JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, July 13, 2018

Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election

The Department of Justice today announced that a grand jury in the District of Columbia returned an indictment presented by the Special Counsel's Office. The indictment charges twelve Russian nationals for committing federal crimes that were intended to interfere with the 2016 U.S. presidential election. All twelve defendants are members of the GRU, a Russian Federation intelligence agency within the Main Intelligence Directorate of the Russian military. These GRU officers, in their official capacities, engaged in a sustained effort to hack into the computer networks of the Democratic Congressional Campaign Committee, the Democratic National Committee, and the presidential campaign of Hillary Clinton, and released that information on the internet under the names "DCLeaks" and "Guccifer 2.0" and through another entity.

"The Internet allows foreign adversaries to attack America in new and unexpected ways," said Deputy Attorney General Rod J. Rosenstein. "Together with our law enforcement partners, the Department of Justice is resolute in its commitment to locate, identify and seek to bring to justice anyone who interferes with American elections. Free and fair elections are hard-fought and contentious, and there will always be adversaries who work to exacerbate domestic differences and try to confuse, divide, and conquer us. So long as we are united in our commitment to the shared values enshrined in the Constitution, they will not succeed."

According to the allegations in the indictment, Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev were officials in Unit 26165 and Unit 74455 of the Russian government's Main Intelligence Directorate.

In 2016, officials in Unit 26165 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through that process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to these networks.

The officials in Unit 26165 coordinated with officials in Unit 74455 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLeaks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hacktivists" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 15, 2016 between 4:19PM and 4:56PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.

Members of Unit 74455 also conspired to hack into the computers of state boards of elections, secretaries of state, and US companies that supplied software and other technology related to the administration of elections to steal voter data stored on those computers.

To avoid detection, defendants used false identities while using a network of computers located around the world, including the United States, paid for with cryptocurrency through mining bitcoin and other means intended to obscure the origin of the funds. This funding structure supported their efforts to buy key accounts, servers, and domains. For example, the same bitcoin mining operation that funded the registration payment for DCLeaks.com also funded the servers and domains used in the spearphishing campaign.

The indictment includes 11 criminal counts:

- Count One alleges a criminal conspiracy to commit an offense against the United States through cyber operations by the GRU that involved the staged release of stolen documents for the purpose of interfering with the 2016 president election;
- Counts Two through Nine charge aggravated identity theft for using identification belonging to eight victims to further their computer fraud scheme;
- Count Ten alleges a conspiracy to launder money in which the defendants laundered the equivalent of more than $95,000 by transferring the money that they used to purchase servers and to fund other costs related to their hacking activities through cryptocurrencies such as bitcoin; and
- Count Eleven charges conspiracy to commit an offense against the United States by attempting to hack into the computers of state boards of elections, secretaries of state, and US companies that supplied software and other technology related to the administration of elections.

There is no allegation in the indictment that any American was a knowing participant in the alleged unlawful activity or knew they were communicating with Russian intelligence officers. There is no allegation in the indictment that the charged conduct altered the vote count or changed the outcome of the 2016 election.

Everyone charged with a crime is presumed innocent unless proven guilty in court. At trial, prosecutors must introduce credible evidence that is sufficient to prove each defendant guilty beyond a reasonable doubt, to the unanimous satisfaction of a jury of twelve citizens.

This case was investigated with the help of the FBI’s cyber teams in Pittsburgh, Philadelphia and San Francisco and the National Security Division. The Special Counsel's investigation is ongoing. There will be no comments from the Special Counsel at this time.

Topic(s):
National Security

Component(s):
Office of the Deputy Attorney General

Press Release Number:
18 - 923

Updated July 13, 2018