Account Manipulation: Device Registration, Sub-technique T1098.005 - Enterprise

Archived: 2026-04-05 16:10:49 UTC

Adversaries may register a device to an adversary-controlled account. Devices may be registered in a multifactor authentication (MFA) system, which handles authentication to the network, or in a device management system, which handles device access and compliance.

MFA systems, such as Duo or Okta, allow users to associate devices with their accounts in order to complete MFA requirements. An adversary that compromises a user’s credentials may enroll a new device in order to bypass initial MFA requirements and gain persistent access to a network.[1][2] In some cases, the MFA self-enrollment process may require only a username and password to enroll the account's first device or to enroll a device to an inactive account. [3]

Similarly, an adversary with existing access to a network may register a device or a virtual machine to Entra ID and/or its device management system, Microsoft Intune, in order to access sensitive data or resources while bypassing conditional access policies.[4][5][6][7]

Devices registered in Entra ID may be able to conduct Internal Spearphishing campaigns via intra-organizational emails, which are less likely to be treated as suspicious by the email client.[8] Additionally, an adversary may be able to perform a Service Exhaustion Flood on an Entra ID tenant by registering a large number of devices.[9]

Source: https://attack.mitre.org/techniques/T1098/005