Russian Hacker behind 'NeverQuest' Malware, Wanted by FBI, Is Arrested in Spain

thehackernews.com/2017/01/neverquest-fbi-hacker.html

January 22, 2017

A Russian computer hacker wanted by the FBI on hacking allegations was arrested and jailed in Spain earlier this week, while a decision on his extradition to the United States has yet to be made.

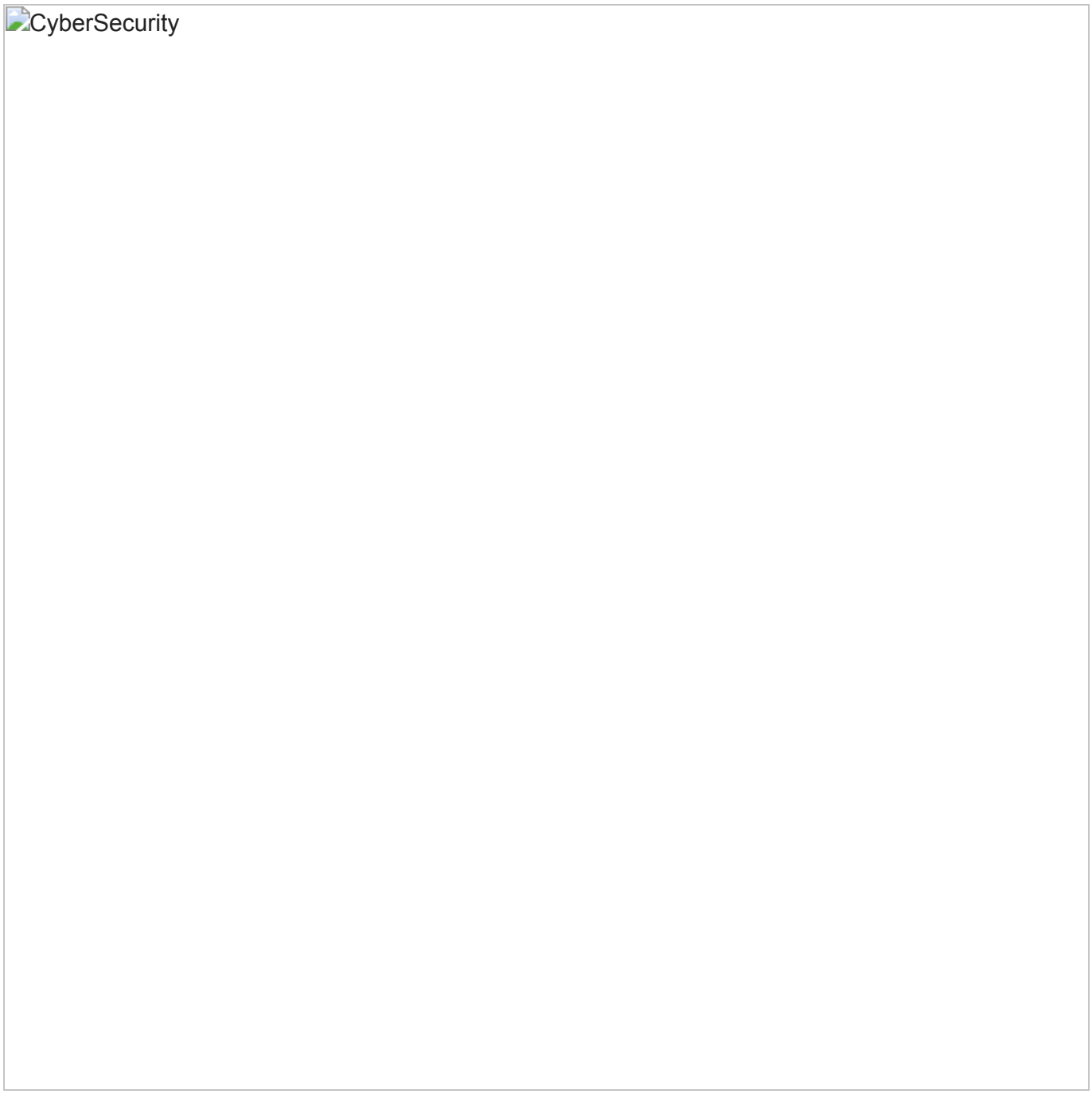
The Guardia Civil, Spanish law enforcement agency officers, have detained 32-year-old **Stanislav Lisov** at Barcelona–El Prat Airport based on an international arrest warrant issued by Interpol at the request of the FBI.

Lisov is arrested on suspicion of creating and operating the **NeverQuest Banking Trojan**, a nasty malware that targeted financial institutions across the world and caused an estimated damage of $5 Million.

The arrest was made after U.S. intelligence agencies found that Russian hackers were behind the November 2016 election hacks that possibly influenced the presidential election in Donald Trump's favor.

However, Spanish police made an official statement, saying that the FBI had requested the arrest of Lisov after an investigation that started in 2014.

NeverQuest banking trojan provided fraudsters access to computers of people and financial institutions to steal banking data.



The Trojan, which spreads itself via social media, email and file transfer protocols, can modify content on banking websites and inject rogue forms into these sites, allowing attackers to steal login credentials from users.

NeverQuest can also allow malicious attackers to take control of a compromised computer through a Virtual Network Computing (VNC) server and then use those computers to log into the victim's online bank and perform the theft.

> "A thorough investigation of the servers operated by Lisov in France and Germany revealed databases with stolen lists of information from accounts of financial institutions, with data indicating, among other things, account balances," the Spanish Civil Guard said Friday.

> "One of the servers leased by Lisov contained files with millions of login credentials, including usernames, passwords, and security questions and answers, for the bank and financial website accounts."

Lisov reportedly works as a systems administrator and website developer for a local company in Taganrog, Russia. The Russian hacker is being held under observation by authorities in the north-eastern region of Catalonia before Spain's High Court decides whether to extradite him to the United States.