New North Korean Malware OtterCookie Uses Fake Job Offers to Steal Credentials

DUBAI, DUBAI, UNITED ARAB EMIRATES, June 3, 2025 /EINPresswire.com/ -- ANY.RUN, a trusted provider of cybersecurity solutions, has published a new malware analysis exposing OtterCookie, a newly identified JavaScript-based stealer deployed by North Korea's Lazarus Group. The in-depth research reveals how the malware is delivered through fake job offers and executes via a deceptively clean Node.js repository, stealing credentials, wallet data, and preparing for second-stage infection.

□□□□□□□□□□□□: □□□□□□□□ □□□□□□□ □□ □ □□□□□ □□□□

OtterCookie is part of a broader social engineering campaign known as Contagious Interview or DevPopper, where threat actors pose as recruiters or hiring managers to lure developers and executives into opening malicious repositories. Once launched, the malware executes by triggering a forced JavaScript error within a try/catch block, used as a delivery mechanism to fetch and run payloads from a remote server.

The campaign targets users in the crypto, fintech, and Web3 spaces, reusing patterns seen in previous Lazarus-linked strains such as Beavertail and InvisibleFerret.

□□-□□□□□□ □□□□□□□□□ □□ □□□□□□□□□□□□□

Key findings include:

· □□□□ □□□□ □□□□□□ □□ □□□□□ – Delivered via LinkedIn or email, offering contract work to fix a

frontend bug.

· □□□□□ □□□□.□□ □□□□□□□□□□ – No implants or suspicious dependencies, lowering suspicion.

· □□□□□□□□□□ □□□ □□□□□□ □□□□□ – Targets browser credentials, macOS keychains, and wallets like Solana and Exodus.

· □□□□□□□□□□□□□□ □□□□□ – Exfiltrates data via port 1224 to servers linked to InvisibleFerret.

· □□□□□□-□□□□□ □□□□□□□□ – Installs a portable Python environment to run InvisibleFerret.

· □□□□□ □□□□□□□□□ □□ □□□.□□□ – Sandbox flags the payload before deobfuscation and maps behavior via MITRE ATT&CK.

To explore the full technical breakdown and see OtterCookie in action inside an interactive sandbox, visit ANY.RUN's cybersecurity blog.

□□□□□ □□□.□□□

ANY.RUN offers a comprehensive suite of cybersecurity tools, including an interactive malware sandbox and Threat Intelligence services. Trusted by over 500,000 professionals worldwide, the platform provides real-time behavioral analysis of threats across Windows, Linux, and Android systems. By giving analysts full visibility into malware activity as it unfolds, ANY.RUN helps teams respond faster, investigate deeper, and make informed decisions with confidence.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
LinkedIn
YouTube
X
