EINPRESSWIRE

Researchers Capture Lazarus APT’s Remote-Worker Scheme on a Live Camera

DUBAI, DUBAI, UNITED ARAB EMIRATES, December 4, 2025 /EINPresswire.com/ -- ANY.RUN together with NorthScan and BCA LTD, uncovered a North Korean scheme in which Lazarus (Famous Chollima) attempted to place covert IT workers inside U.S. companies. Instead of malware, the operation relied on social engineering, identity theft, and remote-access tools. Researchers captured the operators working live inside a controlled environment.

[illegible]

Researchers allowed the Lazarus APT recruiters to believe they had convinced a U.S.-based developer to share his laptop for remote work. In reality, all access went through specially prepared ANY.RUN sandbox environments, giving full visibility into what the operators did on the “laptops” for several weeks.

· Identity rental as the initial access vector, with operators asking victims for SSNs, documents, bank accounts, and 24/7 device access.

· Use of AnyDesk, Google Remote Desktop, and browser-syncing to establish long-term control over compromised machines.

· Recruitment is wide-scale, using GitHub spam, Telegram outreach, and fake job-seeking setups.

· AI-assisted job-application automation, including extensions for interview coaching and mass application submissions.

· Shared infrastructure among operators, exposing overlapping roles and weak operational security.

· Live behavioral capture including click-level actions, file changes, network calls inside the sandbox.

Get the full technical picture, including operator workflows, captured artifacts, and actionable IOCs, on ANY.RUN’s blog.

□□□□□ □□□□□□□□□□□□□□□□ □□□□□□□ □□

Companies should verify identities during hiring, monitor for unusual remote-desktop tools, and flag inconsistencies between applicant location, system configuration, and network behavior. Identity theft and remote-worker infiltration are now common entry points for human-driven operations, and the behavioral signals captured in this investigation offer new clues security teams can use to detect them earlier.

□□□□□□ □□□.□□□

ANY.RUN is a leading platform for interactive malware analysis and threat intelligence, trusted by more than 15,000 organizations and over 500,000 analysts worldwide. The platform provides real-time behavioral visibility with an average 60-second time-to-verdict, enabling fast investigation of files, URLs, and complex attack chains. Alongside its interactive sandbox, ANY.RUN delivers continuously updated Threat Intelligence Feeds sourced from global telemetry, and TI Lookup, a service that reveals related samples, shared infrastructure, and historical context. Together, these capabilities help security teams detect threats earlier, understand attacker behavior, and respond 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.