DoJ: Estonian Man Tried to Acquire US-Made Hacking Tools for Russia

An Estonian national has been charged in the United States for purchasing US-made electronics and computer hacking tools on behalf of the Russian government and military.

The man, Andrey Shevlyakov, was arrested in Estonia on March 28. He was charged in the US on 18 counts of conspiracy and other charges.

According to the indictment, Shevlyakov did business through several Estonian-based shell companies that he and his co-conspirators used to export microelectronics from the US to Estonia. The goods were then shipped to Russia, thus circumventing export regulations.

Since 2012, the indictment says, Shevlyakov was placed by the US government on a ban list for procuring and delivering export-restricted items to Russia. To evade the list's restrictions, he used false names and shell companies to order items and pay for them.

Purchased items included integrated circuits, low-noise pre-scalers, resistors, synthesizers, analog-to-digital converters that are found in defense systems, including avionics, electronic warfare systems, missiles, and software-defined radio.

According to the indictment, email communication between Shevlyakov and a Russia-based individual has revealed that Shevlyakov also attempted to acquire a licensed copy of

Metasploit Pro, a US-made penetration testing tool that cannot be purchased from Russia directly.

The Russian individual said they had previously failed to acquire the hacking tool through other entities outside of Russia. A few days later, Shevlyakov allegedly responded with a list of prices for various versions of Metasploit Pro.

Metasploit is a highly popular hacking tool that has often been abused by malicious actors. The software has a free version and a Pro version, which costs roughly $15,000.

Between 2012 and 2022, Shevlyakov exported at least $800,000 worth of US electronics, the indictment says.

The goods were delivered via an “intricate logistics operation involving frequent smuggling trips across the Russian border”, the US Department of Justice says.

If convicted, Shevlyakov faces up to 20 years in prison.

Related:US Sanctions Several Entities Aiding Russia’s Cyber Operations

Related: Russian Admits in US Court to Laundering Money for Ryuk Ransomware Gang

Related: US, UK Slap Sanctions on Trickbot Cybercrime Gang

DoJ: Estonian Man Tried to Acquire US-Made Hacking Tools for Russia