Lazarus Group Escalates Attacks in 2025: ANY.RUN Reveals Detection Strategies for SOC Teams

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 10, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence, released an in-depth report on the Lazarus Group's intensified cyber campaigns in 2025. The research exposes sophisticated tactics targeting tech and crypto sectors, offering SOC teams actionable insights and detection tips to fortify defenses against this notorious North Korean APT.

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

The Lazarus Group has ramped up operations with social engineering and supply chain exploits, compromising hundreds of firms and causing millions in losses. Tactics include:

· □□□□□□ □□□□□□□ □□ □□□□□□□□: Operatives pose as remote hires using stolen identities to infiltrate U.S. and UK companies, stealing data and deploying malware. A blockchain firm lost $900,000 in crypto to such insiders, per U.S. Department of Justice reports.

· □□□□□□□□□□ □□ (□□□□□□□□□□□□ □□□□□□□□□□): Fake job interviews on LinkedIn lure developers with malicious GitLab tests and NPM packages. Victims face credential theft and system infections, leading to supply chain ripple effects.

· □□□□□□□□□ □□□□-□□□□□□□ □□□□□□□□□: Over 230 malicious GitHub and PyPI uploads since January target developers, enabling backdoor access. The $1.5B ByBit hack stemmed from a tainted

Docker project at Safe{Wallet}, funneling funds to Lazarus.

These attacks erode financial stability, IP, and trust, with recovery costs soaring.

□□□□□□□□□□ □□□□ □□□ □□□ □□□□□

Lazarus deploys evasive tools like InvisibleFerret (keylogging via fake interviews), OtterCookie (token theft in packages), and PyLangGhost RAT (espionage via ClickFix scripts).

ANY.RUN's Interactive Sandbox helps over 15,000 SOCs ensure:

· Faster detection of threats and reduced Mean Time to Detect (MTTD)

· Full visibility into what files and links actually do without any guesswork

· Immediate access to IOCs for SIEM enrichment and faster response

· Less manual effort for analysts, thanks to automated interactivity

· Lower risk of breaches, data loss, and business disruption

Read the full report on active Lazarus Group attacks on ANY.RUN blog.

□□□□□ □□□.□□□

ANY.RUN is an interactive malware analysis and threat intelligence provider trusted by SOCs, CERTs, MSSPs, and cybersecurity researchers. The company's solutions are leveraged by 15,000 corporate security teams for incident investigations worldwide.

With real-time visibility into malware behavior, a focus on real-time interaction and actionable intelligence, ANY.RUN accelerates incident response, supports in-depth research, and helps defenders stay ahead of evolving threats.

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