Google AMP – The Newest of Evasive Phishing Tactic

August 1, 2023

Share Now

Facebook Twitter LinkedIn

Author: Dylan Duncan

A new phishing tactic utilizing Google Accelerated Mobile Pages (AMP) has hit the threat landscape and proven to be very successful at reaching intended targets. Google AMP is an open-source HTML framework used to build websites that are optimized for both browser and mobile use. The websites that we observed in these campaigns are hosted on Google.com or Google.co.uk, both of which are considered trusted domains to most users. This phishing campaign not only employs Google AMP URLs to evade security, but also incorporates a multitude of other tactics, techniques, and procedures (TTPs) known to be successful at bypassing email security infrastructure.

Key Points

- A new tactic employed by threat actors utilizes Google AMP URLs as links embedded been observed by Cofense to be incorporated into the campaigns using Google AMP URLs:

- **Trusted domains** are often used throughout each stage of the phishing campaigns, not just including the initial Google domain.
- **URL redirection** as part of the Google AMP URL as well as an additional stage has been seen throughout several campaigns using the Google AMP tactic. This adds an extra layer to disrupt analysis.
- **Image-based phishing emails** have been used. This allows the threat actor to disrupt analysis by replacing a normal text body with an encoded HTML image that contains the malicious embedded link, which is clickable by the recipient.
- **Cloudflare CAPTCHA** has been a commonly abused tactic in phishing campaigns, therefore it is no surprise they have appeared here. CAPTCHA services disrupt automated analysis and require each phishing campaign to be manually analyzed.

Google AMP – The Latest Legitimate Application to be Abused for Phishing

Google AMP is a web component framework that allows users to create web pages that are also optimized for mobile use. Google allows each web page to be viewable on Google Search and can use Google AMP Cache as well as Google Analytics, both of which provide users with additional features to track other user interactions on AMP pages. Another feature Google AMP offers is that the webpages are initially hosted on a Google AMP URL like the example in Figure 1. This means each URL is hosted on **https://www.google.com/amp/s/** or **https://www.google.co.uk/amp/s/**. In the example below, the left half of the URL is the legitimate Google AMP pathing, and the right half would be the webpage setup by the Google AMP user. To visit this URL, a user can access the webpage link directly or through this extended version of the URL.

Google AMP URL Path
Phishing URL

Figure 1: Example of a Google AMP URL.

The same features that make Google AMP appealing to legitimate users can also attract threat actors that are seeking to use it for malicious reasons. Phishing threat actors have been seen hosting malicious web pages using the Google AMP URL path within their phishing emails seeking to steal email login credentials. This can be difficult for email security infrastructure to detect the malicious nature of the emails since these URLs are hosted on legitimate Google domains. The addition of Google Analytics also provides threat actors with a way to track user interactions within their phishing pages. Figure 2 shows a real example of a phishing URL hosted using Google AMP. The Google AMP URL acts very similar to a redirect by sending users from the initial URL to the URL found within the path. For this example, that is the URL hosted on the domain netbitsfibra[.]com.

Figure 2: Real Google AMP Phishing Example That Reached an Intended Target.

A Month's Worth of Activity – Worth Monitoring

When it comes to monitoring phishing campaigns, it is important to focus on the ones that matter. A phishing URL blocked before it reaches the intended target doesn't pose a threat.

Figure 3: Weekly volume of phishing emails abusing Google AMP.

Phishing campaigns abusing the Google AMP services picked up during May and haven't left the threat landscape since. Overall, we have seen the volume oscillate drastically throughout recent weeks, with the week of May 29th and July 10th showing new heights for the tactic. On June 15th, we saw a change in tactics that included the use of Google.co.uk within the Google AMP URLs. The tactic remains the same, but the URL is hosted on Google's United Kingdom top-level-domain.

Out of all the Google AMP URLs we have observed, approximately 77% were hosted on the domain google.com and 23% were hosted on the domain google.co.uk. The URL pathing is a good indicator for this phishing campaign, but it is difficult to outright block "google.com/amp/s/" due to the legitimate uses. It is recommended organizations discuss the legitimate uses for this pathing for their users before outright blocking. Although blocking the path may be difficult, it could be a good opportunity to flag URLs with it.

Figure 4: Comparison between the domains used by phishing emails utilizing Google AMP.

Threat Actors Combine the Newest Tactic with other Tried and True TTPs

The Google AMP phishing campaigns have proven to successfully reach their intended targets. This is likely due to the trusted status and legitimacy of the Google domains that each URL is hosted on. Although that reason may be sufficient, threat actors employing this new tactic have also incorporated the tried-and-true methods already known to contribute to the evasiveness of a phishing email. The following TTPs have been observed in a variety of phishing emails that are using Google AMP URLs as embedded links within phishing emails:

Trusted Domains – The Google AMP tactic is effective because of the combination of hosting a URL on a trusted domain as well as the redirection-like process it takes going from the Google AMP URL to the phishing site. Trusted domains make automated analysis difficult, since you cannot simply outright block the legitimate parts of a malicious URL abusing the process.

Image-based Phishing Emails – Several of the emails observed are image-based phishing emails. This means the emails do not contain a traditional email body, but rather they contain an HTML image. Emails of this nature are more difficult to detect compared to text-based emails. This is due to the image adding more noise within the email's headers as well as

Figure 5: Example of phishing email that used Google AMP with a clickable HTML image.

URL Redirection – URL redirection has become an increasingly popular method for disrupting email analysis. Having multiple redirects within a single phishing attack chain rather than a single malicious URL can make analysis difficult. The example in Figure 6 below was pulled from a user’s inbox and is a good example of both trusted domains and URL redirection used as a TTP within a phishing email. The redirection is not only redirecting to the Google AMP domain, but it is also hosted on Microsoft.com, which is another trusted domain. This adds an

Figure 6: Phishing URL utilizing a Microsoft domain to redirect to a Google AMP phishing site.

Cloudflare CAPTCHA – The abuse of Cloudflare's CAPTCHA service has become a popular anti-analysis tactic. Cloudflare is a legitimate domain security service used to keep websites secure from bots or other automated visitors. This has proven to be a very effective tactic at evading email security because the CAPTCHAs often come prior to any actual-malicious URLs. The use of a CAPTCHA requires a manual user to be present to reach the final malicious URL within the initial redirection or infection chain. Cloudflare services also allow the blocking of certain geo-locations through IP filtering, and IP proxying services which allow the threat actor to hide the domain's original hosting provider.

Figure 7: Example of Cloudflare CAPTCHA pulled from Google AMP phishing campaign.

Read More Related Phishing Blog Posts

5 Tips for Building a Security Reporting Culture

READ MORE »

June 6, 2023

The Art of Deception: Microsoft Phish Redirects Victims to a Catering Voice Recording

READ MORE »

Man-in-the-Middle (MitM) attacks reaching inboxes increase 35% since 2022

READ MORE »

May 9, 2023

1602 Village Market Blvd, SE #400
Leesburg, VA 20175

(888) 304-9422

Company

Resources

Accept

Get a Demo