New Phishing Campaign Exploits Cloudflare Workers and HTML Smuggling to Steal User Credentials

DUBAI, UNITED ARAB EMIRATE, June 12, 2024 /EINPresswire.com/ -- ANY.RUN reports that a new sophisticated phishing campaign is active in the wild, targeting users in Asia, North America, and Southern Europe.

The campaign exploits Cloudflare Workers and HTML smuggling techniques to steal user credentials from popular services such as Microsoft, Gmail, Yahoo!, and cPanel Webmail.

The phishing attack uses a unique approach where the malicious payload is a phishing page itself, reconstructed and presented to the user in their web browser.

Hackers prompt victims to sign in with their Microsoft Outlook or Microsoft 365 account, claiming that they need to do so to view a supposed PDF document. The fake sign-in pages, hosted on Cloudflare Workers, harvest not only login information but also MFA codes, researchers who analyzed the campaign say.

The phishing page is built using a modified version of an open-source Cloudflare Adversary in the Middle (AitM) toolkit.

When the victim visits the spoofed login page, the attacker collects web request metadata, redirects the victim to the legitimate site, and then collects tokens and cookies from the response, allowing them to track the victim's actions after logging in.

ANY.RUN team warns that phishing campaigns are becoming increasingly sophisticated, employing an array of well-known and new phishing tools, such as:

 Phishing-as-a-Service toolkits like Greatness to steal Microsoft 365 login credentials and circumvent MFA
 DNS tunneling to detect when victims interact with phishing content
 GenAI to write convincing phishing emails
 QR codes inside PDF files to redirect victims to fake login pages
 Real CAPTCHAs placed in front of malicious content to prevent automated detection
 Realistic sign-in forms that mimic popular services

Read more about how these phishing tactics work in ANY.RUN's blog post.

Veronika Trifonova
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X
YouTube