Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace

Press Release

Monday, October 19, 2020

For Immediate Release
Office of Public Affairs

Defendants' Malware Attacks Caused Nearly One Billion USD in Losses to Three Victims Alone; Also Sought to Disrupt the 2017 French Elections and the 2018 Winter Olympic Games

On Oct. 15, 2020, a federal grand jury in Pittsburgh returned an indictment charging six computer hackers, all of whom were residents and nationals of the Russian Federation (Russia) and officers in Unit 74455 of the Russian Main Intelligence Directorate (GRU), a military intelligence agency of the General Staff of the Armed Forces.

These GRU hackers and their co-conspirators engaged in computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize: (1) Ukraine; (2) Georgia; (3) elections in France; (4) efforts to hold Russia accountable for its use of a weapons-grade nerve agent, Novichok, on foreign soil; and (5) the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag, as a consequence of Russian government-sponsored doping effort.

Their computer attacks used some of the world's most destructive malware to date, including: KillDisk and Industroyer, which each caused blackouts in Ukraine; NotPetya, which caused nearly $1 billion in losses to the three victims identified in the indictment alone; and Olympic Destroyer, which disrupted thousands of

computers used to support the 2018 PyeongChang Winter Olympics. The indictment charges the defendants with conspiracy, computer hacking, wire fraud, aggravated identity theft, and false registration of a domain name.

According to the indictment, beginning in or around November 2015 and continuing until at least in or around October 2019, the defendants and their co-conspirators deployed destructive malware and took other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victim computers (hacking). As alleged, the conspiracy was responsible for the following destructive, disruptive, or otherwise destabilizing computer intrusions and attacks:

- **Ukrainian Government & Critical Infrastructure**: December 2015 through December 2016 destructive malware attacks against Ukraine's electric power grid, Ministry of Finance, and State Treasury Service, using malware known as BlackEnergy, Industroyer, and KillDisk;
- **French Elections**: April and May 2017 spearphishing campaigns and related hack-and-leak efforts targeting French President Macron's "La République En Marche!" (En Marche!) political party, French politicians, and local French governments prior to the 2017 French elections;
- **Worldwide Businesses and Critical Infrastructure (NotPetya)**: June 27, 2017 destructive malware attacks that infected computers worldwide using malware known as NotPetya, including hospitals and other medical facilities in the Heritage Valley Health System (Heritage Valley) in the Western District of Pennsylvania; a FedEx Corporation subsidiary, TNT Express B.V.; and a large U.S. pharmaceutical manufacturer, which together suffered nearly $1 billion in losses from the attacks;
- **PyeongChang Winter Olympics Hosts, Participants, Partners, and Attendees**: December 2017 through February 2018 spearphishing campaigns and malicious mobile applications targeting South Korean citizens and officials, Olympic athletes, partners, and visitors, and International Olympic Committee (IOC) officials;
- **PyeongChang Winter Olympics IT Systems (Olympic Destroyer)**: December 2017 through February 2018 intrusions into computers supporting the 2018 PyeongChang Winter Olympic Games, which culminated in the Feb. 9, 2018, destructive malware attack against the opening ceremony, using malware known as Olympic Destroyer;
- **Novichok Poisoning Investigations**: April 2018 spearphishing campaigns targeting investigations by the Organisation for the Prohibition of Chemical Weapons (OPCW) and the United Kingdom's Defence Science and Technology Laboratory (DSTL) into the nerve agent poisoning of Sergei Skripal, his daughter, and several U.K. citizens; and
- **Georgian Companies and Government Entities**: a 2018 spearphishing campaign targeting a major media company, 2019 efforts to compromise the network of Parliament, and a wide-ranging website defacement campaign in 2019.

Cybersecurity researchers have tracked the Conspirators and their malicious activity using the labels "Sandworm Team," "Telebots," "Voodoo Bear," and "Iron Viking."

The charges were announced by Assistant Attorney General John C. Demers; FBI Deputy Director David Bowdich; U.S. Attorney for the Western District of Pennsylvania Scott W. Brady; and Special Agents in Charge of the FBI's Atlanta, Oklahoma City, and Pittsburgh Field Offices, J.C. "Chris" Hacker, Melissa R. Godbold, and Michael A. Christman, respectively.

"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 Assistant Attorney General for National Security John C. Demers. "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. No nation will recapture greatness while behaving in this way."

"The FBI has repeatedly warned that Russia is a highly capable cyber adversary, and the information revealed in this indictment illustrates how pervasive and destructive Russia's cyber activities truly are," said FBI Deputy Director David Bowdich. "But this indictment also highlights the FBI's capabilities. We have the tools to investigate these malicious malware attacks, identify the perpetrators, and then impose risks and consequences on them. As demonstrated today, we will relentlessly pursue those who threaten the United States and its citizens."

"For more than two years we have worked tirelessly to expose these Russian GRU Officers who engaged in a global campaign of hacking, disruption and destabilization, representing the most destructive and costly cyber-attacks in history," said U.S. Attorney Scott W. Brady for the Western District of Pennsylvania. "The crimes committed by Russian government officials were against real victims who suffered real harm. We have an obligation to hold accountable those who commit crimes – no matter where they reside and no matter for whom they work – in order to seek justice on behalf of these victims."

"The exceptional talent and dedication of our teams in Pittsburgh, Atlanta and Oklahoma City who spent years tracking these members of the GRU is unmatched," said FBI Pittsburgh Special Agent in Charge Michael A. Christman. "These criminals underestimated the power of shared intelligence, resources and expertise through law enforcement, private sector and international partnerships."

The defendants, Yuriy Sergeyevich Andrienko (Юрий Сергеевич Андриенко), 32; Sergey Vladimirovich Detistov (Сергей Владимирович Детистов), 35; Pavel Valeryevich Frolov (Павел Валерьевич Фролов), 28; Anatoliy Sergeyevich Kovalev (Анатолий Сергеевич Ковалев), 29; Artem Valeryevich Ochichenko (Артем Валерьевич Очиченко), 27; and Petr Nikolayevich Pliskin (Петр Николаевич Плискин), 32, are all charged in seven counts: conspiracy to conduct computer fraud and abuse, conspiracy to commit wire fraud, wire fraud, damaging protected computers, and aggravated identity theft. Each defendant is charged in every count. The charges contained in the indictment are merely accusations, however, and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt.

The indictment accuses each defendant of committing the following overt acts in furtherance of the charged crimes:

Defendant	Summary of Overt Acts
Yuriy Sergeyevich Andrienko	· Developed components of the NotPetya and Olympic Destroyer malware.
Sergey Vladimirovich Detistov	· Developed components of the NotPetya malware; and · Prepared spearphishing campaigns targeting the 2018 PyeongChang Winter Olympic Games.
Pavel Valeryevich Frolov	· Developed components of the KillDisk and NotPetya malware.
Anatoliy Sergeyevich Kovalev	· Developed spearphishing techniques and messages used to target: - En Marche! officials; - employees of the DSTL; - members of the IOC and Olympic athletes; and - employees of a Georgian media entity.
Artem Valeryevich Ochichenko	· Participated in spearphishing campaigns targeting 2018 PyeongChang Winter Olympic Games partners; and · Conducted technical reconnaissance of the Parliament of Georgia official domain and attempted to gain unauthorized access to its network.
Petr Nikolayevich Pliskin	· Developed components of the NotPetya and Olympic Destroyer malware.

The defendants and their co-conspirators caused damage and disruption to computer networks worldwide, including in France, Georgia, the Netherlands, Republic of Korea, Ukraine, the United Kingdom, and the United States.

The NotPetya malware, for example, spread worldwide, damaged computers used in critical infrastructure, and caused enormous financial losses. Those losses were only part of the harm, however. For example, the NotPetya malware impaired Heritage Valley's provision of critical medical services to citizens of the Western District of Pennsylvania through its two hospitals, 60 offices, and 18 community satellite facilities. The attack caused the unavailability of patient lists, patient history, physical examination files, and laboratory

records. Heritage Valley lost access to its mission-critical computer systems (such as those relating to cardiology, nuclear medicine, radiology, and surgery) for approximately one week and administrative computer systems for almost one month, thereby causing a threat to public health and safety.

The conspiracy to commit computer fraud and abuse carries a maximum sentence of five years in prison; conspiracy to commit wire fraud carries a maximum sentence of 20 years in prison; the two counts of wire fraud carry a maximum sentence of 20 years in prison; intentional damage to a protected computer carries a maximum sentence of 10 years in prison; and the two counts of aggravated identity theft carry a mandatory sentence of two years in prison. The indictment also alleges false registration of domain names, which would increase the maximum sentence of imprisonment for wire fraud to 27 years in prison; the maximum sentence of imprisonment for intentional damage to a protected computer to 17 years in prison; and the mandatory sentence of imprisonment for aggravated identity theft to four years in prison. These maximum potential sentences are prescribed by Congress, however, and are provided here for informational purposes only, as the assigned judge will determine any sentence of a defendant.

Defendant Kovalev was previously charged in federal indictment number CR 18-215, in the District of Columbia, with conspiring to gain unauthorized access into the computers of U.S. persons and entities involved in the administration of the 2016 U.S. elections.

Trial Attorney Heather Alpino and Deputy Chief Sean Newell of the National Security Division’s Counterintelligence and Export Control Section and Assistant U.S. Attorneys Charles Eberle and Jessica Smolar of the U.S. Attorney’s Office for the Western District of Pennsylvania are prosecuting this case. The FBI’s Atlanta, Oklahoma City, and Pittsburgh field offices conducted the investigation, with the assistance of the FBI’s Cyber Division.

The Criminal Division’s Office of International Affairs provided critical assistance in this case. The department also appreciates the significant cooperation and assistance provided by Ukrainian authorities, the Governments of the Republic of Korea and New Zealand, Georgian authorities, and the United Kingdom’s intelligence services, as well as many of the FBI’s Legal Attachés and other foreign authorities around the world. Numerous victims cooperated and provided valuable assistance in the investigation.

The department is also grateful to Google, including its Threat Analysis Group (TAG); Cisco, including its Talos Intelligence Group; Facebook; and Twitter, for the assistance they provided in this investigation. Some private sector companies independently disabled numerous accounts for violations of the companies’ terms of service.

Updated July 13, 2022

Topics

Countering Nation-State Threats

National Security

Press Release Number: 20-1,117