SWEY
CYBEREYE

FORBES

Bypassing Muti-factor authentication (MFA) with Stolen Session Cookies

Attacks on Becs Bank

Hype Value	General Risk	Risk to Becs Bank
Medium	High	High

Title: Using stolen cookies to bypass Muti-factor authentication (MFA)

Date: September 30, 2022

Threat description

A coordinated phishing campaign has been used by attackers to target over 10,000 organizations since September 2021. The campaign makes use of Adversary-in-the-middle (AiTM) to steal user login details, user sessions and bypass multi-factor authentications. The attack has mostly been targeted at institutions that use the Microsoft Azure Active Directory. The campaign also uses a phishing kit call Evilginx2. With this attack, the threat actors send emails to potential victims with supposedly an MP3 file which is actually an html file as an attachment. Once the user clicks to download the audio file, they are redirected to a phishing site which mimics the Azure Active Directory sign-in page where they are asked to enter their credentials. Once the user enters the login details and they are being authenticated, the proxy site then captures the user's session cookie. The user is then redirected to a legitimate office.com site. It is worth noting that the attacker can then use the stolen session cookie to circumvent the entire MFA process to be able to have access to the mailbox of the compromised account. After that, the threat actor starts an attack called Business Email Compromise (BEC). The attacker would then be committing payment fraud by sending fraudulent emails that are finance-related to contacts on the compromised accounts. Replies to emails sent by the attacker are set to be delivered to the "Archive" folder to prevent detection. To coverup tracks, the attacker would delete all conversations they have had from the mailbox. These include sent emails and their responses, archived and deleted messages. They may trick other members of the company or clients of the company to transfer funds to a fake account number.

CVE Number	Description
CVE-2021-36949	Microsoft Azure Active Directory Connect Authentication Bypass Vulnerability

Risk Assessment

This threat targets the vulnerability associated with multi-factor authentication method. The vulnerability affects the organization's Microsoft Azure Active Directory. A single compromised account can be used to attack other accounts on the directory. In addition, a successful payment fraud can cost the organization from several thousands to millions of dollars. Based on the following information, the risk to the client is high.

Actions taken

1. Organized security webinars for client to educate employees on email safety practices and how they can identify phishing sites and phishing emails that originates from external email addresses and those that are from members of the organization.
2. All employees were restricted to use trusted web browsers which provides fraudulent website warnings and have the capability to identify and block malicious sites. They were limited to Safari and Microsoft Edge.

Next Steps and Recommended Actions

1. Procure Microsoft Defender for Cloud Apps to defend the client's systems from AiTM phishing campaigns.
2. Organize cybersecurity awareness trainings for all client's employees once every month.
3. Use Microsoft Azure Active Directory Identity Protection to protect against logins from hijacked session cookies.
4. IT Admins to actively track user authentications that originates from unfamiliar addresses or locations to be able to prevent potential attacks

Sources

https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

https://secureteam.co.uk/articles/phishing-attacks-that-can-bypass-mfa/

Metadata

Report date	29.09.22
Analyst	Stephen Mensah
History	V 1.0