

CREDENTIAL STUFFING ANALYSIS LOG

Evidence ID: CRED-2024-11-14

Source: Breach Database Check / Authentication Attempt Review

Status: Player-facing

[2024-11-14 23:38:02] BREACH_SOURCE_CHECK_STARTED

Source: GamerZone Forum breach

Breach Date: May 2024

[2024-11-14 23:38:04] EXPOSED_ACCOUNT_FOUND

Email: alex.mercer@school.lu

Password Status: Hashed password found in breach data

Password Recovery Status: Hash cracked

[2024-11-14 23:38:06] RECOVERED_PASSWORD_RECORD

Recovered Password: Sk8er!2022

Password Age: Older password

Risk Indicator: PASSWORD_REUSE_POSSIBLE

[2024-11-14 23:41:00] AUTOMATED_LOGIN_TEST_DETECTED

Target Service: Discord

Account Tested: alex.mercer@school.lu

Method: Credential stuffing attempt

Tool Behaviour: Automated password submission

[2024-11-14 23:41:02] AUTHENTICATION_RESULT

Login Result: FAILED

Reason: Incorrect password

Account Status: Password had been changed before attack

[2024-11-14 23:41:05] SECURITY_ASSESSMENT

2FA Challenge Triggered: NO

Reason: Password authentication failed before 2FA step

[2024-11-14 23:41:08] ANALYSIS_SUMMARY

The exposed GamerZone Forum password was tested against Alex Mercer's Discord account, but the login attempt failed. This means the attacker tried credential stuffing, but the old password was no longer valid.

[2024-11-14 23:41:11] FINAL_ASSESSMENT

Classification: FAILED CREDENTIAL STUFFING

Entry Vector: REJECTED

Conclusion: Not the entry vector for the account takeover.

Recommended Evidence Link: Compare with malware token-stealer report and login activity log.