The Russian Hackers Playing 'Chekhov's Gun' With US Infrastructure

wired.com/story/berserk-bear-russia-infrastructure-hacking/

Andy Greenberg October 26, 2020

Over the last half a decade, Russian state-sponsored hackers have triggered blackouts in Ukraine, released history's most destructive computer worm, and stolen and leaked emails from Democratic targets in an effort to help elect Donald Trump. In that same stretch, one particular group of Kremlin-controlled hackers has gained a reputation for a very different habit: walking right up to the edge of cybersabotage—sometimes with hands-on-the-switches access to US critical infrastructure—and stopping just short.

Last week the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency published an advisory warning that a group known as Berserk Bear—or alternately Energetic Bear, TEMP.Isotope, and Dragonfly—had carried out a broad hacking campaign against US state, local, territorial, and tribal government agencies, as well as aviation sector targets. The hackers breached the networks of at least two of those victims. The news of those intrusions, which was reported earlier last week by the news outlet Cyberscoop, presents the troubling but unconfirmed possibility that Russia may be laying the groundwork to disrupt the 2020 election with its access to election-adjacent local government IT systems.

"They're getting us spun up. They're burning our cycles."

Adam Meyers, CrowdStrike

In the context of Berserk Bear's long history of US intrusions, though, it's much harder to gauge the actual threat it poses. Since as early as 2012, cybersecurity researchers have been shocked to repeatedly find the group's fingerprints deep inside infrastructure around the globe, from electric distribution utilities to nuclear power plants. Yet those researchers also say they've never seen Berserk Bear use that access to cause disruption. The group is a bit like Chekhov's gun, hanging on the wall without being fired through all of Act I—and foreshadowing an ominous endgame at a critical moment for US democracy.

"What makes them unique is the fact that they have been so focused on infrastructure throughout their existence, whether it's mining, oil, and natural gas in different countries or the grid," says Vikram Thakur, a researcher at security firm Symantec who has tracked the group over several distinct hacking campaigns since 2013. And yet Thakur notes that in all that time, he's only seen the hackers carry out what appear to be reconnaissance operations. They gain access and steal data, but despite ample opportunity never actually exploit sensitive systems to attempt to cause a blackout, plant data-destructive malware, or deploy any other sort of cyberattack payload.

Instead, the intruders seem content simply demonstrating that they can gain that troubling level of reach into infrastructure targets again and again. "I see them having operated for seven years and till today, I've come across no evidence of them having *done* something," Thakur says. "And that makes me lean toward the theory that they're sending a message: I am in your critical infrastructure space, and I can come back if I want to."

A Long Hibernation

In the summer of 2012, Adam Meyers, the vice president of intelligence at security firm CrowdStrike, remembers first coming across the group's sophisticated backdoor malware, known as Havex, in an energy sector target in the Caucasus region. (CrowdStrike initially called the hackers Energetic Bear due to the energy sector targeting, but later changed the name to Berserk Bear when the group switched up its tools and infrastructure.) "It was the coolest thing I'd ever seen at the time," Meyers says. Crowdstrike would soon find Havex in other energy-related networks around the world—years before other Russian hackers would carry out the world's first blackout-inducing cyberattack in 2015 against Ukraine.

In June of 2014 Symantec published a comprehensive report on the group, which it called Dragonfly. In dozens of intrusions against oil and gas and electric utilities in the US and Europe, the hackers had used "watering hole" attacks that compromised websites their targets visited to plant Havex on their machines. They also hid their malware in infected versions of three different software tools commonly used by industrial and energy firms. Symantec's Thakur says in that first wave of attacks the company found that the hackers had

stolen detailed industrial control system data from their victims. He never saw evidence, however, that the hackers went so far as to attempt to disrupt any target's operations—though given the scale of the campaign, he admits he can't be sure.

In 2017, Symantec discovered the same hackers carrying out a more targeted set of attacks against US energy sector targets. At the time, the security researchers described it as a "handful" of victims, but Thakur now says they numbered in the dozens, ranging from coal mining operations to electric utilities. In some cases, Symantec found, the hackers had gone so far as to screenshot control panels of circuit breakers, a sign that their reconnaissance efforts had gone deep enough that they could have started "flipping switches" at will—likely enough to cause some sort of disruption if not necessarily a sustained blackout. But again, the hackers appear not to have taken full advantage. "We did not see them turning off the lights anywhere," he says.

Six months later, in February of 2018, the FBI and DHS would warn that the hacking campaign—which they named Palmetto Fusion—had been carried out by Russian state-sponsored hackers, and also confirmed reports that the hackers' victims had included at least one nuclear power generation facility. The hackers had gained access only to the utility's IT network, though, not its far more sensitive industrial control systems.

Going Berserk

Today Berserk Bear is widely suspected of working in the service of Russia's FSB internal intelligence agency, the successor to the Soviet-era KGB. CrowdStrike's Meyers says the company's analysts have come to that conclusion with "pretty decent confidence," due in part to evidence that aside from its foreign infrastructure hacking, Berserk Bear has also periodically targeted domestic Russian entities and individuals, including political dissidents and potential subjects of law enforcement and counterterrorism investigation, all in line with the FSB's mission.

That's a contrast with other widely reported state-sponsored Russian hacking groups Fancy Bear and Sandworm, who have been identified as members of Russia's GRU military intelligence agency. Fancy Bear hackers were indicted in 2018 for breaching the Democratic National Committee and the Clinton campaign in a hack-and-leak operation designed to interfere with the 2016 US presidential election. Six alleged members of Sandworm were indicted by the US Department of Justice last week in connection with cyberattacks that have caused two blackouts in Ukraine, the NotPetya malware outbreak that inflicted $10 billion in damage globally, and the attempted sabotage of the 2018 Winter Olympics.

Berserk Bear appears to be the FSB's more restrained version of the GRU's Sandworm cyberwar unit, says John Hultquist, director of intelligence at FireEye. "This is an actor whose mission appears to be to hold critical infrastructure under threat," Hultquist says. "The difference is we've never seen them actually pull the trigger."

Just why Berserk Bear would toe the line of critical infrastructure disruption without crossing it over so many years remains a subject of debate. Hultquist argues that the group may be preparing for a potential future geopolitical conflict, one that warrants an act of cyberwar such as attacking an enemy's power grid—what cybersecurity analysts have long described as "preparing the battlefield."

The latest round of Berserk Bear breaches could be that sort of preparation, Hultquist warns, for coming attacks on state, municipal, and other local governments responsible for administering the current election. According to cybersecurity firm Symantec, three of Berserk Bear's attempted operations also targeted airports on the West coast of the United States, including San Francisco International Airport. Symantec's Thakur imagines a future where Berserk Bear is mobilized to cause disruptive—if not necessarily disastrous—effects, like "lights out in a small part of the country, or a certain airline has trouble refueling their planes."

But CrowdStrike's Meyers, who has tracked Berserk Bear for eight years, says he's come to believe that the group may be playing a more subtle game, one that has more indirect but immediate, psychological effects. Every one of its breaches, no matter how seemingly minor, triggers a disproportionate technical, political, and even emotional response. "If you can make US-CERT or CISA deploy a team every time they find a Berserk Bear target, if you can make them publish stuff for the American public and get their partners from the intelligence community and law enforcement involved, you're basically doing a resource attack against the machine," Meyers says, drawing an analogy with a hacker technique that overwhelms a target computer's resources with requests. Meyers points out that last week's CISA advisory describes widespread scanning for potential victims, not the quieter, more targeted tactics of a group making stealth its highest priority. "The more they can run these theatrics, the more they can make us go freaking nuts... They're getting us spun up. They're burning our cycles."

If triggering that overreaction is indeed Berserk Bear's endgame, it may have already succeeded, given CISA's advisory about its latest round of intrusions and widespread media coverage of those breaches—including in this article. But Myers concedes that the alternative, ignoring or downplaying Russian state-sponsored breaches into US critical infrastructure and election-related systems, hardly seems wise either. If indeed Berserk Bear is Chekhov's gun hanging on the wall, it has to go off before the play is over. But even if it never does, it can be hard to take your eyes off of it—drawing your attention away from the rest of the plot.

- How to trick out your iPhone home screen in iOS 14
- The women who invented video game music
- 🎮 WIRED Games: Get the latest tips, reviews, and more
- 🎧 Things not sounding right? Check out our favorite wireless headphones, soundbars, and Bluetooth speakers