








We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

https://blooteem.com/march-2022  JAN FEB DEC     
 3 captures 17 2023 2024    
 17 Feb 2023 - 15 A  2022 

The image shows a dark-themed website header. On the left, there is a navigation menu with a hamburger icon (three horizontal lines) and three bullet points. In the center, the word 'Home' is displayed in a light blue, underlined font. On the right, the text 'Legacy Authentication' is written in a large, bold, white font. Below this, the text 'Link & Access' is visible in a smaller, light blue font. The background is a solid dark gray.

## How attackers are bypassing MFA in Azure AD

**March 202**

## Curtis Middlehurst

When looking into sign-in logs from Azure AD, you might have come across the user-agent 'BAV2ROPC'. Whilst it is possible that some accounts would legitimately be signing in with this user-agent, what you could be seeing is a successful password spray that has bypassed MFA.

## So what is BAV2ROPC?

BAV2ROPC Can be broken down into two parts, BAV2 = Business Apps V2, which includes older versions of mail apps that use legacy protocols such as IMAP, SMTP or POP3, and ROPC = Resource Owner Password Credential, a password flow in which the application handles a user's password.

Legacy protocols are unable to enforce a MFA requirement. This means that when an older mail app using legacy authentication methods is handling the credentials an attacker can effectively bypass MFA.

This tactic is commonly used in password spraying attacks, highlighted by Microsoft in this blog post: [Microsoft Security Blog](#). The Microsoft blog also points to "CBAinTAR" and "CBAinPROD" as user-agents that are associated with legacy authentication.

## Detection using Azure Sentinel

The first step when making detection rules for this is to baseline current usage of legacy authentication in your estate, it is possible that legacy authentication is being used by accounts performing automated tasks, find these accounts and add them to a Watchlist.

You can detect logins with a simple rule, all we need to look for is sign-in activity from accounts not in our watchlist with BAV2ROPC, CBAinTAR or CBAinPROD as the user-agent.

## Kusto Query Language Example:

Signinlogs  
|where UserPrincipleName !in~( GetWatchlist('knownlegacyaccounts' | project SearchKey)) and UserAgent in~ ("BAV2ROPC", "CBAinTAR", "CBAinPROD")

## Prevention

***Note: If your organization has security defaults enabled in Azure AD, legacy authentication will automatically be blocked.***

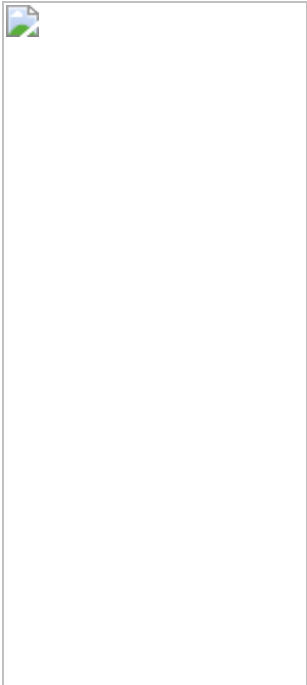
Since this attack is able to bypass MFA, the most painless method of prevention is to use Conditional Access policies in Azure AD by doing the following:

Create a group for all the accounts identified in baselining.

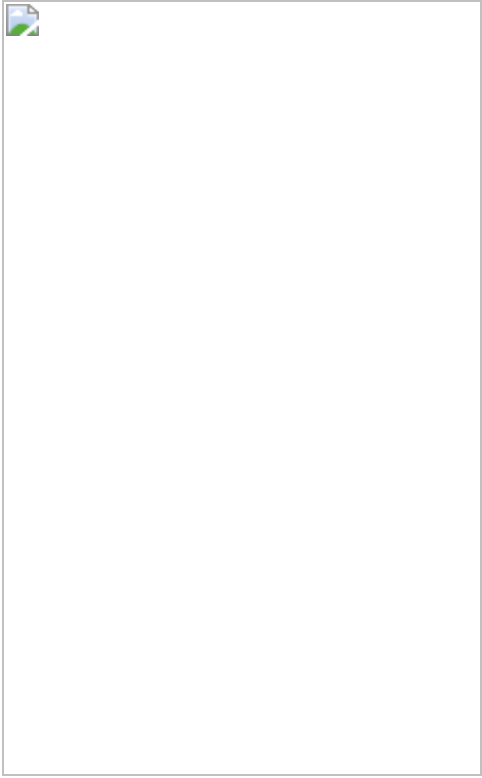
Create a conditional access policy in Azure AD, exclude the newly created group.



In Conditions, configure Client Apps and select both legacy authentication clients option.



In Grant, choose Block Access.



In Enable Policy, select 'On'.



Once this conditional access policy in place, unexpected accounts will not be able to log in using legacy authentication methods.