EINPRESSWIRE

ANY.RUN Reveals PyLangGhost RAT: Emerging Data Stealer from Lazarus Group Targeting Finance and Technology

DUBAI, DUBAI, UNITED ARAB EMIRATES, August 6, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has uncovered new details about PyLangGhost RAT, a sophisticated Python-based remote access trojan linked to the Lazarus Group's Famous Chollima subgroup. Delivered through an innovative "ClickFix" social engineering tactic, PyLangGhost RAT targets the technology, finance, and cryptocurrency sectors.

[illegible]

PyLangGhost RAT is deployed in carefully planned operations rather than mass attacks. Using fake job interviews as a lure, attackers convince victims to run what appears to be a simple "fix" for a fake camera or microphone error. In reality, this action installs a remote access tool disguised as a legitimate Python application.

Once active, PyLangGhost RAT enables attackers to:

· [illegible] and compromise cryptocurrency wallets.

· [illegible], including intellectual property, customer records, and strategic documents.

· [illegible] by maintaining persistent access and deploying additional payloads.

· □□□□□□□□□□ □□□□□□ □□□□□□□□□□□ if the breach becomes public, especially due to its state-sponsored origin.

· □□□□□□□□ □□□□□□□□□□□ □□□ □□□□□□ □□□□□□□ under regulations like GDPR and CCPA.

Given its low detection rate and highly targeted approach, PyLangGhost RAT can remain inside a network for extended periods, increasing both the scope and cost of an incident.

□□□ □□□□□□□□□□ □□□ □□□□□□□□□□□

· □□□□□□□□ □□□□□□□□: Executives, developers, and high-value personnel in finance, technology, and cryptocurrency.

· □□□□□□□□□ □□□□□□: Financial theft, regulatory penalties, operational downtime, and long-term reputational damage.

· □□□□□□□□□□ □□□□□□□□□□: Often bypasses traditional antivirus tools; behavior-based analysis significantly shortens detection and response times.

Discover how PyLangGhost RAT infiltrates organizations and how early detection can reduce financial, operational, and reputational risk by visiting the ANY.RUN blog.

□□□□□□ □□□.□□□

ANY.RUN is a leading provider of interactive malware analysis and threat intelligence solutions used by 15,000+ companies worldwide. Its suite enables real-time analysis of files, links, and advanced threats, helping SOC teams, CERTs, and malware researchers detect, investigate, and respond to cyber incidents faster and with greater confidence.

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

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.