AiTM phishing attack targeting enterprise users of Gmail

zscaler.com/blogs/security-research/aitm-phishing-attack-targeting-enterprise-users-gmail

Summary

This blog is a follow-up to our recent publication which described the details of a large-scale phishing campaign targeting enterprise users of Microsoft email services.

Beginning in mid-July 2022, ThreatLabz started observing instances of adversary-in-the-middle (AiTM) phishing attacks targeted towards enterprise users of **Gmail**. Upon further analysis of the attack chain, we identified multiple similarities between this campaign and the previous AiTM phishing campaign targeting users of Microsoft email services.

G Suite is the business version of Gmail, and is widely used in enterprises. This campaign specifically targeted chief executives and other senior members of various organizations which use G Suite.

As we have already covered the technical details of AiTM techniques in our previous blog, we won't describe them again here. However, it is important to note that AiTM phishing kits can be used to target various websites and bypass multi-factor authentication. By using phishlets crafted to target a specific legitimate website, attackers can quickly re-use the AiTM phishing technique against a new target website.

In this blog, we present the indicators of overlap between the two campaigns (Microsoft and Gmail), and discuss how we reached the conclusion that both these phishing campaigns were run by the same threat actor.

These campaigns used similar tactics, techniques and procedures (TTPs). There was also an overlap of infrastructure, and we even identified several cases in which the threat actor switched from Microsoft AiTM phishing to Gmail phishing using the same infrastructure.

Interestingly, the Gmail AiTM phishing campaign had a much lower volume of targets compared to the Microsoft AiTM phishing attack.

Key Points

- Beginning in July 2022, the same threat actor that used AiTM phishing kits to target enterprise users of Microsoft email services began targeting enterprise users of **G Suite**.
- The attack is capable of bypassing **multi-factor authentication (MFA)** protection of Gmail.
- These phishing emails were sent to chief executives and other senior members of the targeted organizations in the US. In some cases, the emails were also sent to the executive assistants of the CEOs and CFOs.
- The compromised emails of chief executives were used to conduct further phishing attacks by the threat actor.
- Multiple compromised domains were used as an intermediate URL redirector to land the user on the final phishing page.
- A similar client-side fingerprinting script was used for evasion by the threat actor as observed in the previous campaign.
- The same redirector scripts used in the Microsoft phishing campaign were updated to target G Suite enterprise users.

Attack chain

Figure 1 below depicts the attack chain at a high level. The attack begins with the user receiving an email containing a malicious link. This link leverages multiple levels of redirection and abuses Open Redirect pages to land the user on the final attacker-controlled Gmail phishing domain. However, before the actual phishing page is presented to the user, the server does a fingerprinting check on the client in order to make sure that a real user is browsing to the site and not an automated analysis system.

Each component of the attack chain is explained in more detail in the corresponding sections later.

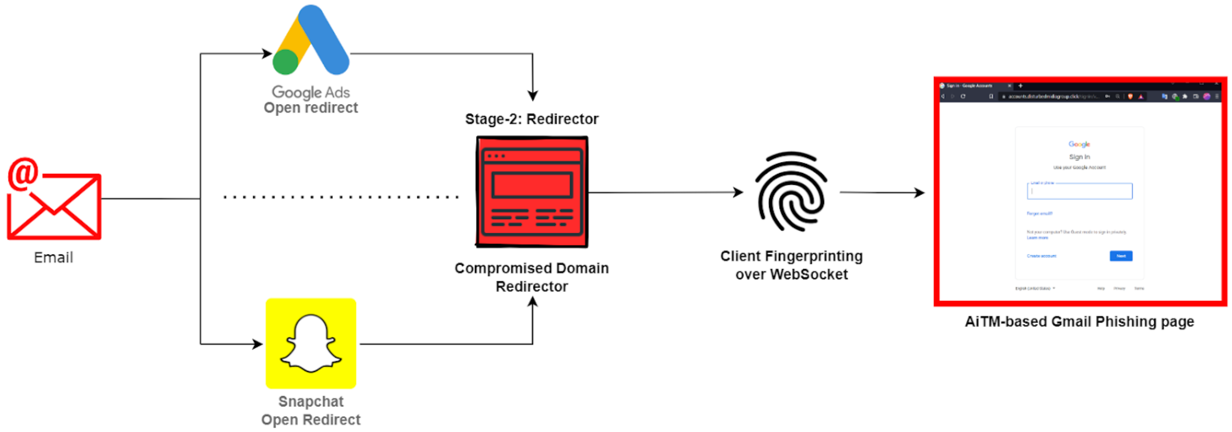


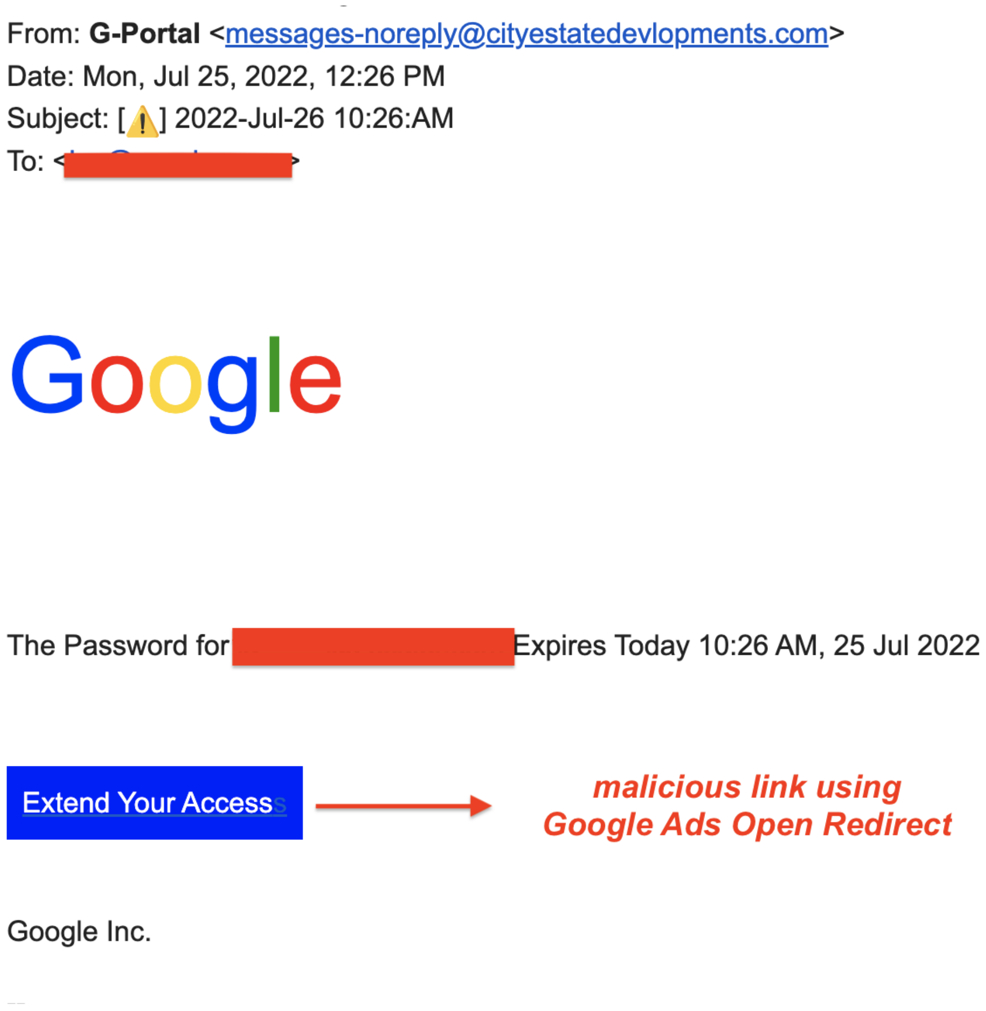
Figure 1: A high-level attack chain of the phishing process

Distribution mechanism

The attack vector used in this campaign was emails with the malicious link embedded in them. These emails were specifically sent to chief executives and senior members of the targeted organization.

The phishing emails impersonated Google and pretended to be password-expiry reminder emails prompting the user to click a link in order to "Extend their access."

Figure 2 shows an example of one such phishing email.



From: **G-Portal** <messages-noreply@cityestatedevlopments.com>
Date: Mon, Jul 25, 2022, 12:26 PM
Subject: [⚠] 2022-Jul-26 10:26:AM
To: <[redacted]>

Google

The Password for [redacted] Expires Today 10:26 AM, 25 Jul 2022

Extend Your Access

malicious link using Google Ads Open Redirect

Google Inc.

Figure 2: G Suite phishing email

URL redirection

The redirection happens in multiple stages which we describe below.

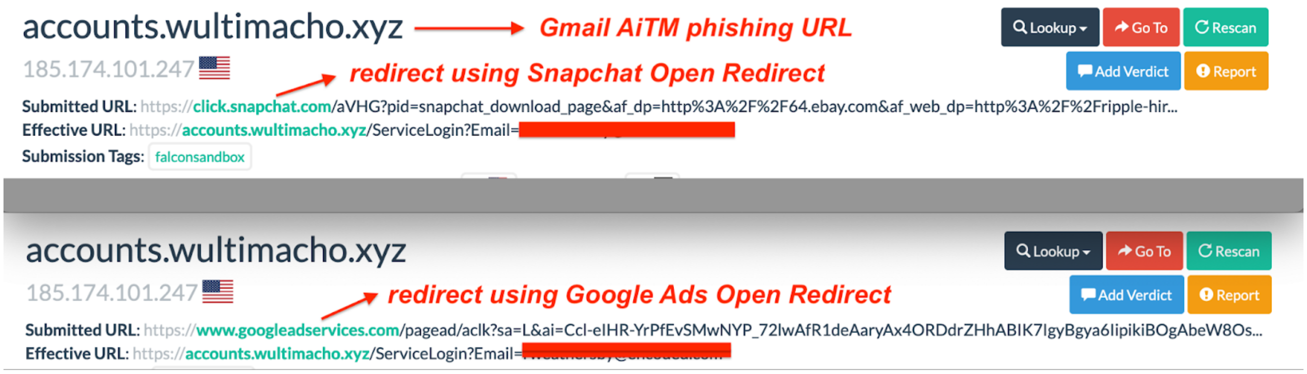
Stage 1

There were two categories of Stage 1 redirect links observed in the Gmail phishing campaign.

Variant #1 [Open Redirect abuse]

This variant abused Open Redirect pages of Google Ads and Snapchat, similar to what we described in our research on Microsoft AiTM phishing campaign.

Figure 3 depicts two instances where the same Gmail phishing URL was delivered using a Snapchat redirect in one case, and the Google Ads redirect in another.



accounts.wultimacho.xyz → Gmail AiTM phishing URL

185.174.101.247

redirect using Snapchat Open Redirect

Submitted URL: https://click.snapchat.com/aVHG?pid=snapchat_download_page&af_dp=http%3A%2F%2F64.ebay.com&af_web_dp=http%3A%2F%2Fripple-hir...

Effective URL: https://accounts.wultimacho.xyz/ServiceLogin?Email=[redacted]

Submission Tags: falconsandbox

accounts.wultimacho.xyz

185.174.101.247

redirect using Google Ads Open Redirect

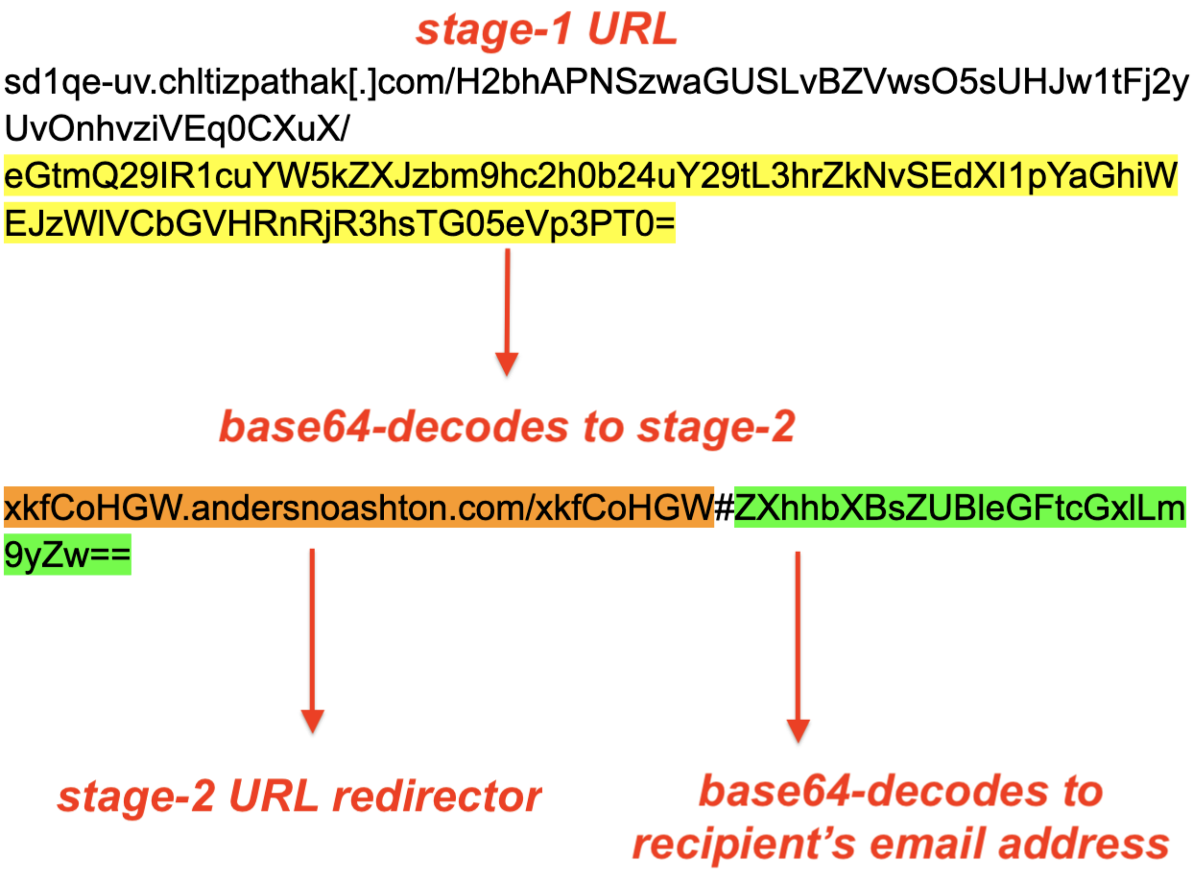
Submitted URL: https://www.googleadservices.com/pagead/aclk?sa=L&ai=Ccl-elHR-YrPfEvSMwNYP_72lwAfR1deAaryAx4ORDdrZHhABIK7IgyBgya6lipikiBOgAbeW8Os...

Effective URL: https://accounts.wultimacho.xyz/ServiceLogin?Email=[redacted]

Figure 3: Redirect using Open Redirect pages

Variant #2

This variant used compromised sites which stored an encoded version of the Stage 2 redirector and the victim's email address in the URL. Figure 4 depicts the format of this variant.



stage-1 URL

sd1qe-uv.chltizpathak[.]com/H2bhAPNSzwaGUSLvBZVwsO5sUHJw1tFj2yUvOnhvziVEq0CXuX/eGtmQ29IR1cuYW5kZXJzbm9hc2h0b24uY29tL3hrZkNvSEdXI1pYaGhiWEJzWlVCbGVHRnRjR3hsTG05eVp3PT0=

base64-decodes to stage-2

xkfCoHGW.andersnoashton.com/xkfCoHGW#ZXhhbXBsZUBleGFtcGxlLm9yZw==

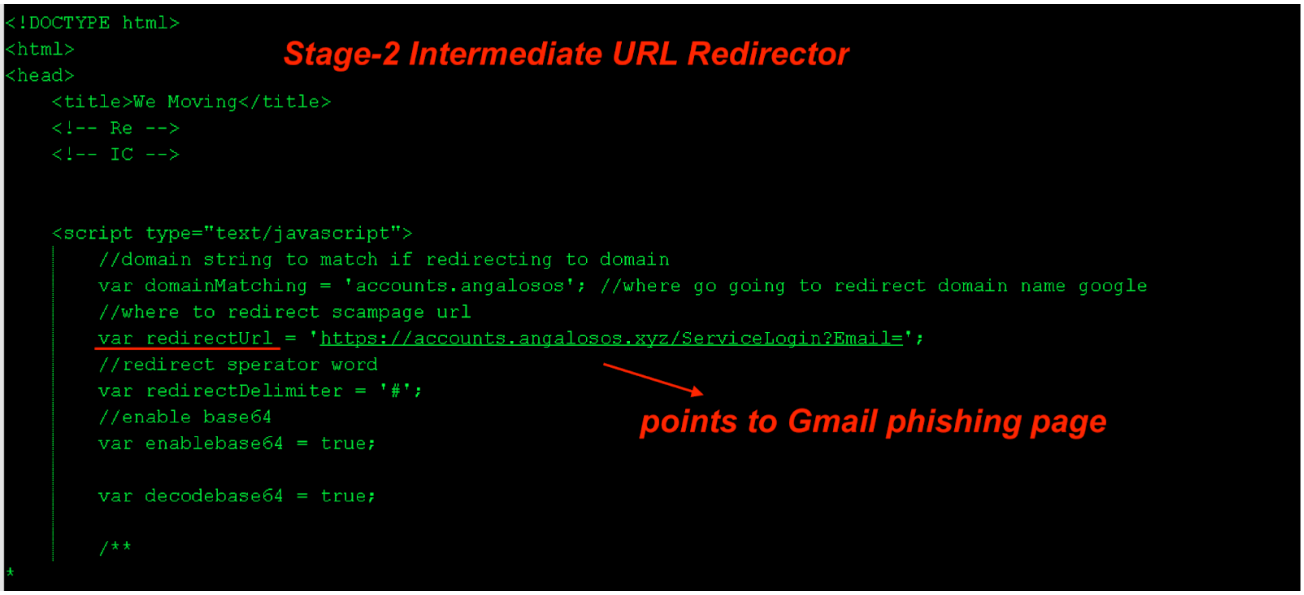
stage-2 URL redirector

base64-decodes to recipient's email address

Figure 4: Second variant of the Stage 1 URL used to redirect users to Stage 2

Stage 2 (Intermediate redirector)

The intermediate redirector is a JavaScript hosted on compromised domains. Figure 5 shows an example of the redirect script. The variable "redirectURL" in the script specifies the final phishing landing page.



Stage-2 Intermediate URL Redirector

```
<!DOCTYPE html>
<html>
<head>
    <title>We Moving</title>
    <!-- Re -->
    <!-- IC -->


    <script type="text/javascript">
        //domain string to match if redirecting to domain
        var domainMatching = 'accounts.angalosos'; //where go going to redirect domain name google
        //where to redirect scampage url
        var redirectUrl = 'https://accounts.angalosos.xyz/ServiceLogin?Email=';
        //redirect sperator word
        var redirectDelimiter = '#';
        //enable base64
        var enablebase64 = true;

        var decodebase64 = true;

        /**
*
```

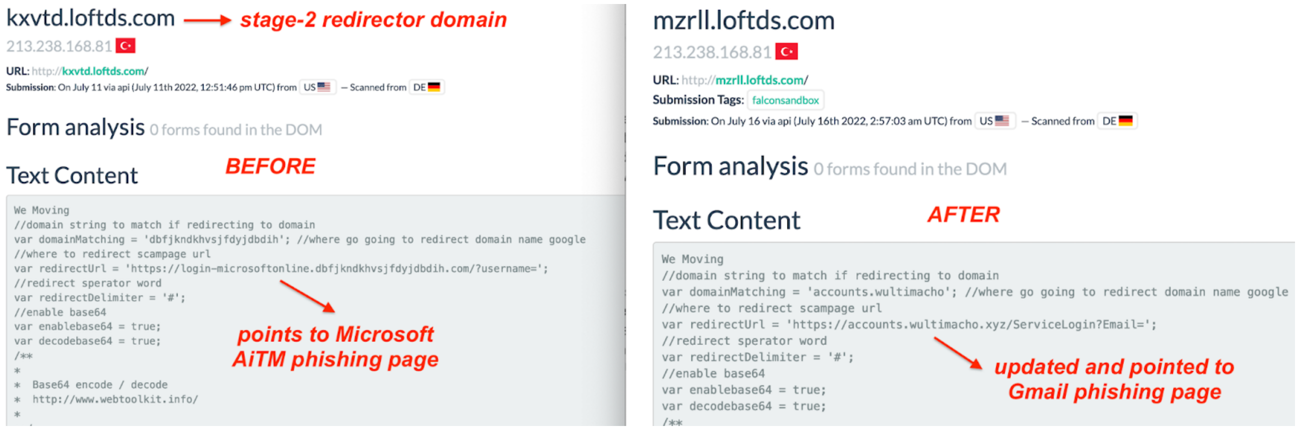
points to Gmail phishing page

Figure 5: Stage 2 intermediate URL redirector

We observed that the threat actor updated this redirectURL variable regularly to ensure it points to the latest phishing page. This allows the threat actor to quickly update their campaign to keep up with URL detections added by security vendors. We regularly monitored these redirector scripts to identify new phishing pages proactively and added detection.

We identified compromised domains hosting URL redirect scripts which were updated to point to the new G suite phishing URLs.

Figure 6 shows a side-by-side comparison of this case. In this example, "loftds[.]com" is the attacker-controlled domain hosting the redirector script. As can be seen on the left-hand side, on July 11th 2022, the redirector script pointed to a URL used in Microsoft AiTM phishing attack. On the right-hand side, we can see that on July 16th 2022, the same script was updated to point to a URL used in the G suite AiTM phishing attack.



kxvtd.loftds.com → stage-2 redirector domain

213.238.168.81

URL: http://kxvtd.loftds.com/

Submission: On July 11 via api (July 11th 2022, 12:51:46 pm UTC) from US — Scanned from DE

Form analysis 0 forms found in the DOM

Text Content BEFORE

```
We Moving
//domain string to match if redirecting to domain
var domainMatching = 'dbfjkndkhvsjfdyjdbdih'; //where go going to redirect domain name google
//where to redirect scampage url
var redirectUrl = 'https://login-microsoftonline.dbfjkndkhvsjfdyjdbdih.com/?username=';
//redirect sperator word
var redirectDelimiter = '#';
//enable base64
var enablebase64 = true;
var decodebase64 = true;
/**
*
*  Base64 encode / decode
*  http://www.webtoolkit.info/
*
```

points to Microsoft AiTM phishing page

mzrll.loftds.com

213.238.168.81

URL: http://mzrll.loftds.com/

Submission Tags: falconsandbox

Submission: On July 16 via api (July 16th 2022, 2:57:03 am UTC) from US — Scanned from DE

Form analysis 0 forms found in the DOM

Text Content AFTER

```
We Moving
//domain string to match if redirecting to domain
var domainMatching = 'accounts.wultimacho'; //where go going to redirect domain name google
//where to redirect scampage url
var redirectUrl = 'https://accounts.wultimacho.xyz/ServiceLogin?Email=';
//redirect sperator word
var redirectDelimiter = '#';
//enable base64
var enablebase64 = true;
var decodebase64 = true;
/**
```

updated and pointed to Gmail phishing page

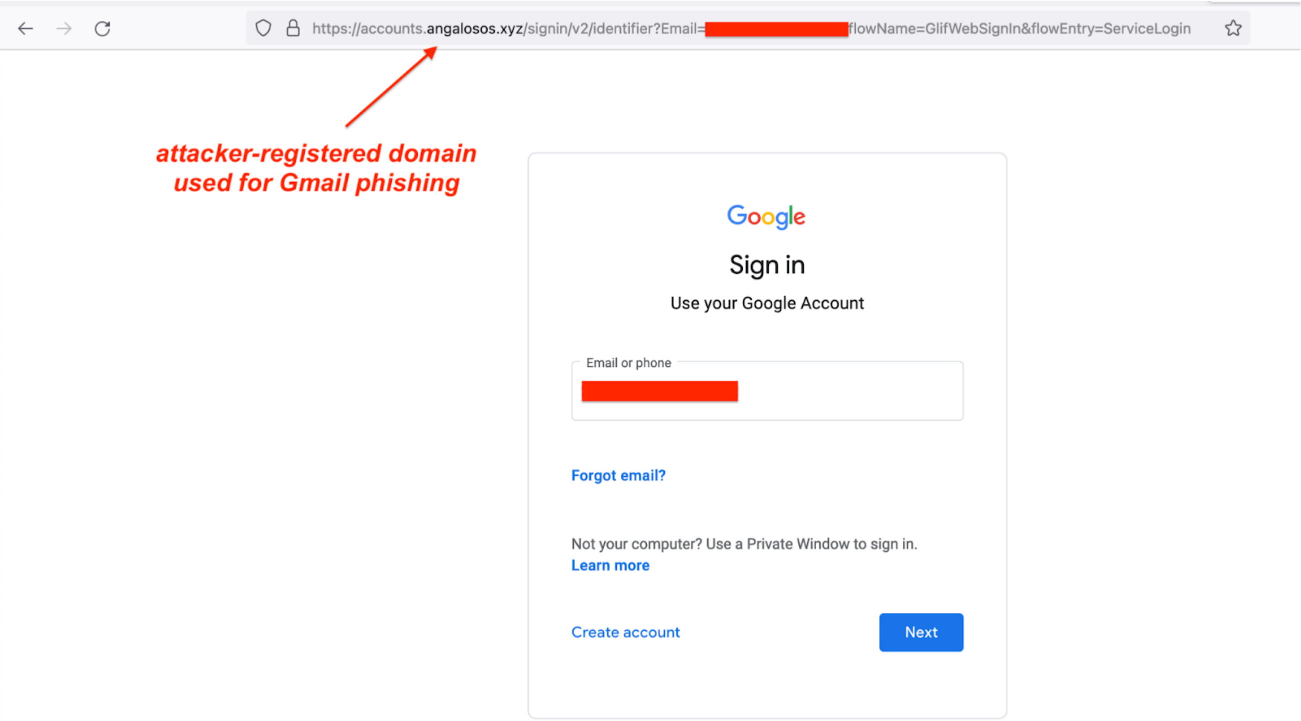
Figure 6: Same redirector page used in Microsoft AiTM and G suite/Gmail AiTM phishing

This was a strong indicator which helped us correlate the two campaigns to the same threat actor.

Fingerprinting-based evasion

The main phishing page used client-side JavaScript-based fingerprinting to detect the presence of automated URL analysis systems. The fingerprint information collected from the device will be sent to the server using websocket. We explained the technical details of this fingerprinting method in our previous blog here.

Once all the stages of URL redirection and the client fingerprinting checks are passed, the user lands on the final Gmail phishing page as shown in Figure 7.



https://accounts.angalosos.xyz/signin/v2/identifier?Email=[redacted]flowName=GlifWebSignIn&flowEntry=ServiceLogin

attacker-registered domain used for Gmail phishing

Google

Sign in

Use your Google Account

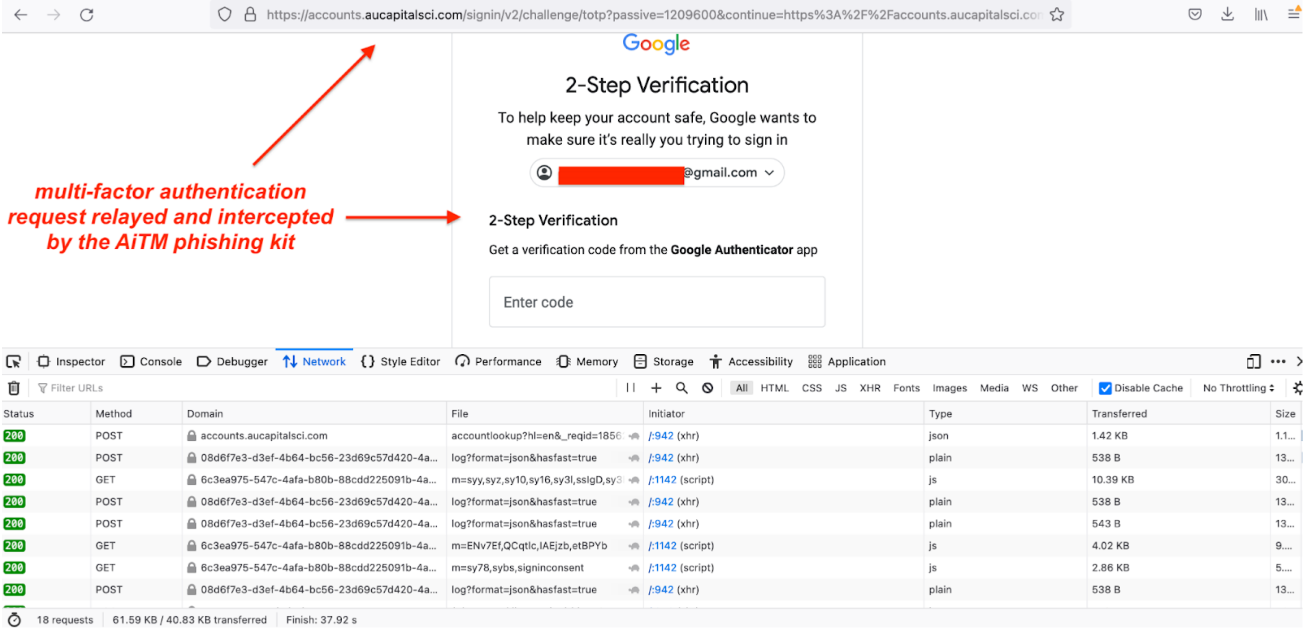
Email or phone: [redacted]

Forgot email?

Not your computer? Use a Private Window to sign in. Learn more

Figure 7: Final Gmail phishing page

Figure 8 below shows that the AiTM phishing kit is able to successfully relay and intercept the multi-factor authentication process used by Gmail / G suite.



https://accounts.aucapitalsci.com/signin/v2/challenge/totp?passive=1209600&continue=https%3A%2F%2Faccounts.aucapitalsci.co

multi-factor authentication request relayed and intercepted by the AiTM phishing kit

Google

2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[redacted]@gmail.com

2-Step Verification

Get a verification code from the **Google Authenticator** app

Enter code

☑ Disable Cache

No Throttling

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	accounts.aucapitalsci.com	accountlookup?hl=en&_reqid=1856	/:942 (xhr)	json	1.42 KB	1.1...
200	POST	08d6f7e3-d3ef-4b64-bc56-23d69c57d420-4a...	log?format=json&hasfast=true	/:942 (xhr)	plain	538 B	13...
200	GET	6c3ea975-547c-4afa-b80b-88cdd225091b-4a...	m=syy,syz,sy10,sy16,sy3l,sslgD,sy3	/:1142 (script)	js	10.39 KB	30...
200	POST	08d6f7e3-d3ef-4b64-bc56-23d69c57d420-4a...	log?format=json&hasfast=true	/:942 (xhr)	plain	538 B	13...
200	POST	08d6f7e3-d3ef-4b64-bc56-23d69c57d420-4a...	log?format=json&hasfast=true	/:942 (xhr)	plain	543 B	13...
200	GET	6c3ea975-547c-4afa-b80b-88cdd225091b-4a...	m=ENv7Ef,QCqtlc,IAEjzb,etBPYb	/:1142 (script)	js	4.02 KB	9....
200	GET	6c3ea975-547c-4afa-b80b-88cdd225091b-4a...	m=sy78,sybs,signinconsent	/:1142 (script)	js	2.86 KB	5....
200	POST	08d6f7e3-d3ef-4b64-bc56-23d69c57d420-4a...	log?format=json&hasfast=true	/:942 (xhr)	plain	538 B	13...

18 requests | 61.59 KB / 40.83 KB transferred | Finish: 37.92 s

Figure 8: Multi-factor authentication (MFA) process of Gmail intercepted by AiTM phishing kit

Zscaler’s detection status

Zscaler’s multilayered cloud security platform detects indicators at various levels, as seen here:

HTML.Phish.Gmail

Conclusion

In this blog we described how the threat actor is leveraging AiTM proxy-based phishing kits to target multiple email providers' users in enterprises. It is important to understand that such attacks are not limited to only Microsoft and Gmail enterprise users. An attacker can bypass multi-factor authentication protection on many different services using this method.

Business email compromise (BEC) continues to be one of the top threats which organizations need to protect against. As described in this blog, the threat actor is constantly registering new domains and targeting more online services often used in enterprises.

Even though security features such as multi-factor authentication (MFA) add an extra layer of security, they should not be considered as a silver bullet to protect against phishing attacks. With the use of advanced phishing kits (AiTM) and clever evasion techniques, threat actors can bypass both traditional as well as advanced security solutions.

As an extra precaution, users should not open attachments or click on links in emails sent from untrusted or unknown sources. As a best practice, in general, users should verify the URL in the address bar of the browser before entering any credentials.

The Zscaler ThreatLabz team will continue to monitor this active campaign, as well as others, to help keep our customers safe.

Indicators of Compromise

Phishing domains

*.angalosos[.]xyz
*.mdks[.]xyz
*.7brits[.]xyz
*.fekir5[.]xyz

*.bantersplid[.]xyz
*.absmg[.]xyz
*.wultimacho[.]xyz
*.gsuiteworkstation[.]com
*.thyxyzjgdrwafzy[.]xyz
*.7dmjmg20p8[.]xyz
*.appfolders[.]xyz
*.4765445b-32c6-4-83e6-1d93765276[.]co
*.aucapitalsci[.]com
*.eaganins.click
*.disturbedmidiagroup.click

Intermediate URL redirectors

Note: These are compromised websites

*.southernlivingsavannah[.]com
*.sunnyislesdental[.]com
*.horticulturatanaka[.]com.br
ripple-hirodai[.]com
pathopowerreport[.]de
pagliaispizzakv[.]com
*.loftds[.]com
*.sabtsaeen[.]ir
*.jarrydrenton[.]com
*.alphamediaam[.]ir
*.hcapinfo[.]com
*.gamea[.]ir