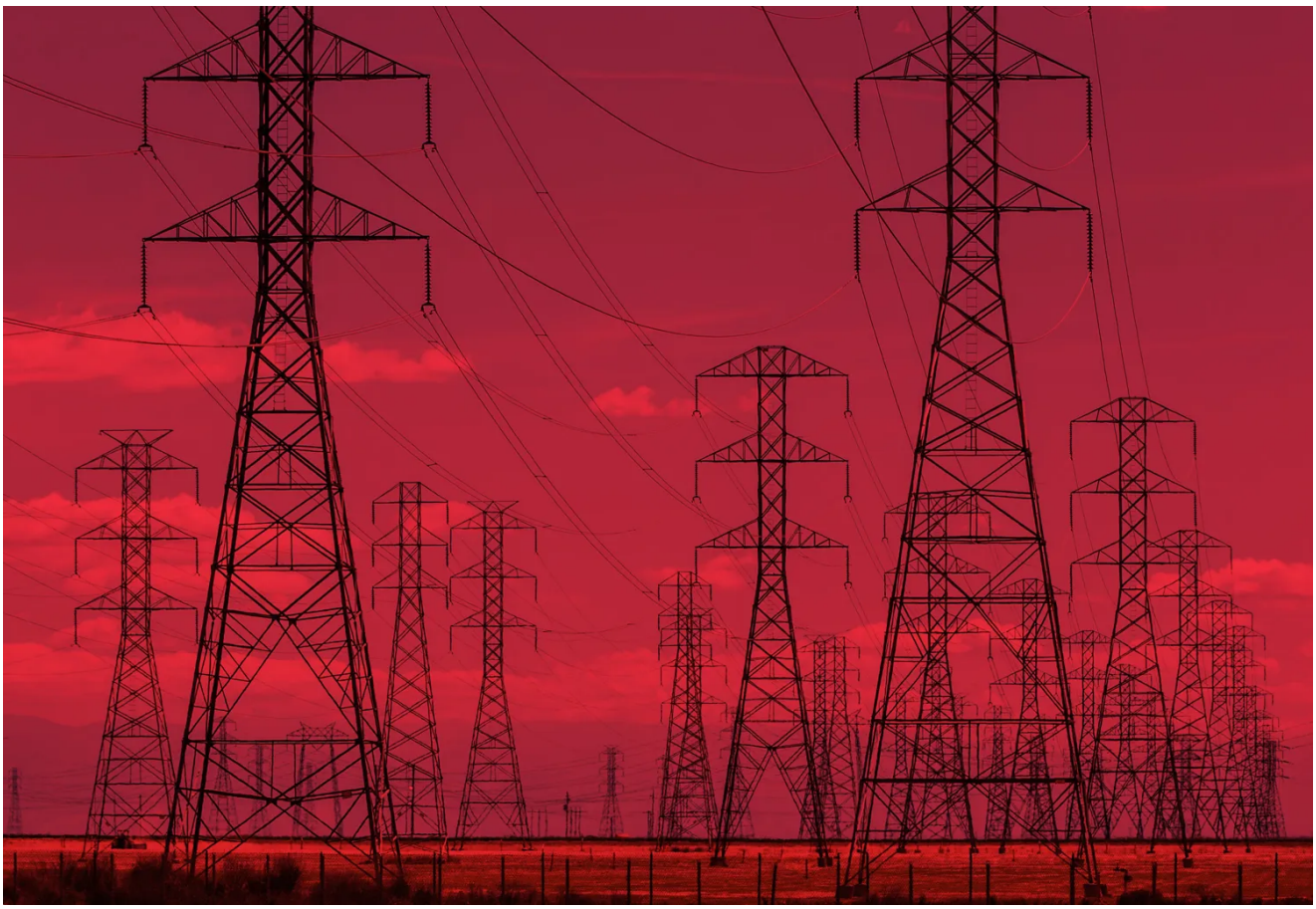
Russian Hackers Haven't Stopped Probing the US Power Grid

wired.com/story/russian-hackers-us-power-grid-attacks/

Lily Hay Newman November 28, 2018



In recent years, hacks against the power grid have gone from a mostly theoretical risk to a real-world problem. Two large-scale blackouts in Ukraine caused by Russian cyberattacks in 2015 and 2016 showed just how feasible it is. But grid hacking comes in less dramatic forms as well—which makes Russia's continued probing of US critical infrastructure all the more alarming.

At the CyberwarCon forum in Washington, DC on Wednesday, researchers from threat intelligence firm FireEye noted that while the US grid is relatively well-defended, and difficult to hit with a full-scale cyberattack, Russian actors have nonetheless continued to benefit from their ongoing vetting campaign.

"There's still a concentrated Russian cyber espionage campaign targeting the bulk of the US electrical grid," says FireEye analyst Alex Orleans says. "The grid is still getting hit."

FireEye calls the Russia-linked hacking group that has been targeting the US grid "TEMP.Isotope." It's also known as Dragonfly 2.0, or Energetic Bear. The group mostly uses generic hacking tools and techniques created by other actors—a strategy known as "living off the land"—to minimize development time and costs, while also making it harder to identify and track its movements. But TEMP.Isotope has also created at least one custom system backdoor, and often uses spearphishing and infected websites to compromise targets. And the group has brought these tools to bear against the US grid in a patient and methodical way.

> "The grid is still getting hit."

Alex Orleans, FireEye

US infrastructure does have some advantages here. In the wake of the massive 2003 Northeastern blackout, utilities implemented resilience and defense standards known as the North American Electric Reliability Corporation Critical Infrastructure Protection requirements, more digestibly referred to as NERC CIP. These created minimum baselines for defending against and dealing with natural disasters, but also promoted best practices for network defense, including two-factor authentication, network segmentation, data storage protections, and strict access controls for both network owners and third-parties.

All of these protections combined have hardened electricity generation and transmission systems against attack. But not all segments of the grid are held to those standards. Distribution entities, which often subcontract with larger organizations to deliver power locally, often lack adequate resources and defenses. And while hackers may have a harder time fully compromising more formidable targets, they can still achieve many of their goals through persistent probing.

In many ways, TEMP.Isotope's actions are in the interest not of triggering large-scale blackouts, but of traditional intelligence-gathering. The group seems to deliver information that can be used both to expand Russian energy capabilities and to vet US systems for weaknesses that could potentially be exploited in attacks. But the FireEye researchers point out that the canvassing also serves other more subtly aggressive counterintelligence goals as well.

"All of this threat activity you see from actors like Isotope requires defensive responses from incident responders, threat intelligence within a given organization, all the way up to potentially governments," Orleans says. "So you have this ripple upward and outward. And this counterintelligence is for the purpose of frustrating your adversary. Utilities are the adversary for active threat Isotope, so wearing them down through activity, creating anxiety, fulfills what is in counterintelligence terminology known as 'degradation.'"

If you can sow discord, confusion, and fatigue, you can attack an adversary by frustrating them rather than by masterminding an all-out physical assault. And though grid hacking may not have yet reached a boiling point in the US, the FireEye researchers warn that consistent probing should be taken as seriously as dramatic attacks. This is particularly true given that the security community has seen hints over the years of potential US grid probing activity from other countries as well, including Iran and North Korea.

For now, though, the FireEye researchers say Russian state-sponsored hackers are the ones to watch in the US grid. "The most consistent people are likely the Russians," Orleans says. "And I also think we likely haven't fully uncovered the extent to which they have gotten into the wires."
