CrowdStrike Services Identifies Microsoft 365 Logging Inconsistencies

crowdstrike.com/blog/crowdstrike-services-identifies-logging-inconsistencies-in-microsoft-365/

Christopher Romano - Vaishnav Murthy

March 31, 2022

- Multiple investigations and testing by the CrowdStrike Services team identified inconsistencies in Azure AD sign-in logs that incorrectly showed successful logins via Internet Mail Access Protocol (IMAP) despite it being blocked.
- Investigators rely on these logs to determine threat actor activity in investigations that often involve legal and regulatory consequences for organizations.
- This blog includes recommendations that should be implemented to block legacy authentication in Microsoft 365 tenants to avoid a threat actor circumventing stronger controls such as multifactor authentication (MFA).

Background

As many organizations move to the cloud, CrowdStrike has noticed a significant increase in both opportunistic and targeted attacks against cloud resources, with a large number of these attacks targeting organizations' Microsoft 365 (M365) infrastructure, often specifically around their business email service, or Exchange Online. In multiple investigations, CrowdStrike has observed a logging inconsistency within the Azure AD sign-in events related to mailbox access using legacy authentication protocols within M365. This article highlights the inconsistency, shows how CrowdStrike was able to replicate it in a lab environment and provides recommendations on configuration settings to help organizations secure their M365 environment.

When investigating anomalous activity involving mailboxes in Exchange Online, CrowdStrike investigators look at a number of log sources, including the Unified Audit Log and Azure AD sign-in logs, to establish the scope of the activity. It is imperative for these log sources to accurately capture information, as they are relied on by investigators to determine threat actor activity in investigations that often involve legal and regulatory consequences for organizations.

Legacy Authentication Protocols

Internet Mail Access Protocol (IMAP) and Post Office Protocol (POP) are authentication protocols most widely used as part of legacy authentication to receive mail to mailboxes. These protocols result in downloading a mailbox’s contents locally to the client from where the authentication request was initiated. Hence, whenever these protocols are seen to be used in an investigation involving email compromise, an assumption is made that the entirety of the mailbox contents, which often include sensitive information, has been exfiltrated by the threat actor. Simple Mail Transfer Protocol (SMTP) is an authentication protocol used as part of legacy authentication to send mail from mailboxes. A threat actor will leverage a compromised account, permitting the SMTP legacy protocol to send massive amounts of spam or phishing emails to both internal and external users.

Tenant Configuration

In recent investigations, CrowdStrike has found a pattern of inaccurate logging in the Azure AD sign-in logs that seems to falsely indicate a mailbox sync via legacy authentication protocols (IMAP or POP). This pattern appears to manifest in M365 tenants that: do not have legacy authentication configured to be blocked via a conditional access policy (CAP); have POP and IMAP blocked at an individual mailbox level; and have the SMTP authentication protocol allowed at the mailbox level.

Inaccurate Azure AD Sign-in Logs

In Azure tenants with no CAP in place blocking legacy authentication, but with IMAP blocked at the Exchange Online mailbox level, CrowdStrike found that Azure AD sign-in logs showed successful logins via an IMAP client application despite it being blocked at the mailbox level. This logging pattern occurred when a third-party mail client, configured to use IMAP and SMTP, was used to authenticate into a mailbox. While the client was able to successfully send an email via SMTP, it was not able to download mail to the local system via IMAP due to the mailbox-level block in place. In other words, the Azure AD log entry showing a successful login via the IMAP protocol was **inaccurate**, as mail synchronization did not take place.

Incorrect Authentication Flow Documentation

If the documented flow was followed, the authentication attempt should have been blocked prior to reaching Azure AD, and thus should not have been picked up by the Azure AD sign-in logs. However, as we show in the proof of concept (POC) section below, the authentication attempt is still logged in Azure AD sign-in logs, despite supposedly being blocked before reaching Azure AD.

This pattern of logging is inconsistent with the documented authentication flow from Microsoft:

When it's blocked, Basic authentication in Exchange Online is blocked at the first pre-authentication step (Step 1 in the previous diagrams) before the request reaches Azure Active Directory or the on-premises IdP. The benefit of this approach is brute force or password spray attacks won't reach the IdP (which might trigger account lockouts due to incorrect login attempts).

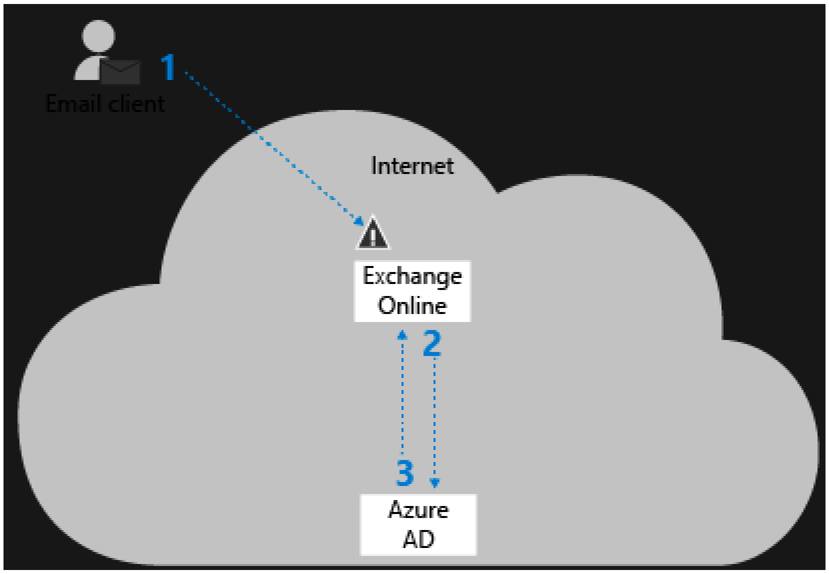
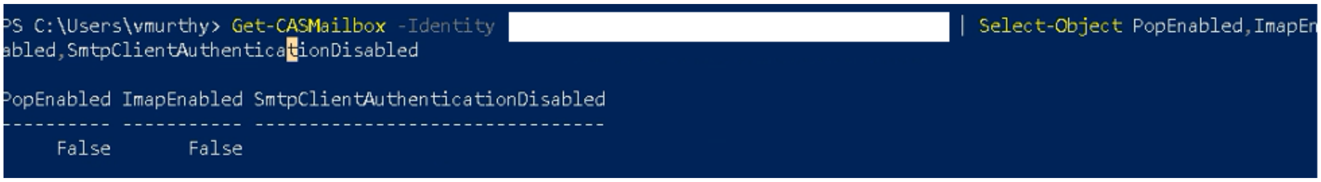


Figure 1. Source: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

Recreating the Logging Inconsistency

CrowdStrike set up a POC environment to demonstrate this logging inconsistency with a mailbox that had POP/IMAP disabled at the mailbox level, but SMTP authentication still allowed (see Figure 2).

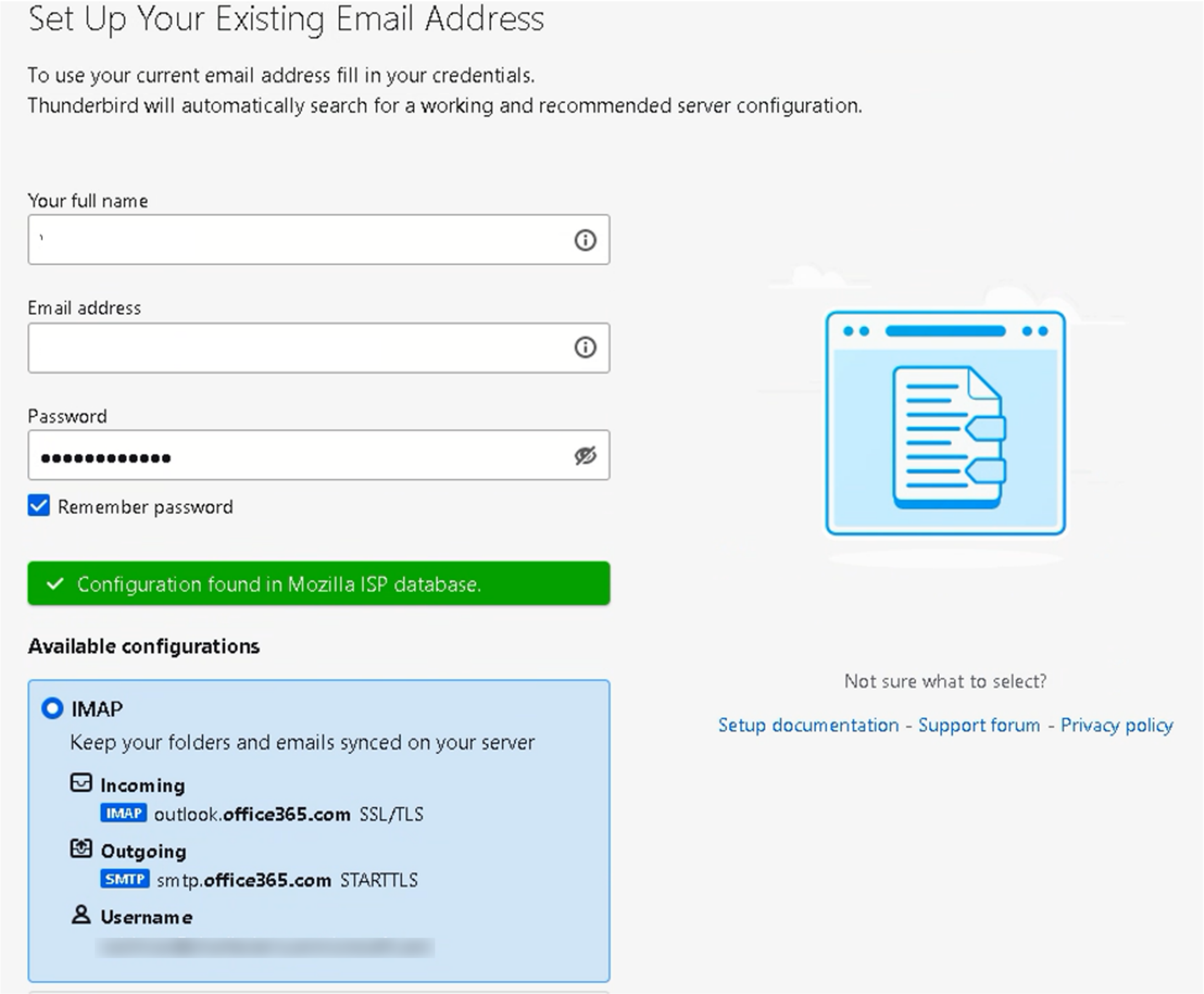


```
PS C:\Users\vmurthy> Get-CASMailbox -Identity [redacted] | Select-Object PopEnabled,ImapEn
abled,SmtpClientAuthenticationDisabled

PopEnabled ImapEnabled SmtpClientAuthenticationDisabled
---------- ----------- --------------------------------
     False       False
```

Figure 2 (Click to enlarge)

The POC environment did **not** have an Azure AD Conditional Access Policy that blocked legacy authentication. CrowdStrike used Mozilla Thunderbird as a third-party mail client to access the simulated victim's mailbox with IMAP as the selected protocol, as shown in the screenshot in Figure 3.



Set Up Your Existing Email Address

To use your current email address fill in your credentials.
Thunderbird will automatically search for a working and recommended server configuration.

Your full name: [redacted]

Email address:

Password: •••••••••••••

☑ Remember password

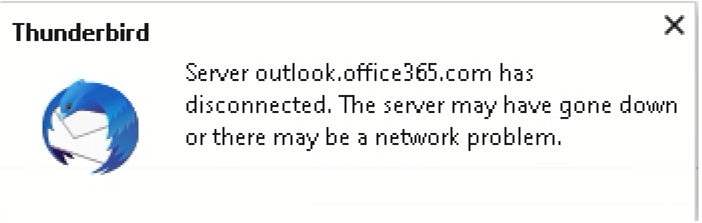
✓ Configuration found in Mozilla ISP database.

Available configurations

● IMAP
Keep your folders and emails synced on your server
Incoming
IMAP outlook.office365.com SSL/TLS
Outgoing
SMTP smtp.office365.com STARTTLS
Username
[redacted]

Figure 3

Authentication using the given credentials was successful, but mail was not allowed to be synced to the local client device, as seen in Figure 4.

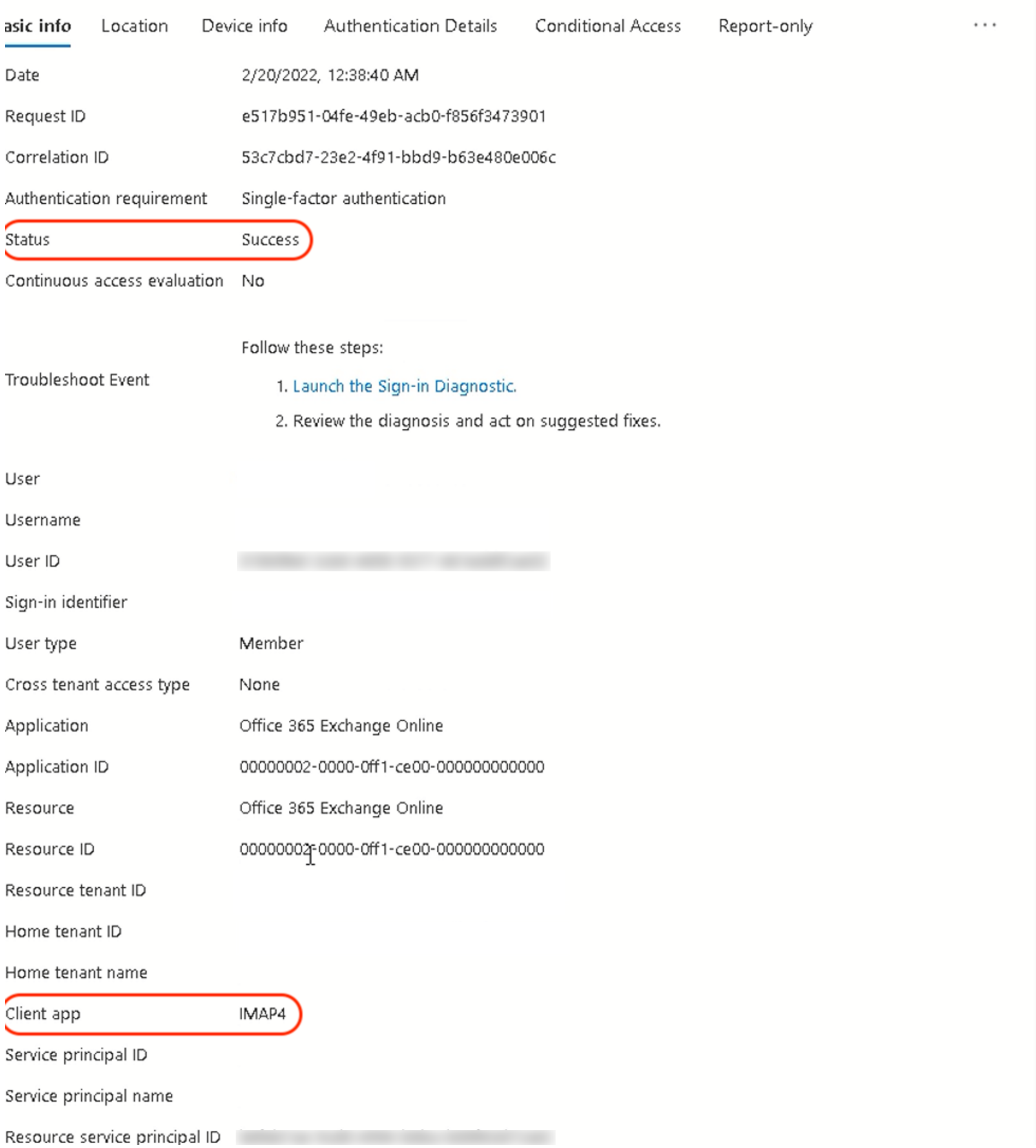


Thunderbird

Server outlook.office365.com has disconnected. The server may have gone down or there may be a network problem.

Figure 4

However, Azure AD sign-in logs showed successful authentication using IMAP, as shown in the screenshot below.



Date 2/20/2022, 12:38:40 AM

Request ID e517b951-04fe-49eb-acb0-f856f3473901

Correlation ID 53c7cbd7-23e2-4f91-bbd9-b63e480e006c

Authentication requirement Single-factor authentication

Status Success

Continuous access evaluation No

Troubleshoot Event Follow these steps:

1. Launch the Sign-in Diagnostic.
2. Review the diagnosis and act on suggested fixes.

User

Username

User ID [redacted]

Sign-in identifier

User type Member

Cross tenant access type None

Application Office 365 Exchange Online

Application ID 00000002-0000-0ff1-ce00-000000000000

Resource Office 365 Exchange Online

Resource ID 00000002-0000-0ff1-ce00-000000000000

Resource tenant ID

Home tenant ID

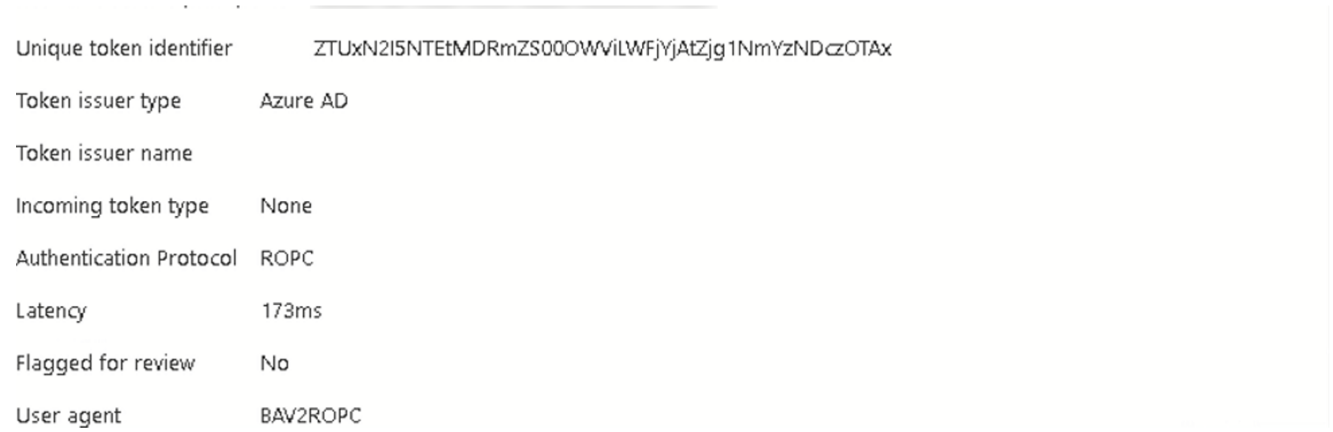
Home tenant name

Client app IMAP4

Service principal ID

Service principal name

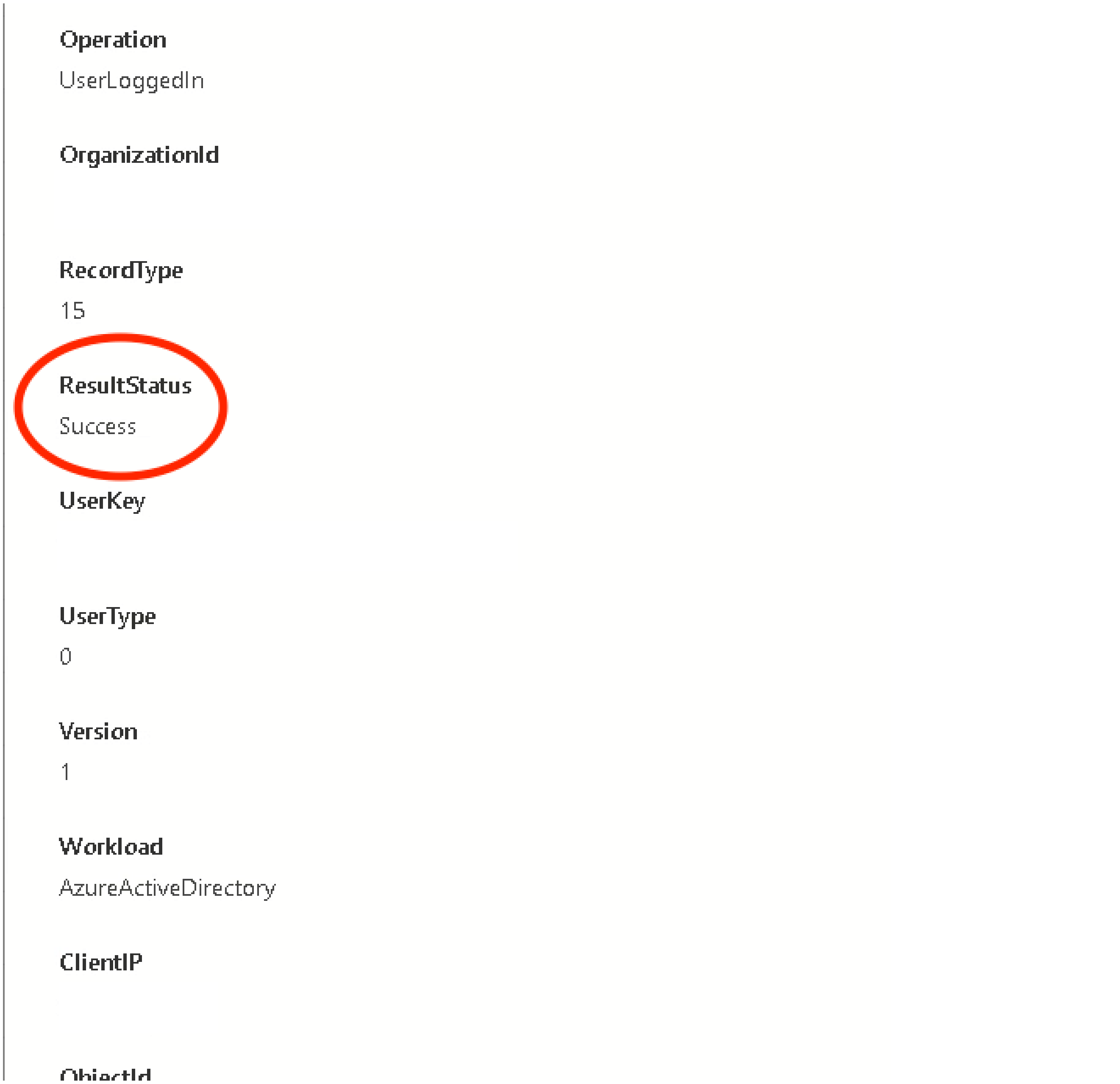
Resource service principal ID [redacted]



Unique token identifier	ZTUxN2I5NTEtMDRmZS00OWViLWFjYjAtZjg1NmYzNDczOTAx
Token issuer type	Azure AD
Token issuer name	
Incoming token type	None
Authentication Protocol	ROPC
Latency	173ms
Flagged for review	No
User agent	BAV2ROPC

Figure 5

The M365 Unified Audit Log also shows successful authentication via the BAV2ROPC user agent, indicating basic authentication was used (see Figure 6).



Operation

UserLoggedIn

OrganizationId

RecordType

15

ResultStatus

Success

UserKey

UserType

0

Version

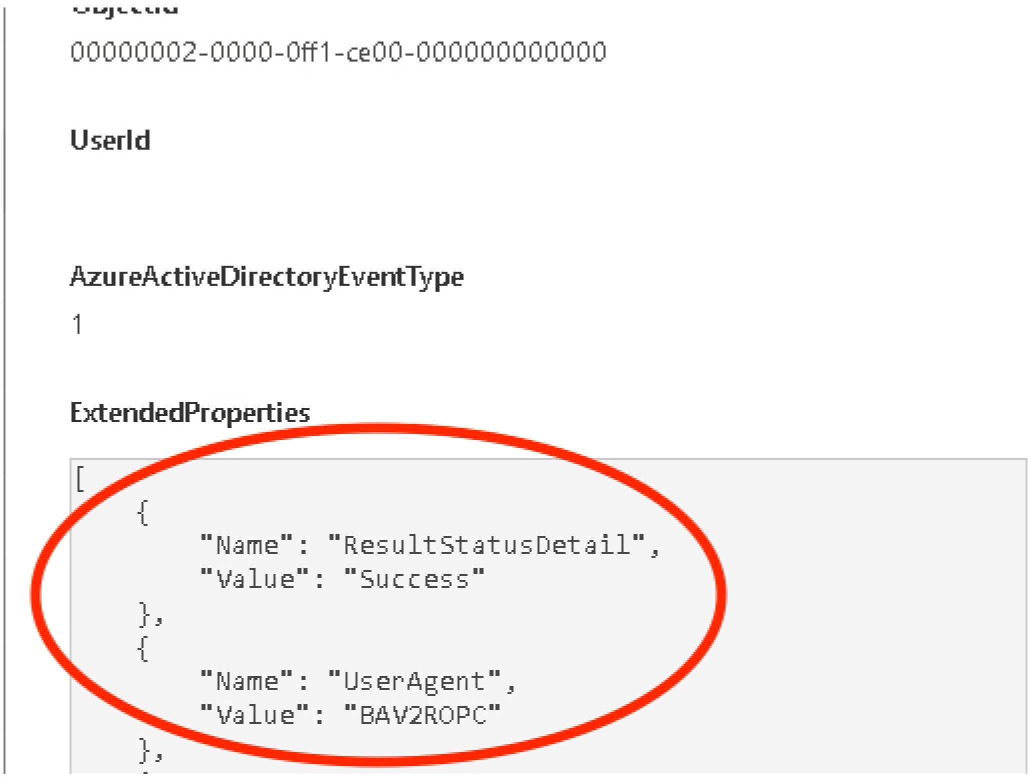
1

Workload

AzureActiveDirectory

ClientIP

ObjectId



ObjectId

00000002-0000-0ff1-ce00-000000000000

UserId

AzureActiveDirectoryEventType

1

ExtendedProperties

```
[
    {
        "Name": "ResultStatusDetail",
        "Value": "Success"
    },
    {
        "Name": "UserAgent",
        "Value": "BAV2ROPC"
    },
```

Figure 6

As shown in CrowdStrike’s POC, the IMAP protocol authentication attempt was logged as successful in the Azure AD sign-in log, but the victim’s mailbox was never successfully synchronized or downloaded to the client machine. This inconsistency could lead a victim organization to inaccurately conclude that the contents of the affected mailbox had been exfiltrated by a threat actor, a scenario that often has regulatory and legal implications.

Also of note, Microsoft will be disabling POP and IMAP authentication to Exchange Online beginning Oct. 1, 2022 per its announcement:

Effective October 1, 2022, we will begin to permanently disable Basic Authentication for Exchange Online in all Microsoft 365 tenants regardless of usage, except for SMTP Authentication.

Recommendations to Prevent Legacy Authentication

The following are recommendations to prevent the usage of legacy authentication protocols. CrowdStrike recommends these actions to minimize the risk of a threat actor exploiting the inherent weakness in legacy authentication that would allow them to gain access to a mailbox.

- Enable and enforce a conditional access policy blocking access that uses legacy authentication to all client applications. This block will ensure that authentication attempts to mailboxes using IMAP, POP or SMTP are blocked before reaching the mailbox.

- Ensure that basic authentication is disabled at the mailbox level, using the `Set-CASMailbox` PowerShell cmdlet at individual mailboxes, and tenant-wide using the `Set-AuthenticationPolicy` and `Set-TransportConfig` cmdlets. (See https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online)
- Enable MailItemsAccessed on all mailboxes. The `MailItemsAccessed` operation as part of Microsoft Advanced Auditing can assist investigators in validating whether a certain mailbox has been downloaded offline to a threat actor-controlled system. This operation covers authentication from both legacy and modern authentication protocols, and records both sync (downloading actions) and bind (viewing actions). (See: https://docs.microsoft.com/en-us/microsoft-365/compliance/mailitemsaccessed-forensics-investigations?view=M365-worldwide)

Conclusion

CrowdStrike was able to demonstrate that in Azure tenants where IMAP/POP was blocked at the Exchange Online mailbox level, but no CAPs were in place to block legacy authentication, SMTP authentication attempts were incorrectly logged as logins via IMAP. This logging pattern could lead to organizations erroneously concluding that the mailbox contents had been downloaded to a client device controlled by a malicious third party, when in fact the settings in place would have blocked any download attempt.

To ensure that threats arising from legacy authentication are mitigated, CrowdStrike recommends that organizations enable and enforce a CAP that blocks legacy authentication to all client applications; disable basic authentication at both the individual Exchange Online mailbox level as well as tenant-wide; and for better monitoring capabilities, enable the MailItemsAccessed operation on all Exchange Online mailboxes.

Additional Resources

- *Learn how the powerful CrowdStrike Falcon platform provides comprehensive protection across your organization, workers and data, wherever they are located.*
- *Visit our Industry Recognition and Technology Validation webpage to see what industry analysts are saying about CrowdStrike and the Falcon platform.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and see for yourself how true next-gen AV performs against today's most sophisticated threats.*