Over 2,000 reports of phishing attacks using CAPTCHAs, QR codes, and complex evasion schemes were reported to ANY.RUN

DUBAI, DUBAI, UNITED ARAB EMIRATES, October 12, 2023 /EINPresswire.com/ -- ANY.RUN, a cybersecurity company developing an interactive sandbox analytical platform for malware researchers. ANY.RUN processes hundreds of thousands of tasks each month. This allows us to offer timely insights into the latest threats and developments within the cybersecurity space.

Here are some highlights from the new phishing attack:

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

Hackers are increasingly using legitimate tools to make their campaigns appear more credible. But now, they've taken it a step further by using actual security solutions in their attacks.
The attack — which begins like a standard credential harvesting attempt and targets O365 credentials — uses a spam email as an initial vector. Hackers lure the user into logging into what appears to be legitimate software.

Also, the credential harvesting forms are concealed behind CloudFlare's captcha service. As a result, the content evades being flagged as malicious, and emails with links to this page slip through spam filters.

But there's even more to this attack.
Attackers append the victim's email address as a GET parameter after the target completes the captcha. They then execute a script to extract the domain name of the target's organization,

using this data to display a custom login page that mimics the victim's actual login portal.

After the victim lands on the login page, the remainder of the attack follows a standard credential harvesting pattern. Once the victim enters their login credentials, a "wrong credentials" error message is displayed. The attackers then quickly redirect the victim to a legitimate website, while exfiltrating the credentials to their Command-and-Control server.

This poses challenges for investigation as well, given that not all automated sandboxes can bypass a captcha. This is where the interactivity in ANY.RUN becomes valuable — you can manually complete the captcha within the Virtual Machine view and see the most interesting aspects of the attack.

At ANY.RUN we understand the importance of cybersecurity in today's digital landscape. Our team of experts is dedicated to providing cutting-edge cybersecurity solutions to help organizations stay protected against evolving threats.

Read our article for more information on the new phishing attack.

Vlada Belousova
ANYRUN FZCO
2027889264
email us here
Visit us on social media:
Twitter
YouTube
