Russian TrickBot malware dev sentenced to 64 months in prison

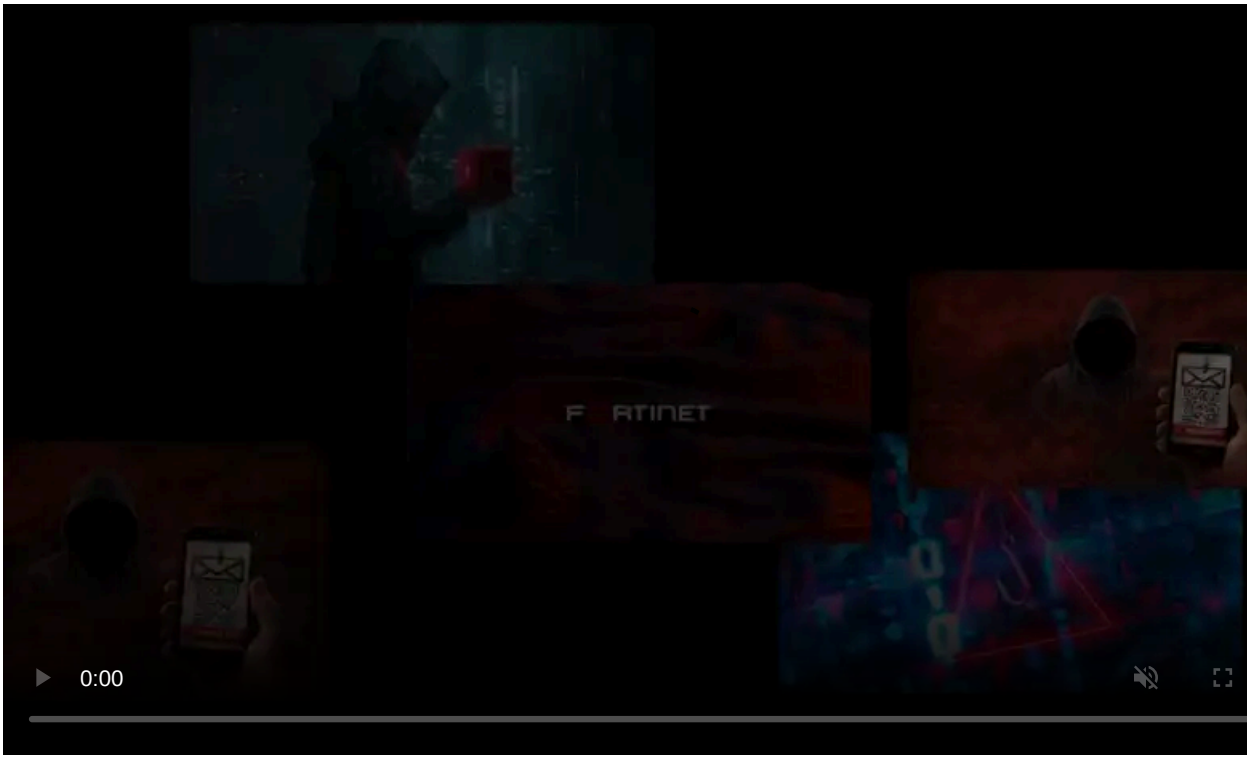
By Sergiu Gatlan

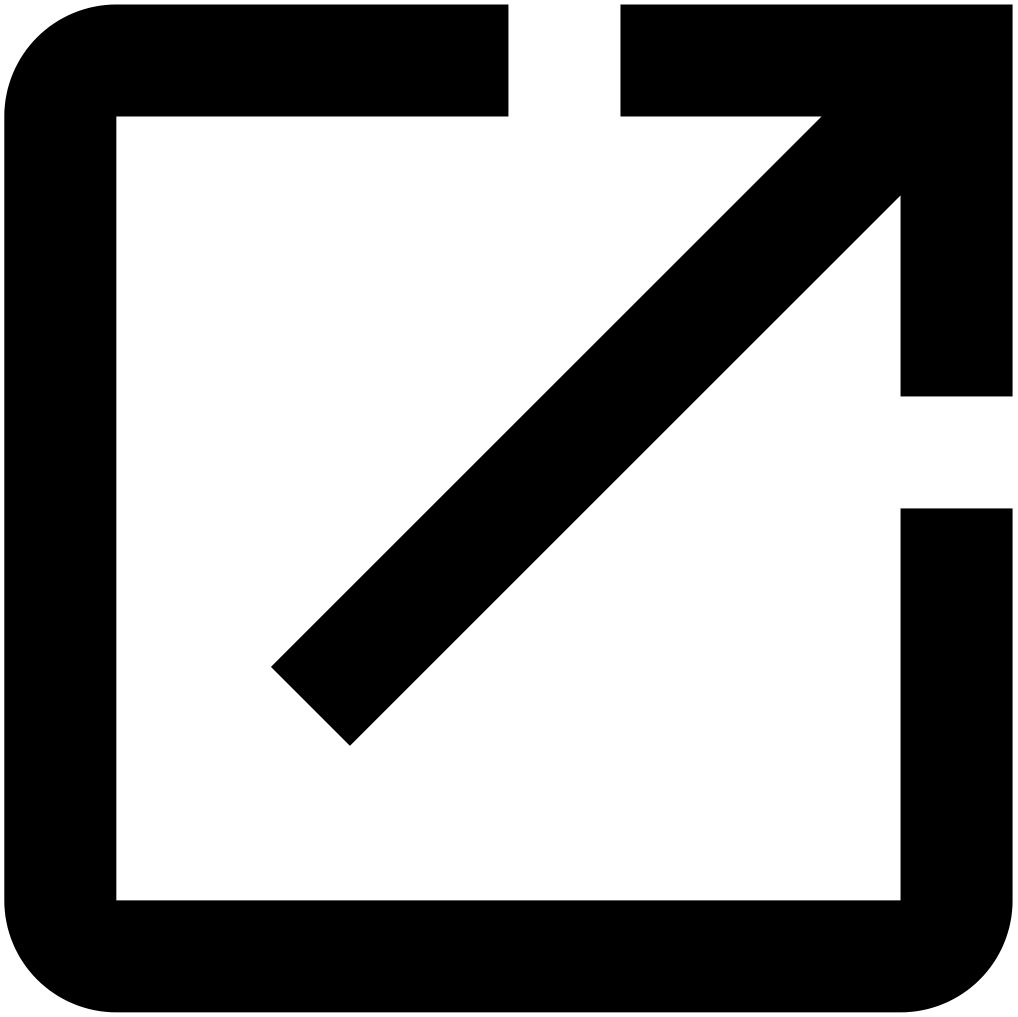
Published: 2024-01-25 · Archived: 2026-04-05 21:33:48 UTC

Russian national Vladimir Dunaev has been sentenced to five years and four months in prison for his role in creating and distributing the Trickbot malware used in attacks against hospitals, companies, and individuals worldwide.

According to court documents, the 40-year-old individual (also known as FFX) was the one who oversaw the development of the malware's browser injection component.

In September 2021, Dunaev was arrested while trying to leave South Korea after being stuck there for over a year due to COVID-19 travel restrictions and an expired passport. The extradition process to the United States was completed on October 20, 2021.


F RTINET
0:00



After his arrest, he pleaded guilty to charges related to conspiring to commit computer fraud and identity theft, in addition to conspiring to commit wire and bank fraud, facing a maximum sentence of 35 years in prison for both offenses.

The initial indictment accused Dunaev and eight co-defendants of engaging in the development, deployment, administration, and financial gains from the Trickbot malware operation.

"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.

"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."

TrickBot arrests and sanctions

Dunaev began working for the TrickBot malware syndicate in June 2016 as a developer following a recruitment process that required him to create a SOCKS server app and modify the Firefox browser for malware delivery.

The TrickBot malware he helped develop enabled cybercriminals to collect infected victims' sensitive information (such as login credentials, credit card information, emails, passwords, social security numbers, and addresses) and siphon off funds from victims' bank accounts

Dunaev is the second TrickBot malware dev prosecuted by the U.S. Department of Justice after Latvian national Alla Witte (aka Max) was apprehended in February 2021 and charged with helping develop the module designed to deploy ransomware on compromised networks.

In February and September, the U.S. and the U.K. sanctioned 18 Russians linked to the TrickBot and Conti cybercrime gangs for their involvement in the extortion of at least $180 million, warning that some Trickbot group members were also associated with Russian intelligence services.

TrickBot's evolution and Conti links

Initially focused on banking credentials theft upon its emergence in 2015, TrickBot quickly mutated into a modular tool used by cybercrime organizations (including the Ryuk and Conti ransomware operations) to gain initial access to corporate networks.

Despite several takedown attempts, the Conti cybercrime group assumed control of the malware, using it to develop other complex and stealthier malware variants like Anchor and BazarBackdoor.

However, in the wake of Russia's invasion of Ukraine, a Ukrainian researcher leaked Conti's internal communications online, exposing its links with the TrickBot operation.

An anonymous entity (TrickLeaks) later disclosed more information on the TrickBot gang, shedding further light on its links with Conti.

These disclosures ultimately expedited Conti's shutdown, which fragmented into other ransomware groups now tracked as Royal, Black Basta, and ZEON.
