ANY.RUN Exposes Tycoon 2FA’s Evolving Evasion Tactics to Beat Defenses in Corporate Phishing Attacks

DUBAI, DUBAI, UNITED ARAB EMIRATES, May 14, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has released a detailed report on the evolution of Tycoon2FA, a phishing-as-a-service (PhaaS) kit targeting credentials of corporate clients of Microsoft 365.

□□□□□□□□□□: □□□□□□□□□ □□□□ □□□□□□□□□ □□□□□□□□ □□□□□□□□

ANY.RUN’s research shows that Tycoon2FA has undergone significant updates over the past 6 months, incorporating a growing arsenal of evasion mechanisms. The newly introduced tactics help the threat evade endpoint protection, automated analysis, and corporate defenses. Key techniques include:

· □□□□□□□ □□□□□□□□ □□□□□□□□□□□□□□□□: Transitioning from Cloudflare Turnstile to custom HTML5 canvas-based CAPTCHAs with randomized elements, enhancing stealth and blocking automated detection.

· □□□□□□□□ □□□□□□□□□□□ □□□□□□□□□□□□□: Employs invisible Unicode characters (e.g., Hangul Filler) and encryption-based obfuscation, leveraging JavaScript Proxy objects to delay execution and evade static analysis.

· □□□□□□□□□ □□□□□-□□□□□□□□□□ □□□□ □□□□□□□□ □□□□□□□□□□□□□□□□: Detects debugging environments (e.g., Selenium), manipulates clipboard content, and uses browser fingerprinting to tailor attacks.

· [illegible]: Utilizes legitimate CDNs for corporate logos and extended redirect chains to mask malicious infrastructure.

From basic obfuscation observed in October 2024 to recent additions like encryption-based obfuscation and custom fake page redirects noted in April and May 2025, Tycoon2FA's continuous evolution underscores its ability to adapt and challenge even the most robust corporate defenses.

Read the full analysis on ANY.RUN's Cybersecurity Blog.

[illegible]

ANY.RUN's Interactive Sandbox equips SOC and DFIR teams with real-time analysis to detect and analyze Tycoon2FA campaigns. Businesses can extract Indicators of Compromise (IOCs), monitor phishing behaviors, and map attack tactics using the MITRE ATT&CK framework.

[illegible]

ANY.RUN is a trusted partner for over 15,000 organizations in finance, healthcare, retail, technology, and beyond, delivering advanced malware analysis and threat intelligence products. Its cloud-based Interactive Sandbox, Threat Intelligence Lookup, and TI Feeds enable businesses to analyze, investigate, and detect the latest malware and phishing campaigns to streamline triage, response, and proactive security.

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