Russian sentenced to five years in prison for Trickbot malware

January 25 2024

A Russian man involved in developing the Trickbot malware has been sentenced to more than five years in prison in Ohio.

A Russian man has been sentenced to more than five years in prison for his involvement in developing the Trickbot malware used to extort

businesses, including hospitals during the COVID pandemic, the US Justice Department said Thursday.

Vladimir Dunaev, 40, who was extradited from South Korea to the United States in 2021, pleaded guilty in November to conspiracy to commit computer fraud and identity theft and conspiracy to commit wire fraud and bank fraud.

Dunaev, originally from Amur Oblast, was sentenced to five years and four months in prison by a judge in the midwestern state of Ohio on Wednesday, the Justice Department said in a statement.

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 developed malicious ransomware and deployed it to attack American hospitals, schools, and businesses," US Attorney Rebecca Lutzko said.

"He and his co-defendants caused immeasurable disruption and financial damage, maliciously infecting millions of computers worldwide."

According to the indictments, the Trickbot group deployed malware and an associated ransomware program called Conti to attack hundreds of targets across 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 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.

Citation: Russian sentenced to five years in prison for Trickbot malware (2024, January 25) retrieved 10 May 2024 from https://techxplore.com/news/2024-01-russian-sentenced-years-

prison-trickbot.html