Mphasis
The Next Applied

‘Tycoon’ Malware Kit Bypasses Microsoft, Google MFA

Date: 14th May 2024 | Severity: High

Summary

A Stealthy Phishing Kit Used to Bypass Microsoft 365 and Google MFA. Tycoon 2FA is a phishing-as-a-service (PhaaS) platform that was first seen in August 2023. Like many phish kits, it bypasses multifactor authentication (MFA) protections and poses a significant threat to users.

Attack Vectors

- The primary goal of Tycoon 2FA is to harvest Microsoft 365 session cookies, allowing threat actors to bypass the MFA process during subsequent authentication. This means that even if users have enabled MFA for their accounts, the phishing campaign can still gain unauthorized access.
- “Cloudflare Turnstile challenge” — used as a replacement for a CAPTCHA challenge — in which users clicking on the phishing URL are redirected to a page embedding such a challenge to prevent unwanted traffic then executes a JavaScript code in the background that’s not visible to the user, to redirect the target to another page.
- The attack is a yet another background redirect that leads the target to another webpage of the phishing domain. From there, a fake Microsoft authentication login page via HTML code that embeds a deobfuscation function and obfuscated HTML code.
- The MFA aspect that’s key to the kit occurs in of the attack vector, in which the JavaScript code interacts with the HTML of the previous stage to build and display the Microsoft MFA page, which prompts the user to authenticate themselves. Finally, redirects the user one last time, in this case to a legitimate URL so the victim doesn’t realize the previous page was malicious.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• p1v12[.]17nor[.]com • q908q[.]refec7[.]com • kjlvo[.]ningeona[.]com • 0q5e0[.]nemen9[.]com • 4343w[.]jgu0[.]com • pmd8ot6xhw[.]3qjpc[.]com • 8000n[.]uqin[.]ru • xva[.]tjlpkcia[.]com • zaqaxu[.]dthiterp[.]ru • buneji[.]fiernmar[.]com • gz238[.]uatimin[.]com • libudi[.]oreversa[.]com • x12y[.]restrice[.]ru • 8uecv[.]gnornamb[.]com • roriku[.]orankfix[.]com • l846d[.]ferver8[.]com • tlger-surveillance[.]com • wasogo[.]shantowd[.]com • ex1uo[.]rhknt[.]ru • xrs[.]chenebystie[.]com • k348d[.]venti71[.]com • 9c43r[.]theq0[.]com • oo99v[.]coqqwx[.]ru • 98q5e[.]ructin[.]com • fisaca[.]trodeckh[.]com • explore[.]atlester[.]ru • 4m2swl[.]7e2r[.]com • 43rw98nop8[.]m1p8z[.]com • 77p3e[.]rimesh3[.]com • bloggcenter[.]com • 25rw2[.]canweal[.]com • 5me78[.]methw[.]ru • rlpq[.]tk9u[.]com • tycoongroup[.]ws • r298y[.]sem01[.]com • o6t94g[.]3tdx2r[.]com • n29k4[.]ilert[.]ru • galume[.]aricente[.]com • beacon[.]diremsto[.]com • 9oc0y2isa27[.]demur3[.]com • codecrafterspro[.]com • codecrafters[.]su • zekal6[.]tnjxb[.]com • 35fu2[.]ouchar[.]ru • devcraftingsolutions[.]com • n9zph[.]lw8opi[.]com • kjsdflwe[.]nitertym[.]ru • horizon[.]sologerg[.]com • zemj4f[.]ymarir[.]ru • e85t8[.]nechsha[.]com • 6j312[.]rchan0[.]com • tnyr[.]moporins[.]com • fiq75d[.]rexj[.]ru • jp1y36[.]it2ua[.]com

Recommendation

- Implementing additional security measures, such as using strong passwords, enabling two-factor authentication, and regularly undergoing security awareness training, can also help mitigate the risk.
- Furthermore, organizations should consider implementing security products that can detect and block phishing attempts, as well as regularly update their security protocols to stay ahead of evolving threats.

Reference Links

- https://www.darkreading.com/application-security/tycoon-malware-kit-bypasses-microsoft-google-mfa
- https://www.inacom-sby.com/tycoon-2fa-phishing-kit-bypasses-mfa-protections/