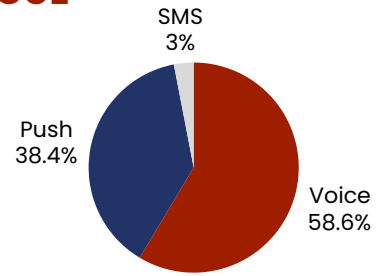
MFA Bypass Attacks

This document provides practical guidance on identifying and addressing the recent uptick in MFA bypass attacks.

TOP 3 ATTACKS

MFA FATIGUE



TOKEN THEFT

+111% FROM 2022-23

MACHINE-IN-THE-MIDDLE

19%

OF SUCCESSFUL ATTACKS

These figures are taken from the Microsoft Digital Defense Report 2023, and the numbers continue to rise.

CRMWG
Cyber Resilient Massachusetts Working Group

MassCyberCenter.org

Why is this important?

Multi-Factor Authentication (MFA) is a fundamental element of contemporary cybersecurity, yet **even this reliable layer of protection is vulnerable to advanced bypass attacks.** Recognizing these vulnerabilities is essential for staying one step ahead of cybercriminals who exploit methods such as phishing, token theft, and session hijacking to infiltrate sensitive systems. By understanding these risks, leaders can effectively evaluate their organization's security stance and pinpoint areas that require enhancement, creating a defense-in-depth strategy.

What do these attacks mean?

- **MFA Fatigue:** Cybercriminals exploit user exhaustion to bypass MFA. This social engineering tactic involves attackers who already have a username and password continually sending fake authentication requests to a user, hoping they will eventually approve one out of sheer annoyance.
- **Token Theft:** A token acts as a hidden key on your device that keeps your login session active after completing an MFA challenge. Attackers often use phishing emails or other means to steal this key. Once obtained, they can impersonate you and access your account without needing a second authentication factor.
- **Machine-in-the-Middle**: This token theft strategy tricks users into clicking on seemingly legitimate links that actually lead to fraudulent websites. These sites are designed to capture credentials and steal the hidden key/token, enabling attackers to bypass MFA challenges.

Key Terms Defined

- **Multi-Factor Authentication (MFA)**: MFA is a security feature that protects online accounts with more than one factor for authentication(like a password). Factors can include an SMS (text) message, a 6-9 digit rotating code from an authenticator app, a phone call, or biometric verification (such as FaceID or fingerprint recognition).
- **MFA Bypass Attacks** can be defined as any attempt by a threat actor to circumvent multi-factor authentication in order to gain access to user accounts
- **MFA Challenge:** This refers to the prompt for additional confirmation or authentication that occurs when a user attempts to log into their account.
- **Push Notifications**: These are alerts that appear on your phone, often used by MFA applications to confirm a login attempt.

How can I protect my organization from these attacks?

- **Limit Push Notifications:** To mitigate MFA fatigue attacks, restrict the number of MFA push notifications allowed before granting access, or consider eliminating them entirely. Microsoft has removed push notifications from its authenticator app, introducing number matching instead, which prevents users from simply tapping “OK” on an MFA prompt.
- **Awareness Training:** Most attackers aim to exploit human mistakes. Implementing security awareness training is vital to educate users about the importance of sound security practices, thereby reducing the likelihood of errors. Informed users are less susceptible to phishing scams and persistent push notifications.
- **Conditional Access:** Major providers like Microsoft allow administrators to establish rules that must be met for users to access their accounts. Examples of these rules include restricting access to only devices owned by the organization or requiring users to be located within the US for account access.
- **Hardware Tokens:** MFA challenges transmitted via phone or software methods are at risk of interception by attackers. A viable solution is to utilize physical tokens that connect directly to devices for authentication. These tokens, assigned to users, are compact enough to be attached to key rings or ID badge clips. Duplicating these devices is nearly impossible, ensuring only the designated user can use it to authenticate.

Rev - April 3, 2025