ANY.RUN Exposed Tykit: New Phishing Kit Targeting Microsoft 365 Accounts Across Multiple Sectors

DUBAI, DUBAI, UNITED ARAB EMIRATES, October 21, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has uncovered Tykit; a new phishing kit responsible for stealing hundreds of Microsoft 365 credentials from companies across North America and Europe. Targeting mainly the finance and construction sectors, Tykit uses SVG-based payloads and a multi-stage credential theft process, pointing to a growing phishing-as-a-service model now spreading across global campaigns.

□□□ □□□ □□□□□□□ □□□□□□

ANY.RUN observed around 180 related submissions, confirming that Tykit operates as a reusable phishing kit active across multiple attacks.

□□□□□□□□□□ □□□□□□□□□ □□ □□□□□□:

□□□□□□□□□: SVG files act as the initial payload, embedding JavaScript to trigger redirects.

□□□□□□□□□□ □□□□□□: Victims pass through trampoline pages and CAPTCHA validation before reaching the phishing page.

□□□□-□□□□□□□□□: Pages use simple anti-debugging methods, such as blocking DevTools and disabling right-click.

□□□□□□□□□□ □□□□□: The fake Microsoft 365 page captures login details and sends them to the attacker’s server.

□□□□□□□□□□□□□□ □□□□□: Multiple samples share the same structure and behavior, confirming a templated phishing kit in circulation.

Read the full analysis, explore live sessions, collect IOCs and detection rules, and learn how to defend against Tykit attacks; all on the ANY.RUN blog.

□□□□□ □□□.□□□

ANY.RUN is a leading provider of interactive malware analysis and threat intelligence solutions trusted by over 500,000 cybersecurity professionals and 15,000+ organizations worldwide. The interactive sandbox enables teams to observe malware behavior in real time, extract indicators of compromise, and accelerate detection and response. Paired with Threat Intelligence Lookup and TI Feeds, ANY.RUN delivers actionable insights that help SOC teams, MSSPs, and researchers 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
