US charges Russian military officers over international hacking and disinformation campaigns

By Written by Danny Palmer, Senior WriterSenior Writer Oct. 4, 2018 at 8:13 a.m. PT

Archived: 2026-04-05 19:54:26 UTC

The United States Department of Justice has charged Russian military intelligence officers with international hacking offences.

Security

-
-
-
-

All seven defendants are officers in the Russian Main Intelligence Directorate (GRU), the military intelligence agency of Russia's armed forces. They've been charged with offences including computer hacking, wire fraud, identity theft and money laundering.

The charges from the United States come as the UK and Australia blamed the Russian GRU for a number of recent global cyber attacks.

Some of the charges relate to attacks against the World Anti-Doping Agency (WADA) in an effort to undermine the body following the exposure of a Russian state-sponsored athlete doping program.

Others are in connection with attacks against the Organisation for the Prohibition of Chemical Weapons -- the body investigating the Novichok poisoning of former GRU officer Sergei Skripal and his daughter, Yulia, in Salisbury in March this year. However, this hacking campaign was thwarted by the Dutch defense intelligence service

SEE: A winning strategy for cybersecurity (ZDNet special report) | Download the report as a PDF (TechRepublic)

Spear-phishing emails, spoofed domains, fictitious identities and malware were all used in an effort to remotely steal credentials, which led to the leaking of private and medical information of 250 athletes from almost 30 countries.

In cases where remote attacks weren't successful, GRU officers were sent abroad to conduct hacking operations against hotel Wi-Fi networks used by anti-doping officials during the Olympic Games.

One of these saw officers deployed to Rio de Janeiro, Brazil in August 2016, in an intrusion that resulted in an International Olympic Committee official's credentials being captured and used to gain unauthorised access to

accounts.

Attackers also compromised equipment used in closed access Wi-Fi networks of a hotel hosting an anti-doping conference in Lausunna, Switzerland in Septmeber 2016. This compromised network was used to steal credentials and compromise members of the Canadian Centre for Ethics in Sport.

As part of the campaign, the GRU officers set up a Twitter account claiming to be the 'Fancy Bears' Hack Team and selectively released stolen information, which had often been modified in an effort to besmirch or undermine particular athletes.

According to the indictment, operations were running from December 2014 until at least May this year, and involved "persistent and sophisticated computer intrusions" based on strategic interest to the Russian government.

"The actions of these seven hackers, all working as officials for the Russian government, were criminal, retaliatory, and damaging to innocent victims and the United States' economy, as well as to world organizations," said FBI director Christopher Wray.

"We worked closely with our international partners to identify the actors and disrupt their criminal campaign -- and today, we are sending this message: The FBI will not permit any government, group, or individual to threaten our people, our country, or our partners. We will work tirelessly to find them, stop them, and bring them to justice," he added.

SEE: 10 ways to raise your users' cybersecurity IQ (free PDF)

The defendants are all Russian nationals based in Russia and are Aleksei Sergeyevich Morenets, 41, Evgenii Mikhaylovich Serebriakov, 37, Ivan Sergeyevich Yermakov, 32, Artem Andreyevich Malyshev, 30, Dmitriy Sergeyevich Badin, 27 , Oleg Mikhaylovich Sotnikov, 46, and Alexey Valerevich Minin, 46. They are all GRU officers.

Each defendant is charged with one count of conspiracy to commit computer fraud and abuse, which carries a maximum sentence of five years in prison, one count each of conspiracy to commit wire fraud and conspiracy to commit money laundering, both of which carry a maximum sentence of 20 years.

"We want the hundreds of victims of these Russian hackers to know that we will do everything we can to hold these criminals accountable for their crimes," said U.S. Attorney Scott Brady.

However, like the recent indictment of a North Korean hacker for WannaCry, it's very unlikely anything will come from this announcement -- Russia will not send its citizens to go on trial in the United States.

READ MORE ON CYBER CRIME

- **Cyber security: Nation-state cyber attacks threaten everyone, warns ex-GCHQ boss**
- **Here's what happens during a social engineering cyber-attack (TechRepublic)**
- **Cyber defence: We'll hack back at attackers, says US**
- **Russian hackers target US athlete information, anti-doping agency says [CNET]**
- **Cyber security strategy must be a board-level issue**