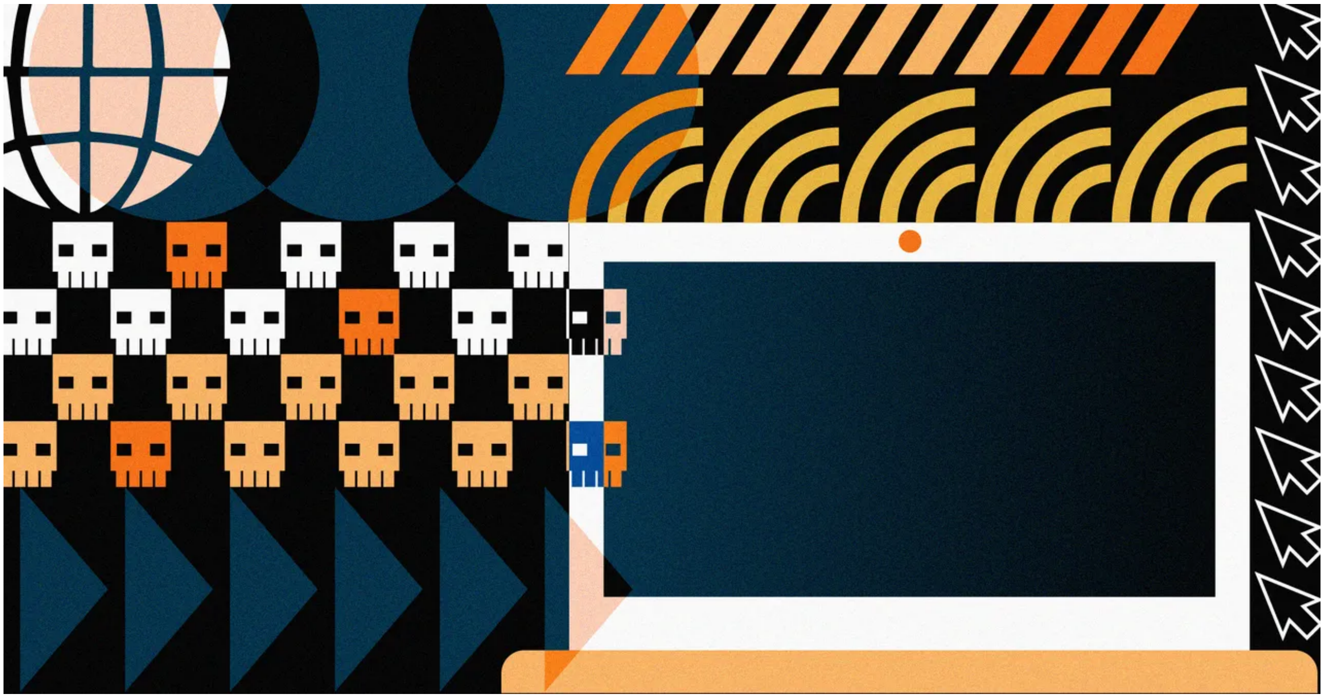
VPN Hacks Are a Slow-Motion Disaster

wired.com/story/vpn-hacks-pulse-secure-espionage/

Brian Barrett

April 25, 2021



This year has seen no shortage of blockbuster hacks, from the SolarWinds supply chain meltdown to China's blitz against Microsoft Exchange servers. It's a lot. But the outsized focus on those hacking sprees obscures another threat that has built steadily in the background for years, with no clean resolution in sight: the sustained assault on virtual private networks.

The latest example of a VPN meltdown—we're talking corporate connections, not your personal setup—is among the most dramatic. Security firm FireEye this week revealed that it had found a dozen malware families, spread across multiple hacking groups, feasting on vulnerabilities in Pulse Secure VPN. The victims spanned the globe and ranged across the usual high-value targets: defense contractors, financial institutions, and governments. The attackers used their perch to steal legitimate credentials, improving their chances of gaining access that's both deep and sustained.

Which is the thing about VPN hacks. Since the whole point of a VPN is to create a secure connection to a network, worming into one can save hackers a lot of hassle. "Once hackers have those credentials, they don't need to use spearphishing emails, they don't need to bring in custom malware," says Sarah Jones, senior principal analyst at FireEye. "It's kind of a perfect situation."

The campaign that FireEye uncovered is especially ambitious and potentially troubling. It’s too early for firm attribution, but the groups behind it appear to be linked to China, and their targets seem chock full of the kind of sensitive information on which espionage groups thrive. One of the malware families, called Slowpulse, could get around two-factor authentication protections, sidestepping a key safeguard against credential harvesting.

“The new issue, discovered this month, impacted a very limited number of customers,” said Pulse Secure parent company Ivanti in a statement. “The team worked quickly to provide mitigations directly to the limited number of impacted customers that remediates the risk to their system.”

“If the haystack keeps increasing, it’s impossible to find the needle.”

Vijay Sarvepalli, CERT

A patch to fix the vulnerability at the heart of the attacks, though, won’t be available until next month. And even then, it may not provide much of a salve. Companies are often slow to update their VPNs, in part because downtime means employees effectively can’t get their work done. Some of the intrusions FireEye spotted, in fact, appear related to vulnerabilities that had been reported as far back as 2019. That same year, a Pulse Secure VPN flaw offered an inroad for a ransomware group to hold up Travelex, a travel insurance company, for millions of dollars. A year later—despite warnings from researchers, national cybersecurity organizations, and law enforcement—thousands of organizations remained vulnerable, says Troy Mursch, chief research officer of the cyber-threat intelligence company Bad Packets.

It wasn’t always like this. VPNs used to typically rely on a set of protocols known as Internet Protocol Security, or IPsec. While IPsec-based VPNs are considered secure and reliable, they can also be complicated and clunky for users. In recent years, as remote work expanded then exploded, more and more VPNs have been built instead on ubiquitous encryption technologies known as secure sockets layer and transport layer security. The distinctions descend rapidly into weeds, but essentially SSL/TLS VPNs made logging onto your company’s network much more seamless—the difference between merging onto the interstate in a minivan versus a Miata.

“That was a big step for convenience,” says Vijay Sarvepalli, a senior security solutions architect with the CERT Coordination Center at Carnegie Mellon University. CERT helps catalog vulnerabilities and coordinate their public disclosure. “When they designed those things, the risks were not yet considered. It’s not impossible to protect these, but people are not prepared to monitor and respond quickly to attacks against them.”

Software of all stripes have vulnerabilities, but because VPNs by definition act as a conduit for information that’s intended to be private, their bugs have serious implications. The pandemic's shift to remote work has thrust the underlying issues into the spotlight. “Many

SSL VPN vendors had serious flaws in their products to begin with," says Mursch. "The increased usage of SSL VPNs over the last year led to more scrutiny from security researchers—and threat actors interested in exploiting them."

More flaws means more opportunities for attackers. More users on a given VPN also makes it that much more difficult to spot the bad guys, especially for large, multinational companies. "It makes it harder to monitor when you have a lot more events going on," says Sarvepalli. "If the haystack keeps increasing, it's impossible to find the needle."

To the extent that there's a silver lining here, it's that the hackers behind the latest set of Pulse Secure-related intrusions are incredibly sophisticated. OK, yes, that's also bad news, in that they've likely stolen sensitive data from who knows how many corners of the world. But it also means that copycats are unlikely to be able to replicate their moves before the vulnerability gets patched, at least not without a lot of work.

"It's rather specific in the knowledge you need to exploit it," say Stephen Eckels, a reverse engineer at FireEye. "For us to understand what their malware was doing, we had to be in contact with the authors of the code from Pulse Secure. An attacker was able to figure out that same information on their own. "

Still, VPN vulnerabilities that are easier to exploit persist. Hackers will eventually reverse engineer this one after the patch comes out. And corporations continue not to address the exposure to their networks, despite frantic warnings from the security community. That status quo adds up to months or years of quiet espionage, the kind that may never lend itself to a full accounting. "There's a lot to be done still," says Sarvepalli of the work required to shore up VPNs. "We are making progress, and some of these big hammers wake us up."

More Great WIRED Stories

- 📩 The latest on tech, science, and more: Get our newsletters!
- The cold war over McDonald's hacked ice cream machines
- What octopus dreams tell us about the evolution of sleep
- The lazy gamer's guide to cable management
- How to log in to your devices without passwords
- Help! Am I oversharing with my colleagues?
- 👁️ Explore AI like never before with our new database
- 🎮 WIRED Games: Get the latest tips, reviews, and more
- 🏃‍♀️ Want the best tools to get healthy? Check out our Gear team's picks for the best fitness trackers, running gear (including shoes and socks), and best headphones