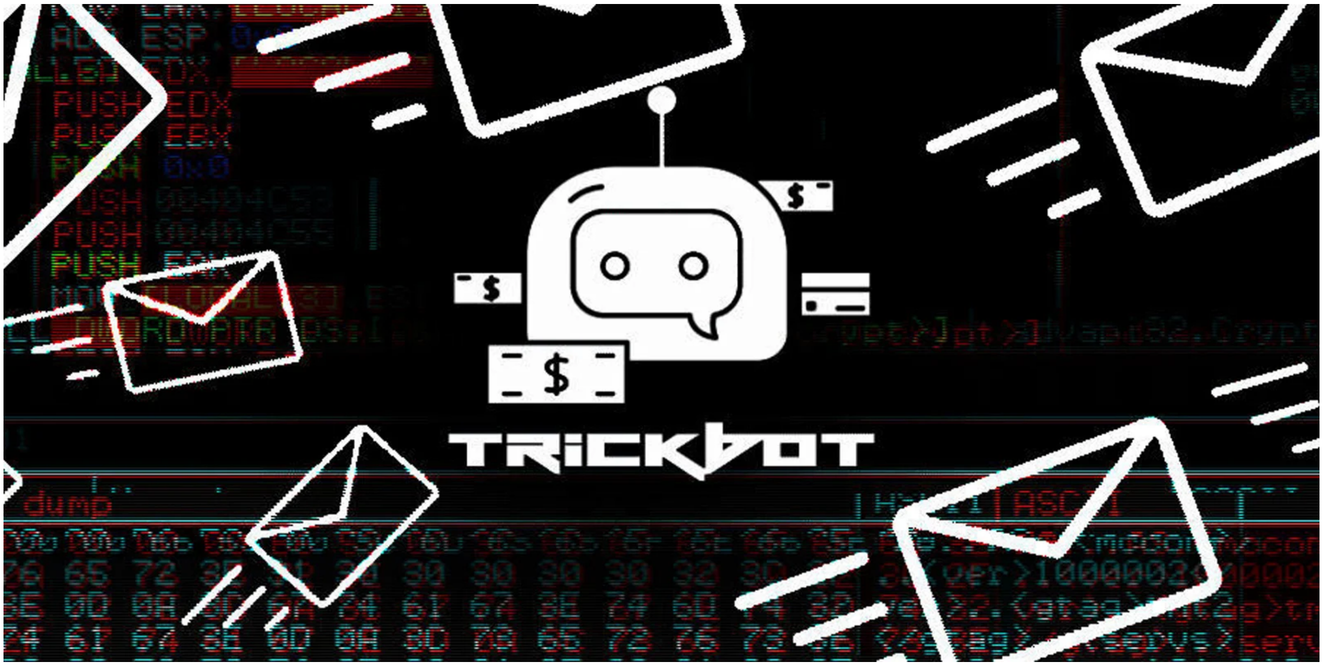
TrickBot gang developer arrested when trying to leave Korea

bleepingcomputer.com/news/security/trickbot-gang-developer-arrested-when-trying-to-leave-korea/

Lawrence Abrams

By
Lawrence Abrams

- September 6, 2021
- 11:24 AM
- 0



An alleged Russian developer for the notorious TrickBot malware gang was arrested in South Korea after attempting to leave the country.

The TrickBot cybercrime group is responsible for a variety of sophisticated malware targeting Windows and Linux devices to gain access to victim's networks, steal data, and deploy other malware, such as ransomware.

Seoul's KBS (via The Record) first reported that a Russian man was stranded in South Korea due to COVID-19 restrictions, and his passport subsequently expired.

After waiting for over a year for his passport to be renewed, the individual attempted to depart South Korea again but was arrested at the airport due to an extradition request by the USA.

It is alleged that the man worked as a web browser developer for the TrickBot operation while he lived in Russia in 2016.

However, the Russian man claims that he did not know he worked for a cybercrime gang after getting hired from an employment site.

"When developing the software, the operation manual did not fall under malicious software," the man told the Seoul High Court.

The Russian individual's attorney is currently fighting the USA extradition attempt, claiming that the USA will prosecute the individual unfairly.

"If you send him to the United States, it will be very difficult to exercise your right of defense and there is a high possibility that you will be subjected to excessive punishment," argued the alleged TrickBot developer's attorney.

Law enforcement's siege on TrickBot

The TrickBot gang is responsible for numerous malware, including TrickBot, BazaLoader, BazaBackdoor, PowerTrick, and Anchor. All of these (malicious tools) are used to gain access to corporate networks, steal files and network credentials, and ultimately deploy ransomware on the network.

Both the Ryuk and Conti ransomware operations are believed to be operated by the TrickBot gang and are known to be deployed through their malware.

Due to the enormous damage and economic loss inflicted by this gang on U.S. interests, the U.S. Cyber Command and a partnership between Microsoft and numerous security companies independently attempted to take down the gang's infrastructure in October 2020.

While there was some disruption of the gang's activities, the malware group quickly rebuilt its infrastructure and continued to launch new malware campaigns targeting organizations worldwide.

More recently, the U.S. Department of Justice charged a Latvian national named Alla Witte with 19 counts in a 47-count indictment for allegedly helping to develop the backend platform for a new ransomware operation.

In court documents from Witte's indictment, prosecutors shared chat logs between TrickBot gang members discussing how they hired developers for various tasks. While some developers realized that the job involved "black hat" activities, conversations indicated that some developers might not have realized they were working for cybercriminals.

While the court document does not name the ransomware operation that Witte is believed to have helped develop, BleepingComputer has been told that she worked on the recently released Diavol ransomware.

Related Articles:

Google exposes tactics of a Conti ransomware access broker

New ChromeLoader malware surge threatens browsers worldwide

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Practice your development skills with lifetime access to DevDojo

Interpol arrests alleged leader of the SilverTerrier BEC gang

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.