

## 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 indepth 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.

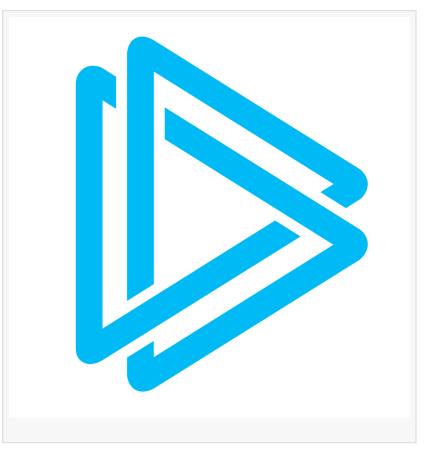
OtterCookie is part of a broader social





## Key findings include:

· 🛮 🔻 🗠 🗠 🗠 - Delivered via LinkedIn or email, offering contract work to fix a



## frontend bug.

- · 🛮 🖺 🖺 🖺 🖺 🗎 🗎 🗎 Exfiltrates data via port 1224 to servers linked to InvisibleFerret.
- · 🛮 🖺 🖺 🖺 🖺 🗎 🖺 🗎 🗎 🗎 Installs a portable Python environment to run Invisible Ferret.
- DDDDD DDDDDDDD DD DDD.DDD 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.

## 00000 000.000

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

This press release can be viewed online at: https://www.einpresswire.com/article/818604454

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.