Cyber-Criminals Increasingly Using Official reCAPTCHA Walls in Phishing Attacks

BY MICHAEL HILL

New research from Barracuda Networks has revealed that cyber-criminals are increasingly using official reCAPTCHA walls to disguise malicious content from email security systems and trick unsuspecting users.

reCAPTCHA walls are typically used to verify human users before allowing access to web content, thus sophisticated scammers are beginning to use the Google-owned service to prevent automated URL analysis systems from accessing the actual content of phishing pages, and to make phishing sites more believable in the eyes of the victim, Barracuda Networks warned.

In fact, the security solutions provider observed a single phishing campaign that sent out 128,000 emails to a variety of organizations and employees using reCAPTCHA walls to conceal fake Microsoft log-in pages. This campaign used the lure of a voicemail receipt to fool users into solving the reCAPTCHA wall before being redirected to the malicious page, with any log-in info entered then sent straight to the scammers.

Steve Peake, UK systems engineer manager at Barracuda Networks, explained that users are particularly susceptible to phishing attacks at the current time due to mass remote working and large numbers of COVID-19-themed scams.

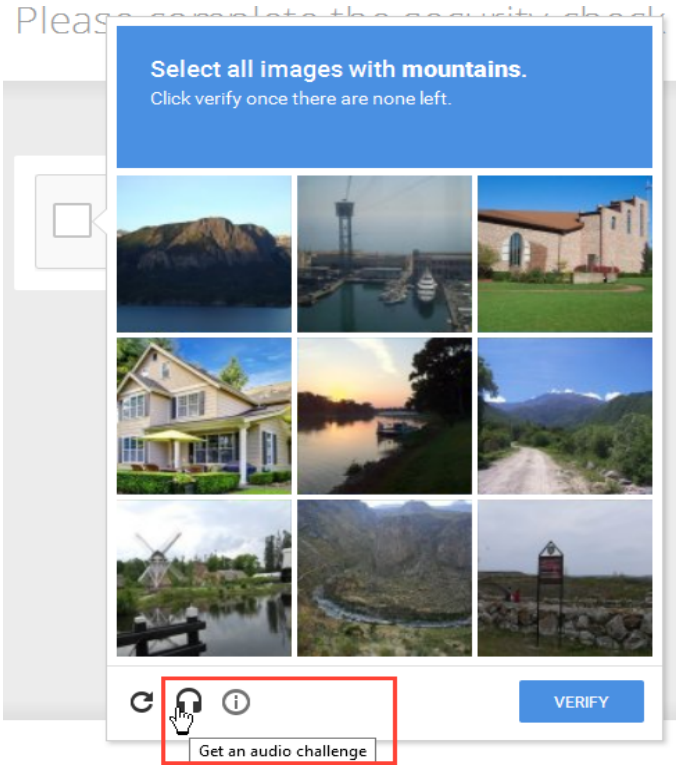
“In this difficult time, it is no surprise to see that cyber-scammers are seeking increasingly sophisticated methods of stealing log-in credentials and data from unsuspecting, remote workers.”

Fortunately, he added, there are a number of proactive measures employers and business owners can take to prevent a security breach.

“Most importantly, users must be educated about the threat so they know to be cautious instead of assuming a reCAPTCHA is a sign that a page is safe. Furthermore, whilst reCAPTCHA-based

scams make it harder for automated URL analysis to be conducted, sophisticated email security solutions can still detect these phishing attacks using AI-based email protection solutions. Ultimately, however, no security solution will catch everything, and the ability of the user to spot suspicious emails and websites is key."

Retrieve on 4/30/2020 from https://www.infosecurity-magazine.com/news/cybercriminals-using-recaptcha/



EXAMPLES OF reCAPTCHA