U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations

Published: 2018-10-04 · Archived: 2026-04-06 01:48:54 UTC

A grand jury in the Western District of Pennsylvania has indicted seven defendants, all officers in the Russian Main Intelligence Directorate (GRU), a military intelligence agency of the General Staff of the Armed Forces of the Russian Federation, for computer hacking, wire fraud, aggravated identity theft, and money laundering.

According to the indictment, beginning in or around December 2014 and continuing until at least May 2018, the conspiracy conducted persistent and sophisticated computer intrusions affecting U.S. persons, corporate entities, international organizations, and their respective employees located around the world, based on their strategic interest to the Russian government.

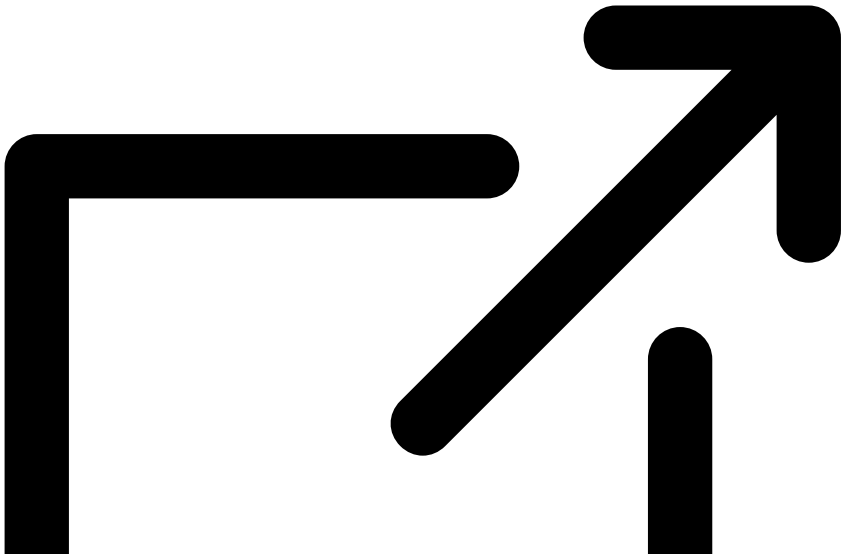
Among the goals of the conspiracy was to publicize stolen information as part of an influence and disinformation campaign designed to undermine, retaliate against, and otherwise delegitimize the efforts of international anti-doping organizations and officials who had publicly exposed a Russian state-sponsored athlete doping program and to damage the reputations of athletes around the world by falsely claiming that such athletes were using banned or performance-enhancing drugs.

The charges were announced at a press conference by Assistant Attorney General for National Security John C. Demers, United States Attorney for the Western District of Pennsylvania Scott W. Brady, FBI Deputy Assistant Director for Cyber Division, Eric Welling, and Director General Mark Flynn for the Royal Canadian Mounted Police.

"State-sponsored hacking and disinformation campaigns pose serious threats to our security and to our open society, but the Department of Justice is defending against them," Attorney General Jeff Sessions said. "Today we are indicting seven GRU officers for multiple felonies each, including the use of hacking to spread the personal information of hundreds of anti-doping officials and athletes as part of an effort to distract from Russia’s state-sponsored doping program. The defendants in this case allegedly targeted multiple Americans and American entities for hacking, from our national anti-doping agency to the Westinghouse Electric Company near Pittsburgh. We are determined to achieve justice in these cases and we will continue to protect the American people from hackers and disinformation."

“The investigation leading to the indictments announced

t



oday is the FBI at its best," said FBI Director Christopher Wray. "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. Their actions extended beyond borders, but so did the FBI's investigation. 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."

"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 Brady. State actors who target U.S. citizens and companies are no different than any other common criminal: they will be investigated and prosecuted to the fullest extent of the law."

The defendants, all Russian nationals and residents, are Aleksei Sergeyevich Morenets, 41, Evgenii Mikhaylovich, Serebriakov, 37, Ivan Sergeyevich Yermakov, 32, Artem Andreyevich Malyshev, 30, and Dmitriy Sergeyevich Badin, 27, who were each assigned to Military Unit 26165, and Oleg Mikhaylovich Sotnikov, 46, and Alexey Valerevich Minin, 46, who were also GRU officers.

The indictment alleges that defendants Yermakov, Malyshev, Badin, and unidentified conspirators, often using fictitious personas and proxy servers, researched victims, sent spearphishing emails, and compiled, used, and monitored malware command and control servers.

When the conspirators' remote hacking efforts failed to capture log-in credentials, or if the accounts that were successfully compromised did not have the necessary access privileges for the sought-after information, teams of GRU technical intelligence officers, including Morenets, Serebriakov, Sotnikov, and Minin, traveled to locations around the world where targets were physically located. Using specialized equipment, and with the remote support of conspirators in Russia, including Yermakov, these close access teams hacked computer networks used

by victim organizations or their personnel through Wi-Fi connections, including hotel Wi-Fi networks. After a successful hacking operation, the close access team transferred such access to conspirators in Russia for exploitation.

Among other instances, the indictment alleges that following a series of high-profile independent investigations starting in 2015, which publicly exposed Russia's systematic state-sponsored subversion of the drug testing processes prior to, during, and subsequent to the 2014 Sochi Winter Olympics (according to one report, known as the "McLaren Report"), the conspirators began targeting systems used by international anti-doping organizations and officials. After compromising those systems, the defendants stole credentials, medical records, and other data, including information regarding therapeutic use exemptions (TUEs), which allow athletes to use otherwise prohibited substances.

Using social media accounts and other infrastructure acquired and maintained by GRU Unit 74455 in Russia, the conspiracy thereafter publicly released selected items of stolen information, in many cases in a manner that did not accurately reflect their original form, under the false auspices of a hacktivist group calling itself the "Fancy Bears' Hack Team." As part of its influence and disinformation efforts, the Fancy Bears' Hack Team engaged in a concerted effort to draw media attention to the leaks through a proactive outreach campaign. The conspirators exchanged e-mails and private messages with approximately 186 reporters in an apparent attempt to amplify the exposure and effect of their message.

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. Defendants Morenets, Serebriakov, Yermakov, Malyshev, and Badin are each also charged with two counts of aggravated identity theft, which carries a consecutive sentence of two years in prison. Defendant Yermakov is also charged with five counts of wire fraud, which carries a maximum sentence of 20 years.

Defendants Yermakov, Malyshev, and Badin are also charged defendants in federal indictment number CR 18-215 in the District of Columbia, and accused of conspiring to gain unauthorized access into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election.

According to the indictment:

Context of the Hacking and Related Influence and Disinformation Efforts

In July 2016, the World Anti-Doping Agency's (WADA) Independent Person Report (the "First McLaren Report") was released, describing Russia's systematic state-sponsored subversion of the drug testing process prior to, during, and subsequent to the 2014 Sochi Winter Olympics. This investigation had the support of advocates for clean sports, including the United States Anti-Doping Agency (USADA), the Canadian Centre for Ethics in Sport (CCES, Canada's anti-doping agency). Eventually, in some instances only after arbitration rulings by the International Court of Arbitration for Sport (TAS/CAS), approximately 111 Russian athletes were excluded from the 2016 Summer Olympic Games, in Rio de Janeiro, Brazil, by a number of international athletics federations, including track-and-field's International Association of Athletics Federations (IAAF). The International

Paralympic Committee (IPC) further imposed a blanket ban of Russian athletes from the 2016 Paralympic Games, which were also held in Rio.

Intrusion Activities in Rio de Janeiro, Brazil

Days after the release of the First McLaren Report and the International Olympic Committee's and IPC's subsequent decisions regarding the exclusion of Russian athletes, the conspirators prepared to hack into the networks of WADA, the United States Anti-Doping Agency (USADA), and TAS/CAS. The conspirators, including specifically defendants Yermakov and Malyshev, procured spoofed domains (which mimicked legitimate WADA and TAS/CAS domains) and other infrastructure, probed such entities' networks, and spearphished WADA and USADA employees. Although Yermakov and Malyshev are both alleged to have prepared to send spearphishing e-mails to TAS/CAS, the indictment does not allege that organization was compromised.

Likely as a result of the conspirators' failure to capture necessary log-in credentials, or because those victim accounts that were successfully compromised did not have the necessary access privileges for the sought-after information, defendants Morenets and Serebriakov, in at least one instance with the remote support of Yermakov, deployed to Rio to conduct hacking operations targeting and maintaining persistent access to Wi-Fi networks used by anti-doping officials. As a result of these efforts, in August 2016, the conspirators captured that IOC official's credentials and thereafter used them, and another set of credentials belonging to the same official to gain unauthorized access to an account in WADA's ADAMS database and medical and anti-doping related information contained therein. (The broader ADAMS database was not compromised in the intrusion.)

Also in 2016, a senior USADA anti-doping official traveled to Rio de Janeiro for the Olympics and Paralympic games. While there, the USADA official used Wi-Fi at the hotel and other Wi-Fi access points in Rio to remotely access USADA's computer systems and conduct official business. While the USADA official was in Rio, conspirators successfully compromised the credentials for his or her USADA email account, which included summaries of athlete test results and prescribed medications.

Intrusion Activities in Lausanne, Switzerland

In mid-September 2016, WADA hosted an anti-doping conference in Lausanne, Switzerland. On September 18, 2016, defendants Morenets and Serebriakov traveled to Lausanne with equipment used in close access Wi-Fi compromises. On or about September 19, 2016, Morenets and Serebriakov compromised the Wi-Fi network of a hotel hosting the conference and leveraged that access to compromise the laptop and credentials of a senior CCES official staying at the hotel. Other conspirators thereafter used the stolen credentials to compromise CCES's networks in Canada, using a tool used to extract hashed passwords, the metadata of which indicated it was compiled by Badin.

Intrusion Targeting Anti-Doping Officials at Sporting Federations

In December 2016 and January 2017, conspirators successfully compromised the networks of IAAF and the Fédération Internationale de Football Association ("FIFA") and targeted computers and accounts used by each organization's top anti-doping official. Among the data stolen from such officials were keylogs, file directories,

anti-doping policies and strategies, lab results, medical reports, contracts with doctors and medical testing labs, information about medical testing procedures, and TUEs.

Related GRU Influence and Disinformation Operations

On September 12, 2016, shortly after the compromise of the IOC official's ADAMS credentials, but before the compromise of USADA's and CCES's networks, conspirators claiming to be the hacktivist group Fancy Bears' Hack Team used online accounts and other infrastructure procured and managed by Unit 74455, as well as the website fancybears.net, to publicly release TUEs, other medical information, and emails stolen from anti-doping officials at WADA, USADA, CCES, IAAF, FIFA, and approximately 35 other anti-doping agencies or sporting organizations. In some instances, the WADA documents were modified from their original form. Ultimately, the Fancy Bears' Hack Team released stolen information that included private or medical information of approximately 250 athletes from almost 30 countries.

The conspirators' release of the stolen information was, in some instances, accompanied by posts and other communications that parroted or supported themes that the Russian government had used in its official narrative regarding the anti-doping agencies' investigative findings. From 2016 through 2018, the conspirators engaged in a proactive outreach campaign, using Twitter and e-mail to communicate with approximately 186 reporters about the stolen information. After articles were published, conspirators used the Fancy Bears' Hack Team social media accounts to draw attention to the articles in an attempt to amplify the exposure and effect of their message.

Other Targets of the Conspiracy

The conspiracy is also alleged to have targeted other entities in the Western District of Pennsylvania and abroad that were of interest to the Russian government. For example, as early as November 20, 2014, Yermakov performed reconnaissance of Westinghouse Electric Company's (WEC) networks and personnel. In the following months, Yermakov and conspirators created a fake WEC domain and sent spearphishing emails to WEC employees' work and personal email accounts, which were designed to harvest the employees' log-in credentials.

More recently, in April 2018, Morenets, Serebriakov, Sotnikov, and Minin, all using diplomatic passports, traveled to The Hague in the Netherlands in furtherance of another close access operation targeting the Organisation for the Prohibition of Chemical Weapons (OPCW) computer networks through Wi-Fi connections. All four GRU officers intended to travel thereafter to Spiez, Switzerland, to target the Spiez Swiss Chemical Laboratory, an accredited laboratory of the OPCW which was analyzing military chemical agents, including the chemical agent that the United Kingdom authorities connected to the poisoning of a former GRU officer in that country. However, Morenets, Serebriakov, Sotnikov, and Minin were disrupted during their OPCW hacking operation by the Militaire Inlichtingen- en Veiligheidsdienst (MIVD), the Dutch defense intelligence service. As part of this disruption, Morenet's and Serebriakov's abandoned the Wi-Fi compromise equipment, which they had placed in the trunk of a rental car parked adjacent to the OPCW property. Data obtained from at least one item of this equipment confirmed its operational use at multiple locations around the world, including connections to the Wi-Fi network of the CCES official's hotel in Switzerland (the dates the conspirators conducted the Wi-Fi compromise of the senior CCES official's laptop at the same hotel), and at another hotel in Kuala Lumpur, Malaysia in December 2017.

Source: https://www.justice.gov/archives/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and