Related news

cyberscoop.com/russian-hackers-notpetya-charges-gru/

October 19, 2020

government

US charges Russian GRU officers for NotPetya, other major hacks

(Getty)
Written by Tim Starks
Oct 19, 2020 | CYBERSCOOP
A federal grand jury returned an indictment against six alleged Russian intelligence officers who, collectively, were responsible for “conducting the most disruptive and destructive series of computer attacks ever attributed to a single group,” the Justice Department announced Monday.

Their attacks spanned the globe, including the worldwide 2017 NotPetya outbreak that did more than $1 billion in damage to a number of U.S. organizations, according to the indictment; estimates place its worldwide cost at as much as $10 billion. The six accused

hackers work for the Russian Main Intelligence Directorate, commonly known as the GRU, that's been connected to interference in the 2016 U.S. election and other major cyberattacks.

Besides NotPetya, the alleged co-conspirators were behind destructive malware attacks beginning in December 2015 that disrupted Ukraine's electricity grid; 2017 spearphishing campaigns linked to hack-and-leak efforts to interfere in the French election; attacks related to the Winter Olympics in 2017 and 2018, during a time where Russia was feuding with the Olympics over a doping scandal; spearphishing attacks in 2018 against investigations into the nerve agent poisoning of former Russian intelligence officer Sergei Skripal and others; and 2018 and 2019 campaigns against numerous targets in Georgia, including an attempt to compromise the network of Parliament.

Cybersecurity researchers have labeled the hackers "Sandworm Team," "Telebots," "Voodoo Bear" and "Iron Viking." They are long believed to be behind those attacks and many others among the most high-profile in history.

"No country has weaponized its cyber capabilities as maliciously or irresponsibly as Russia, wantonly causing unprecedented damage to pursue small tactical advantages and to satisfy fits of spite," said John Demers, the assistant attorney general for national security. "Today the Department has charged these Russian officers with conducting the most disruptive and destructive series of computer attacks ever attributed to a single group, including by unleashing the NotPetya malware."

The defendants — Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko and Petr Nikolayevich Pliskin — face charges of conspiracy to conduct computer fraud and abuse, conspiracy to commit wire fraud, wire fraud, damaging protected computers and aggravated identity theft.

The Justice Department previously charged Kovalev, in 2018, alongside a group of other Russian officers for hacking Democrats during the 2016 campaign.

Even though the announcement comes mere weeks before Election Day in the U.S., Demers told reporters that the timing was "not particularly" tied to the vote. The indictment follows a surge in U.S. government responses to accused hacking by Russia, China and Iran, all three of whom are among the top nations the intelligence community has accused of seeking to interfere in the 2020 campaign.

In a background briefing with reporters, a DOJ official said: "Generally, it is a warning. It's a warning to these countries and the actors working with them these activities are not quite as deniable as they might have hoped they were, originally."

The U.S. NotPetya victims cited in the indictment include "hospitals and other medical facilities in the Heritage Valley Health System ('Heritage Valley') in the Western District of Pennsylvania; a A FedEx Corporation subsidiary, TNT Express B.V.; and a large U.S.

pharmaceutical manufacturer.” A grand jury in Pittsburgh returned the indictment.

The December, 2015 attack on the Ukrainian power grid left nearly 230,000 people without power, with the hackers using the BlackEnergy, Industroyer and KillDisk malware in attacks that stretched into late 2016.

The department worked on the indictment with authorities in Ukraine, South Korea, New Zealand, Georgia, the U.K. and other governments, as well as Google, Cisco, Facebook and Twitter.

Also Monday, the U.K. said the GRU conducted cyber reconnaissance against officials and organizations involved in the 2020 Tokyo Olympics before they were postponed.

“The GRU’s actions against the Olympic and Paralympic Games are cynical and reckless,” said Foreign Secretary Dominic Raab. “We condemn them in the strongest possible terms.”

The indictment is available in full below.

[documentcloud url=”http://www.documentcloud.org/documents/7245159-2020-10-19-Unsealed-Indictment-0.html” responsive=true]