ESET Research: China-aligned FamousSparrow expands operations in Latin America, targets governments with new backdoor



DUBAI , DUBAI, UNITED ARAB EMIRATES, September 23, 2026 /EINPresswire.com/ -- ESET Research's ongoing monitoring of FamousSparrow discovered that the China-aligned APT group had developed a new backdoor, SparroWocky, and has been deploying it to several countries in Latin America since at least August 2025. In what was probably China's reaction to the U.S. showing increased interest in Latin America, FamousSparrow increased its extensive targeting of governmental organizations there. ESET researchers chose to name the backdoor SparroWocky because the first samples collected all contained the first stanza of "Jabberwocky," a nonsense poem by English author, poet, and mathematician Lewis Carroll (author of Alice's Adventures in Wonderland).

SparroWocky is a modular C++ backdoor. Its architecture and the techniques used by its authors indicate strong knowledge of anti-analysis tricks and Windows internals. With the switch to SparroWocky, FamousSparrow started to incorporate code from open-source projects directly into its malware. "Fortunately, while advanced, SparroWocky's inner workings are much less arcane than a 'gyre and gimble in the wabe,' so a 'through and through [of] the vorpal blade' allowed us to bring you a detailed analysis of the backdoor," quotes ESET researcher Alexandre Côté Cyr from the world-famous poem. Côté Cyr made the latest discovery during his investigation of the China-aligned group.

This cyberespionage trend against high-profile targets in Latin America started no later than in July 2025 and has continued with the more recent introduction of SparroWocky. In fact, from mid-2025 and into 2026, 90% of the group's targets registered in ESET telemetry have been located in the region. "We have seen the new backdoor deployed against governmental entities in Argentina, Ecuador, Guatemala, Honduras, Panama, Peru, Puerto Rico, and Venezuela. This represents a rare occurrence among the China-aligned APT groups that ESET tracks, which are

generally observed throughout various world regions within such an extended time frame," says Côté Cyr.

ESET believes that this undivided focus is not coincidental and likely reflects China's reaction to various recent U.S. initiatives in the region. Indeed, U.S. President Donald Trump's second term has brought about an aggressive reaffirmation of U.S. interests in Latin America, which threatens various long-term investments that China has cultivated throughout the continent over the last decade, in domains such as energy, mining, and telecommunications. FamousSparrow's activities are probably intended to help China better monitor and anticipate the reaction of local governments to current U.S. pressures. In some cases, certain elements clearly seem to confirm this hypothesis. For instance, one of the Panamanian entities targeted is directly involved in the ongoing commercial dispute regarding two major ports located in the canal area, which were, until recently, operated by a China-based company.

Some of SparroWocky's notable features include the ability to launch arbitrary files, to act as a TCP proxy, and to execute commands. The backdoor also collects general information about the compromised machine, such as the computer name, username, domain name, Windows version, and IP addresses of its network interfaces. SparroWocky is also capable of exfiltrating files and taking screenshots periodically. Exfiltrated information is encrypted using RC4 and sent over the TLS protocol. Depending on its configuration, SparroWocky can establish persistence either by creating a dedicated service or an entry in a registry Run key.

The malware employs a few techniques to complicate its analysis and to evade security software that may be in place. The backdoor manipulates low-level structures in memory, and patches code at runtime in order to avoid detection. FamousSparrow still uses open-source offensive tooling for its own malicious ends. Previously, these tools were mainly used side by side with the group's backdoor. With SparroWocky, ESET researchers observe that it also has the development capabilities to integrate open-source code directly into its own custom backdoor. SparroWocky has the capability to load and execute Beacon Object Files, a special type of executable file supported by many red-teaming and penetration-testing tools.

FamousSparrow is a China-aligned cyberespionage group believed to have been active since at least 2019. ESET Research first publicly documented the group in a blogpost from September 2021, when it exploited the ProxyLogon vulnerability. The group was initially known for targeting hotels around the world but has also targeted governments, international organizations, trade groups, engineering companies, and law firms.

ESET attributes the latest campaign and the SparroWocky backdoor to FamousSparrow with high confidence, since in some of the first attacks involving this backdoor, SparroWocky was deployed by the FamousSparrow-exclusive SparrowDoor. Moreover, not only does the victimology match FamousSparrow's previous targeting, but ESET also recorded attempts to deploy SparroWocky at many of the same organizations that had previously been targeted with SparrowDoor. FamousSparrow is the only known user of the SparrowDoor backdoor.

For a more details and technical analysis of SparroWocky, check out the ESET Research blog post “Beware the SparroWock: The backdoor that bites, the commands that catch” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), Bluesky, and Mastodon for the latest news from ESET Research.

About ESET
ESET protects organizations, critical infrastructure, and individuals, helping them build digital resilience and confidence in an increasingly AI-driven world. With more than 35 years of cybersecurity expertise, over 25 years of AI innovation, and 11 global R&D centers, ESET develops proprietary technologies designed to protect against evolving cyber threats and secure the broader AI ecosystem. Grounded in scientific rigor and taking a preemptive approach to security, ESET delivers effortless protection that remains under expert human oversight. Headquartered in the European Union and privately owned, ESET protects millions of users and more than 500,000 organizations across 178 countries. Committed to responsible AI and customer trust, ESET protects the progress that technology enables. For more information, visit www.eset.com or follow ESET’s social media, podcasts, and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/944526132

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.