Chinese APT Uses VPN Bug to Exploit Worldwide OT Orgs

By Nate Nelson

Published: 2025-02-27 · Archived: 2026-04-05 20:23:40 UTC

Source: Ken Hawkins via Alamy Stock Photo

Chinese cybercriminals have penetrated sensitive manufacturing companies worldwide through a virtual private network (VPN) bug.

In an exclusive interview with Dark Reading at CPX 2025, Check Point researchers provided new information about a monthslong espionage campaign aimed at prized intellectual property (IP). In short: Through a months-old path traversal vulnerability in Check Point's security gateways, attackers attributed with low confidence to APT41 (aka Winnti) managed to gain initial access into dozens of operational technology (OT) organizations globally.

In fact, Check Point has only tracked compromises of its own customers. For that reason, the researchers say, it's entirely possible that plenty more organizations have been touched by the same campaign.

Chinese Attackers Exploit a Gateway CVE

The activity occurred in waves: beginning shortly after that vulnerability was disclosed and patched in May 2024, peaking in November, and continuing until last month. All these victims fell victim to CVE-2024-24919, a vulnerability in Check Point security gateways exposed to the open Internet and configured to enable remote access.

The issue resulted from a minor oversight in how the appliances validated file paths. With specially crafted requests, even unauthenticated attackers could access directories and files they otherwise shouldn't. These files might contain password hashes, for example, which, once decrypted, could be used to obtain superuser privileges, and thereby full control over a device. This risk earned CVE-2024-24919 a "high" score of 8.6 out of 10 in the Common Vulnerability Scoring System (CVSS).

The threat actor took advantage of the access afforded by the bug to perform lateral movement in targeted networks, gaining higher privileges and access to more systems along the way, including domain controllers. Finally, they'd install remote access points in the form of the modular ShadowPad backdoor. Check Point's researchers believe that their goal was to steal valuable IP.

The researchers have not observed any cases in which attackers caused disruption to their victims. For this reason, they track this activity as a separate cluster from what Orange Cyberdefense disclosed on Feb. 18, where a group it tracks as "Green Nailao" used CVE-2024-24919 to infect European organizations with ShadowPad, PlugX, and the previously undocumented "NailoLocker."

Global OT Orgs Targeted

In all, Check Point identified two or three dozen victim organizations spanning broad geographic regions. Many are based in the US and Latin America — around 20% of all targets come from Mexico alone — but Europe, the Middle East, and Africa have also been touched.

Though they didn't limit themselves to one part of the world, the attackers were largely focused on specific, highly valuable OT industries. For example, a number of targets were significant supply chain manufacturers to aviation and aerospace companies. Around half of all victims tracked were manufacturers of one kind or another.

A lesser share of victims came from unrelated industries in more obscure locations — utilities from various small countries and finance companies in Africa, for example. Lotem Finkelsteen, Check Point director of threat intelligence, argues that "we tend to believe that attackers are surgical — that they know exactly what to do, with flawless operation — but sometimes there are, let's say, collateral targets that were not part of the strategy. And once they have that access, why not just gain access anyway and utilize it later?"

And Check Point research group manager Eli Smadja emphasizes that "you never know what an attacker is thinking. A seemingly not-so-meaningful company could be a door into another company. They can use a finance company to get access to their real target."

Small OT Orgs Under Fire

Just as noteworthy as the industries these hackers targeted are the sizes of the companies they infected.

"We tend to believe manufacturers are very big, but no, most of them are very small organizations," Finkelsteen points out. Plenty of manufacturers operate just one factory, or something more akin to a workshop, but they can be just as valuable as their larger counterparts. "We've seen it in other operations from Chinese actors over the last few years — that many targets have been small businesses," he says.

Small OT organizations make good targets for the same reasons any other businesses do. "They usually don't have cybersecurity personnel," explains Sergey Shykevich, threat intelligence group manager at Check Point. "It's one IT person at most, doing security, IT, and all kinds of other stuff." Sometimes, even, the contact person threat researchers have to reach out to when something goes wrong is the business owner.

As a result, Finkelsteen says, "they usually don't patch quickly, or they're not even aware of the security measures needed to support their gateway, router, or whatever it may be. Small businesses need to be aware that if they buy something, it's being continuously supported, so they're not vulnerable to the very powerful groups that are after them."

He laments that "very advanced threat actors with very advanced tools, targeting small businesses, is not a fair game."

About the Author

Contributing Writer

Nate Nelson is a journalist and scriptwriter. He writes for "Darknet Diaries" — the most popular podcast in cybersecurity — and co-created the former Top 20 tech podcast "Malicious Life." Before joining Dark Reading, he was a reporter at Threatpost.