‘Tycoon 2FA’ Phishing-as-a-Service updated to prevent security inspection - Barracuda research

The widely used Tycoon 2FA Phishing-as-a-Service (PhaaS) has been updated with a range of tactics designed to make it harder for security tools to confirm its malicious intent and inspect its webpages, according to a new research report from Barracuda’s threat analysts. The findings underscore how PhaaS developers are investing significant resources into building advanced and evasive toolsets and templates to enable cyber attackers to quickly deploy complex and targeted phishing campaigns.

According to Barracuda threat analysts, around 30% of the credential attacks seen in 2024 made use of PhaaS and this is expected to rise to 50% in 2025.

Tycoon 2FA allows attackers to intercept and bypass two factor authentication (2FA) security measures by collecting and using Microsoft 365 session cookies. In early November 2024, Barracuda threat analysts noted a rise in the use of a new version of Tycoon 2FA that is stealthier than earlier editions and makes use of a range of sophisticated tactics to obstruct detection and analysis.

These tactics include:

- The use of legitimate — possibly compromised — email accounts to launch attacks
- Specially crafted source code to obstruct web page analysis
- Measures to block the use of automated security scripts and penetration-testing tools
- Listening for keystrokes that suggest web inspection and then blocking further activity
- Disabling the right-click menu that could reveal the web pages’ true intent
- Blocking users from copying meaningful text from the webpage for offline analysis

“Phishing has evolved into a complex and sophisticated attack vector that is increasingly well resourced,” **said Deerendra Prasad, Associate Threat Analyst at Barracuda.** “PhaaS groups play a key role in this new ecosystem, and we expect their role to increase. We have observed Tycoon 2FA used in numerous phishing campaigns over the past months and expect cyber attackers to continue to refine their methods to circumvent traditional security measures and thwart deeper analysis. It is essential to have agile and innovative multilayered defense strategies in place and foster a strong security culture to stay ahead of this ever-evolving threat.”

To read the blog: https://blog.barracuda.com/2025/01/22/threat-spotlight-tycoon-2fa-phishing-kit

ENDS