TrickBot malware dev pleads guilty, faces 35 years in prison

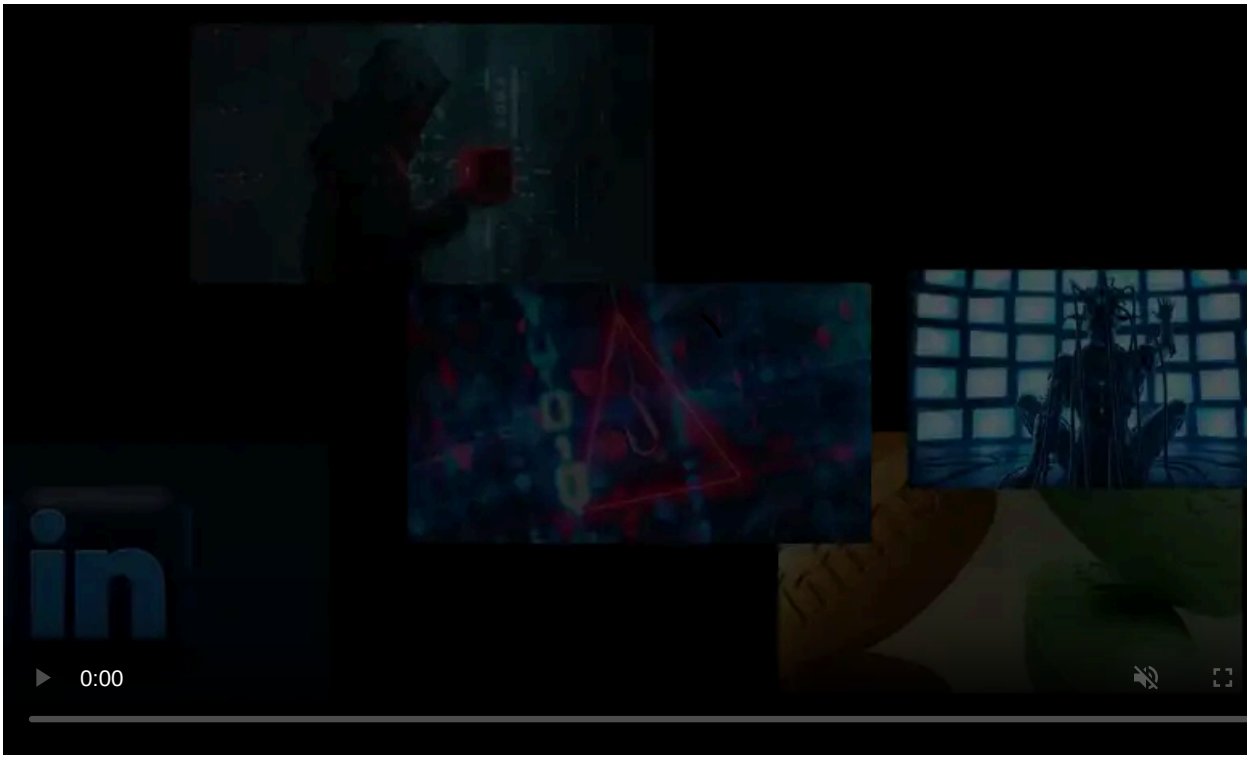
By Sergiu Gatlan

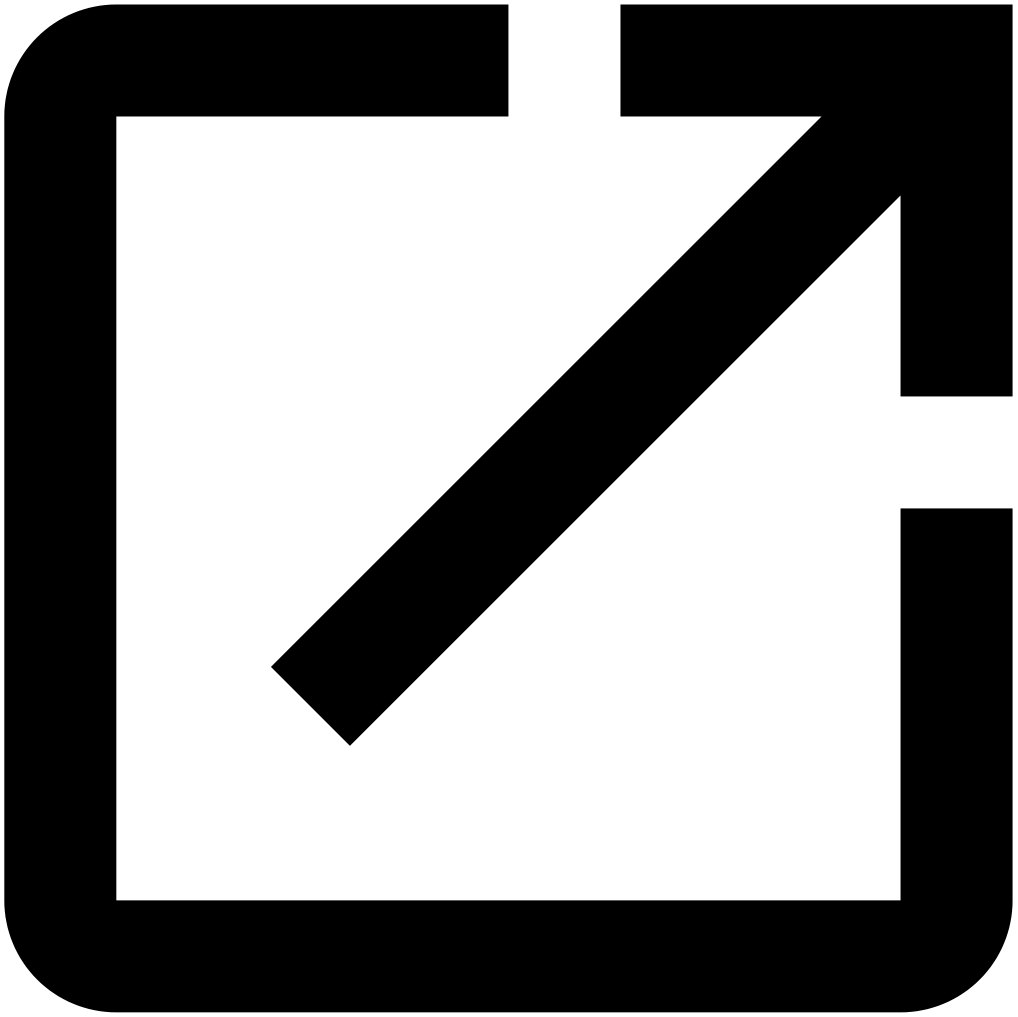
Published: 2023-12-01 · Archived: 2026-04-05 18:16:13 UTC

On Thursday, a Russian national pleaded guilty to charges related to his involvement in developing and deploying the Trickbot malware, which was used in attacks against hospitals, companies, and individuals in the United States and worldwide.

According to court documents, a 40-year-old individual, also known as FFX, oversaw the development of TrickBot's browser injection component as a malware developer.

Allegedly, Dunaev's association with the TrickBot malware syndicate started in June 2016 after being hired as a developer following a recruitment test requiring him to create an app simulating a SOCKS server and to alter the Firefox browser.


0:00



In September 2021, he was arrested in South Korea while attempting to depart. Due to COVID-19 travel restrictions and an expired passport, he had been forced to remain in South Korea for over a year. The extradition process was finalized on October 20, 2021.

"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.

"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 TrickBot malware helped its operators harvest personal and sensitive information (including credentials, credit cards, emails, passwords, dates of birth, SSNs, and addresses) and steal funds from their victims' banking accounts.

Dunaev entered a guilty plea for charges related to conspiracy to commit computer fraud and identity theft, alongside conspiracy charges for wire and bank fraud. His sentencing is set for March 20, 2024, and he is facing a maximum sentence of 35 years in prison for both offenses.

The initial indictment charged Dunaev and eight codefendants for their alleged involvement in developing, deploying, administering, and profiting from the Trickbot operation.

Dates	**Code description**
July 2016 - time of arrest	Modifying the Firefox web browser
December 2016	Machine Query that lets TrickBot determine the description, manufacturer, name, product, serial number, version, and content of the root file directory of an infected machine
August 2016 - December 2018	Code that grabs and saves from the web browser its name, ID, type, configuration files, cookies, history, local storage, Flash Local Shared Objects/LSO (Flash cookies)
October 2016 - time of arrest	Code that searches for, imports, and loads files in the web browser's 'profile' folders; these contain cookies, storage, history, Flash LSO cookies. It also connects to the browser databases to make queries and modify them
July 2016 - time of arrest	An executable app/utility to launch and manage a web browser
July 2016 - time of arrest	Code that collects and modifies data entries in Google Chrome LevelDB database, browsing history included

Dunaev is the second TrickBot gang malware developer arrested by the U.S. Department of Justice. In February 2021, Latvian national Alla Witte (aka Max) was apprehended and charged with helping write the code used to control and deploy ransomware on victims' networks.

In February and September, the United States and the United Kingdom sanctioned a total of 18 Russian nationals associated with the TrickBot and Conti cybercrime gangs for their involvement in the extortion of at least $180 million from victims worldwide. Also, they warned that some Trickbot group members are associated with Russian intelligence services.

Initially focused on stealing banking credentials when it surfaced in 2015, the TrickBot malware evolved into a modular tool leveraged by cybercrime organizations such as Ryuk and Conti ransomware for initial access into compromised corporate networks.

Following several takedown attempts, the Conti cybercrime gang gained control of TrickBot, harnessing it to develop more sophisticated and stealthy malware strains, including Anchor and BazarBackdoor.

However, following Russia's invasion of Ukraine, a Ukrainian researcher leaked Conti's internal communications in what is now known as the "Conti Leaks."

Shortly after, an anonymous figure using the TrickLeaks moniker began leaking details about the TrickBot operation, further outlining its links with the Conti gang.

Ultimately, these leaks precipitated the shutdown of the Conti ransomware operation, resulting in its fragmentation into numerous other ransomware groups, such as Royal, Black Basta, and ZEON.

Source: https://www.bleepingcomputer.com/news/security/trickbot-malware-dev-pleads-guilty-faces-35-years-in-prison/