Multi-Factor Authentication Request Generation, Technique T1621 - Enterprise

Archived: 2026-04-02 11:07:14 UTC

Adversaries may attempt to bypass multi-factor authentication (MFA) mechanisms and gain access to accounts by generating MFA requests sent to users.

Adversaries in possession of credentials to Valid Accounts may be unable to complete the login process if they lack access to the 2FA or MFA mechanisms required as an additional credential and security control. To circumvent this, adversaries may abuse the automatic generation of push notifications to MFA services such as Duo Push, Microsoft Authenticator, Okta, or similar services to have the user grant access to their account. If adversaries lack credentials to victim accounts, they may also abuse automatic push notification generation when this option is configured for self-service password reset (SSPR).[1]

In some cases, adversaries may continuously repeat login attempts in order to bombard users with MFA push notifications, SMS messages, and phone calls, potentially resulting in the user finally accepting the authentication request in response to "MFA fatigue."[2][3][4]
