AL2023_61 Threat actors abuse Google AMP for evasive phishing attacks (August 10, 2023)

Description

Security researchers have issued a warning about an increase in phishing activity exploiting Google Accelerated Mobile Pages (AMP) to bypass email security measures and reach the inboxes of enterprise employees.

Google AMP is an open-source HTML framework co-developed by Google and its partners to enhance mobile web content loading speed. By hosting AMP pages on Google's servers, content is simplified, and heavy media elements are pre-loaded, resulting in faster delivery. Phishers use Google AMP URLs in their emails to evade email protection technology, leveraging Google's reputable image to avoid detection as malicious or suspicious. These AMP URLs redirect users to phishing sites, adding an extra layer that hinders analysis.

Details

According to data from Cofense (anti-phishing protection company), there has been a significant increase in phishing attacks using Google Accelerated Mobile Pages (AMP) around mid-July of 2023. Out of all the observed Google AMP URLs, approximately 77% were hosted on the domain google.com, and 23% were hosted on google.co.uk.

Blocking the common "google.com/amp/s/" path may also affect legitimate uses of Google AMP. However, flagging such URLs could be the most appropriate action to raise awareness among recipients and caution them about potential malicious re-directions.

According to Cofense, phishing actors using the Google AMP service employ various techniques to evade detection and increase their success rate. These techniques include using image-based HTML emails instead of traditional text to confuse scanners, employing an extra redirection step using Microsoft.com URLs, and utilizing Cloudflare's CAPTCHA service to thwart automated analysis by security bots. These tactics collectively make it challenging for targets and security tools to detect and block phishing threats effectively. As a result, it becomes crucial for organizations to stay vigilant and adopt comprehensive security measures to protect against such sophisticated attacks.

Remediation

1. Keep computer systems updated with the latest security patches.
2. Avoid opening emails from unknown senders nor do not interact with its attachments and hyperlinks.
3. Provide necessary cybersecurity training to employees that will help to identify phishing attempts and how to avoid them.
4. Change passwords for various accounts on a regular basis.
5. Install a reputable malware software from a trusted source such as Avast antivirus and perform scheduled scans.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2023, August 1). *Threat actors abuse Google AMP for evasive phishing attacks*. Bleeping Computer. Retrieved from: https://www.bleepingcomputer.com/news/security/threat-actors-abuse-google-amp-for-evasive-phishing-attacks/
- Simister, A. (2022, November 24). *10 Ways to Prevent Phishing Attacks*. Lepide. Retrieved from: https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/