Silver Fox APT Blurs the Line Between Espionage & Cybercrime

By Nate Nelson

Published: 2025-08-08 · Archived: 2026-04-05 16:10:54 UTC

Source: Zoonar GmbH via Alamy Stock Photo

A Chinese threat actor has been performing both intelligence-oriented and financially motivated attacks against a wide variety of primarily Chinese-speaking organizations.

Compared to most, Silver Fox has a wide span of tactics, techniques, and procedures (TTPs) at its disposal. It might gain initial access to victims by impersonating major organizations in phishing emails with malicious attachments. Or it will spread fake applications, or Trojanized versions of legitimate applications, through Telegram channels or websites boosted by search engine optimization (SEO) poisoning. Post-compromise, you can expect a remote access Trojan (RAT), such as ValleyRAT, Winos 4.0, or Gh0stCringe or the HoldingHands RAT, two variants of Gh0st RAT. Or, perhaps, there'll be a keylogger waiting for you, with a cryptominer using your machine resources to earn money.

This operational variety allows Silver Fox to wear different hats. Recent analyses by Picus Security, Trustwave, and other research firms have connected the group to the Chinese state, thanks to its penchant for stealing

sensitive information from or disrupting organizations involved in critical infrastructure, cybersecurity, government, etc., particularly in Taiwan.

Related:Iran Hacktivists Make Noise but Have Little Impact on War

At the same time, though, it has been carrying out attacks against gaming, healthcare, and finance companies, as well as educational institutions, again largely in Taiwan, but also in Japan and North America. Many of these cases resemble run-of-the-mill cybercrime, with the clear goal of making money.

"While it's a more complex model than pure espionage or pure crime, this dual approach gives Silver Fox more flexibility, better cover, and broader reach," explains Sıla Özeren, security research engineer with Picus Security. "Silver Fox is a major player, and it's also a warning sign. It signals a future where more Chinese APTs operate like businesses: nimble, multimission, and willing to innovate in how they achieve both geopolitical and economic objectives."

The Best of Both Worlds

Historically, North Korea has used its advanced persistent threats (APTs) for both characteristically nation-state-style attacks (e.g., intelligence gathering, disrupting critical industries) and cybercriminal attacks (e.g., scams, ransomware, cryptomining).

Crossing the line like this might appear uncharacteristic for China, whose APTs specialize not only in certain types of attacks, but even in granular roles within those attacks. There's precedent, however, most notably in the form of APT41 (aka Barium, Double Dragon, Winnti), which has been tied to both espionage and financial theft. According to Özeren, APT41 and Silver Fox signal a "broader trend" in China's threat landscape.

Related:EU Sanctions Companies in China, Iran for Cyberattacks

But how to explain it? Why try to be a jack-of-all-trades when it's so much simpler to be a master of one?

"First, financially motivated attacks create a layer of plausible deniability. If a victim sees cryptocurrency miners or fake invoices, they're more likely to dismiss the intrusion as generic cybercrime rather than a coordinated state-backed operation. That misdirection buys the group time and helps them operate under the radar," Özeren explains.

Second, she says, the financial angle gives Silver Fox to ability to fund itself. "Instead of relying entirely on government resources, they generate their own money, whether through cryptojacking or theft, which could be used to support broader operations," she says. "It also suggests a degree of autonomy, or at least tolerance, from Chinese authorities."

Lastly, "by casting a wide net, the group opens itself up to more targets and more data. Even if some victims are low-value from an intelligence standpoint, they might be useful for initial access, infrastructure, or long-term strategic positioning. And occasionally, what starts as a low-level compromise might expose something much bigger, like credentials for a critical system or access to a partner network."

Related:SideWinder Espionage Campaign Expands Across Southeast Asia

At the end of the day, says Karl Sigler, senior security research manager at Trustwave, "it's not too surprising. If anything, it's surprising that many other groups are so focused. Silver Fox's modus operandi suggests a broad skill set, from exploit development to social engineering and phishing attacks. If you have the resources, you might not have to decide between a specific APT-type mission or an opportunistic, financially motivated attack."

For defenders in the Asia-Pacific region, Özeren says, "that means facing threat actors who are not only persistent and stealthy, but also financially motivated and operationally diverse. Silver Fox fits that mold perfectly: aggressive, fast-evolving, and hard to attribute."

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.
