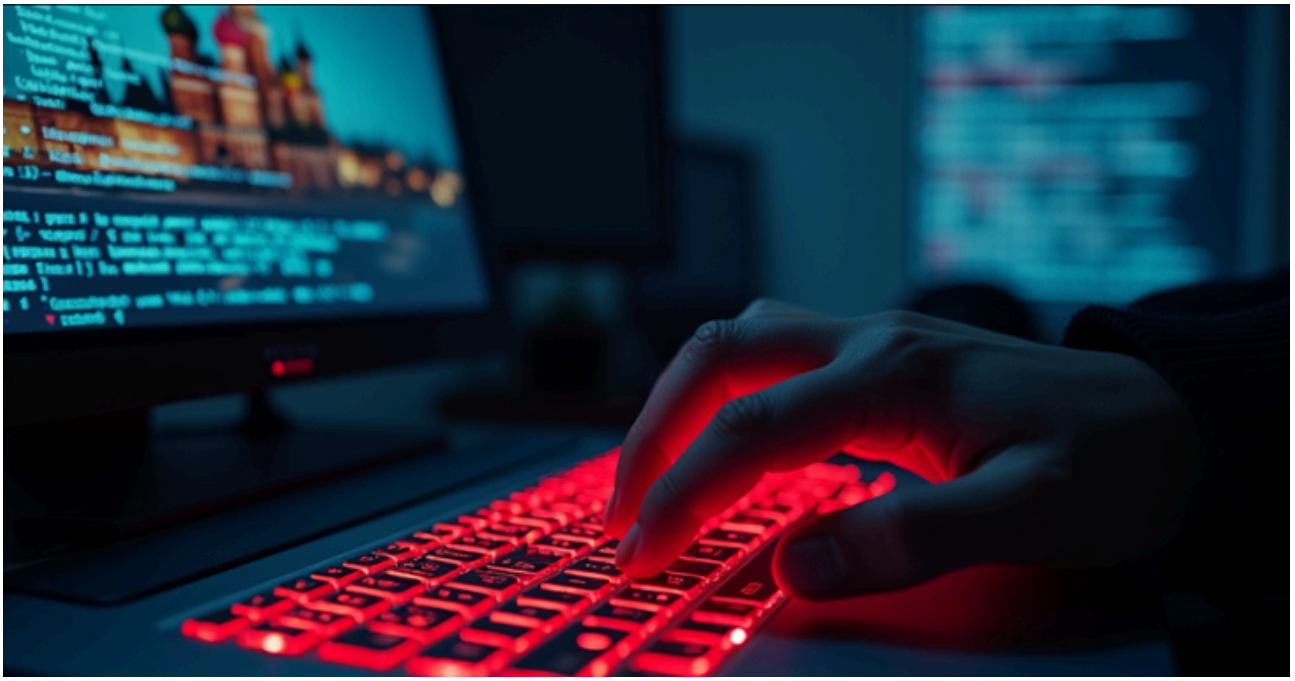
Space Pirates Targets Russian IT Firms With New LuckyStrike Agent Malware

By The Hacker News

Published: 2025-02-27 · Archived: 2026-04-05 21:04:31 UTC



The threat actor known as Space Pirates has been linked to a malicious campaign targeting Russian information technology (IT) organizations with a previously undocumented malware called LuckyStrike Agent.

The activity was detected in November 2024 by Solar, the cybersecurity arm of Russian state-owned telecom company Rostelecom. It's tracking the activity under the name Erudite Mogwai.

The attacks are also characterized by the use of other tools like Deed RAT, also called ShadowPad Light, and a customized version of proxy utility named Stowaway, which has been previously used by other China-linked hacking groups.

"Erudite Mogwai is one of the active APT groups specializing in the theft of confidential information and espionage," Solar researchers said. "Since at least 2017, the group has been attacking government agencies, IT departments of various organizations, as well as enterprises related to high-tech industries such as aerospace and electric power."

The threat actor was first publicly documented by Positive Technologies in 2022, detailing its exclusive use of the Deed RAT malware. The group is believed to share tactical overlaps with another hacking group called Webworm. It's known to target organizations in Russia, Georgia, and Mongolia.

In one of the attacks targeting a government sector customer, Solar said it discovered the attacker deploying various tools to facilitate reconnaissance, while also dropping LuckyStrike Agent, a multi-functional .NET backdoor that uses Microsoft OneDrive for command-and-control (C2).

"The attackers gained access to the infrastructure by compromising a publicly accessible web service no later than March 2023, and then began looking for 'low-hanging fruit' in the infrastructure," Solar said. "Over the course of 19 months, the attackers slowly spread across the customer's systems until they reached the network segments connected to monitoring in November 2024."

Also noteworthy is the use of a modified version of Stowaway to retain only its proxy functionality, alongside using LZ4 as a compression algorithm, incorporating XXTEA as an encryption algorithm, and adding support for the QUIC transport protocol.

"Erudite Mogwai began their journey in modifying this utility by cutting down the functionality they didn't need," Solar said. "They continued with minor edits, such as renaming functions and changing the sizes of structures (probably to knock down existing detection signatures). At the moment, the version of Stowaway used by this group can be called a full-fledged fork."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
