DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit

security-blog-prod-wp01.azurewebsites.net/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/

March 13, 2023

Adversary-in-the-middle (AiTM) phishing kits are part of an increasing trend that is observed supplanting many other less advanced forms of phishing. AiTM phishing is capable of circumventing multifactor authentication (MFA) through reverse-proxy functionality. DEV-1101 is an actor tracked by Microsoft responsible for the development, support, and advertising of several AiTM phishing kits, which other cybercriminals can buy or rent. The availability of such phishing kits for purchase by attackers is part of the industrialization of the cybercriminal economy and lowers the barrier of entry for cybercrime.

DEV-1101 offers an open-source kit that automates setting up and launching phishing activity and provides support services to attackers. The threat actor group began offering their AiTM phishing kit in 2022, and since then has made several enhancements to their kit, such as the capability to manage campaigns from mobile devices, as well as evasion features like CAPTCHA pages. These attributes make the kit attractive to many different actors who have continually put it to use since it became available in May 2022. Actors using this kit have varying motivations and targeting and might target any industry or sector.

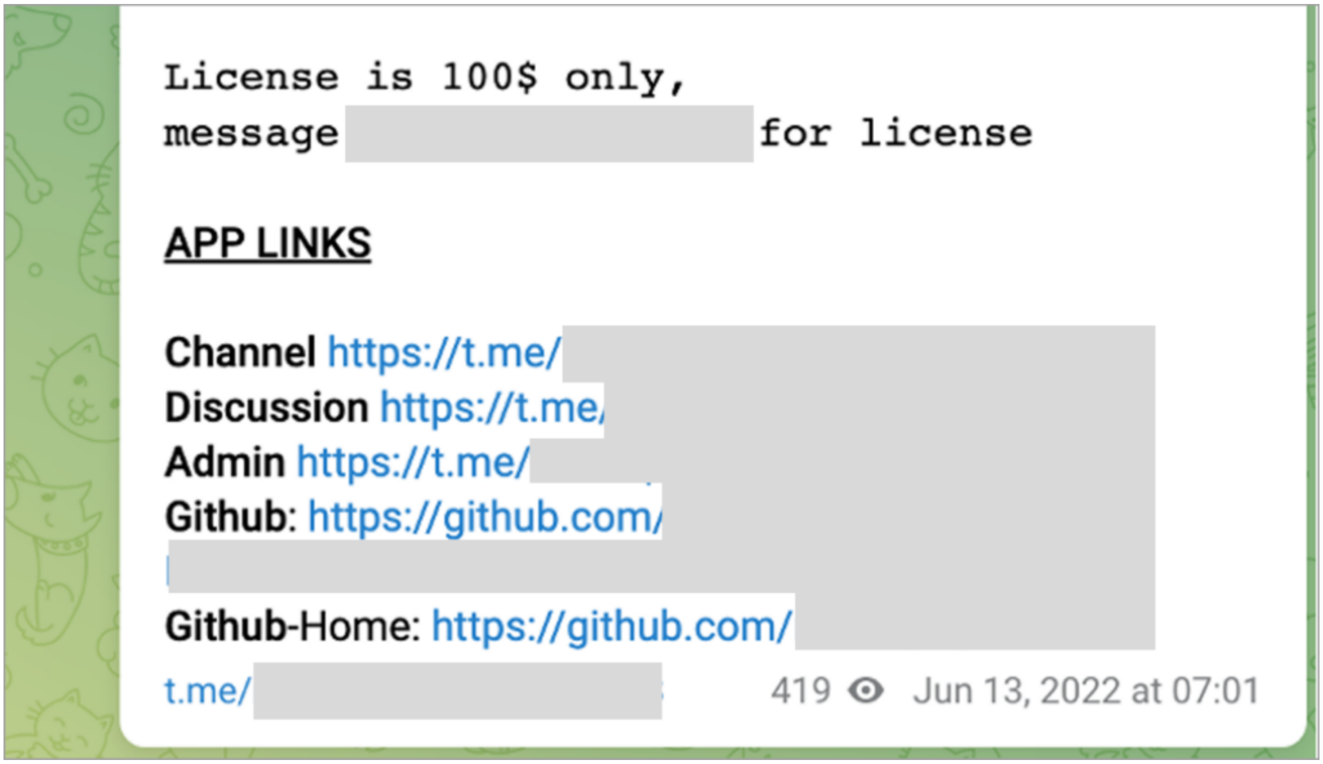
Microsoft 365 Defender detects suspicious activities related to AiTM phishing attacks and follow-on activities, such as session cookie theft and attempts to use the stolen cookies to sign in.

In this blog post, we share information on DEV-1101, the tool they offer, and details on related AiTM campaigns. We also share best practices and detection details to further protect organizations from AiTM phishing attacks.

AiTM tool promotion

DEV-1101 began advertising their AiTM kit around May 2022 through a Telegram channel and an advertisement in *exploit[.]in*, a popular cybercrime forum. The advertisement describes the AiTM kit as a phishing application written in NodeJS with PHP reverse-proxy capabilities, automated setup, detection evasion through an *antibot* database, management of phishing activity through Telegram bots, and a wide range of ready-made phishing pages mimicking services such as Microsoft Office or Outlook.

On June 12, 2022, DEV-1101 announced that the kit would be open source with a $100 monthly licensing fee. The actor also provided links to additional Telegram channels and a now-defunct GitHub page.



License is 100$ only,
message [redacted] for license

APP LINKS

Channel https://t.me/[redacted]
Discussion https://t.me/[redacted]
Admin https://t.me/[redacted]
Github: https://github.com/[redacted]

[redacted]

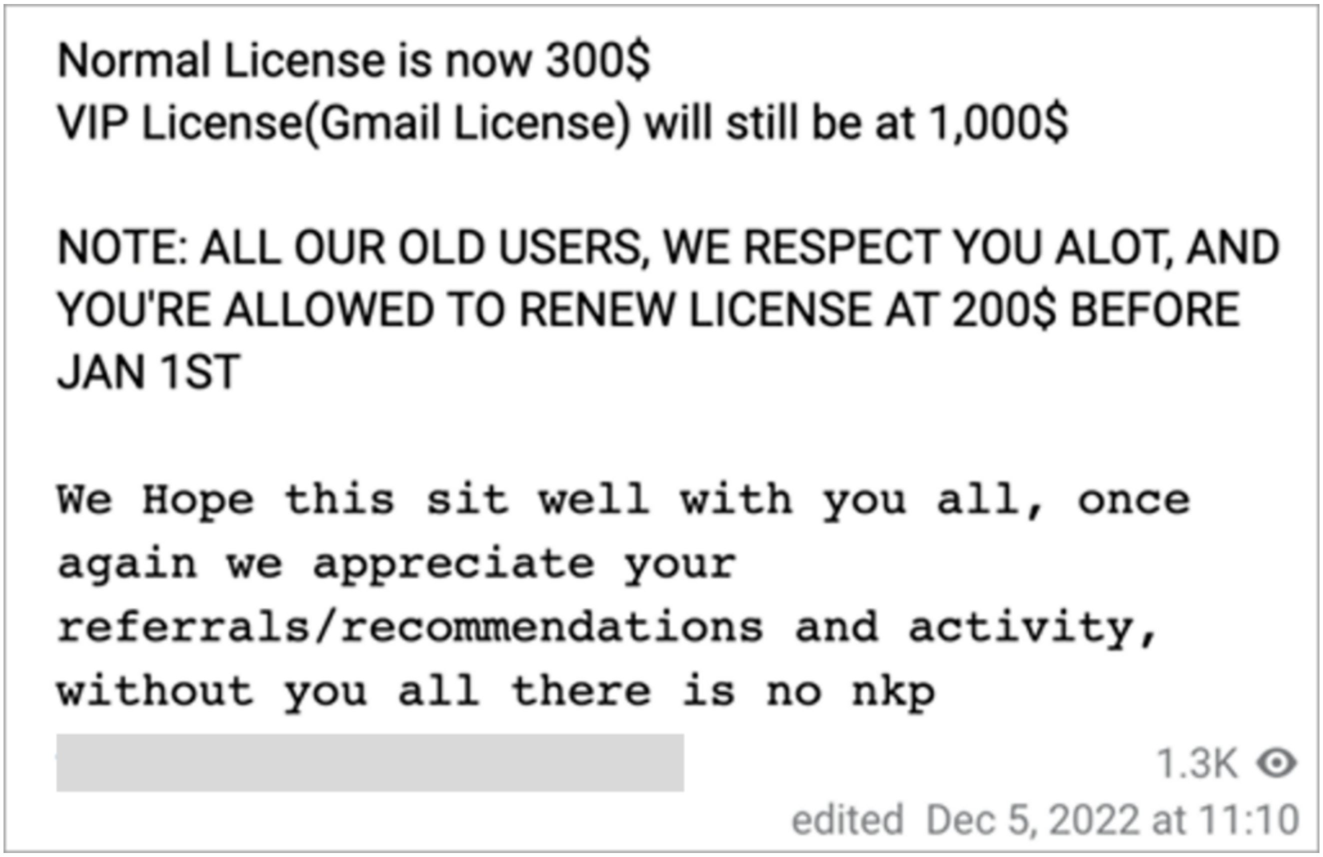
Github-Home: https://github.com/[redacted]

t.me/[redacted] 419 👁 Jun 13, 2022 at 07:01

Figure 1. DEV-1101 announcement on their AiTM tool license

In September 2022, DEV-1101 added the ability to manage servers running their kit through a Telegram bot rather than requiring the use of cPanel, further facilitating phishing activities and letting their customers manage campaigns from mobile devices.

DEV-1101 was able to increase the price of their tool multiple times due to the rapid growth of their user base from July through December 2022. This allowed DEV-1101 to dedicate themselves fully to the development and support of their tool. As of this writing, DEV-1101 offers their tool for $300, with VIP licenses at $1,000. Legacy users were permitted to continue purchasing licenses at $200 prior to January 1, 2023.



Normal License is now 300$
VIP License(Gmail License) will still be at 1,000$

NOTE: ALL OUR OLD USERS, WE RESPECT YOU ALOT, AND YOU'RE ALLOWED TO RENEW LICENSE AT 200$ BEFORE JAN 1ST

We Hope this sit well with you all, once again we appreciate your referrals/recommendations and activity, without you all there is no nkp

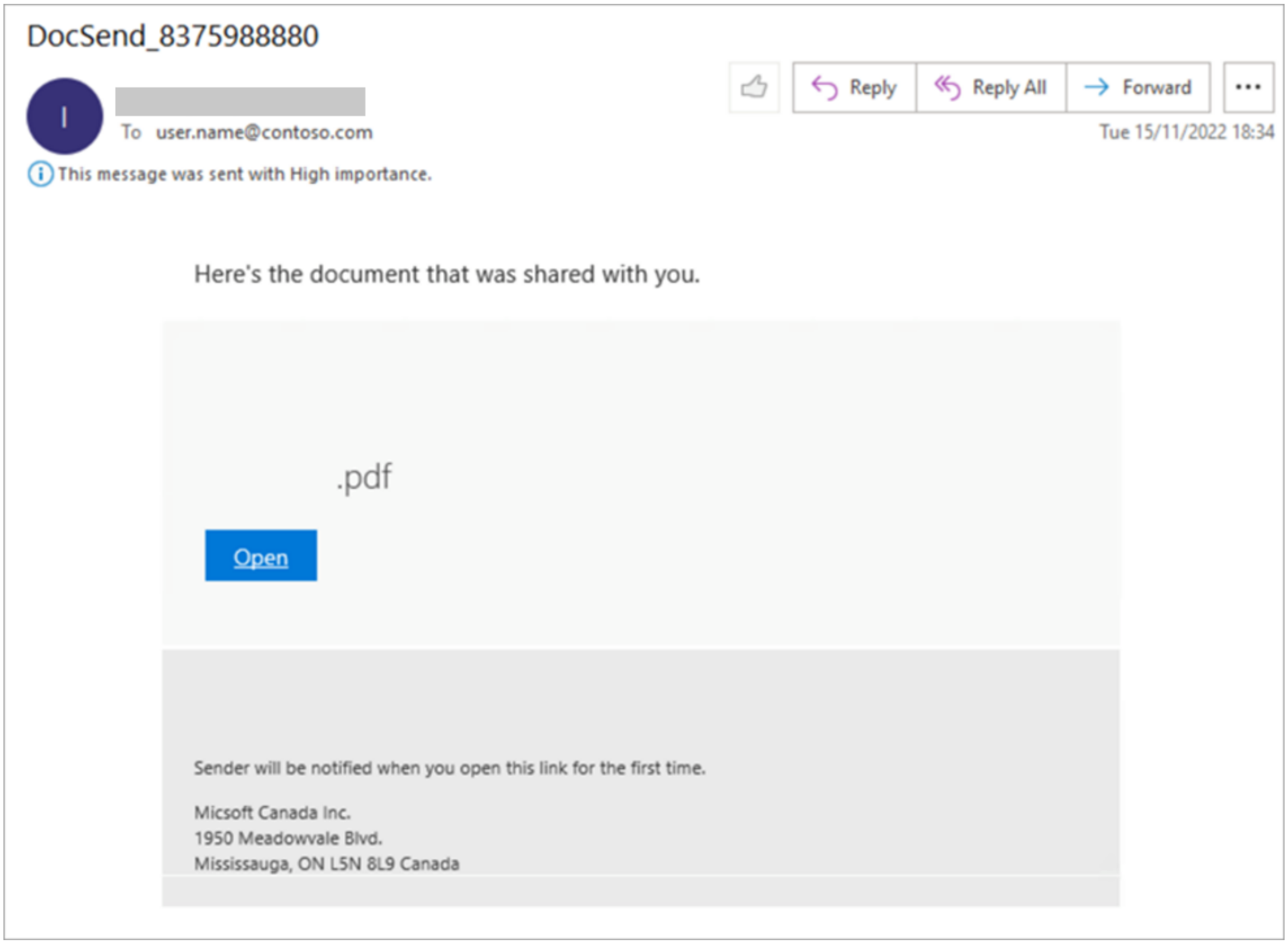
[redacted]

Figure 2. DEV-1101 increased their prices repeatedly due to rapid growth.

Microsoft observed several high-volume phishing campaigns from various actors using the tool offered by DEV-1101, comprising millions of phishing emails per day. DEV-0928, an actor Microsoft has tracked since September 2022, is one of DEV-1101's more prominent patrons and was observed launching a phishing campaign involving over one million emails.

DEV-1101 phishing sequence

DEV-1101's many different patrons take different approaches to phishing attacks. The example below is of an initial phishing message from a campaign launched by DEV-0928 using the DEV-1101 phishing kit. Clicking the *Open* button in the email leads to the next step in the sequence.



DocSend_8375988880

[redacted]
To user.name@contoso.com

Tue 15/11/2022 18:34

This message was sent with High importance.

Here's the document that was shared with you.

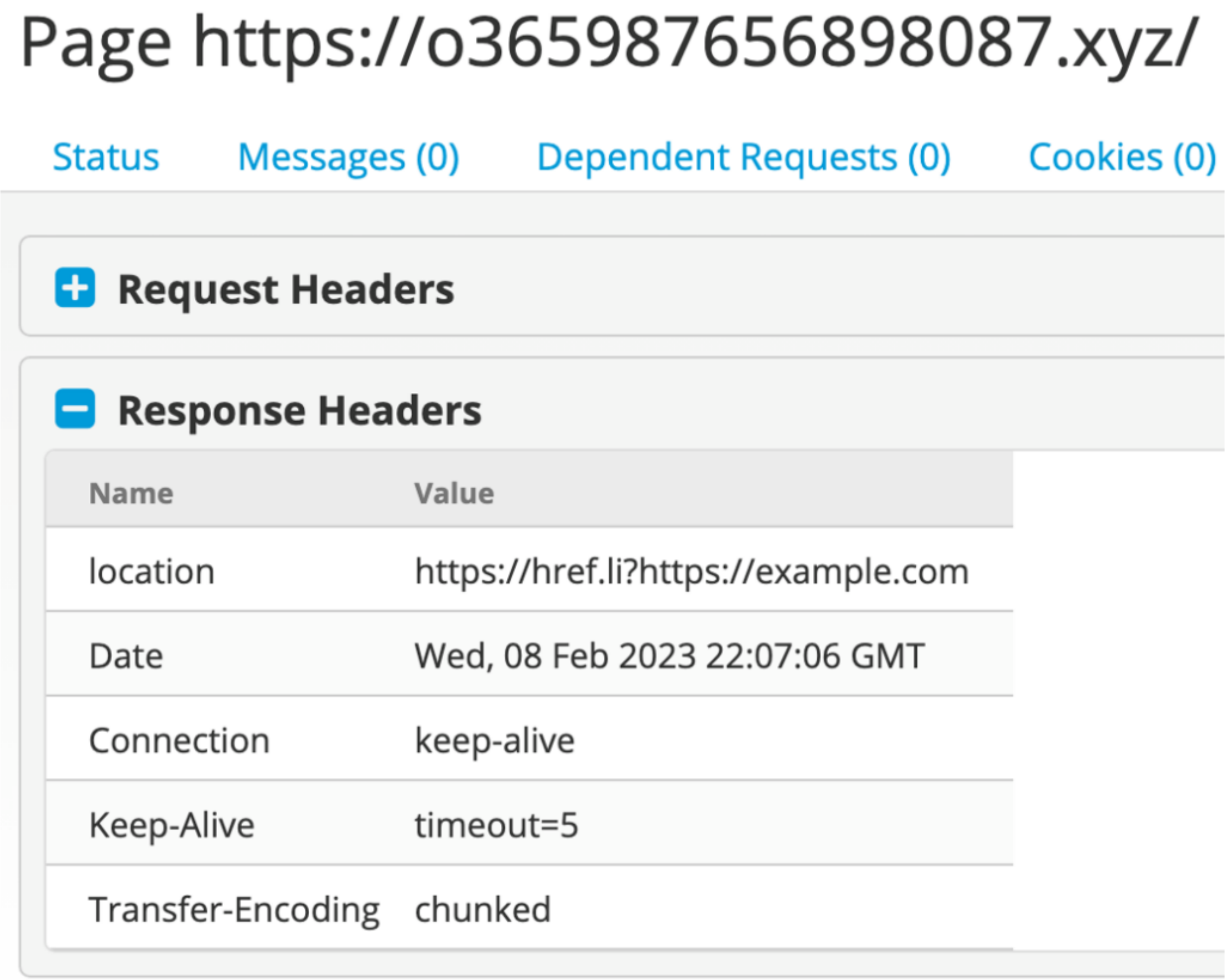
.pdf

Sender will be notified when you open this link for the first time.

Micsoft Canada Inc.
1950 Meadowvale Blvd.
Mississauga, ON L5N 8L9 Canada

Figure 3. Malicious link shared in a phishing message for an AiTM campaign.

Two different evasions might result from clicking the link in the phishing message. The DEV-1101 kit’s *antibot* functionality might trigger an *href* redirection to a benign page. In this example, the DEV-0928 domain *o365987656898087[.]xyz* redirects to *example.com*:

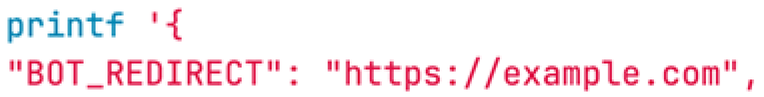


Page https://o365987656898087.xyz/

Name	Value
location	https://href.li?https://example.com
Date	Wed, 08 Feb 2023 22:07:06 GMT
Connection	keep-alive
Keep-Alive	timeout=5
Transfer-Encoding	chunked

Figure 4. DEV-1101 benign redirect response headers

The default redirection domain defined in the source code is *example.com*; however, any actor using the kit may define a different redirection domain.



```
printf '{
"BOT_REDIRECT": "https://example.com",
```

Figure 5. DEV-1101 benign redirect in source-code

The kit also allows threat actors to use CAPTCHA to evade detection. Inserting a CAPTCHA page into the phishing sequence could make it more difficult for automated systems to reach the final phishing page, while a human could easily click through to the next page.

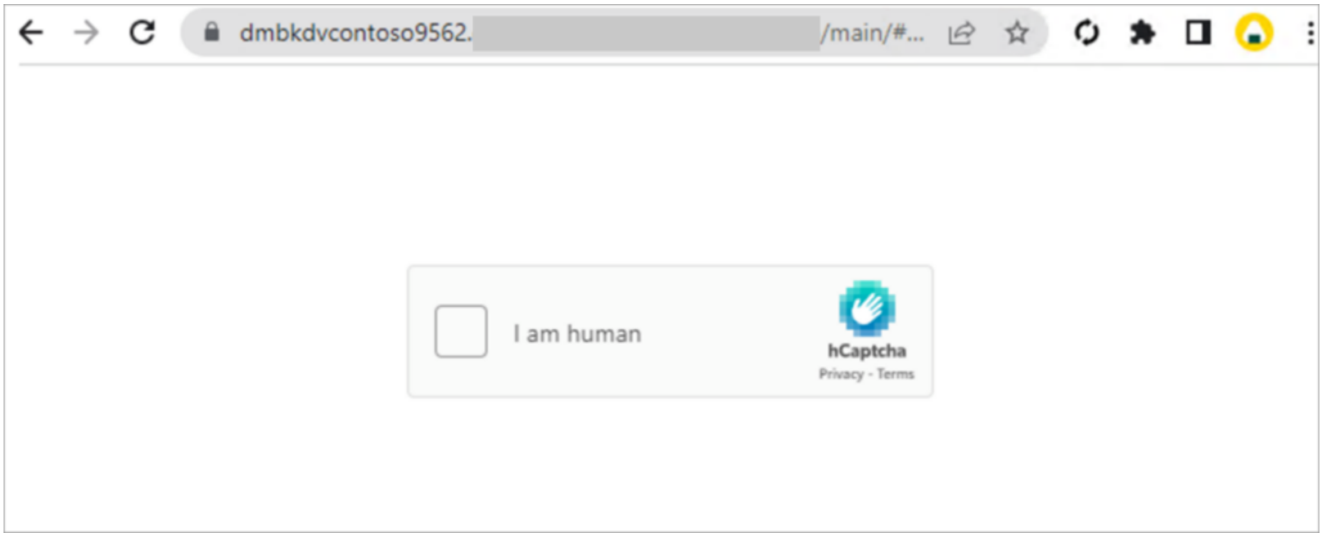
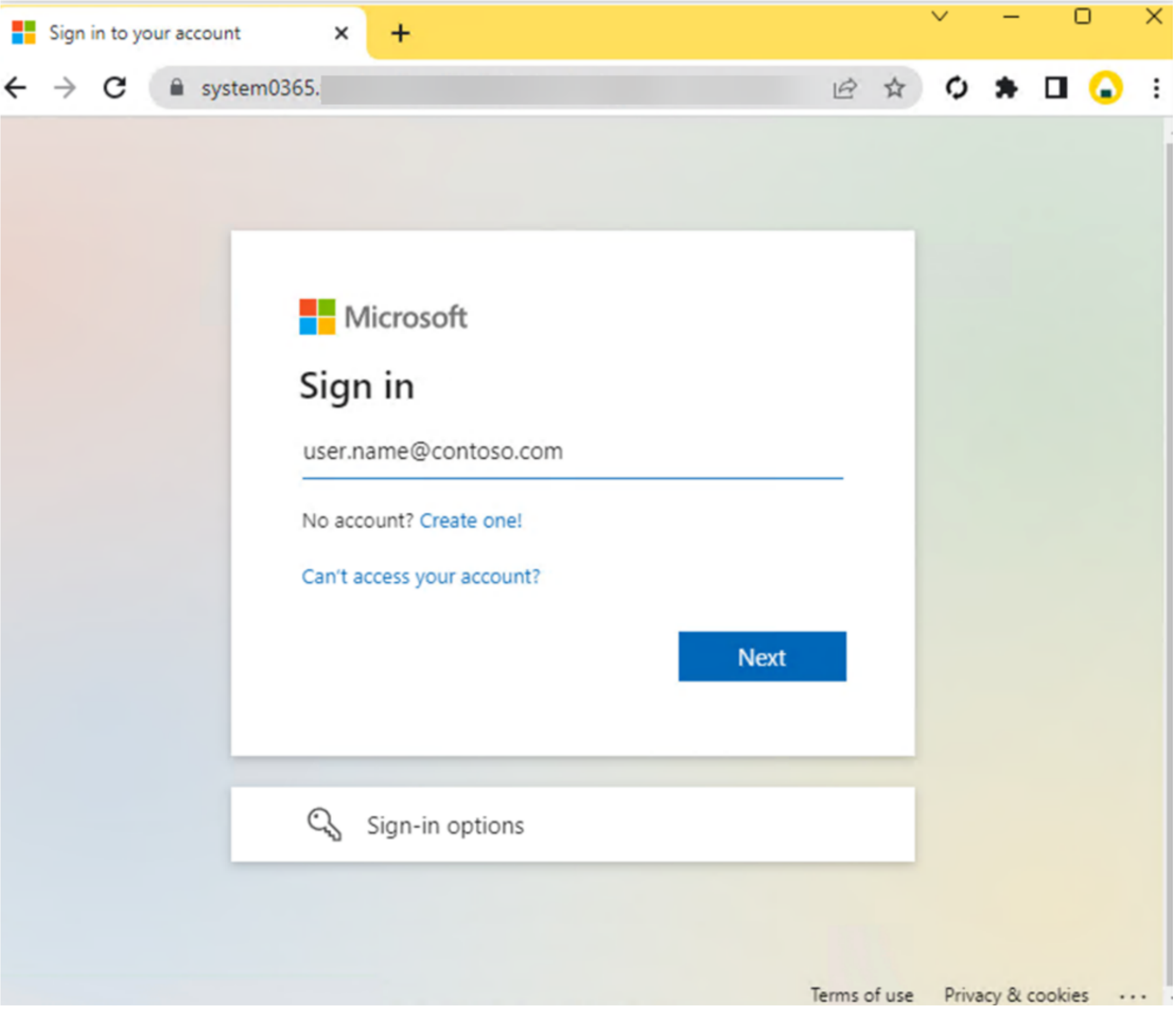

dmbkdvcontoso9562.[redacted]/main/#...

Figure 6. Evasion through CAPTCHA page

While evasion through CAPTCHA was introduced in August 2022, the functionality then required active engagement from DEV-1101's support to complete the setup for any requesting users. DEV-1101 later added CAPTCHA as a core functionality.

After the evasion pages, a phishing landing page is presented to the target from an actor-controlled host through the phishing actor's reverse proxy setup:



Sign in to your account

system0365.[redacted]

Microsoft

Sign in

user.name@contoso.com

No account? Create one!

Can't access your account?

Next

Sign-in options

Terms of use Privacy & cookies ...

Figure 7. Credential harvester mimicking a Microsoft sign-in portal.

At this point, the actor's server captures credentials entered by the user. If the user has MFA enabled, the AiTM kit continues to function as a proxy between the user and the user's sign-in service, meaning, as the user completes an MFA sign-in, the server captures the resulting session cookie. The attacker can then bypass MFA with the session cookie and the user's stolen credentials.

The following diagram illustrates the AiTM phishing attack chain:

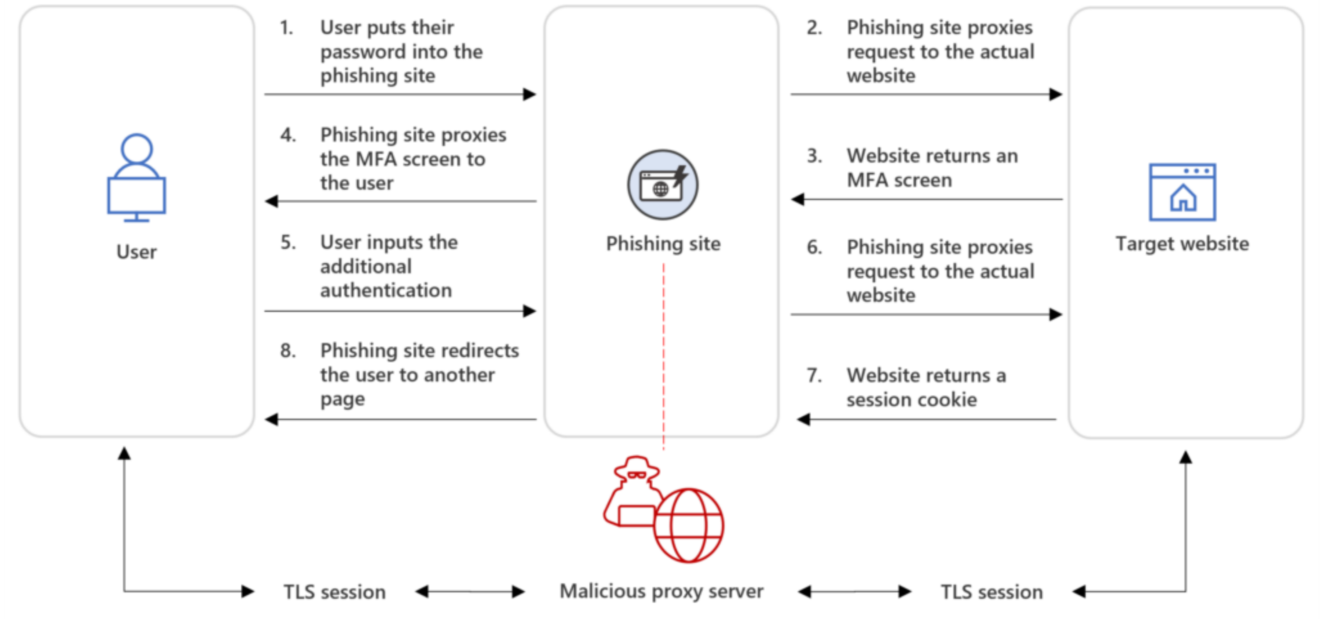

1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page
User
Phishing site
Target website
TLS session
Malicious proxy server
TLS session

Figure 8. AiTM phishing attack diagram

For additional in-depth information on how AiTM phishing works, refer to the blog, From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud.

Mitigating AiTM phishing attacks

While AiTM phishing attempts to circumvent MFA, MFA implementation remains an essential pillar in identity security and highly effective at stopping a wide variety of threats. MFA is the reason that threat actors developed the AiTM session cookie theft technique in the first place. Organizations are advised to work with their identity provider to ensure security controls like MFA are in place. Microsoft customers can implement MFA in Azure AD through various methods, such as using the Microsoft Authenticator, FIDO2 security keys, and certificate-based authentication.

Defenders can also complement MFA with the following solutions and best practices to further protect their organizations from such attacks:

- **Use security defaults** as a baseline set of policies to improve identity security posture. For more granular control, **enable conditional access policies.** Conditional access policies evaluate sign-in requests using additional identity-driven signals like user or group membership, IP location information, and device status, among others, and are enforced for suspicious sign-ins. Organizations can protect themselves from attacks that leverage stolen credentials by enabling policies such as compliant devices or trusted IP address requirements.
- **Implement continuous access evaluation.**

- **Invest in advanced anti-phishing solutions** thatmonitor and scan incoming emails and visited websites. For example, organizations can leverage web browsers that automatically identify and block malicious websites, including those used in this phishing campaign, and solutions that detect and block malicious emails, links, and files.
- **Continuously monitor suspicious or anomalous activities.** Hunt for sign-in attempts with suspicious characteristics (for example, location, ISP, user agent, and use of anonymizer services).

Detection details and hunting queries

Microsoft 365 Defender

Because AiTM phishing attacks are complex threats, they require solutions that leverage signals from multiple sources. Microsoft 365 Defender uses its cross-domain visibility to detect malicious activities related to AiTM, such as session cookie theft and attempts to use stolen cookies for signing in.

Using Microsoft Defender for Cloud Apps connectors, Microsoft 365 Defender raises AiTM-related alerts in multiple scenarios. For Azure AD customers using Microsoft Edge, attempts by attackers to replay session cookies to access cloud applications are detected by Defender for Cloud Apps connectors for Office 365 and Azure. In such scenarios, Microsoft 365 Defender raises the following alert:

> Stolen session cookie was used

In addition, signals from these Defender for Cloud Apps connectors, combined with data from the Defender for Endpoint network protection capabilities, also triggers the following Microsoft 365 Defender alert on Azure AD environments:

> Possible AiTM phishing attempt

A specific Defender for Cloud Apps connector for Okta, together with Defender for Endpoint, also helps detect AiTM attacks on Okta accounts using the following alert:

> Possible AiTM phishing attempt in Okta

In addition, Microsoft 365 Defender has the following related alerts for activity related to the DEV-0928 threat actor, as well as high-risk Azure AD sign-in activity:

- DEV-0928 activity group
- Suspicious network connection to AiTM phishing site
- Connection to Adversary-in-the-Middle (AiTM) phishing site

Microsoft Sentinel

Microsoft Sentinel customers can use the following Microsoft Sentinel Analytics template to identify potential AiTM phishing attempts:

> Possible AiTM Phishing Attempt Against Azure AD

This detection uses signals from Azure AD Identity Protection, specifically it looks for successful sign ins that have been flagged as high risk, and then combines this with data from Web Proxy services such as ZScaler to identify where users might have connected to the source of those sign ins immediately prior. This can indicate a user interacting with a AiTM phishing site and having their session hijacked. This detection uses the Advanced Security Information Model (ASIM) Web Session schema. More details on the schema and its requirements can be found in the documentation: https://learn.microsoft.com/azure/sentinel/normalization-schema-web

In addition, customers can use the following identity-focused Analytics and Hunting Queries to detect and investigate anomalous sign-in events that may be indicative of a compromised user identity being accessed by a threat actor:

Microsoft Sentinel customers can also use the data provided by Microsoft Sentinel’s UEBA engine to hunt for anomalous login events such as where the ISP being logged in from is not commonly seen in the tenant, or if the user agent is uncommon amongst the user’s peer group. More details on Microsoft Sentinel UEBA feature can be found here: https://learn.microsoft.com/azure/sentinel/ueba-reference.