HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER COMMAND
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2025-03

Beware of the Fake CAPTCHA Attack Spreading Malware

Beware of the Fake CAPTCHA Attack Spreading Malware Across Industries

Overview

Cybercriminals are employing a new social engineering tactic known as the Fake CAPTCHA Attack to spread malware across multiple industries. Instead of serving a legitimate CAPTCHA challenge, these fraudulent prompts trick users into downloading malicious files, leading to credential theft, financial fraud, and dark web exploitation.

How the Fake CAPTCHA Attack Works:

1. **Fake CAPTCHA Prompt**

   - Victims encounter a CAPTCHA challenge while visiting a website.
   - The prompt asks them to “verify” that they are human before continuing.

2. **Malware Download**

   - Clicking on the challenge initiates a malicious file download instead of a real CAPTCHA verification.

3. **Information Theft**

- When executed, the malware installs an info stealer that harvests:
  - Login credentials
  - Browser cookies
  - Cryptocurrency wallet details
  - Other sensitive user data

4. **Potential for Future Exploitation**

- Stolen data is used for:
  - Identity theft
  - Unauthorized financial transactions
  - Sales on dark web marketplaces
- This can result in significant security breaches for individuals and organizations.

What to Do If You Encounter This Attack

1. Do Not Click or Download Anything

- Avoid clicking CAPTCHA challenges on unfamiliar websites.
- If an automatic download begins, do not open or run the file.

2. Close the Tab or Browser

- Immediately close the browser tab or window where the suspicious CAPTCHA appeared.
- Restart your browser and clear cache and cookies to remove potential tracking scripts.

3. Report and Isolate the Threat

- If a malicious file was mistakenly downloaded, do not open it, delete it immediately.
- Report the incident to your Cyber Incident Response Team (CIRT) for investigation and mitigation.

4. Scan Your System for Malware

- Conduct a full system scan using an up-to-date and reputable antivirus or endpoint protection tool.
- If malware is detected, escalate the issue to your CIRT for proper remediation.

5. Reset Compromised Credentials

- If you suspect credential theft, immediately change your passwords.
- Enable Multi-Factor Authentication (MFA) for enhanced security.

6. Stay Vigilant and Train Your Team

- Implement cybersecurity awareness training to educate personnel about phishing and malware tactics.
- Keep all security tools, browsers, and operating systems updated to protect against evolving threats.

Conclusion

The Fake CAPTCHA Attack highlights the growing sophistication of cybercriminals and their ability to manipulate common security mechanisms for malicious purposes. Organizations and individuals must remain proactive in their cybersecurity efforts, ensuring strong defensive strategies, regular training, and continuous threat monitoring.

Reference: *https://centurygroup.net/beware-of-the-fake-captcha-attack-spreading-malware-across-industries/*