Hackers Have Penetrated Energy Grid, Symantec Warns | Fortune

By Robert Hackett

Archived: 2026-04-06 15:29:52 UTC

Hackers have been burrowing their way inside the critical infrastructure of energy and other companies in the U.S. and elsewhere, warns cybersecurity giant Symantec.

In a new report, Symantec (SYMC) claims that the threat of cyberattack-induced power outages in the west has elevated from a theoretical concern to a legitimate one in recent months. “We’re talking about activity we’re seeing on actual operational networks that control the actual power grid,” Eric Chien, technical director of security technology and response at Symantec, told *Fortune* on a call.

Reports surfaced over the summer of hackers targeting staff at nuclear energy facilities with phishing attacks, designed to steal login credentials or install malware on machines. The extent of the campaign as well as the question of whether the attackers had breached operational IT networks, rather than merely administrative ones, was unclear at the time.

Symantec is now erasing all doubt. “There are no more technical hurdles for them to cause some sort of disruption,” Chien said of the hackers. “All that’s left is really motivation.”

Get Data Sheet, Fortune’s *technology newsletter.*

Symantec detailed its findings in a report released Wednesday morning. The paper tracks the exploits of a hacker group that Symantec has dubbed DragonFly 2.0, an outfit that the company says it has linked to an earlier series of attacks perpetrated between 2011 and 2014 by a group it dubbed DragonFly.

Adam Meyers, vice president of intelligence at CrowdStrike, a billion-dollar cybersecurity startup, said his team had been tracking the group, which it dubbed Berserk Bear, since 2015. He disputed Symantec’s attribution, saying there is no reason to believe that DragonFly—nicknamed “Energetic Bear” by CrowdStrike—and DragonFly 2.0 (aka Berserk Bear) were linked.

In Meyers view, there’s not enough evidence to tie the two groups together, especially given that source code for some of the malicious software used in the most recent attacks leaked in 2010, he said. In other words, anyone could incorporate the code into their own hacking tools.

Meyers did wager a guess about the origin of the attacks, however. “It’s likely a Russian actor targeting global energy and related industries,” Meyers added, noting that the intrusions appeared to align with Moscow’s strategic interests.

The most recent wave of attacks hit energy companies in the U.S., Turkey, Switzerland, Afghanistan, and elsewhere. The first phase began in December 2015 with a set of phony New Year’s Eve party invitations that were actually boobytrapped emails. The intensity and frequency of attacks picked up this year, Symantec said.

Chien said Symantec had notified more than 100 companies in the U.S., Europe, and elsewhere about the attacks. Even if businesses remove the malware on their computers, the attackers might still be able to use stolen login credentials to commandeer the corporate systems, he said.

Such an attack would echo tactics employed in Ukraine, where attackers infiltrated computers and caused a temporary blackout at the end of last year.

Rob Lee, CEO of Dragos, a startup that protects critical infrastructure networks, told *Fortune* that he was, like Meyers, not sold on Symantec's attribution work. "I'm not yet confident linking this to Dragonfly, but what Symantec highlights is a consistent and worrying trend of adversaries targeting U.S. industrial infrastructure," he wrote in an email. "Our infrastructure is resilient so folks shouldn't worry, but we do need to do more in the face of an aggressive adversary."

Other experts are more outwardly alarmed by the recent breaches. "We used to talk about what *could* a cyber attack do—it *could* shut down the power grid. That was all hypothetical," Chien told *Fortune*. "Now we're seeing activity where, to be honest, if they wanted to disrupt something in the power grid, they could have done it yesterday."

Before President Donald Trump took office, he vowed to conduct a sweeping review of the nation's and federal government's cyber defenses. At the end of last month, a quarter of the president's National Infrastructure Advisory Council quit their advisory posts, saying that the president had devoted "insufficient attention" to cybersecurity threats to critical infrastructure.
