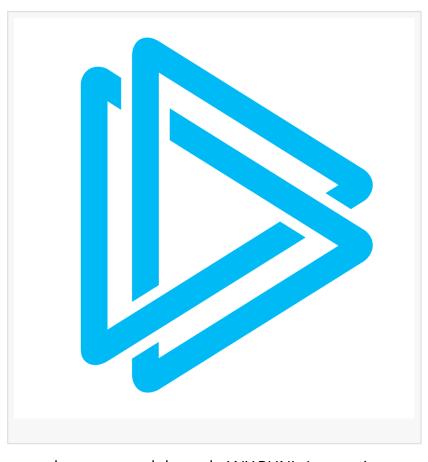


ANY.RUN Report Exposes Rising Cyber Threats Targeting Telecom Sector

DUBAI, DUBAI, UNITED ARAB EMIRATES, September 24, 2025 /EINPresswire.com/ -- ANY.RUN, a leading cybersecurity platform trusted by over 500,000 professionals and 15,000+ companies worldwide, today released critical findings from its latest threat intelligence report revealing a dramatic escalation in cyberattacks targeting the telecommunications industry.

The comprehensive analysis exposes how threat actors are weaponizing telecom brand trust to launch sophisticated phishing campaigns and credential theft operations.



The report, analyzing thousands of threat samples processed through ANY.RUN's Interactive Sandbox, reveals several alarming trends:

🛮 🖺 🖺 🖺 🖺 🖺 🖺 🖺 🖺 🖺 🖺 🖺 🖺 🖽 Each of all observed advanced persistent threat (APT) campaigns between May and July 2025 targeted telecom and media operators.

□ □□□□□□□□□□□□□□□□□□□□□□□□□□□: The notorious phishing framework designed to steal Microsoft credentials and circumvent two-factor authentication continues to pose significant risks to enterprise telecom environments.

The report details a real-world case study involving a major British telecommunications holding company operating in approximately 180 countries. Using ANY.RUN's threat intelligence solutions, researchers uncovered dozens of malicious emails targeting company employees, including sophisticated phishing attempts using DGA-generated domains designed to harvest credentials.

For details, access the full report in ANY.RUN's Blog.

ANY.RUN's analysis demonstrates how modern cybersecurity tools can provide early warning systems for telecom defenders:

🛮 🖺 🖺 🖺 🖺 🖺 🗎 🖺 🖺 🗎 🖺 🖺 🖺 🖺 🖺 🖺 🖽 The Interactive Sandbox captured complete attack flows from initial PDF attachments to final phishing pages.

□ □□□□□□□ □□□□□□□□□□□: Simple YARA rules successfully exposed large-scale operations targeting specific industry sectors.

The research identified over 86 analysis sessions involving domains containing "telecom" labels associated with phishing activities, along with 70 related malicious domains. This extensive infrastructure suggests coordinated, well-resourced campaign operations targeting the telecommunications sector specifically.

☐ Integrate real-time threat intelligence feeds into existing SIEM and EDR systems
☐ Conduct regular analysis of suspicious communications using interactive sandbe

☐ Conduct regular analysis of suspicious communications using interactive sandbox environments.

☐ Develop comprehensive defense strategies before attacks succeed through proactive threat hunting.

Designed to accelerate threat detection and improve response times, ANY.RUN equips teams with interactive malware analysis capabilities and real-time threat intelligence.

ANY.RUN's cloud-based sandbox supports investigations across Windows, Linux, and Android environments. Combined with Threat Intelligence Lookup and Feeds, our solutions give security teams full behavioral visibility, context-rich IOCs, and automation-ready outputs, all with zero infrastructure overhead.

The ANY.RUN team

ANYRUN FZCO +1 657-366-5050 email us here Visit us on social media: LinkedIn YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/852045524

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.