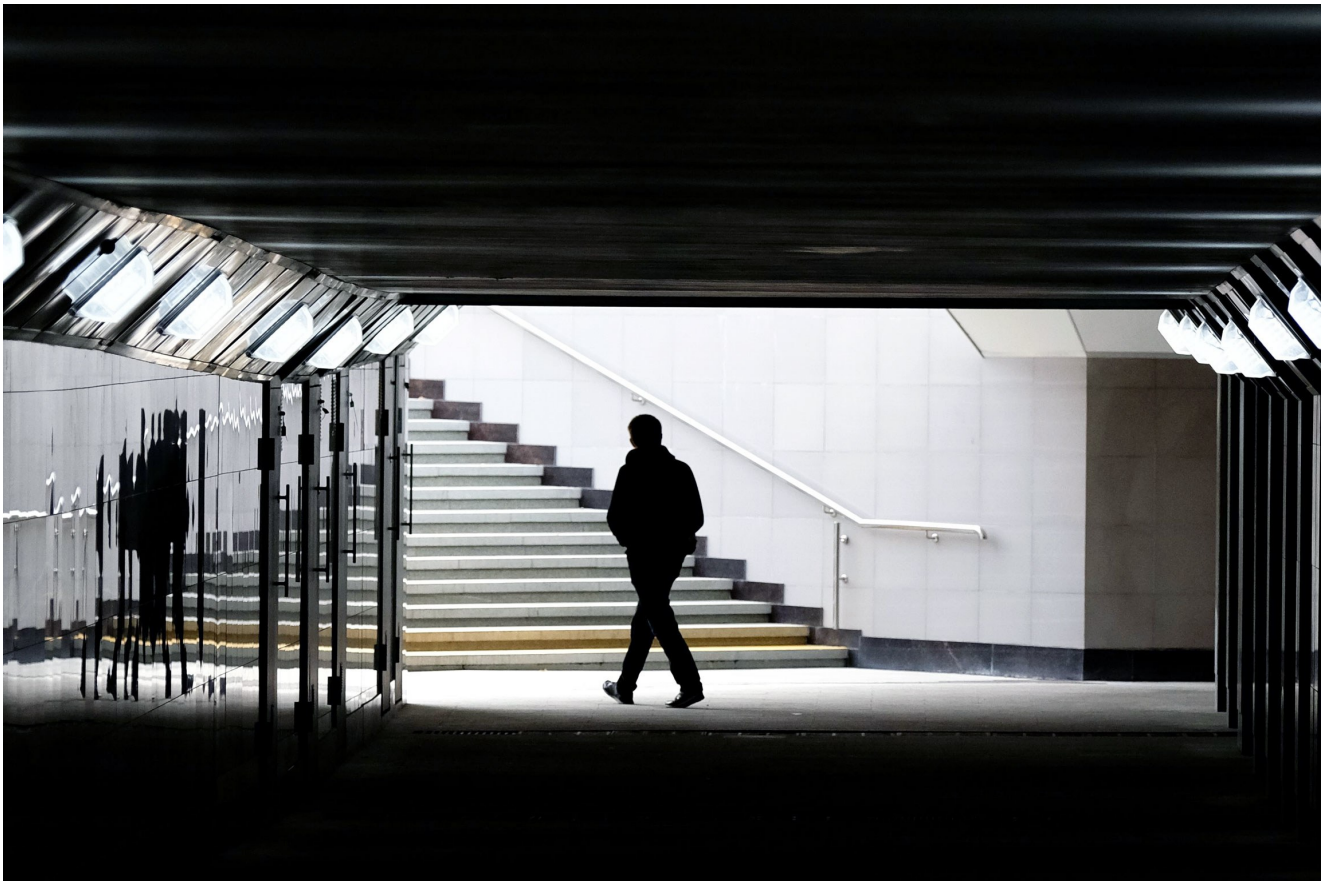
Here's the Evidence That Links Russia's Most Brazen Cyberattacks

wired.com/story/sandworm-russia-cyberattack-links/



Since the Russian military agency known as the GRU first entered the spotlight as the hackers that targeted the 2016 US election, it's become increasingly known as the actor behind much of the Kremlin's most brazen digital behavior. It's responsible for everything from the first-ever blackout triggered by hackers—turning off the power to a quarter million Ukrainians in December 2015—to NotPetya, the worst cyberattack in history, a worm that inflicted $10 billion in damage.

In recent years, security researchers have also found a web of evidence—some of which has until now remained unpublished—that definitively ties the group to other, more mysterious incidents. Those include the breach of two US state boards of elections in 2016, the cyberattack on the 2018 Winter Olympics, and the hacking of the French election in 2017. In fact, those fingerprints link much of that global chaos not just to the GRU, but to a single group of hackers within the agency known as Sandworm.

"This group is tasked with the most aggressive behavior we see from Russia, and possibly the most aggressive we see, period," says John Hultquist, the director of intelligence analysis at security firm FireEye, whose team discovered and named Sandworm in the fall of 2014. "That behavior seems to run the gamut from election interference to technical disruption of the power grid. I can't think of another group that can claim to have not only tried so many brazen acts, but actually pulled them off."

I've also followed Sandworm's escalating attacks over the last three years, telling its story in a book, *Sandworm*, published last week. In the process of that reporting, security researchers from companies including FireEye and ESET have shared crucial forensic connections that tie the group's hacking incidents into a single, connected, and evolving series of operations.

Russia's GRU has long been suspected of responsibility for the breach that leaked 9 gigabytes of emails from the campaign of French presidential candidate Emmanuel Macron just before the French election in early May of 2017—nearly a year after carrying out a similar campaign against the Democratic National Committee and the Clinton Campaign in the US. Now one fresh data point from security firm FireEye ties that operation directly to Sandworm, and specifically the NotPetya malware that would hit Ukraine and spread globally just a month after the French election.

"These guys are really about the impact. They're about sabotage and disruption."

Robert Lipovsky, ESET

That link began with a hacking tool first spotted by cybersecurity firm ESET in 2016, a backdoor program written in the Visual Basic Scripting programming language that Sandworm had used in data-destroying attacks against Ukraine. The following year, ESET found that same VBS tool had been installed on the network of a Ukrainian financial sector victim. It had been placed there using the same hijacked updates to Ukrainian accounting software, MEDoc, that had enabled the release of NotPetya just days before. ESET would later point to that VBS backdoor as a key point of evidence that Sandworm—which ESET calls Telebots—was responsible for NotPetya.

In May of 2018, FireEye took a closer look at that VBS backdoor, specifically a command-and-control server based in Bulgaria that Sandworm had apparently used to communicate with it. That server was also, strangely, a "relay" in the anonymity network Tor, serving as one of the volunteer computers in the Tor network that bounces encrypted connections around the world. In this case, the hackers appear to have used that Tor relay trick to obscure the connection from their command-and-control server back to whatever computer they used to administer it.

FireEye analyst Michael Matonis says he noticed something unusual in the Bulgarian Tor relay's configuration; he declined to share details for fear of tipping the hackers off to their

A chart of connections in an unreleased FireEye report showing Sandworm's likely involvement in targeting everything from the Olympics to the US and French elections to NotPetya (which FireEye here calls EternalPetya).
Courtesy of FireEye

tell. But it allowed FireEye to find a collection of 20 other Tor nodes that seemed to have been set up by the same person or group, all in 2017.

Matonis began checking DNS records, a kind of phone book for the internet, to see what domains had been hosted at the IP addresses of those Tor nodes, and then googled those domains to look for other connections. A search for one the first domains he saw—an apparent Google-spoofing phishing link—yielded a telling result. It appeared in one of the emails stolen and leaked by the hackers who had breached the Macron campaign.

In their haste to leak the Macron campaign's emails, the GRU seemed to have not bothered even to remove the phishing link they'd emailed themselves to their targets. By leaking that phishing link in the trove of stolen emails, they exposed evidence that Sandworm had targeted the French election from the same infrastructure it would later use in the NotPetya attack.

FireEye deployed a similar technique to get to the bottom of one of the most confounding cyberattacks in history: The data-wiping malware released inside the IT network of the Pyeongchang Winter Olympics in February of 2018, which took down the event's Wi-Fi, app, and ticketing services in the middle of the opening ceremony.

The WIRED Guide to Cyberwar

The threat of cyberwar looms over the future: a new dimension of conflict capable of leapfrogging borders and teleporting the chaos of war to civilians thousands of miles beyond its front.

By
Andy Greenberg

Despite layers of code snippets intended to make the attack look North Korean or Chinese in origin, FireEye was able to match a phishing document used in the Olympics attack to a collection of other phishing documents in VirusTotal, a malware repository. All of the infected attachments in that grouping were created by the same public tool, Malicious Macro Generator, and the metadata of the files had user names in common as well. Other documents in the collection appeared to target Ukrainians, including LGBT activists, as well as the Spiez Laboratory in Switzerland, which was investigating the chemical weapon attack

on GRU defector Sergey Skripal—both strong indications that Russian hackers were behind the campaign. Other documents in the collection, more mysteriously, seemed to target Russian oligarchs.

One of the Ukrainian-targeted documents FireEye tied to the Olympic Destroyer attack, including the Ukrainian coat of arms.
Courtesy of FireEye

But FireEye analyst Matonis eventually found even more telling evidence. He connected a command-and-control server used by one of those phishing documents to a domain that the FBI had previously identified as being used in phishing attacks against two US state boards of elections. In July of 2018, special counsel Robert Mueller indicted 12 GRU hackers for interference in the US election and tied GRU Unit 74455 member Anatoliy Sergeyevich Kovalev to the boards-of-elections hacks specifically.

A chart showing similarities among the hosting providers and other characteristics of servers used across three hacking campaigns: the NotPetya attack (which hijacked the updates of the Ukrainian accounting software MEDoc), the phishing campaign linked to the Olympic Destroyer malware, and Sandworm intrusions from prior years. Together, they indicate that all three campaigns were likely the work of Sandworm.

That logical chain implicates GRU Unit 74455 not only in US election targeting but in the 2018 Olympics attack. In fact, the Olympics cyberattack had likely been an act of vengeance over Russia's ban from the 2018 games for doping. And the connections run deeper still: Matonis saw that many of command-and-control servers the Olympics hackers used were hosted by the same two companies, Global Layer and Fortunix, as those in previous Sandworm campaigns. Some of those servers—just as in the NotPetya and French election connection—were also running as Tor relays. All of which suggested that the Olympics attack had been carried out not just by Russia, or the GRU's Unit 74455, but specifically the same Sandworm group of GRU hackers responsible for NotPetya and the blackouts in Ukraine.

Backdoors and Blackouts

A larger web of forensic links tying together Sandworm's earlier attacks stretches back years. From 2014 to 2015, the group helpfully used versions of the same BlackEnergy malware in many of its intrusions, from attacks that destroyed Ukrainian media company data to the first blackout it inflicted on Ukrainian civilians.

Then last year ESET revealed that it had spotted a backdoor known as Exaramel in a breach on a customer's network that it attributed to Sandworm. The hackers had also used a custom credential stealer known as Credraptor that ESET had only seen Sandworm use in the past. ESET noted the significance of that discovery: Code from Exaramel had also shown

up in the breach of Ukraine's national electric utility that triggered a second blackout in Ukraine—this time in the capital of Kyiv—in late 2016. ESET argues that confirms Sandworm's involvement in the second-ever hacker blackout operation, just as in the first.

"It’s like putting together pieces of a puzzle, bits of evidence that basically raise our confidence that these things are related," says ESET researcher Robert Lipovsky. The resulting picture created by those assembled pieces, Lipovsky says, is a uniquely aggressive group of hackers. "These guys are really about the impact. They’re about sabotage and disruption."

That portrait of a single, highly dangerous hacking group is more than just a curiosity, says FireEye's Hultquist. It should serve as a warning—and a key piece of intelligence if Sandworm's fingerprints ever appear on a potential target's network. "We’re talking about one actor that’s carried out all these heinous acts," says Hultquist. "If you can attribute an incident to this actor, that’s a very dangerous scenario to find yourself in."
