Russian Accused of Developing NLBrute Malware Extradited to US

A Russian national accused of developing a piece of malware named NLBrute has been extradited to the United States from the Eastern European country of Georgia.

The suspect, Dariy Pankov, aka dpxaker, was extradited from Georgia in October 2022 and he appeared before a US judge this week. It's unclear for how long he had been in Georgia before being detained, but more than 100,000 Russians reportedly fled to the neighboring country last year, often in an effort to avoid being drafted into Russia's armed forces as the country wages its war against Ukraine.

Pankov has been charged with computer fraud, conspiracy, and access device fraud, and faces up to 47 years in prison. The man will remain in custody during his trial.

According to the Justice Department, Pankov made at least $350,000 from cybercrime activities between 2016 and 2019. He is believed to have developed and sold NLBrute, a tool that has been widely used by cybercriminals to obtain credentials.

The fact that NLBrute was created by a Russian developer has been known. The tool is designed for brute-forcing RDP credentials and at one point it was used in tandem with a botnet in an effort to distribute the brute-forcing process.

US authorities said Pankov used the malware to obtain login credentials for tens of thousands of computers around the world, and offered to sell 35,000 credentials on a cybercrime

forum.

Two law firms in Florida are mentioned as victims in the indictment, but they have not been named.

US authorities said they also plan on forfeiting more than $350,000 that can be traced to the proceeds of Pankov’s crimes.

In addition to the Pankov extradition, the DoJ announced this week that two men from Maryland have been sentenced to a combined 14 years in prison for laundering money as part of a business email compromise (BEC) scheme.

Related: Russian Businessman Guilty in Hacking, Insider Trade Scheme

Related: Russian National Arrested in Canada Over LockBit Ransomware Attacks

Related: Russian Man Extradited to US for Laundering Ryuk Ransomware Money

https://www.securityweek.com/russian-accused-of-developing-nlbrute-malware-extradited-to-us/