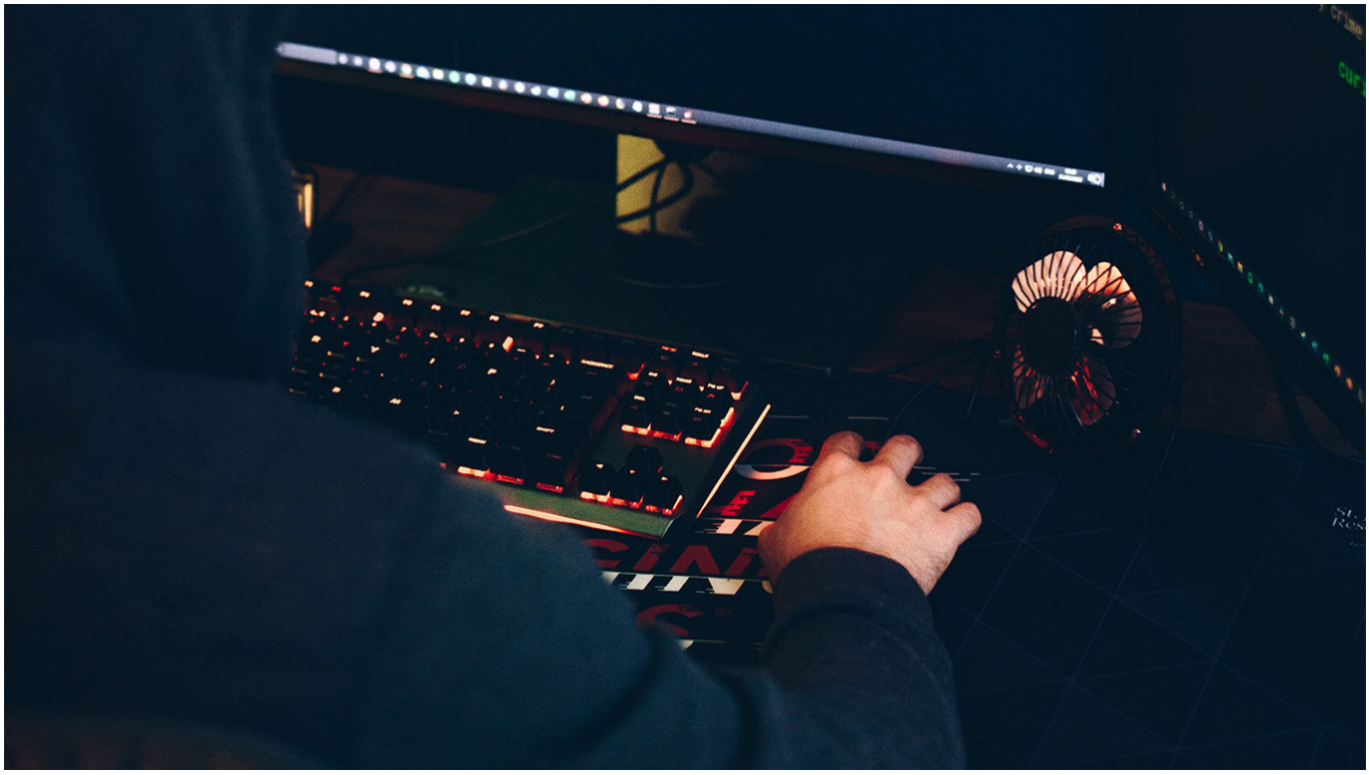
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Indicts 9 Russians Behind 'Trickbot' Malware

By AFP

September 07, 2023



Anete Lusina / pexels

The United States announced indictments Thursday of nine Russians allegedly part of the Trickbot cybercrime group which plied ransomware schemes to extort businesses including hospitals during the Covid-19 pandemic.

The nine, some of whom were alleged to have links to Russian intelligence services, were named in a series of indictments across multiple U.S. states where several of their extortion targets were located.

In parallel, the U.S. Treasury and the State Department, along with British authorities, placed the nine indicted hackers and two others on their sanctions blacklists.

The indictments said 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 countries since 2016.

According to Britain's National Crime Agency, the operation reaped at least $180 million worldwide, including 27 million pounds ($33.7 million) from British targets.

The group particularly targeted hospitals and healthcare services during the 2020-2021 coronavirus pandemic.

Related article: U.S., Britain Slap Joint Sanctions on Russian Cybercrime Gang Trickbot

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

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

"Members of the Trickbot group publicly gloated over the ease of targeting the medical facilities and the speed with which ransoms had been paid to the group," according to a Treasury statement.

In July 2020, an attack hit a local government in a Tennessee town and used that to lock 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.

Scripps later said the cyberattack cost it tens of millions of dollars, including lost revenue and the costs of a lawsuit charging it did not adequately protect patient records.

The nine included Andrey Zhuykov, identified as the senior administrator of the Trickbot operations, as well as coders, testers, a Trickbot "human resources manager," and a finance manager.

The nine faced multiple charges of conspiracy and fraud. All remain at large.

Original url:
https://www.themoscowtimes.com/2023/09/07/us-indicts-9-russians-behind-trickbot-malware-a82394