ANY.RUN Discovers a New Salty2FA and Tycoon2FA Phishing Hybrid Targeting Enterprises

DUBAI, DUBAI, UNITED ARAB EMIRATES, December 2, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has identified a new hybrid phishing framework that merges two major Phishing-as-a-Service (PhaaS) kits: Salty2FA and Tycoon2FA. This discovery reveals a significant shift in the 2FA-focused phishing and raises new questions about the operators behind these kits.

□□□□□□□□□ □□ □□□ □□□ □□□□□□□□□ □□□□□□□

Following an abrupt drop in Salty2FA activity, ANY.RUN began seeing samples that combine Salty's early stages with Tycoon2FA's later payloads. The consistent overlap in indicators and behavior confirms that recent phishing campaigns are now running a unified chain built from both frameworks

Key findings include:
• Hybrid payloads observed: Samples showed Salty2FA's initial stages followed by Tycoon2FA's execution chain almost line-for-line.
• Fallback behavior identified: When Salty domains failed with SERVFAIL, the payload switched to Tycoon2FA hosting and delivery infrastructure.
• Cross-kit indicators detected: Shared IOCs, overlapping TTPs, and matched detection rules confirmed the presence of both kits within single sessions.
• Potential operator link: The overlap aligns with earlier assessments pointing to Storm-1747, known operators of Tycoon2FA, suggesting shared control or cooperation behind both kits.

• Impact on attribution: The merging of client-side code complicates traditional kit-level attribution and requires updated detection logic.
• Operational shift expected: More cross-kit blending is likely, meaning defenders should prepare for phishing campaigns that move between frameworks mid-execution.

For a deeper look at the hybrid samples, full code comparisons, and guidance for SOC teams, visit the ANY.RUN blog.

□□□ □□□□ □□□□□□ □□□□□□□ □□□ □□□□□

The unified Salty2FA–Tycoon2FA workflow means phishing incidents may shift frameworks mid-execution. This complicates attribution and weakens traditional signatures. SOC teams should monitor both kits together, emphasize behavioral detection, and watch for fallback payloads that bridge one framework to the other.

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/871855873

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.