Campaign Profile – AiTM Phishing

Executive Summary

Adversary-in-the-middle (AiTM) phishing campaigns are a growing threat because they are highly effective and can bypass even the most advanced security measures. They are particularly dangerous when they target large organizations, which can have a significant impact on the organization's operations and reputation. Phishing remains to be one of the most common techniques attackers use in their attempts to gain initial access to organizations. It remains important for organizations to be vigilant and aware of this type of attack and take steps to protect themselves.

Threat Assessment

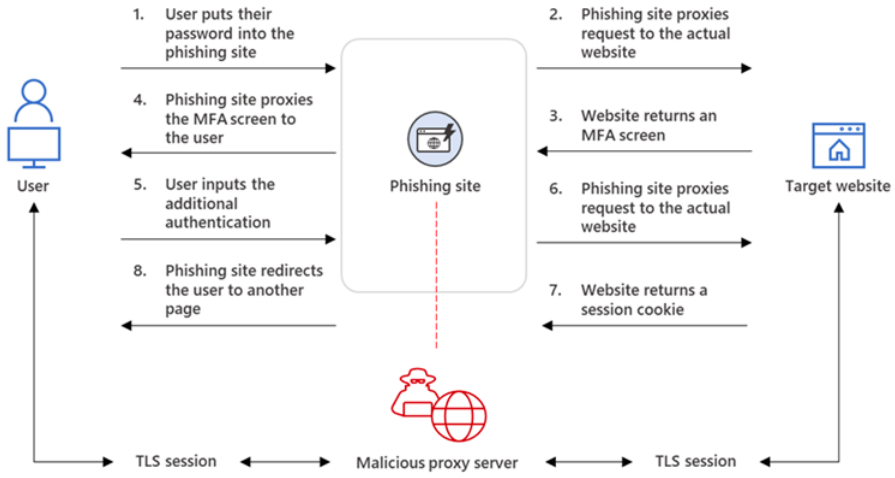
The AiTM phishing campaign poses a high risk to all organizations. Critical Start threat intelligence data suggests that the campaign is likely to be successful in compromising organizational security protocols, potentially resulting in significant loss if a compromise occurs.

This is a sophisticated and targeted attack that is designed to exploit security weaknesses within organizations. The campaign is highly effective in exploiting the vulnerabilities, as evidenced by the success of the campaign in more than 10000 organizations since September 2021 according to Microsoft 365 Defender threat data. The campaign is also highly targeted, as it is designed to target specific, often high-profile, individuals within an organization.

Based on our analysis, the risk posed by the AiTM phishing campaign is high and the activity level is also high as it has been identified within our data set on two occasions in the past 24 hours. The assessment of this campaign has been made based on its highly effective exploitation of security weaknesses and vulnerabilities of organizations and its highly targeted approach.

Detailed Analysis

Adversary-in-the-Middle technique allows an adversary to attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.



The above image illustrates the AiTM phishing process. AiTM phishing website intercepting the authentication process. Image Credit Microsoft.com

AiTM phishing campaigns are a type of phishing attack that is highly sophisticated and difficult to detect, designed to bypass even the most advanced security measures. In this type of attack, the attacker creates a fake website or login page that looks identical to a legitimate website, but which has a different URL.

When a user attempts to login to the fake website, the attacker intercepts their credentials and login session. This is possible because every modern web service implements a session with a user after successful authentication. This is done through a session cookie provided by an authentication service after initial authentication. This session cookie is the proof for the web server that the user has been authenticated and has an ongoing session on the website.

To obtain the session cookie, the attacker deploys a webserver that acts as a proxy between the user visiting the phishing site and the target server the attacker wishes to impersonate. The attacker then proxys HTTP packets from the user visiting the phishing site to the target server, and the other way around. This allows the attacker to create a phishing site that is visually identical to the original website, as every HTTP request is proxied to and from the original website.

By obtaining the user's session cookie, the attacker is able to bypass the authentication process and act on the user's behalf, gaining access to sensitive information, stealing money, or causing damage to the organization.

Adversary-in-the-middle (AiTM) phishing attacks intercept the target's authentication process and obtain sensitive information such as passwords and session cookies. The phishing page establishes two different Transport Layer Security (TLS) sessions; one with the target and another with the actual website the target wants to access. This allows the attacker to function as an AiTM agent, intercepting the authentication process and extracting valuable data. Once the attacker obtains the session cookie, they can inject it into their browser to bypass the authentication process, even if the target's multi-factor authentication (MFA) is enabled.

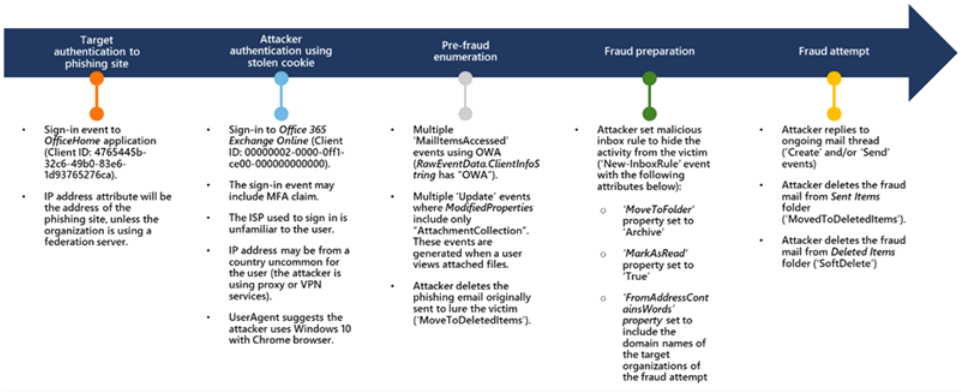
When an attacker uses a stolen session cookie, the “SessionId” attribute in the AADSignInEventBeta table will be identical to the SessionId value used in the authentication process against the phishing site.

AiTM phishing attacks can be automated using open-source phishing toolkits such as Evilginx2, Modlishka, and Muraena which are widely accessible.

Observed Intrusions

In one of the instances we’ve observed, the attacker sent emails with a malicious URL to multiple recipients within the organizations. The email message attempted to hijack the session and steal credentials. In the second instance, the URL was likely probing for session or credential hijacking.

While these attempts were documented by Critical Start within the last 24 hours, Microsoft 365 Defender Research Team and Microsoft Threat Intelligence Center (MSTIC) have documented more than 10000 instances related to the AiTM campaign. This AiTM phishing campaign is another example of how threats continue to evolve in response to the security measures and policies organizations put in place to defend themselves against potential attacks.



Above is a summary of the campaign’s end-to-end attack chain based on threat data from Microsoft 365 Defender: AiTM phishing campaign and follow-on BEC in the context of Microsoft 365 Defender threat data. Image credit: Microsoft.com

Critical Start Recommended Mitigation

AiTM phishing is an advanced form of phishing, and it's important to take actions to prevent this kind of attack- these steps should include:

Mitigation 1

Implement robust security measures, such as multi-factor authentication and enable conditional access policies like compliant and trusted devices and known IP address requirements.

Consider implementing additional measures to protect organizational data and systems such as encryption and data loss prevention solutions as well as implementing measures to detect and respond to malicious activity like intrusion detection systems and the maintenance of an incident response plan.

Mitigation 2
Ensure that their employees are trained on how to recognize and respond to phishing attempts and implementing security awareness training for employees.

Mitigation 3
Regularly monitor for suspicious and/or anomalous activity. Implement measures to reduce the risk of data exfiltration, such as data classification and access control solutions. Hunt for sign-in attempts with suspicious characteristics (for example, location, ISP, user agent, use of anonymizer services) and unusual mailbox activities, such as the creation of Inbox rules with suspicious purposes or unusual amounts of mail item access events by untrusted IP addresses or devices.

Mitigation 4
Invest in advanced anti-phishing solutions thatmonitor and scan incoming emails and visited websites. For example, organizations can leverage web browsers that can automatically identify and block malicious websites, including those used in this phishing campaign.

Critical Start Actions

Action 1
The messages containing a malicious file are delivered to mailboxes in an organization and the infected messages are removed from Exchange Online mailboxes using zero-hour auto purge (ZAP) if this event occurs.

Action 2
Any messages associated with a campaign are delivered to mailboxes in an organization and the infected messages are removed from Exchange Online mailboxes using ZAP if this event occurs.

Action 3
Critical Start Cyber Threat Intelligence team identifies the alerts as a part of the larger AiTM Campaign and alerts the SOC as well as disseminating intelligence communications to customers.

Action 4
Detection Engineering has validated the Defender alerts ‘Email messages containing malicious file removed after delivery’ AND ‘Email messages from a campaign removed after delivery’ as well as assessed if any product gaps exist within our coverage.

IOCs

Redirector Domains (rendered inoperable)
http://cdv.m3f.moonislam[.]net

http://bdp.p8z.moonislam[.]net

References

https://www.microsoft.com/en-us/security/blog/2021/10/11/how-cyberattacks-are-changing-according-to-new-microsoft-digital-defense-report/

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

https://www.microsoft.com/en-us/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/

https://www.microsoft.com/en-us/security/blog/2022/01/26/evolved-phishing-device-registration-trick-adds-to-phishers-toolbox-for-victims-without-mfa/