MoldyRoost

CAMPAIGN · CYBER DESK

Compiled by machine from news coverage; not reviewed analysis. A snapshot taken on 23 Nov 2026. Numbers in brackets point to the Sources list at the end. The live page: https://morningstarsecurity.com/wiki/moldyroost

FACTS

- **Objective:** exfiltrate crypto wallet seed phrases, iCloud Keychain data, messages, and photos (low confidence, 1 independent source) [1]

ENTRY

MoldyRoost is a campaign mentioned in the news MorningStar covers.

Drawn from 1 news source; the facts and relationships below show where each detail comes from.

ABOUT MORNINGSTAR SECURITY

MorningStar Security is a security news reader and community, started in 2009 and relaunched in 2026. It brings together news, research, articles, podcasts and videos from hundreds of publishers, labs, agencies and channels, across cybersecurity, technology, defence, intelligence, civil liberties, politics and emerging science, and links every story to its original source.

Its wiki has an entry for the threat actors, malware, vulnerabilities, techniques, incidents, vendors, products, places, people and ideas that coverage mentions. Each entry is compiled by machine from the stories the site indexes. Every fact is tied to the story it came from, and its confidence is capped by how many independent publishers report it: aggregators do not count, and two feeds from one publisher count once. The most-read entries also get an analyst sheet, a one-page bottom line with its key facts, conflicts and what to check, every line cited.

Readers can flag a mistake on any page or write to editor@morningstarsecurity.com.

- This entry, live: https://morningstarsecurity.com/wiki/moldyroost
- More campaigns: https://morningstarsecurity.com/wiki/kind/campaign
- The Cyber desk, for the news: https://morningstarsecurity.com/desk/cyber
- The whole wiki: https://morningstarsecurity.com/wiki
- About MorningStar Security: https://morningstarsecurity.com/about
- How the site is made: https://morningstarsecurity.com/editorial
- The newsletter: https://morningstarsecurity.com/newsletter

SOURCES

1. ⚡ Weekly Recap: VMware 0-Day, Java4Shell, NGINX2Root, Ruby2Shell, and a Whole Lot of Shell Trouble · The Hacker News · 23 Nov 2026 · https://thehackernews.com/2026/11/weekly-recap-vmware-0-day-java4shell.html

---

Snapshot of https://morningstarsecurity.com/wiki/moldyroost taken 23 Nov 2026 17:50 UTC. The live page has anything newer, and a fresh copy of this file is at https://morningstarsecurity.com/md/wiki/moldyroost