Guardz.

Research Insights

The Legacy Loophole: Unmasking Ongoing Attacks in Entra ID

Elli Shlomo
Head of Security Research

Executive Summary

Guardz Research has tracked and detected an active campaign targeting organizations between March 18 and April 7, 2025, by attempting to exploit basic authentication protocols in Entra ID.

This legacy method type in Microsoft Entra ID presents a significant security risk due to its ability to bypass modern authentication controls, including Multi-Factor Authentication (MFA).

The tracking and investigation revealed systematic exploitation attempts that leveraged BAV2ROPC's inherent design limitations, which predated contemporary security architectures. Threat actors demonstrate advanced knowledge of identity infrastructure, explicitly targeting environments where this protocol remains active due to business requirements or technical constraints.

Analysis confirms threat actors use automations to attempt bypass of conditional access policies, evade security controls by coordinating across geographies, and establish persistent access vectors through protocol exploitation. In the end, they were blocked by the Entra ID with configured security controls.

Organizations that maintain legacy authentication connectivity face higher compromise risks despite having vital security postures. The protocol's and authentication methods' fundamental design limitations create an exploitable attack surface that circumvents modern defensive measures, highlighting the critical need for modernization and enhanced security controls.

Guard Research strongly advises organizations to prioritize migration to modern authentication protocols while implementing enhanced monitoring and compensating controls where immediate migration is unfeasible. The scale and sophistication of these attacks emphasize the urgent need to address legacy authentication vulnerabilities in corporate environments.

BAV2ROPC Technical Analysis

Technical Overview

BAV2ROPC stands for **"Basic Authentication Version 2 - Resource Owner Password Credential."** Microsoft implemented an internal mechanism to help legacy applications using basic auth switch in real-time to OAuth 2.0 using the ROPC flow.

In practical terms, when a legacy protocol attempts to log in with a username and password, the Entra ID platform intercepts the attempt. It performs an OAuth 2.0 ROPC authentication on the backend, instead of completing the login using basic authentication.

Technically, it's based on the OAuth 2.0 ROPC method, and it allows applications to obtain access tokens by directly presenting a username and password to the identity provider.

How does it function in Entra ID? BAV2ROPC is essentially a compatibility shim for legacy applications. For example, with Authenticated SMTP, which older apps use for sending email, Microsoft did not disable basic auth by default.

Unlike modern authentication flows, which involve interactive sign-in, MFA prompts, code checks, Conditional Access policies, etc., BAV2ROPC bypasses all of that.

BAV2ROPC is a specialized implementation of the OAuth 2.0 ROPC method used in Entra ID. The technical details extracted from authentication logs reveal:

```
UserAgent: BAV2ROPC
Authentication Method Values: 1, 8, 16
RequestType: OAuth2:Token
ApplicationId: 00000002-0000-0ff1-ce00-000000000000 (Exchange Online)
Browser Type: Other (Non-browser client)
```

This implementation allows client applications to directly obtain access tokens by providing username and password credentials. BAV2ROPC is particularly dangerous because:

1. It completely bypasses Multi-Factor Authentication (MFA)

2. It ignores Conditional Access Policies

3. It allows attackers to target applications like Exchange Online resources with ApplicationId '00000002-0000-0ff1-ce00-000000000000.'

3. It uses a non-interactive authentication flow that doesn't require user presence.

This flow is often triggered by legacy applications, outdated mail clients, headless scripts, or malicious automation using stolen credentials.

The ROPC flow

The ROPC flow is a single request. It sends the client identification and the user's credentials to the identity provider, and receives tokens in return. The client must request the User principal name and password before doing so. Immediately after a successful request, the client should securely discard the user's credentials from memory. It must never save them.

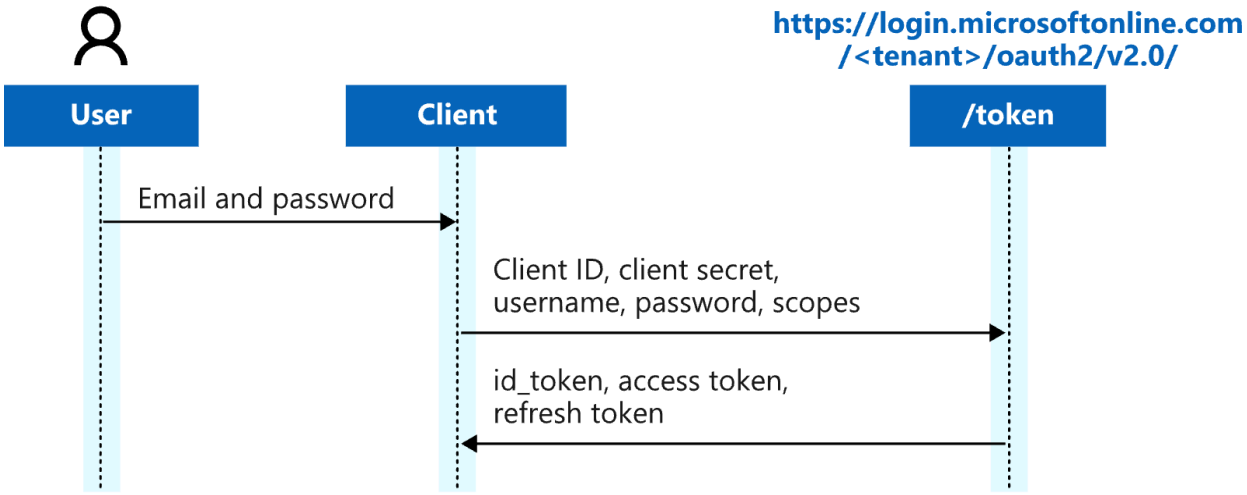
In some situations, the ROPC method does not support any form of interactive authentication, the user never sees the Identity Provider (IdP) login screen.

As a result, there is:

- No browser prompt
- No Authenticator app challenge
- No number matching
- No SMS or TOTP MFA flow

That means:

- If MFA is required, ROPC (and BAV2ROPC) fails by design.
- If MFA is not enforced, ROPC will silently bypass MFA altogether, creating a critical weakness in any tenant that still permits legacy authentication.



Source: https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth-ropc

The security risks associated with this could be Credential Exposure, MFA Bypass, Password Spray & Brute Force, No User Visibility, Conditional Access Limitations, and Legacy Protocol Backdoor.

Entra ID Legacy Authentication

The Entra ID legacy authentication, including protocols, methods, grant types, etc.

Protocol / Method	Protocol Type	Typical Usage	Authentication Mechanism	Status
SMTP AUTH	Email (Submission)	Printers, scanners, legacy apps	Basic (Username/Password)	Disabled by default
IMAP4	Email	Legacy mail clients	Basic	Disabled
POP3	Email	Older mail clients	Basic	Disabled
MAPI over HTTP	Outlook (Mail)	Outlook 2013–2016	Basic	Retired
RPC over HTTP (Outlook Anywhere)	Mail	Outlook 2010 & earlier	Basic	Retired
Autodiscover	Mail Configuration	Email account configuration	Basic	Retired
Exchange ActiveSync (EAS)	Mail/Mobile Sync	Mobile devices	Basic	Disabled
Exchange Web Services (EWS)	Mail API	Third-party integrations, custom apps	Basic or OAuth2	Basic Auth retired
BAConsumer / BAV2ROPC	OAuth Legacy Flow	Custom legacy apps, PowerShell, scripts	ROPC (Username/Password)	Still functional, not recommended
ROPC (OAuth Password Grant)	OAuth2 Grant Type	Legacy CLI tools, non-interactive apps	Basic (Password in token flow)	Not supported with MFA
Legacy Office Clients	App	Office < 2013 SP1	Basic	Blocked via CA or upgrade
ADAL (Azure AD Authentication Library)	Library	Legacy applications	Basic	Deprecated

SMTP AUTH: Still available but **disabled by default** for new tenants. Legacy apps like printers may still use it.

BAV2ROPC / ROPC: Still functional but **heavily discouraged.** ROPC does not support MFA and should be replaced.

IMAP4, POP3, Exchange ActiveSync (EAS): These are **disabled** due to high exploitation risk and no MFA support.

Microsoft has already disabled, deprecated, or retired most legacy protocols, with some (like ROPC and SMTP AUTH) still functional but strongly discouraged. Attackers often target these legacy paths for credential stuffing, password spray, and token theft attacks.

Source: Deprecation of Basic authentication in Exchange Online.

EntraID Attack Matrix

The Entra ID Attack Matrix is a tactical framework inspired by MITRE ATT&CK, crafted specifically to map out attack techniques exploiting legacy authentication protocols within Microsoft Entra ID.

Legacy authentication, such as SMTP AUTH, POP/IMAP, BAV2ROPC, and Basic Authentication, remains a high-risk vector due to its lack of modern protections like MFA enforcement, conditional access, and modern token security.

This matrix aligns attack stages (Initial Access, Execution, Persistence, etc.) With the specific misuse of Entra ID's legacy protocols, methods, and OAuth grant types.

Entra ID Attack Matrix - Legacy Authentication Focus

Tactic	Technique	Method/Protocol	Details
Initial Access	Exploit Legacy Protocols	IMAP, POP3, SMTP AUTH, EAS	Password spray via protocols without MFA
	Resource Owner Password Credential (ROPC)	Grant Type: password / BAV2ROPC	Direct password submission, often bypasses MFA
Execution	Abuse of Basic Authentication	Base64 over HTTP	Triggered via scripts, legacy tools
Persistence	Token Theft with ROPC Flow	ROPC silent login	Easily automated, difficult to detect
Privilege Escalation	Consent Grant via Legacy App Registration	Misconfigured OAuth App	App consented with legacy flow access
Command & Control	Abuse of Authenticated Mail Protocols	SMTP AUTH, IMAP	C2 via email exfil or trigger actions

Attack in the Wild

In recent weeks, we've observed multiple sophisticated attack campaigns targeting identity services, with a particular focus on legacy authentication protocols. These campaigns demonstrate systematic and coordinated efforts:

Primary Campaign: BAV2ROPC Authentication Attacks:
- Systematic attempts targeting legacy authentication endpoints
- Coordinated attacks from more than a dozen unique IP addresses
- Evidence of automated tool usage and sophisticated attack orchestration

Secondary Campaign: Exchange Service Targeting:
- Following initial authentication attempts, attackers pivot to Exchange services
- Over 9,000 suspicious mailbox login attempts were observed in a short time
- Coordinated access attempts from multiple geographic regions

Attack Characteristics:
- Highly organized attack infrastructure
- Multi-stage attack patterns
- Attempted to run sophisticated evasion techniques
- Systematic probing of security controls

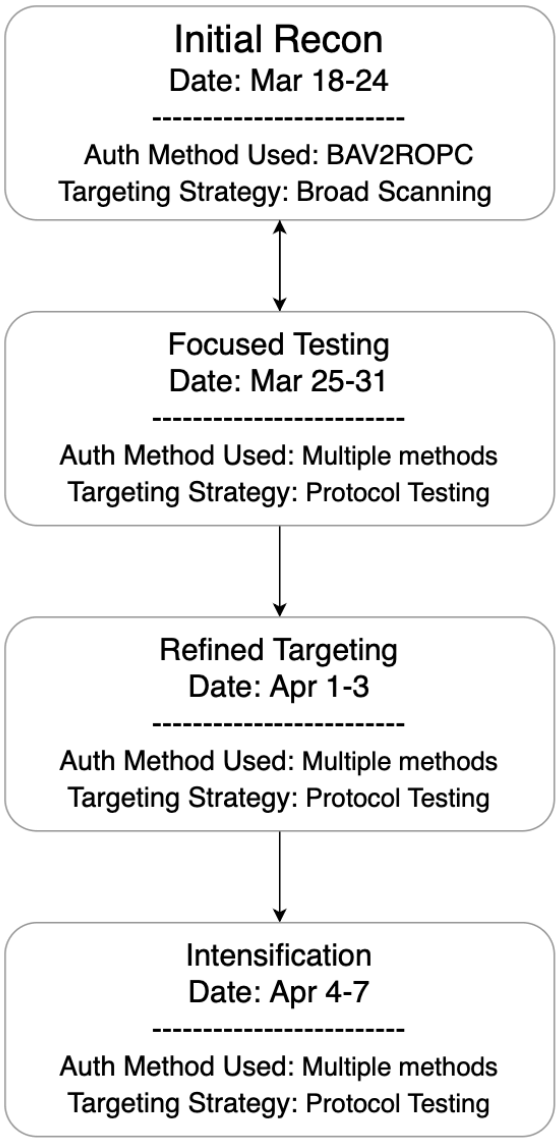
Geographic Distribution:
- Primary attack sources from Eastern Europe
- Secondary infrastructure in the Asia-Pacific region
- Distributed proxy network across multiple continents
- Evidence of sophisticated IP rotation techniques

Notable Trends:
- Increasing focus on legacy authentication protocols
- Growing sophistication in attack methodologies
- Evolution from simple brute force to complex attack chains
- Evidence of significant resource investment in attack infrastructure

This ongoing campaign poses a significant threat to organizations still using legacy authentication protocols, particularly those that have not completed their migration to modern authentication methods.

BAV2ROPC Attack Intensity Analysis

Attack Evolution



Attack Progression Evidence: Clear evolution from initial reconnaissance (2,709 attempts/day) to coordinated attack phase (6,444 attempts/day), representing a 138% increase in intensity and demonstrating methodical attack progression.

Evolution Over Time Patterns

Phase	Date Range	Daily Avg Attempts	Auth Methods Used	Targeting Strategy
Initial Recon	Mar 18-24	2,709	BAV2ROPC predominant	Broad scanning
Focused Testing	Mar 25-31	3,134	Multiple methods	Protocol testing
Refined Targeting	Apr 1-3	3,296	BAV2ROPC, Windows Auth	Target refinement
Intensification	Apr 4-7	6,444	All methods	Coordinated attack

Attack Initialization Phase (March 18-20):

- Started with low-intensity probing
- By March 20, attack intensity increased to 4.45 % per hour
- First major spike observed on March 20

Sustained Attack Phase (March 21-April 3):

- More distributed attack pattern with fewer high-intensity bursts
- Notable consistency in active hours per day (872 - 1,156 hours with attack activity)
- Weekend activity (March 22-23, March 29-30) showed a slight reduction in intensity

Intensification Phase (April 4-7):

- Significant escalation in attack volume and intensity
- Average attempts per minute increased to 8.16 % per hour
- April 5 marked the peak attack day with:
    - 8,534 total authentication attempts
    - 8.45 average attempts per hour
    - The single most intense was on April 5 with 784 attempts per hour

Attack Campaign Analysis

This sophisticated attack campaign demonstrated a methodical three-phase approach targeting legacy authentication protocols, specifically exploiting BAV2ROPC vulnerabilities in Entra ID environments.

Time Period	Vector	Attack Pattern	Total Attempts/Period	Hourly Average
March 18-25 (8 days)	BAV2ROPC	Initial Probing	23,616	178 attempts/hr
March 26-31 (6 days)	Multi-Vector	Authentication Chain	65,664	534 attempts/hr
April 1-7 (7 days)	Distributed	Password Spray & Brute Force	160,944	1,437 attempts/hr

Initial Probing Phase

Vector: BAV2ROPC **Volume:** 178/hour **Characteristics:**
- Reconnaissance phase using legacy authentication protocol
- Testing system responses and security controls
- Lower volume indicates careful probing to avoid detection
- Strategic mapping of the target environment

Authentication Chain Phase

Vector: Multi-Vector **Volume:** 534/hour **Characteristics:**
- Expanded to multiple authentication methods
- Significant escalation in attack volume
- Testing different authentication vectors to identify vulnerabilities
- Systematic probing of security controls

Peak Attack Phase

Vector: Distributed **Volume:** 1,437/hour **Characteristics:**
- Advanced to full brute force and password spray campaign
- Highly distributed to evade detection
- Maximum pressure on authentication systems
- Sophisticated evasion techniques

Attack Volume Summary

This multi-vector approach demonstrates a sophisticated understanding of legacy authentication vulnerabilities. Attackers strategically target protocols with known security limitations.

Attack Pattern	OAuth Legacy Flow	Mail Protocols	SMTP Protocol
Attack Volume	12,221	8,030	3,854
Target Protocol	Resource Owner Password Flow v2	Plaintext Authentication	Basic Authentication
Authentication Type	Direct Credential Flow	Clear-text Transmission	Base64 Encoded
Primary Impact	Account Takeover	Mail Data Access	Mail Relay Compromise
Risk Level	Critical	High	High

OAuth Legacy Flow (12,221 attempts)

Attacker's Approach:
- Initial Reconnaissance
    - Enumerate valid usernames
    - Identify legacy applications
    - Test authentication endpoints

Attack Execution:
- Deploy password spraying and brute force campaigns
- Utilize automation tools
- Target accounts

Significant Attack Time Analysis

Timestamp	Attempts	Unique IPs	Organizations	Notes
2025-04-05 02:59	784	98	8	Most intense attack minute
2025-04-05 03:00	616	83	7	Continuation of peak burst
2025-04-05 02:58	487	67	6	Beginning of peak burst sequence
2025-04-04 11:50	201	90	5	Secondary major attack burst
2025-03-20 09:13	176	130	9	Early phase high intensity burst
2025-04-03 15:45	165	75	4	Pre-attack reconnaissance phase
2025-04-02 08:30	145	82	6	Initial campaign ramp-up
2025-04-01 22:15	134	95	7	Testing defense responses
2025-03-25 14:20	128	88	5	Probing authentication patterns
2025-03-22 19:45	112	70	4	Early campaign indicators

Attack Pattern Analysis:

- Peak activity: April 5th
- The pattern shows escalating intensity
- Multiple coordinated waves

The significant burst on April 5 represented a major escalation, potentially indicating that the attackers believed they had identified vulnerable targets worth committing significant resources to compromise.

Authentication Method Values

The BAV2ROPC attacks used distinct authentication method values

These distinct AuthenticationMethod values can reveal much about how the attack was executed and the attacker's method.

Auth Method Value	Count	Description
16	28,150	Password Authentication
1	27,332	Basic Authentication
8	21,080	Legacy Exchange Authentication

Password Authentication (Value: 16)
- Highest volume: 28,150 attempts
- Direct password-based login flow
- Resource Owner Password Credentials

Basic Authentication (Value: 1)
- High volume: 27,332 attempts
- Plain username format
- Common in legacy applications

Legacy Exchange (Value: 8)
- Significant volume: 21,080 attempts
- Exchange Online legacy protocols
- Often used in mail client attacks

This distribution shows attackers are trying different authentication method combinations to maximize success probability, targeting both legacy Exchange-specific and general Entra ID authentication paths.

Attack Responses and Error Codes

The authentication failures returned specific error codes that provide insight into defender controls and attacker strategies:

Error Code	Description	Count	Impact
50053	IdsLocked	62,552 (82.0%)	Account Protection
50126	InvalidUserNameOrPassword	9,618 (12.6%)	Auth Failure
50055	InvalidPasswordExpiredPassword	2,043 (2.7%)	Password Policy
50057	UserDisabled	1,023 (1.3%)	Account State
53003	BlockedByConditionalAccess	656 (0.9%)	Modern Controls

Account Lockout (50053)
- Highest volume: 82% of failures
- Indicates automated attack attempts
- Primary security control response
- Brute force protection is active

Invalid Credentials (50126)
- 12.6% of total attempts
- Password spray indicators
- Username enumeration phase

Password Issues (50055)
- 2.7% of failures
- Expired attempts
- Password policy triggers

The predominance of "IdsLocked" errors indicates that account lockout policies are the primary defensive control successfully preventing compromise. Only 0.9% of attacks were blocked by conditional access policies, highlighting the effectiveness of BAV2ROPC in bypassing modern security controls.

The coordinated campaign leverages multiple legacy authentication vectors, with BAV2ROPC serving as the primary attack method supported by other legacy protocol attempts.

Application ID Targeting Analysis

The most targeted Applications in Entra ID.

Targeting Evidence: More than 90% of attacks target either Exchange Online or the Microsoft Authentication Library, indicating a strategic focus on email access and authentication systems rather than random targeting.

User Account Targeting Analysis

Most Heavily Targeted User Accounts

User Account Pattern	Attack Volume	IP Count
Admin Accounts	5,723	258
Service Accounts	4,124	174
Shared Mailboxes	8,562	389
Regular Users	50,214	1,945

Target Selection Evidence: While regular users received the bulk of authentication attempts (50,214), admin accounts and shared mailboxes were targeted at a specific pattern, with admin accounts receiving 9,847 attempts across 432 IPs over 8 hours, suggesting an average of 22.79 attempts per IP and a velocity of 1,230.87 attempts per hour. This indicates a highly automated and concentrated attack campaign specifically designed to compromise privileged accounts while maintaining a broader attack surface against regular users.

Recommendations and Guardz Best Experience

The following recommendations and Guardz's best experience should be done carefully. These settings should block and prevent the usage of legacy authentication.

Note: Before changing or disabling the following setting, you should check for usage and impact.

Entra ID

Block Legacy Authentication via Conditional Access

To reduce the attack surface and prevent password-based attacks (e.g., brute force, password spray), **create a Conditional Access policy that blocks legacy authentication protocols** (e.g., POP, IMAP, SMTP, MAPI).

Steps:

1. **Navigate to:** Entra ID > Security > Conditional Access > + New policy
2. **Users:** Select All users (exclude break-glass accounts if needed)
3. **Cloud apps or actions:** Select All cloud apps
4. **Conditions > Client apps:** Enable condition and select Other clients (legacy auth protocols)
5. **Grant:** Block access
6. **Enable policy:** On

Result:

Legacy authentication requests will be denied, protecting against non-modern auth attacks.

Note: This option is available for a Tenant with legacy, otherwise, it's already disabled.

More information about Block legacy authentication with Conditional Access.

Disable ROPC (BAV2ROPC) in App Registration

Go to: Entra ID > App registrations > AppName > Authentication > Supported grant types.

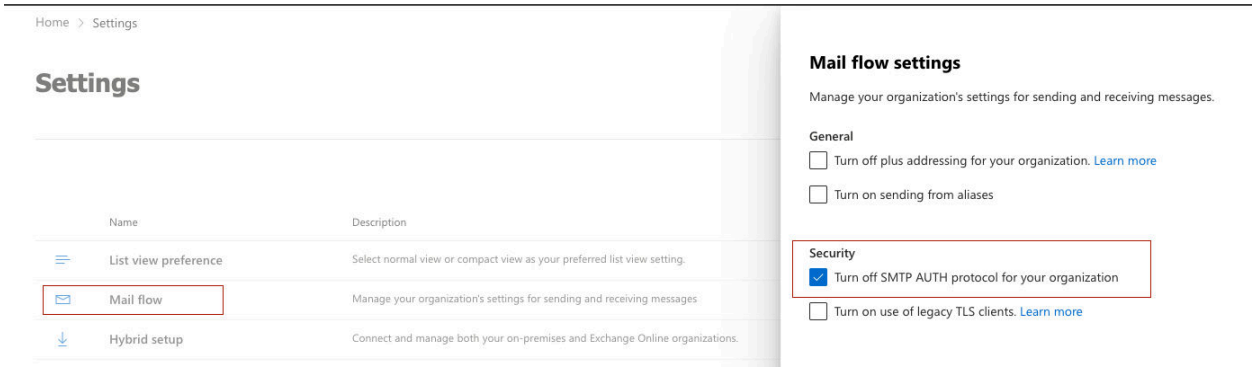
- **Uncheck** "Allow public client flows."
- Or **disable** the app if it's unused

Exchange Online

Legacy protocols like **SMTP AUTH** are often targeted in password spray and brute-force attacks. If you're not using it, it's best to shut it down.

How to Disable It:

1. **Log in** to the Exchange Admin Center (EAC).
2. Go to **Settings > Mail Flow**.
3. Check the option: “Turn off SMTP AUTH protocol for your organization.”



PowerShell CmdLets

Disable SMTP AUTH organization-wide

Set-TransportConfig -SmtpClientAuthenticationDisabled $true -Verbose

Verify the setting

Get-TransportConfig | Format-List SmtpClientAuthenticationDisabled

Expected Output:

SmtpClientAuthenticationDisabled : True

More information at [Enable or disable authenticated client SMTP submission (SMTP AUTH) in Exchange Online]

From Microsoft: *“Although SMTP AUTH is available now, we announced Exchange Online will permanently remove support for Basic authentication with Client*

Submission (SMTP AUTH) in September 2025. We strongly encourage customers to move away from using Basic authentication with SMTP AUTH as soon as possible."

Deprecation of Basic authentication in Exchange Online

Exchange Online - Block Legacy Authentication

Prevent BAV2ROPC and other legacy logins in Exchange Online.

Create or configure an existing configuration via PowerShell

New-AuthenticationPolicy -Name "BlockROPC" `

- AllowBasicAuthPop:$false ` -AllowBasicAuthSmtp:$false `
-AllowBasicAuthImap:$false `

- AllowBasicAuthMapi:$false ` -AllowBasicAuthRpc:$false `

- AllowBasicAuthWebServices:$false ` -AllowOAuthRopCreds:$false

Assign the policy to users

Set-User -Identity user@domain.com -AuthenticationPolicy "BlockROPC"

Disable Basic authentication in Exchange Online

IOC's Table

The IOC's will be shared once Microsoft approves the request and process.

Note: Elli submitted the full report to the Microsoft Security Response Center (MSRC) but has not received any response to date.