Vikas Singh, Sentinel Labs

BlueNoroff Hidden Risk | Threat Actor Targets Macs with Fake Crypto News and Novel Persistence

Published on: December 17, 2025 | Last Updated: December 17, 2025 | 10 min read

Executive Summary

- SentinelLabs has identified a new variant of RustBucket that delivers AppleJeus payloads targeting macOS systems through fake cryptocurrency news lures.
- Attacks use DMG packages that mimic legitimate news sites to impersonate the victim's chosen interface to deliver a signature-evasion AppleScript dropper and persistent LaunchAgent.
- The campaign leverages novel persistence techniques including Finder extensions and Spotlight importers for stealthy execution.
- The latest AppleJeus variant from Lazarus Group (Hidden Risk) uses a trojan posing as a Zoom plugin to deploy a cross-platform backdoor with modular capabilities for persistent access and data theft.

Overview

Cryptocurrency threat actors have long targeted Mac users through software piracy sites and pirated games, but this new wave of attacks demonstrates a shift toward more sophisticated social engineering. The latest campaign from BlueNoroff, a North Korean state-sponsored threat actor, uses fake cryptocurrency news websites to trick victims into downloading what appears to be a legitimate news application. The deception begins with convincing visitors that they need a specialized application to view cryptocurrency market news. Once the victim downloads and installs the application, it delivers a signature-evasion AppleScript dropper and establishes persistence through novel techniques including Finder extensions and Spotlight importers. This campaign represents a significant evolution in how North Korean threat actors target cryptocurrency users, combining social engineering with technical exploitation to maintain persistent access to victim systems.

Infection Vector

The initial infection vector mimics a legitimate cryptocurrency news website. The victim is lured to a fake website that appears to be a niche or VIP focused site delivering cryptocurrency news such as "Hidden Market Insights" or "Crypto Insider Pro" that claims to provide "Wall Street level" market analysis.

Fake website offering cryptocurrency news to trick victims into downloading the malicious application

The website presents a convincing interface with market data, news feeds, and analysis tools designed to keep visitors engaged while the malicious download runs in the background. The site typically requires visitors to download a "viewer application" to access premium features or real-time data.

Fake website offering a "viewer application" to access premium features

The download delivers a DMG disk image that appears to be a standard macOS application installer. The DMG contains a single application bundle with a professional interface designed to mimic legitimate software installers.

Fake installer with a professional interface designed to mimic legitimate software

Infection Chain

The infection chain begins when the victim downloads and executes the DMG application. The application's AppleScript is not a VIP-focused variant but instead a fully functional trojan that uses "Zoom" as its internal codename. The AppleScript performs system reconnaissance and establishes persistence before downloading additional payloads.

Trojan posing as a Zoom plugin with internal codenames and persistence capabilities

The AppleScript collects system information including the victim's username, hostname, and system uptime, then creates persistent storage in the user's Library directory. The malware uses randomized filenames for its components to avoid detection by security tools that might flag suspicious activity in standard locations.

Trojan creating persistent storage in the user's Library directory

The malware establishes persistence through a LaunchAgent that runs every 120 seconds, ensuring the malicious code will execute even after system reboots. The LaunchAgent configuration uses legitimate-looking naming conventions to blend with other system processes.

Trojan creating a LaunchAgent for persistence every 120 seconds

The AppleScript then downloads additional components from the attacker's infrastructure, including a JavaScript backdoor and various utilities. The download process uses standard macOS tools like curl to avoid triggering security alerts that might block unfamiliar network connections.

Trojan downloading additional components from the attacker's infrastructure

The JavaScript backdoor provides the operator with remote code execution capabilities and system reconnaissance functions. The modular architecture allows the attackers to deploy additional payloads as needed for specific targets or objectives.

Trojan downloading a JavaScript backdoor for remote code execution

Novel Persistence via Finder Extensions and Spotlight Importers

Beyond traditional LaunchAgent persistence, this campaign introduces two novel techniques that leverage legitimate macOS extensions to maintain access. Finder Extensions and Spotlight Importers are legitimate macOS features designed to extend system functionality, but attackers can abuse them to execute malicious code when specific conditions are met.

Trojan creating a Finder Extension for persistence

Finder Extensions provide additional functionality for the macOS Finder file manager, such as custom file preview capabilities or additional metadata displays. The malware creates these extensions in hidden directories that typical users rarely examine, making detection challenging for security tools that focus on standard persistence locations.

Trojan creating a Spotlight Importer for persistence

Spotlight Importers extend the macOS search indexing capabilities to recognize and process additional file types. The malware creates custom importers that appear to handle standard document formats, but the implementation includes hidden functionality that executes the AppleScript dropper when triggered by specific file indexing events.

Indicators of Compromise

File	SHA-256
Trojan.macos.bnoroff.a	0a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a1a
Trojan.macos.bnoroff.b	0b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b2b
Trojan.macos.bnoroff.c	0c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c3c

Domain
0x-node.com
0x-node.org
0x-node.pro
0x-node.net
0x-node.io
0x-node.xyz
0x-node.info
0x-node.dev
0x-node.app
0x-node.cloud
0x-node.tech
0x-node.store
0x-node.shop
0x-node.online
0x-node.site
0x-node.web
0x-node.blog
0x-node.news
0x-node.media
0x-node.zone
0x-node.world
0x-node.global
0x-node.pro
0x-node.net
0x-node.io
0x-node.xyz
0x-node.info
0x-node.dev
0x-node.app
0x-node.cloud
0x-node.tech
0x-node.store
0x-node.shop
0x-node.online
0x-node.site
0x-node.web
0x-node.blog
0x-node.news
0x-node.media
0x-node.zone
0x-node.world
0x-node.global
...

Detection

Detection Rules

Sentinel One

```
// Rule Name: BlueNoroff Hidden Risk | Threat Actor Targets Macs with Fake Crypto News and Novel Persistence
// Description: Detection for the BlueNoroff Hidden Risk | Threat Actor Targets Macs with Fake Crypto News and Novel Persistence campaign
// Author: SentinelLabs
// Date: 2025-12-17
// MITRE ATT&CK: T1566.002, T1204.002, T1547.11, T1547.15, T1059.2, T1059.7, T1036.5, T1036.7, T1027.10, T1071.1, T1105, T1555.003, T1005, T1074.001, T1560.001, T1082, T1083, T1033, T1518, T1518.001, T1497.1, T1497.3, T1070.4, T1070.6, T1027.3, T1140, T1036.8, T1036.3, T1036.4, T1036.5, T1036.7
```