# Ongoing Microsoft 365 password spray and OpenBullet / SilverBullet credential stuffing

A low-and-slow password spray against Microsoft 365 / Entra ID accounts has been running since at least October 1, 2026, and is still active. Fluency sees it in 42 of 104 monitored Microsoft 365 tenants.

Fluency Corp, Inc. · Security advisory · November 1, 2026 · Status: campaign active

| 42/104 | 2,173 | ~3,400 | 0 |
|---|---|---|---|
| MONITORED M365 TENANTS REACHED | IP ADDRESSES IN ONE TENANT, 30 DAYS | ATTEMPTS IN THE LARGEST TENANT, 30 DAYS | SUCCESSFUL ATTACKER SIGN-INS FOUND |

## Summary

HOW IT WORKS

The attacker tries one password per account from a fresh IP address almost every time, so per-IP lockouts and thresholds never trigger. Part of the traffic comes from OpenBullet / SilverBullet credential-stuffing configs.

WHAT WE FOUND

In October the attacker entered the **correct password** for accounts in several customer tenants. MFA or Entra Smart Lockout was the only thing that stopped each of those sign-ins. We found no successful attacker sign-in. On October 31 the attacker was still retrying known passwords from new countries and new clients, so a password that is not reset stays in use.

WHAT FLUENCY CHANGED

On October 30 and 31 we released two new detections and two updated ones that alert on a correct password from this campaign, including on tenants without Microsoft Entra ID P2 (Identity Protection). The newest, 102189, does not depend on the attacker's user agent.

WHAT YOU SHOULD DO NOW

**Reset and revoke every account where the attacker had the correct password**

Any such account must have its password reset and its sessions revoked, even if the sign-in failed. If we found such an account in your tenant, we will contact you directly.

§ 1

# What we observed

The spray targets interactive browser sign-ins and rotates through thousands of IP addresses, so each address appears only once or twice.

| MEASURE | VALUE |
|---|---|
| **First seen** | October 1, 2026 (earlier activity is likely; it predates our window) |
| **Last seen** | October 31, 2026, still active |
| **Tenants reached** | 42 of 104 monitored Microsoft 365 tenants |
| **Attempts in the largest tenant** | about 3,400 in 30 days |
| **IP addresses in one tenant, 30 days** | 2,173; 92% used once, none more than 5 times |
| **Accounts per IP address** | at most 4 |
| **Target application** | One Outlook Web (Office 365 Exchange Online), browser sign-in |
| **Successful attacker sign-ins found** | none |

About half of the attempts end in Entra Smart Lockout (error 50053); the rest are wrong passwords (50126). The rare correct passwords ended in an MFA prompt the attacker could not answer (50074 / 50076) or in Smart Lockout.

The same accounts are also hit by other toolsets that use different clients: Azure CLI and Azure AD PowerShell over the legacy password (ROPC) flow, SMTP basic authentication, Go and Python HTTP clients. One of them used hosting infrastructure (FranTech, AS53667) also seen in the Huntress LSHIY campaign. We treat them as one wave of credential attacks against the same accounts.

> UPDATE · OCTOBER 31
> On accounts whose password the attacker already had, the correct password kept coming back, now from networks in Bangladesh, India, Iraq, Thailand and the US. The clients were Azure CLI with the spray user agent, SMTP basic authentication ( `BAV2ROPC` ) and a Go client on the Azure Portal. Each attempt ended in Smart Lockout. The attacker is reusing passwords it holds, from any client, until they are reset.

Not every burst of failures is the spray. A phone or mail client with an old saved password fails many times an hour, but always with the wrong password, from the user's own home and mobile networks. The spray presents the correct password, from networks the user never uses.

§ 2

# Indicators

The most reliable indicator is the client, not the network: one fixed user agent across every attempt.

| TYPE | INDICATOR | NOTES |
|---|---|---|
| **User agent** | `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36` | Exactly this, with nothing after `537.36`. Real browsers continue with `(KHTML, like Gecko) Chrome/... Safari/...`. No successful sign-in from this string in any monitored tenant. |
| **User agent** | `<RndUA>` | The literal text, angle brackets included: the unfilled random-user-agent placeholder of an OpenBullet / SilverBullet credential-stuffing config. Seen against the same accounts from 2026-10-03, on One Office (OfficeHome), one or two attempts per IP. No browser sends it. |
| **Application** | One Outlook Web (app id `9199bf20-a13f-4107-85dc-02114787ef48`) | Interactive browser sign-in |
| **Result codes** | 50126, 50053, 50074 / 50076 | Wrong password, Smart Lockout, MFA required |
| **Networks (ASN)** | 6079, 26658, 45102 (Alibaba), 36352 (ColoCrossing), 2914 (NTT), 16509 and 14618 (Amazon), 132203 (Tencent), 16276 (OVH), 174 (Cogent), 63949, 3257, 7843, 979, 7459 | Top 15 by attempts. Almost all geolocate to the US. |
| **Example IP addresses** | 104.128.116.147, 104.128.116.166, 51.38.192.143 | Each was used for a correct-password attempt. IPs rotate per attempt, so blocking them has little effect. |
| **Related toolsets** | Azure CLI or Azure AD PowerShell over ROPC; `BAV2ROPC` (SMTP); `Go-http-client`; `python aiohttp`; FranTech AS53667 | Same accounts, other clients |

Individual IP addresses are listed for investigation, not blocking: they change on almost every attempt.

§ 3

# Why it slips past common defenses

The campaign is built to stay under every per-IP and per-account threshold, and most tenants lack the licence for Microsoft's own detection.

IP ROTATION DEFEATS IP THRESHOLDS

With one or two attempts per address, “many failures from one IP” rules and IP block lists never trigger.

FEW ATTEMPTS PER ACCOUNT

Accounts see a handful of tries spread over days, below brute-force thresholds.

#### IDENTITY PROTECTION NEEDS ENTRA ID P2

Microsoft's sign-in risk scoring and its Password Spray alert only exist for P2-licensed users; elsewhere the risk field reads `hidden`. In P2 tenants it flagged the correct-password sign-ins as high risk. In the other tenants nothing flagged them.

#### SMART LOCKOUT WAS OFTEN THE LAST BARRIER

Several correct passwords ended in a lockout (50053), not in MFA. Once the lockout clears, the password still works. For legacy flows such as ROPC and SMTP basic authentication, MFA may not apply at all.

#### A FAILED SIGN-IN STILL MEANS A KNOWN PASSWORD

“Correct password” followed by an MFA prompt or a lockout is easy to dismiss as a failed attempt. The attacker now knows the password and can retry it later or elsewhere. Spray tools read these error codes as a valid password (TrustedSec).

§ 4

## Fluency detections

Four rules released on October 30 and 31, 2026 alert on a correct password from this campaign. They are live on every monitored tenant and apply to sign-ins from then on, not retroactively.

| RULE | STATUS | SEVERITY | LICENCE NEEDED | ALERTS WHEN |
|---|---|---|---|---|
| **102189** `EntraID_Correct_Password_Lockout_New_Network` | NEW October 31 | HIGH | Any | Smart Lockout refuses a sign-in that presented the correct password, from a network (ASN) the user has had no successful sign-in from in 30 days. Works for any client or user agent. Not raised for Microsoft's network or the tenant's trusted named locations; once per user and network a day. Its context rule 102188 `EntraID_Password_Lockout` records the lockouts and raises nothing itself. |
| **102187** `EntraID_Spray_Client_Correct_Password` | NEW | HIGH | Any | A sign-in from either spray user agent (see Indicators) presents the correct password, whatever the result: success, MFA required, locked out or blocked. |
| **102127** `EntraID_Valid_Password_Blocked` | UPDATED | MEDIUM | Any for blocks; P2 for the new MFA case | A correct password is stopped by Conditional Access. Now also covers a correct password held at an MFA requirement it did not meet (50074 with Conditional Access failure) on a sign-in rated low, medium or high risk. |
| **102128** `EntraID_High_Risk_SignIn` | UPDATED | HIGH | P2 | Entra rates a sign-in high risk. It no longer raises a second alert when Entra re-sends the same sign-in after the risk is remediated, dismissed or confirmed safe. |

## Existing rules that also apply

102124 · ENTRAID_BRUTE_FORCE_USER

More than 15 failed sign-ins for one user within an hour. A device with an old saved password can also set it off; those failures are wrong passwords from the user's own networks.

102185 · ENTRAID_SIGNIN_AFTER_BLOCK

A successful sign-in shortly after a high-risk block that presented the correct password, from a different IP address.

MICROSOFT DEFENDER ALERTS

Identity Protection's Password Spray and risky sign-in alerts (P2 tenants), ingested as behavior events.

### How the rules were tested

Each rule was replayed on Fluency's rule test site; 102187 was checked against 30 days of sign-ins in 104 tenants, where its user agent never had a successful sign-in. For 102189, 30 days of sign-ins in 52 tenants gave about 60 alerts a month across all tenants, almost all of them confirmed attacker sign-ins. In its first day live it raised 6 alerts, all on accounts already known to be compromised, and caught two sign-ins 102187 cannot see because they did not use the spray user agent.

§ 5

# Recommended actions

Treat every correct-password attempt as a compromised password, then close the legacy paths that let a sprayer test passwords without MFA.

01 **Reset and revoke.** For any account with a “Correct password” sign-in you do not recognise, reset the password and revoke its sessions (Entra admin center → Users → Revoke sessions), even if the sign-in failed.

02 **Review the account.** Check for new MFA methods, newly registered devices, app consents, inbox rules and mail forwarding since the first correct-password attempt.

03 **Block legacy authentication.** Use Conditional Access to block legacy authentication, and turn off SMTP AUTH for mailboxes that do not need it.

04 **Restrict admin and scripting clients.** Block Azure CLI, Azure AD PowerShell and the ROPC password flow for users who are not administrators.

05 **Require MFA for every user and every app.** Review report-only policies, and named-location exclusions that could exempt sign-ins from MFA.

06 **Check your MFA coverage.** Accounts without a registered MFA method are the ones a correct password can open.

07 **Consider Entra ID P2** for privileged and high-value users: it adds sign-in risk scoring and risk-based Conditional Access.

Blocking the attacker's IP addresses or ASNs is of little use: the campaign moves to a new address on almost every attempt.

§ 6

## How to check your tenant

Two questions matter: is the spray reaching you, and did it ever present a correct password. Fluency customers can ask us to run both; the queries below are for Microsoft Sentinel or Log Analytics (`SigninLogs`).

**Is the spray client reaching your tenant?**

```
SigninLogs
| where TimeGenerated > ago(30d)
| where UserAgent in ("Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36", "<RndUA>")
| summarize Attempts = count(), Users = dcount(UserPrincipalName), IPs = dcount(IPAddress) by UserAgent,
ResultType
```

**Which accounts had a correct password on a sign-in that did not succeed, from any client?**

```
SigninLogs
| where TimeGenerated > ago(30d)
| where ResultType != "0"
| mv-expand Step = todynamic(AuthenticationDetails)
| where tostring(Step.authenticationStepResultDetail) == "Correct password"
| summarize Attempts = count(), First = min(TimeGenerated), Last = max(TimeGenerated),
            IPs = make_set(IPAddress, 20), Clients = make_set(UserAgent, 10), Apps =
make_set(AppDisplayName, 10)
    by UserPrincipalName, ResultType
| order by Last desc
```

The second query also returns real users who walked away from an MFA prompt. Look for IP addresses, countries or clients the user does not normally sign in from. Without Sentinel, filter the Entra sign-in logs (Entra admin center → Monitoring → Sign-in logs) by user agent, or open a user's sign-ins and check the authentication details.

§ 7

## What comes next

The detection that does not depend on the user agent is now live as 102189. Next come alerts for the other ways a stolen password gets used.

NEW SIGN-IN DETECTIONS · RELEASING NOVEMBER 1

Alerts when a user signs in for the first time with the password-only (ROPC) flow, an admin or scripting tool (Azure CLI, PowerShell), legacy authentication or a device code, or sends a first guest invitation. These are the ways a stolen password is often used next.

LEARNED SPRAY CLIENTS

A client that fails for many users and never succeeds is marked automatically, and a correct password from it alerts. This replaces the fixed user-agent list in 102187.

DAILY PASSWORD-SPRAY REPORT

Failed sign-ins grouped by client, network and user, plus any success, as a scheduled report.

### Questions, or a check of your tenant

Contact your Fluency SOC team. We will update this advisory as the campaign changes.

## Sources

Huntress: No (Bad) CAP, Inside an Ongoing LSHIY Password Spray Attack

Microsoft: Password spray investigation playbook

Microsoft: Entra ID Protection risk detections

TrustedSec: From Error to Entry, Cracking the Code of Password-Spraying Tools