

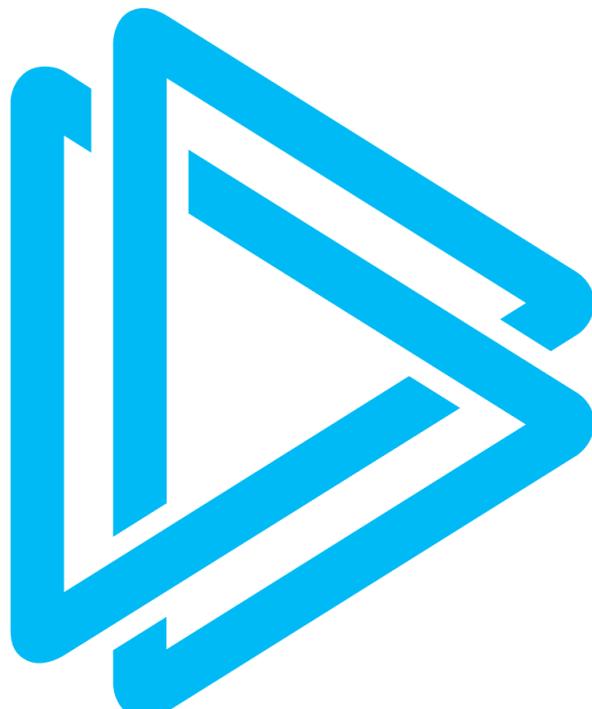
October's Top Cyber Attacks Target Companies Worldwide: Google Careers Phishing, Figma Abuse, LockBit 5.0, and TyKit

DUBAI, DUBAI, UNITED ARAB

EMIRATES, October 29, 2025

/EINPresswire.com/ -- Cyberattacks are accelerating in complexity, and this October was no exception. [ANY.RUN](#), a leading provider of interactive malware analysis and threat intelligence solutions, reports that organizations worldwide faced an escalation of sophisticated phishing and ransomware campaigns exploiting trusted cloud infrastructure.

The October 2025 Threat Analysis highlights how threat actors are misusing legitimate platforms like Google, ClickUp, and Figma, while ransomware groups like LockBit continue expanding into new environments.



□□□□□□□ □□□□□□ □□□□□□□ □□□□□□□□

Attackers are increasingly abusing Google Careers, ClickUp, and Figma to host phishing flows that look legitimate. These campaigns use Salesforce redirects, Cloudflare CAPTCHAs, and public prototypes to mimic Microsoft 365 or job application portals and steal credentials. By chaining multiple trusted domains, they bypass filters and reputation systems, leaving SOCs blind without behavioral analysis.

□□□□□□ □.□ □□□□□□□□

On its sixth anniversary, LockBit released a new version targeting Linux and VMware ESXi, marking a strategic move toward critical infrastructure. The variant can disable multiple virtual

machines simultaneously, causing widespread outages across data centers and enterprise environments.

ANY.RUN

ANY.RUN researchers uncovered TyKit, a reusable phishing kit hiding JavaScript inside SVG files to execute redirects and steal Microsoft 365 credentials. Active across finance, government, telecom, and education, it demonstrates how simple obfuscation can outsmart legacy detection.

For full technical details, live analyses, IOCs, and guidance on faster detection, visit the [ANY.RUN blog](#).

ANY.RUN

ANY.RUN helps more than 15,000 organizations worldwide, including leaders in finance, healthcare, telecom, retail, and technology, strengthen cybersecurity operations with real-time malware analysis and live threat intelligence.

The suite combines interactive sandboxing with dynamic intelligence, enabling faster investigations, deeper visibility, and proactive threat prevention.

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/862598840>

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.