# ANY.RUN Warns About 5 Sophisticated Phishing Campaigns

DUBAI, DUBAI, UNITED ARAB EMIRATES, August 21, 2024 /EINPresswire.com/ -- ANY.RUN has recently detected and analyzed 5 sophisticated phishing campaigns targeting users worldwide.

The Tycoon 2FA campaign, discovered by ANY.RUN researchers, attacks via compromised Amazon Simple Email Service accounts. It uses a complex redirection chain involving social networks and news outlets to hide the final phishing domain. The campaign employs advanced techniques such as empty PDF attachments and custom redirectors to evade detection.

An evolved variant of the Tycoon 2FA campaign was subsequently identified, using fake error messages like "No Internet Connection" or "Error 500" to trick users into revealing their credentials. This version adds a layer of authenticity by incorporating CAPTCHA steps and only revealing the phishing page at the end of the process.

Another Tycoon 2FA evolution targets US government organizations by impersonating Microsoft Teams. This campaign filters victims based on a list of 338 organizations within the .GOV domain, demonstrating a highly targeted approach to phishing attacks.

The Fake Freshdesk campaign exploits the customer support platform Freshdesk to create and host lure pages with phishing links. Attackers use Freshdesk's knowledge base and email API to send convincing phishing emails to targets, leveraging the platform's legitimacy to increase the success rate of their attacks.

Researchers at ANY.RUN also uncovered a massive phishing campaign exploiting SharePoint to

store PDFs containing phishing links. This campaign is particularly dangerous due to its use of legitimate services at every step, making detection by security mechanisms more challenging. In just 24 hours, ANY.RUN observed over 500 public sandbox sessions related to this SharePoint phishing campaign.

For more detailed information about these phishing campaigns ad please visit ANY.RUN's analysis.

□□□□□ □□□.□□□
ANY.RUN supports over 400,000 cybersecurity professionals globally with its cutting-edge sandbox and threat intelligence tools. Specializing in malware analysis for both Windows and Linux systems, ANY.RUN’s platform delivers fast, detailed insights, empowering users to detect, analyze, and respond to emerging cybersecurity threats with confidence.

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

---