Russian pleads guilty in US to role in Trickbot malware scheme

December 1 2023

A Russian man has pleaded guilty to involvement in developing the Trickbot malware used to extort businesses.

A Russian man pleaded guilty on Thursday to involvement in developing the Trickbot malware used to extort businesses, including hospitals

during the COVID pandemic, the US Justice Department said.

Vladimir Dunaev, 40, was extradited from South Korea to the United States in 2021 to face charges of conspiracy to commit computer fraud and identity theft and conspiracy to commit wire fraud and bank fraud.

Dunaev pleaded guilty to both charges in an Ohio court on Thursday, the Justice Department said. He will be sentenced on March 20 and faces a maximum penalty of 35 years in prison on both counts.

Dunaev was among nine Russians, some of whom are alleged to have links to Russian intelligence services, who were indicted in the United States for involvement in Trickbot, which was taken down in 2022.

According to the Justice Department, Dunaev provided "specialized services and technical abilities in furtherance of the Trickbot scheme."

"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," US Attorney Rebecca Lutzko said in a statement.

According to the indictments, the Trickbot group deployed malware and an associated ransomware program called Conti to attack hundreds of targets across nearly all of the United States and in more than 30 other countries since 2016.

The malware was also used to steal bank account logins and passwords from victims' computers in order to drain money from the accounts.

According to Britain's National Crime Agency, the operation reaped at least $180 million worldwide.

The group particularly targeted hospitals and health care services during the 2020-2021 coronavirus pandemic, authorities said.

They would invade a computer system and encrypt all the data, demanding hundreds of thousands or even millions of dollars, paid in cryptocurrency, to free up the systems.

In one attack, the group used ransomware against three Minnesota medical facilities, disrupting their computer networks and telephones and causing a diversion of ambulances, US officials said.

In July 2020, an attack hit a local government in a Tennessee town, locking down local emergency medical services and the police department.

A May 2021 virtual incursion against a California hospital network, Scripps Health, locked up the computers of some 24 acute-care and outpatient facilities.

Another Trickbot member, Alla Witte, a Latvian national, pleaded guilty to conspiracy to commit computer fraud in Ohio in June after being extradited from Suriname, where she helped write code for Trickbot and laundered proceeds from the ransomware.

Witte was sentenced to two years and eight months in prison.

© 2023 AFP

Citation: Russian pleads guilty in US to role in Trickbot malware scheme (2023, December 1) retrieved 12 May 2024 from https://techxplore.com/news/2023-12-russian-guilty-role-trickbot-malware.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.