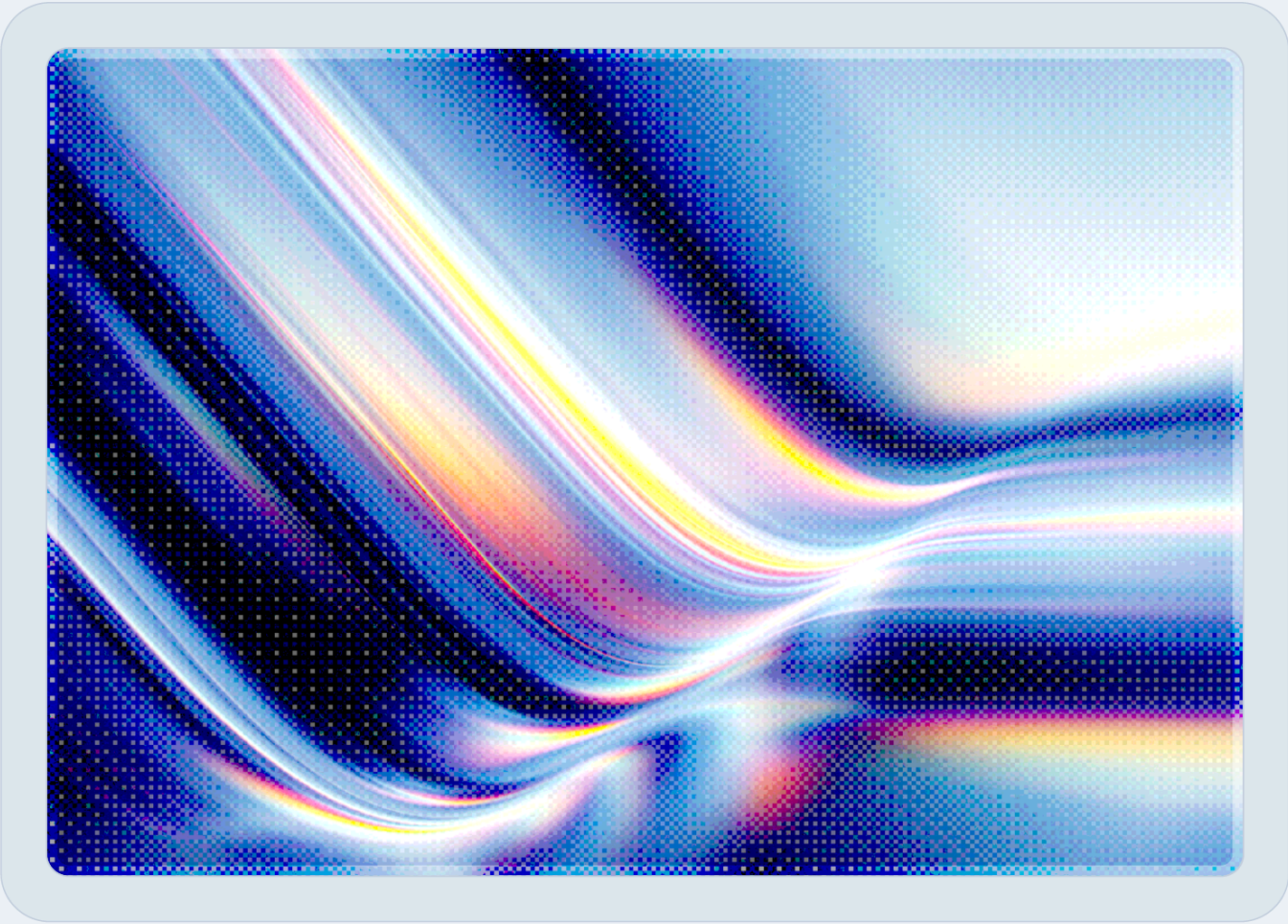
CSAI Foundation | Cloud Security Alliance

SparroWocky: FamousSparrow's New Backdoor Hits Latin America

2026-09-17

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

ESET researchers disclosed SparroWocky, a new modular C++ backdoor that the China-aligned espionage group FamousSparrow began deploying in August 2025 as a replacement for its long-standing SparrowDoor implant [1]. Telemetry gathered from mid-2025 through mid-2026 shows that roughly 90 percent of FamousSparrow's observed activity has concentrated on government and public-sector targets in Latin America, including Argentina, Ecuador, Guatemala, Honduras, Panama, Peru, Puerto Rico, and Venezuela [1][2]. SparroWocky incorporates open-source components — Mbed TLS, the MinHook API-hooking library, and a COFF/Beacon Object File loader — alongside call-stack spoofing and dynamic API resolution, which ESET characterizes as reflecting a deliberate investment in anti-analysis tradecraft rather than a rushed rewrite [1]. One documented victim, a Panamanian entity involved in a commercial dispute over ports in the canal area, points to an intelligence-collection interest tied to Chinese commercial and strategic positioning in the region [1][2]. The campaign extends a multi-year FamousSparrow pattern: the group was first documented in 2021 after exploiting ProxyLogon vulnerabilities and was observed again in 2024 and 2025 compromising a U.S. financial-sector trade group, a Mexican research institute, and a Honduran government network [3][4]. FamousSparrow's demonstrated persistence and evasion capability make its indicators a priority for regional defenders and for multinationals with government-facing operations in the region.

Background

FamousSparrow is a China-aligned cyberespionage group that ESET has tracked publicly since September 2021, when the group was caught exploiting the ProxyLogon set of Microsoft Exchange vulnerabilities to compromise hotel networks worldwide [3]. Over the following years the group's targeting broadened well beyond hospitality to include governments, international organizations, engineering firms, and law firms, and its toolset matured alongside that expansion. In March 2025, ESET reported that FamousSparrow had resurfaced after a period of reduced visibility, compromising a U.S. financial-sector trade group in July 2024 as well as a research institute in Mexico and a governmental institution in Honduras, and that the group had introduced two previously undocumented versions of its flagship SparrowDoor backdoor along with its first observed use of the ShadowPad backdoor [3][4].

That report already showed a group willing to iterate quickly on its malware rather than rely on static tooling, and it established that Latin American government and research networks were squarely within FamousSparrow's target set well before the events described here.

The picture that ESET published on September 17, 2026 shows that pattern accelerating and narrowing geographically [1][2]. Beginning in July 2025, FamousSparrow's telemetry footprint shifted to focus almost exclusively on Latin America, and within a month the group began fielding an entirely new backdoor, which ESET named SparroWocky after discovering that early samples embedded the first stanza of "Jabberwocky," Lewis Carroll's nonsense poem, reused as RFC 7539 test vectors inside the code [1]. SparroWocky effectively retired SparrowDoor as FamousSparrow's primary implant within a matter of weeks, a transition timeline that suggests the new backdoor had been in development well before its public debut rather than being assembled hastily in response to detection. By the time ESET published its analysis, sample timestamps indicated the malware had reached at least version 1.8, and infrastructure tied to the campaign remained active into mid-2026 [1].

The victimology described by both ESET and BleepingComputer is consistent across sources: government entities and affiliated organizations in Argentina, Ecuador, Guatemala, Honduras, Panama, Peru, Puerto Rico, and Venezuela [1][2]. ESET frames the motivation in explicitly geopolitical terms, linking the campaign to China's interest in tracking how Latin American governments are responding to increased U.S. political, economic, and strategic engagement in the region, particularly around energy, mining, and telecommunications investment [1]. Among the documented victims is a Panamanian entity connected to a commercial dispute over two major ports in the canal area [1][2]. That target suggests an intelligence-collection interest weighted toward commercial and strategic advantage rather than classified government material.

Security Analysis

SparroWocky is a modular backdoor written in C++ that ESET assesses reflects deep familiarity with Windows internals and established anti-analysis techniques, rather than an opportunistic reuse of commodity code [1]. Deployment relies on DLL side-loading, with a loader component reading an accompanying `.dat` file that holds an RC4-encrypted configuration block and the backdoor payload itself, which the loader decrypts and executes reflectively in memory. Once running, SparroWocky supports more than 30 distinct commands spanning reconnaissance, interactive shell access, file upload and download, screenshot capture, TCP proxying, and execution of Beacon Object Files loaded through an embedded COFF loader, a format popularized by the Cobalt Strike framework and widely reused across red-team and offensive tooling, giving operators a way to run additional in-memory tooling without dropping new binaries to disk [1]. BleepingComputer's reporting adds that the screenshot

function captures changed regions of the screen roughly every 500 milliseconds rather than full frames, which reduces both the data volume sent to command-and-control infrastructure and the forensic footprint left on disk [2].

The backdoor's evasion engineering is a notable departure from the group's earlier tooling. SparroWocky performs dynamic resolution of Windows API calls rather than importing them statically, spoofs call stacks using a technique consistent with the publicly documented "SilentMoonwalk" method, and hooks the `CreateThread` function — using the open-source MinHook library — to make malicious threads appear to originate from legitimate system processes such as `AnimateWindow` [1][2]. Persistence is established through either a Windows service or a registry Run key, which can provide redundancy if one mechanism is detected and removed. For network communications, SparroWocky encrypts its command-and-control channel with TLS layered over a custom message format, and connects preferentially to hardcoded IP addresses on ports 443 and 8080 rather than to domain names, a design choice that has the practical effect of denying defenders the ability to disrupt the campaign through DNS sinkholing or domain takedowns. ESET identified at least 18 distinct command-and-control addresses associated with the campaign, hosted across a mix of providers including The Constant Company, Kaopu Cloud, Cogent Communications, and LightNode, with one primary address — 216.238.110[.]120 — first observed in December 2025 [1][2]. The group also supports HTTP and SOCKS5 proxying, which can allow compromised hosts to relay traffic for other implants and complicate network-based attribution of any single connection to a specific victim.

The shift from SparrowDoor to SparroWocky represents more than a rename; it reflects a change in engineering philosophy that is easier to see side by side than described in isolation.

Attribute	SparrowDoor (2021–2025)	SparroWocky (2025–present)
Language / architecture	C++, monolithic implant, iterated in versioned releases [3][4]	C++, modular design with pluggable command handlers [1]
Code provenance	Largely custom, traceable across publicly documented versions [4]	Directly incorporates open-source Mbed TLS, MinHook, and a COFF/BOF loader [1]
Evasion techniques	Standard obfuscation; no documented call-stack spoofing	Dynamic API resolution, SilentMoonwalk-style call-stack spoofing, `CreateThread` hooking via MinHook [1][2]

Attribute	SparrowDoor (2021–2025)	SparroWocky (2025–present)
In-memory execution	Not documented	Beacon Object File (BOF) execution via embedded COFF loader [1]
C2 communication	Custom protocol over TCP	TLS-wrapped custom protocol, hardcoded IPs on ports 443/8080, HTTP/SOCKS5 proxy support [1][2]
Primary 2025–2026 targeting	Hotels, government, international organizations, law firms, financial sector (global) [3][4]	~90% of activity concentrated on Latin American governments [1][2]

Two additional aspects of SparroWocky's engineering are worth emphasizing for defenders beyond the specific indicators. First, SparroWocky's direct incorporation of Mbed TLS, MinHook, and a COFF/BOF loader is consistent with a pattern CSA has observed in other campaigns this year [5][6] of building implants atop actively maintained open-source components rather than custom primitives, an approach that can shorten development cycles and make static signature detection less reliable across malware families that share underlying libraries. Second, the shift from SparrowDoor to SparroWocky within weeks, combined with the code quality ESET describes, indicates a well-resourced development effort operating on a deliberate release cadence rather than reactive patching, a pattern consistent with what CSA has documented in other China-nexus campaigns this year, including the BRICKSTORM backdoor's BSD-variant deployment against Linux-based network appliances [5] and UNC6508's multiyear INFINITERED implant campaign against REDCap research servers [6]. In both of those cases, as in this one, initial detection lagged actual compromise by months, and the intrusion set proved resilient to point fixes that did not address the underlying access the actor had already established.

Recommendations

Immediate Actions

Defenders should hunt for the network indicators ESET published, including the 216.238.110[.]120 command-and-control address and the broader set of at least 18 associated IP addresses communicating over TCP 443 and 8080 with non-standard TLS handshake characteristics, particularly from Windows Server and Exchange-facing infrastructure [1][2]. Windows services and registry Run keys

on internet-facing servers, especially IIS and Exchange hosts, should be inspected for unrecognized persistence entries, alongside a review of DLL search-order behavior for signs of side-loading involving unexpected `.dat` companion files. Endpoint detection telemetry should also be reviewed for `CreateThread` calls that originate from or inject into processes such as `AnimateWindow`, and for API-hooking behavior consistent with MinHook, since these are concrete, ESET-documented indicators rather than generic heuristics.

Short-Term Mitigations

Government agencies and regional offices of multinationals operating in Argentina, Ecuador, Guatemala, Honduras, Panama, Peru, Puerto Rico, or Venezuela should prioritize threat-hunting exercises against this specific campaign given the concentration of confirmed targeting in those jurisdictions [1][2]. Internet-facing Exchange and IIS servers should be patched and hardened, since FamousSparrow's documented initial-access pattern has repeatedly relied on webshells deployed against outdated or unpatched Windows Server and Exchange deployments [3][4]. Centralized logging and EDR coverage should be extended to any server segment that historically falls outside routine monitoring; the group's use of proxying and hardcoded IP infrastructure has the effect of blending into normal outbound traffic and evading DNS-based detection, regardless of intent.

Strategic Considerations

Organizations that sit adjacent to U.S.-China commercial or strategic friction points in Latin America — ports, telecommunications, energy, and mining, along with the government ministries that regulate them — should treat themselves as plausible targets independent of their own perceived intelligence value, since FamousSparrow's Panama port case demonstrates an interest in secondary and commercial intelligence, not only classified government material. Given that the group replaced its entire flagship implant within weeks and continues to iterate on evasion tradecraft, defenders should assume that indicator-based detection alone will have a limited shelf life and should invest instead in behavioral detection around DLL side-loading, in-memory execution, and anomalous outbound TLS connections to non-domain destinations. Regional CERTs and government IT security teams would also benefit from establishing information-sharing channels specifically focused on China-nexus activity in Latin America, since the concentrated, multi-country targeting pattern ESET describes suggests that indicators found in one country are likely to recur in neighboring jurisdictions.

CSA Resource Alignment

FamousSparrow's campaign fits a pattern CSA has tracked closely across two 2026 China-nexus threat intelligence briefs that offer directly applicable defensive frameworks. CSA's analysis of VerdantBamboo's deployment of a FreeBSD variant of the BRICKSTORM backdoor against Linux-based network appliances documents a comparable combination of long-dwell-time persistence, in-memory execution, and proxy-based evasion of Zero Trust conditional-access controls, and maps those behaviors to the AI Controls Matrix (AICM) v1.1 supply-chain, identity, and logging domains [5]. The recommendations in that report — extending EDR and centralized logging to infrastructure that typically falls outside routine monitoring, and testing detection tooling against natively compiled, obfuscated malware — apply with little modification to SparroWocky's own use of reflective loading and API hooking. CSA's report on UNC6508's multiyear compromise of REDCap research servers using the INFINITERED implant family similarly illustrates how a China-nexus actor can sustain access for years by favoring stealth and administrative-surface abuse over noisy exploitation, reinforcing the strategic point that indicator lists alone will not keep pace with an actively developed implant family [6]. Together, these prior analyses support treating SparroWocky not as an isolated incident but as the latest expression of a broader China-nexus operating pattern that CSA's AI Controls Matrix v1.1 is designed to help organizations govern through its threat-and-vulnerability-management and identity-and-access-management domains, regardless of which specific implant a given campaign happens to deploy [7].

References

[1] ESET. "Beware the SparroWock: The backdoor that bites, the commands that catch." WeLiveSecurity, September 2026.

[2] BleepingComputer. "Chinese hackers use SparroWocky malware in govt espionage attacks." BleepingComputer, September 2026.

[3] ESET. "ESET Research: China-aligned FamousSparrow expands operations in Latin America, targets governments with new backdoor." GlobeNewswire, September 17, 2026.

[4] ESET. "You will always remember this as the day you finally caught FamousSparrow." WeLiveSecurity, March 26, 2025.

[5] Cloud Security Alliance. "VerdantBamboo Deploys BRICKSTORM BSD Variant on Linux Appliances." Cloud Security Alliance, June 2026.

[6] Cloud Security Alliance. "UNC6508: A Multiyear China-Nexus Campaign in Medical Research." Cloud Security Alliance, June 2026.

[7] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance.