Russian National Extradited to United States to Face Charges for Alleged Role in Cybercriminal Organization

Published: 2021-10-28 · Archived: 2026-04-05 23:21:07 UTC

A Russian national, residing in the Yakutsk region of Russia and in Southeast Asia, had his initial appearance in federal court today after his extradition from the Republic of Korea to the Northern District of Ohio to face charges for his alleged role in a transnational, cybercriminal organization.

According to court documents, Vladimir Dunaev, 38, was a member of a transnational, cybercriminal organization that deployed a computer banking trojan and ransomware suite of malware known as “Trickbot.”

“Trickbot attacked businesses and victims across the globe and infected millions of computers for theft and ransom, including networks of schools, banks, municipal governments, and companies in the health care, energy, and agriculture sectors,” said Deputy Attorney General Lisa O. Monaco. “This is the second overseas Trickbot defendant arrested in recent months, making clear that, with our international partners, the Department of Justice can and will capture cyber criminals around the world. This is another success for the Department’s recently launched Ransomware and Digital Extortion Task Force in dismantling ransomware groups and disrupting the cybercriminal ecosystem that allows ransomware to exist and to threaten our critical infrastructure.”

“The FBI is determined to utilize our unique tools and capabilities to disrupt transnational cybercriminal organizations, such as the group that developed and delivered Trickbot, and remains committed to imposing risk and consequence upon these criminals,” said Deputy Director Paul Abbate of the FBI. “Pursuing cyber criminals requires considerable patience, expertise, and resources, but the FBI has a long memory and will ensure that these malicious actors cannot evade detection or avoid the full weight of law enforcement actions.”

“The Trickbot malware was designed to steal the personal and financial information of millions of people around the world, thereby causing extensive financial harm and inflicting significant damage to critical infrastructure within the United States and abroad,” said Acting U.S. Attorney Bridget M. Brennan of the Northern District of Ohio. “Today’s announcement underscores the great lengths federal law enforcement officials and our international partners will go to hold these alleged cybercriminals accountable for their actions.”

“This indictment reflects the dynamic landscape in which international criminals utilize sophisticated cyber methods to take advantage of and defraud, unsuspecting victims anywhere in the world,” said Special Agent in Charge Eric Smith of the FBI’s Cleveland Field Office. “This multi-year investigation demonstrates the commitment by the FBI to aggressively pursue these individuals despite the complexity and global character cyber investigations can so often bring. The FBI encourages any victim of cyber fraud to file a report with the FBI’s Internet Crime Complaint Center at www.ic3.gov.”

The indictment alleges that beginning in November 2015, and continuing through August 2020, Dunaev and others stole money, confidential information, and damaged computer systems from unsuspecting victims, including individuals, financial institutions, school districts, utility companies, government entities, and private

businesses. To perpetuate their criminal scheme, the defendants allegedly used a network of co-conspirators and freelance computer programmers, known as the Trickbot Group, to create, deploy, and manage the Trickbot malware, which infected millions of computers and computer systems worldwide.

Dunaev is alleged to have been one such co-conspirator, working as a malware developer for the Trickbot Group. Dunaev allegedly performed a variety of developer functions in support of the Trickbot malware, including managing the malware's execution, developing popular browser modifications and helping to conceal the malware from detection by security software.

Earlier this year, the Justice Department announced the arrest and arraignment of Alla Witte, a Latvian national charged for her role in the Trickbot Group.

According to court documents, the Trickbot malware was designed to capture online banking login credentials and harvest other personal information, including credit card numbers, emails, passwords, dates of birth, social security numbers, and addresses from infected computers through the use of web injects and keystroke logging. Later versions of Trickbot were adapted to facilitate the installation and use of ransomware.

According to the indictment, the defendants used these stolen login credentials and other personal information to gain access to online bank accounts, execute unauthorized electronic funds transfers and launder the money through U.S. and foreign beneficiary accounts.

Dunaev was extradited from the Republic of Korea on Oct. 20. He is charged with conspiracy to commit computer fraud and aggravated identity theft, conspiracy to commit wire and bank fraud, conspiracy to commit money laundering, and multiple counts of wire fraud, bank fraud, and aggravated identity theft. If convicted of all counts, Dunaev faces a maximum penalty of 60 years' imprisonment. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

This case was investigated by the FBI's Cleveland Field Office.

The Justice Department's Office of International Affairs provided invaluable assistance in securing the arrest and extradition of Dunaev to the United States, with substantial support provided by the Republic of Korea.

Senior Counsel C.S. Heath of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Daniel J. Riedl and Duncan T. Brown of the Northern District of Ohio are prosecuting the case.

This case is part of the Department of Justice's Ransomware and Digital Extortion Task Force, which was created to combat the growing number of ransomware and digital extortion attacks. As part of the Task Force, the Criminal Division, working with the U.S. Attorneys' Offices, prioritizes the disruption, investigation, and prosecution of ransomware and digital extortion activity by tracking and dismantling the development and deployment of malware, identifying the cybercriminals responsible, and holding those individuals accountable for their crimes. The department, through the Task Force, also strategically targets the ransomware criminal ecosystem as a whole and collaborates with domestic and foreign government agencies as well as private sector partners to combat this significant criminal threat.

An indictment is merely an allegation, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.
