The p0sT5n1F3r Backdoor

By Mario Ciccarelli

Published: 2019-10-16 · Archived: 2026-04-05 17:08:12 UTC

By Mario Ciccarelli in malware analysis — 16 Oct 2019

P0sT5n1F3r, a stealthy Apache backdoor built to sniff HTTPS traffic. Undetected by anti-malware platforms, the module used RC4 encryption to hide its activities. Reverse engineering revealed the key, exposing a targeted payload designed to steal credit card data.

How does a malicious backdoor designed to sniff sensitive HTTPS traffic go completely undetected?

During an IR case, we found and dissected a highly targeted malware sample, a custom Apache module we call `p0sT5n1F3r`.

This threat was specifically engineered for its target's environment and was rated 100% clean by all major security vendors due to its extensive use of custom encryption.

This report details the reverse engineering journey, from the initial static analysis to the critical breakthrough: cracking its custom RC4 encryption scheme. This discovery allowed us to unveil its true purpose—intercepting financial transaction data—and even uncover a hidden HTML interface used by the attackers.

Read the full technical deep dive to learn how this threat was unmasked.
