ANY.RUN Exposes North Korean ‘Fake Interview’ Campaign: BeaverTail Loader Deploys InvisibleFerret Malware

DUBAI, DUBAI, UNITED ARAB EMIRATES, January 21, 2025 /EINPresswire.com/ -- ANY.RUN released technical research on a new wave of North Korean-linked malware campaigns disguised as job interviews. □□□□□□□□□□, a JavaScript-based loader, deploys □□□□□□□□□□□□□□□□, a Python stealer designed to steal crypto wallets, source code, and more. By posing coding challenges and software installs, attackers trick victims into downloading malicious components.

□□□ □□□□□□□□□□ □□□□ □□□□□□□□□□ □□□□□□□□□

Below are the key findings from ANY.RUN technical analysis:

· □□□□□□□□ □□□□□□□□□□ □□□ □□□□□: Campaigns primarily affect technology, finance, and crypto organizations, specifically targeting developers and engineers with job-related lures.
· □□□□-□□□□□ □□□□□□□: BeaverTail downloads a Python environment to deploy InvisibleFerret, which can kill browser processes, exfiltrate files, and persist in the system.
· □□□□□□□□ □□□□□□□□□□□□ □□□□□□□: Depending on configuration, attackers can push stolen data over FTP, SMTP, or Telegram.
· □□□□□□□□□□□□ □□□ □□□.□□□: The platform’s real-time timeline view and thorough TTP mapping provide actionable intelligence for security teams.

For the full deep dive, including IOCs and technical breakdowns, see ANY.RUN’s blog.

□□□□□□□□□□□□ □□□ □□□□□□□□□□

This campaign highlights how attackers disguise malware as ordinary job tasks, making it easy for even well-defended organizations to be caught off guard. Companies in tech and crypto should use advanced sandbox analysis for suspicious files and attachments. Regular monitoring of development environments and stronger access controls can help prevent these covert infiltration attempts and protect valuable corporate assets.

□□□□□ □□□.□□□

ANY.RUN is a trusted provider of cybersecurity solutions used by over 500,000 professionals. By offering real-time sandbox environments for Windows and Linux, along with advanced threat intelligence tools and team collaboration features, ANY.RUN empowers organizations to detect, analyze, and counteract cyber threats efficiently.

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