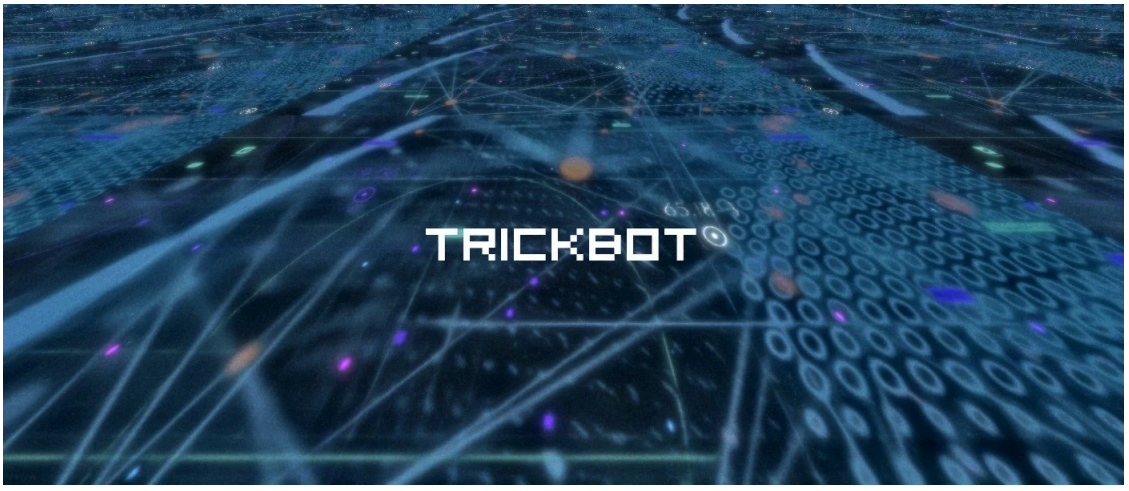
TrickBot malware dev extradited to U.S. faces 60 years in prison

By Ionut Ilascu

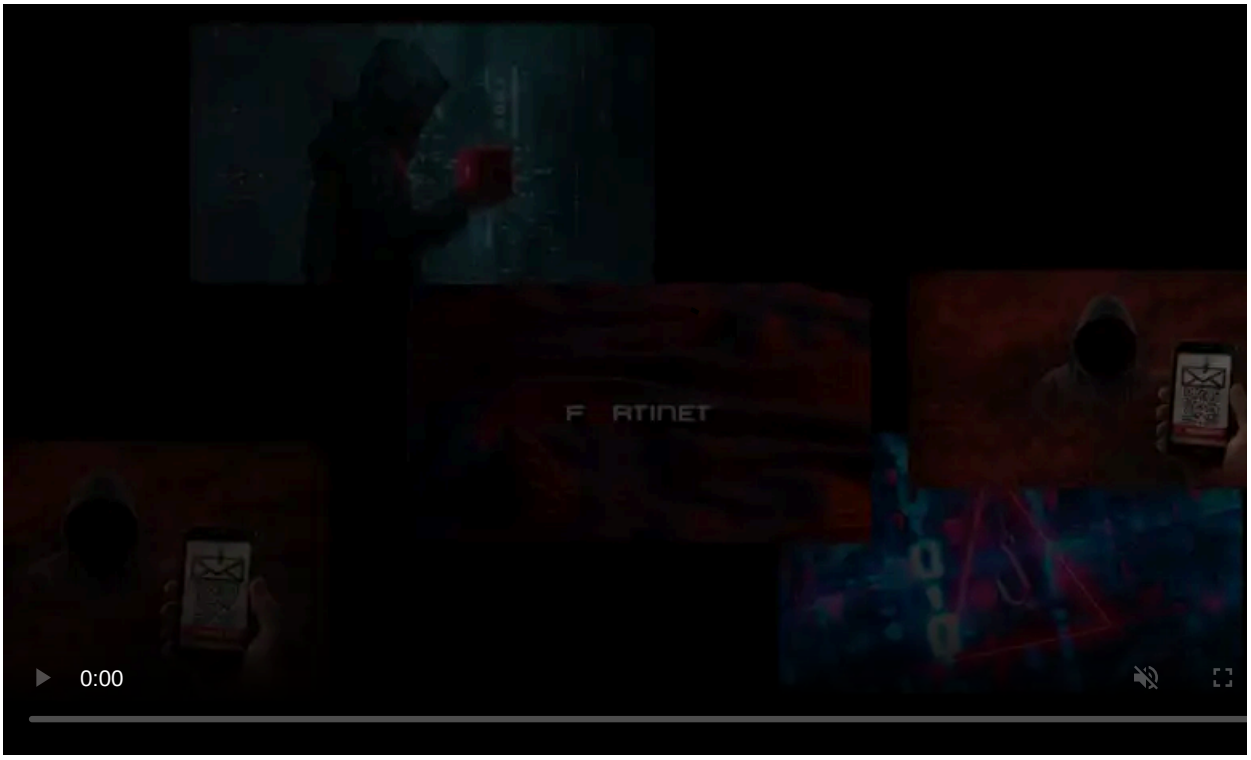
Published: 2021-10-29 · Archived: 2026-04-05 22:45:08 UTC

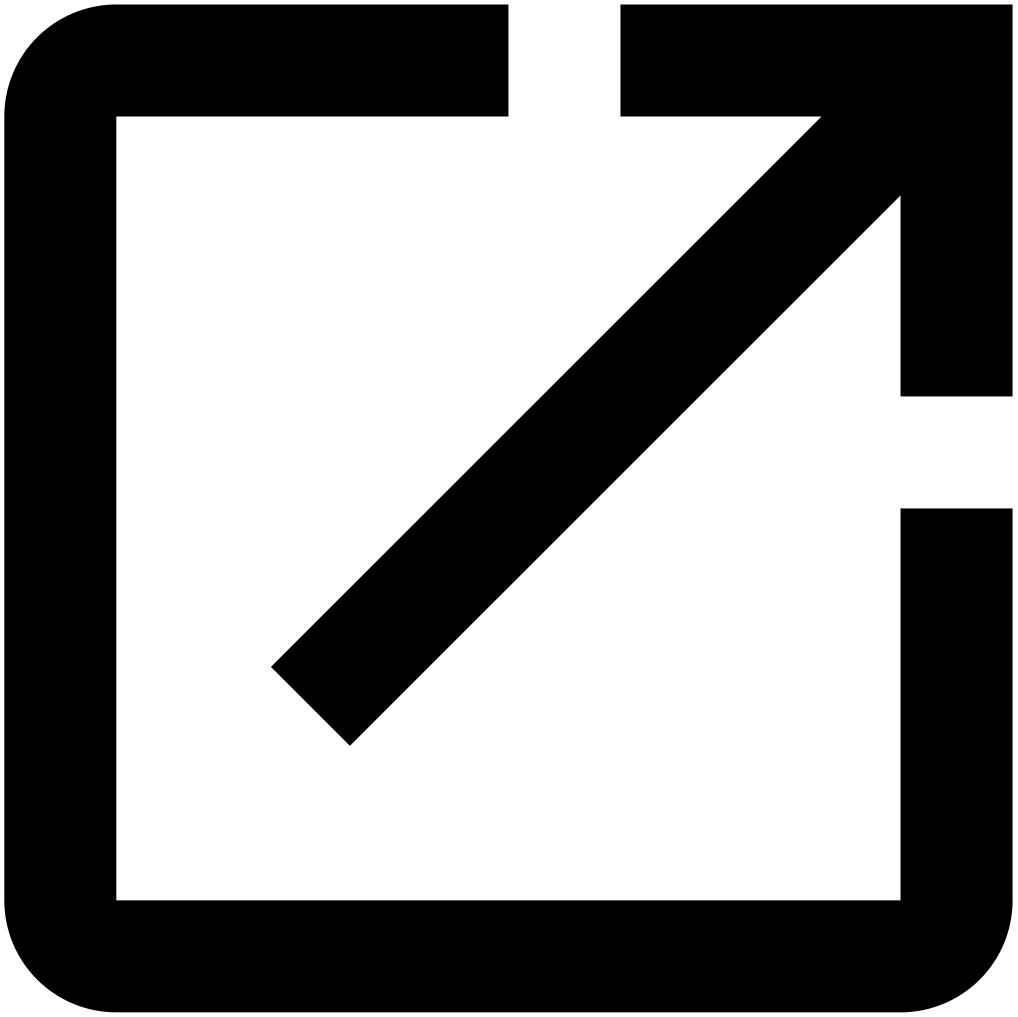


A Russian national believed to be a member of the TrickBot malware development team has been extradited to the U.S. and is currently facing charges that could get him 60 years in prison.

38-year old Vladimir Dunaev, also known as FFX, was a malware developer that supervised the creation of TrickBot's browser injection module, the indictment alleges.

He is the second malware developer associated with the TrickBot gang that the Department of Justice arrested this year. In February, Latvian national Alla Witte, a.k.a. Max, was arrested for writing code related to the control and deployment of ransomware.


F RTINET
0:00



Old member of the gang

Dunaev was arrested in South Korea in September as he was trying to leave the country. He had been forced to stay there for more than a year due to Covid-19 travel restrictions and his passport expired. The extradition completed on October 20.

Dunaev is believed to have been involved with the TrickBot gang since mid-2016 following a recruitment test that involved creating an application that simulated a SOCKS server and altering a copy of the Firefox browser.

He passed both tests with flying colors, showing skills that the TrickBot gang needed. “He’s capable of everything. Such a person is needed,” reads a conversation between two members of the gang responsible for recruiting developers.

Starting June 2016, the defendant created, modified, and updated code for the TrickBot malware gang, the indictment alleges.

Dates	Code description
July 2016 - time of the arrest	modifying Firefox web browser
December 2016 - time of the arrest	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 the 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 to modify them
July 2016 - time of the arrest	An executable app/utility to launch and manage a web browser
July 2016 - time of the arrest	Code that collects and modifies data entries in Google Chrome LevelDB database, browsing history included

Between October 19, 2017, and March 3, 2018, members of the TrickBot gang that included Dunaev and Witte successfully wired more than $1.3 million from victim bank accounts.

Large, well-organized group

According to the indictment, the TrickBot gang has at least 17 members, each with specific attributes within the operation:

- Malware Manager - who outlines the programming needs, manages finances, deploys TrickBot
- Malware Developer - who develops TrickBot modules and hands them to others to encrypt
- Crypter - who encrypt the TrickBot modules so that they evade antivirus detection
- Spammer - who use distribute TrickBot through spam and phishing campaigns

Created from the ashes of the Dyre banking trojan in 2015, TrickBot focused on stealing banking credentials initially, via web injection and logging the victim user’s keystrokes.

Later, it developed into modular malware that could also distribute other threats. These days, the gang has a preference for dropping ransomware on company networks, Conti in particular.

TrickBot is believed to have infected millions of computers, enabling its operators to steal personal and sensitive information (logins, credit cards, emails, passwords, dates of birth, SSNs, addresses) and steal funds from victims' banking accounts.

The malware has impacted businesses in the United States, United Kingdom, Australia, Belgium, Canada, Germany, India, Italy, Mexico, Spain, and Russia.

Apart from Dunaev and Witta, the DoJ has indicted other members of the TrickBot gang whose names have not been revealed and are located in various countries, Russia, Belarus, and Ukraine among them.

Dunaev is currently facing multiple counts of aggravated identity theft, wire fraud, bank fraud. as well as conspiracy to commit computer fraud, aggravated identity theft, and money laundering.

All the charges against him come with a maximum penalty of 60 years in a federal prison.

Source: https://www.bleepingcomputer.com/news/security/trickbot-malware-dev-extradited-to-us-faces-60-years-in-prison/