they reside.”

“As the world of technology is ever-changing, cybercrime continues to evolve. This case underscores the FBI’s relentless pursuit of cyber criminals and highlights our expertise to find and dismantle criminal networks,” said Special Agent in Charge Gregory Nelsen of the FBI Cleveland Field Office. “We appreciate the coordinated work among our public and private sector global colleagues together with our federal, state, and local law enforcement partners to further protect the public from destructive malware.”

In 2021, Dunaev was extradited from the Republic of Korea to the Northern District of Ohio.

Dunaev pleaded guilty to conspiracy to commit computer fraud and identity theft and conspiracy to commit wire fraud and bank fraud. He is scheduled to be sentenced on March 20, 2024, and faces a maximum penalty of 35 years in prison on both counts. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The original indictment returned in the Northern District of Ohio charged Dunaev and eight other defendants for their alleged roles in developing, deploying, managing, and profiting from Trickbot.

In June, one of Dunaev’s co-conspirators, Alla Witte, who was a Trickbot malware developer and Latvian national, pleaded guilty to conspiracy to commit computer fraud and was sentenced to two years and eight months in prison.

In February and September, the Treasury Department’s Office of Foreign Assets Control (OFAC) issued financial sanctions against multiple suspected Trickbot members.

The FBI Cleveland Field Office is investigating the case.

Trial Attorney Candy Heath of the Criminal Division’s Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Duncan Brown and Daniel Riedl for the Northern District of Ohio are prosecuting the case. The Justice Department’s Office of International Affairs and National Security Division, as well as the Treasury Department’s OFAC, provided significant assistance.

The Justice Department’s Office of International Affairs worked with the International Criminal Affairs Division of the South Korean Ministry of Justice to secure the arrest and extradition of Dunaev.

Updated November 30, 2023
