

# Russian National Sentenced for Involvement in Development and Deployment of Trickbot Malware

[justice.gov/opa/pr/russian-national-sentenced-involvement-development-and-deployment-trickbot-malware](https://www.justice.gov/opa/pr/russian-national-sentenced-involvement-development-and-deployment-trickbot-malware)



Press Release

Thursday, January 25, 2024

## For Immediate Release

Office of Public Affairs

A Russian national was sentenced yesterday to five years and four months in prison for his involvement in developing and deploying the malicious software known as Trickbot, which was used to launch cyberattacks against American hospitals and other businesses.

According to court documents and public reporting, Vladimir Dunaev, 40, of Amur Oblast, Russia, 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.

“This sentencing demonstrates the department’s ability to place cybercriminals behind bars, no matter where they are located,” said Acting Assistant Attorney General Nicole M. Argentieri of the Justice Department’s Criminal Division. “In cooperation with our partners around the world, we will continue to bring cybercriminals to justice.”

“Dunaev developed malicious ransomware and deployed it to attack American hospitals, schools, and businesses in the Northern District of Ohio and throughout our country, all while hiding behind his computer,” said U.S. Attorney Rebecca C. Lutzko for the Northern District of Ohio. “He and his co-defendants caused immeasurable disruption and financial damage, maliciously infecting millions of computers worldwide, and

Dunaev will now spend over five years behind bars as a result. Dunaev’s case demonstrates that the Justice Department and our office will use all available resources to investigate and prosecute cybercrime, and we thank our international partners for their cooperation in helping us stop cybercriminals like Dunaev and bring them to justice.”

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.

“The FBI relentlessly investigates criminal activity impacting the American people even when the perpetrators reside beyond our borders,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “Combating malicious cyber actors is a team sport, and we are proud of the coordinated effort that brought about this sentencing.”

“This case and subsequent sentencing sends a strong message to cybercriminals and other bad actors who target individuals and businesses with malicious intent,” said Special Agent in Charge Greg Nelsen of the FBI Cleveland Field Office. “The complexities of this case required careful coordination among our domestic and international partners and their commitment to meticulous investigative work. I am proud of the synchronized effort to see that justice was served.”

In 2021, Dunaev was extradited from the Republic of Korea to the Northern District of Ohio. On Nov. 30, 2023, Dunaev pleaded guilty to conspiracy to commit computer fraud and identity theft and conspiracy to commit wire fraud and bank fraud.

The original indictment returned in the Northern District of Ohio charged Dunaev and six 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 2023 [↗](#), the Treasury Department’s Office of Foreign Assets Control (OFAC) issued financial sanctions against multiple suspected Trickbot members.

The FBI Cleveland Field Office investigated 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 prosecuted 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 January 25, 2024

---

**Topic**

Cybercrime

Press Release Number: 24-86