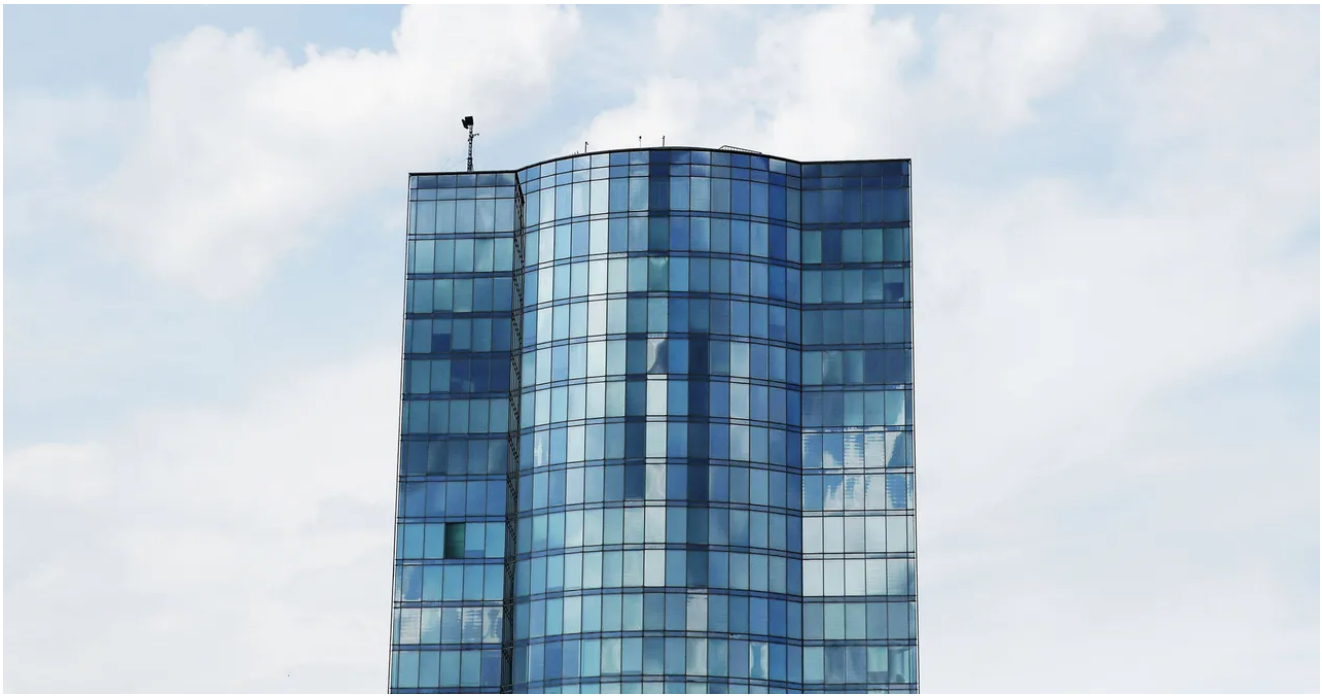
US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit

wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/

Andy Greenberg October 19, 2020



Nearly half a decade ago, the Russian hackers known as Sandworm hit Western Ukraine with the first-ever cyberattack to cause a blackout, an unprecedented act of cyberwar that turned off the lights for a quarter million Ukrainians. They were just getting started. From there Sandworm embarked on a years-long spree of wantonly destructive attacks: another blackout attack on the Ukrainian capital of Kyiv in 2016, the release of the NotPetya worm in 2017 that spread globally from Ukraine to cause $10 billion in damage, and a cyberattack that temporarily destroyed the IT backend of the 2018 Winter Olympics in South Korea, among others.

Yet in spite of crossing every red line the cybersecurity world has tried to draw to protect civilian critical infrastructure from catastrophic hacking, Sandworm's members had never been charged or even officially named in connection with those attacks. Until now.

On Monday, the Department of Justice unsealed charges including computer fraud and conspiracy against six of the hackers who allegedly make up Sandworm, a group also known in the security industry by the names Telebots, Voodoo Bear, and Hades, and confirmed earlier this year to work in Unit 74455 of Russia's GRU military intelligence agency based in a building known as the Tower in the Moscow suburb of Khimki. The indictment names all six Russian men, who are in their late twenties to early thirties: Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Artem Valeryevich Ochichenko, and

Petr Nikolayevich Pliskin, as well as Anatoliy Sergeyevich Kovalev, who was previously indicted two years ago for his allegedly role into hacking US States' Boards of Election in 2016.

Courtesy of Department of Justice

“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,” assistant attorney general John Demers said in a statement.

"They continue to do disruptive and destructive attacks against anyone they perceive to be an adversary to Russia or to have slighted Russia in some way," added a senior Justice Department official who asked not to be identified, in a call with WIRED. "This is probably one of the most dangerous and aggressive groups of hackers that’s out there."

The charges represent not only the first criminal charges against Sandworm for its most destructive attacks, but the first time that most of the charged hackers have been publicly identified as members of the hacker group. Two other GRU hackers believed to be part of Sandworm—Aleksey Aleksandrovich Potemkin and Aleksandr Vladimirovich Osadchuk—were previously named in the separate, 2018 indictment of 12 GRU hackers for hacking that interfered in the 2016 US election. Kovalev, who in the new indictment is accused of helping to hack the 2017 campaign of French president Emmanuel Macron, was also named in those 2018 charges.

The new indictment also represents the first official acknowledgement from the US government that Sandworm was responsible for a cyberattack on the 2018 Winter Olympics, in which a piece of malware known as Olympic Destroyer took down much of the IT infrastructure of the Games just as the opening ceremony was beginning in Pyeongchang, South Korea. Olympic Destroyer contained layers of "false flags," spoofed clues in its code designed to trick investigators into blaming North Korea or China. And according to the new indictment, Sandworm also tried to breach two Olympic partner organizations responsible for timekeeping in the Olympics, not just the Wifi, Olympics app, ticketing, and displays that were ultimately disrupted—perhaps an attempt to corrupt the Olympics sporting events' actual results, too.

In the more than two years that followed, no government in the world officially seemed willing to blame the cyberattack on Russia, even as private intelligence firms like FireEye found strong evidence of Sandworm's involvement, and US intelligence leaked their findings of Russia's culpability to *The Washington Post*. (The European Union did finally name "Olympic Destroyer" as one of the known names for Sandworm in sanctions against the group in July, but without explicitly saying that the sanctions were in response to the Olympics attack.)

That long silence led to warnings from the cybersecurity community that Russia would no doubt attempt to attack the 2020 Olympics in Tokyo, too. And separately from the Sandworm indictment, those warnings were proven true today when the UK's National Cybersecurity Center revealed that it had tracked, in a joint operation with US intelligence agencies, reconnaissance activities by Russian hackers seeking to disrupt the 2020 Olympics as predicted—though the games were ultimately delayed due to Covid-19—targeting the games' organizers, logistics partners, and sponsors.

The Justice Department's new indictment against the hackers includes a long history of other GRU hacking around the world: The hackers allegedly targeted the Organization for the Prohibition of Chemical Weapons in the Netherlands and the United Kingdom's Defense Science and Technology Laboratory while those two organizations were investigating the Novichok poisoning of GRU defector Sergei Skripal and his daughter, an attack not previously linked to Sandworm despite known GRU involvement. The indictment also lays out new details of Sandworm's targeting of the nation of Georgia in 2019, which included an attempt to compromise the Georgian parliament in addition to a previously known campaign of web defacements across the country's internet, affecting 15,000 sites.

Perhaps most significantly, the criminal charges mark the first global law enforcement response targeting Sandworm's hackers for their release of the NotPetya malware that ravaged networks across the world. To initially install its data-destroying, self-spreading code on its victims' machines, Sandworm hijacked the update mechanism of MEDoc, a common piece of Ukrainian accounting software. But beyond infecting hundreds of Ukrainian companies and government agencies, NotPetya also spread far beyond Ukraine's borders, inflicting $10 billion in damage to companies including Merck, FedEx, Maersk, Mondelez, as well as paralyzing updates to medical record systems in hospitals across the US and causing serious collateral damage to Russian firms, too.

The indictment accuses Andrienko, Detistov, Frolov, and Pliskin specifically of developing different components of the NotPetya malware. It goes so far as to state that Andrienko and Pliskin "celebrated" after the malware was deployed.

Despite US and EU sanctions against Russia for NotPetya, no hackers were criminally charged with the global cyberattack, or even named as individually responsible for it, until now. That apparent inaction led many in the cybersecurity world to marvel for years at Western governments' failure to hold Sandworm accountable. "NotPetya tested the red lines of the West, and the result of the test was that there are no red lines yet," Johns Hopkins professor of strategic studies Thomas Rid told WIRED in 2018. "The lack of any proper response is almost an invitation to escalate more."

Now, however belatedly, that accountability has arrived for Sandworm's hackers. But as with so many indictments of foreign, state-sponsored hackers, the defendants will likely never see the inside of a US courtroom, given their protection by the Russian government. Nonetheless, indictments against foreign hackers limit their ability to use the Western

financial system or to travel to any country that may have an extradition agreement with the US. "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," US attorney Scott W. Brady said in a statement.

The Sandworm indictment also sends a message to the GRU and others hackers engaged in reckless attacks around the world that they, too, can be named and shamed, says John Hultquist, director of intelligence at FireEye, who first named Sandworm in 2014 and has tracked the hackers across their long, chaotic career. "It's obviously great that they're finally being accused," Hultquist says.

A Justice Department official speaking to WIRED denied that the timing of the indictment was related to the approach of Election Day in just two weeks. "We charge the cases when they're ready to be charged," the official said.

But Hultquist notes that Sandworm was, in fact, involved in the 2016 election interference, and that Microsoft has already linked another GRU group known as Fancy Bear or APT28 to attempts to breach campaigns and other political organizations involved in the 2020 election. "Plainly, I think they're attempting to discourage them from acting in this election by using legal tools and outing their involvement in other incidents," Hultquist says of the Justice Department's indictment.

Election aside, the signaling to state-sponsored hackers is clear, belated as it may be, says Hultquist: "We know who you are and what you've done," he says. And the consequences of that knowledge will catch up with hackers who cross red lines—even if it takes five years.
