

 FLASH

DEEPFAKE ATTACKS POSE A GROWING THREAT TO MFA

ZEROFOX INTELLIGENCE

F-2023-02-14a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Synthetic Media Evolution of Tooling

February 14, 2023



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 3:00 PM (EST) on February 14, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Deepfake Attacks Pose a Growing Threat to MFA

Key Findings

- The use of synthetic media to bypass multi-factor authentication (MFA) systems is a growing threat to organizational security.
- Attackers use social engineering techniques to collect data from users for generating realistic audio and video content.
- The AI-based deepfake technology can deceive MFA systems that rely on voice, face, or behavior recognition, enabling attackers to access sensitive information, accounts, and systems.
- The use of social engineering tactics to collect data further emphasizes the need for continuous user education and awareness training.

Analyst Commentary

Threat actors have increasingly leveraged phishing techniques where traditionally-strong MFA gives little or no protection. This includes “in-the-middle” techniques, MFA fatigue¹—as encouraged by Lapsus\$—and OAuth Consent phishing attempts.² Attackers increasingly use phishing attacks to bypass multifactor authentication (MFA) in Microsoft 365. Frameworks such as Evilginx2 are used to steal login credentials and session cookies for initial access and MFA bypass. While certificate-based authentication and FIDO2 can mitigate these attacks, many organizations still use time-based one-time passwords (TOTPs) and push notifications

¹ MFA fatigue is the practice whereby threat actors utilize social engineering (frequently phishing), in order to gain user credentials, and then bombard the user with MFA push notifications to their device in order to try to get the user to confirm their identity through these notifications.

²

[hXXps://www.csoonline\[.\]com/article/3674156/multi-factor-authentication-fatigue-attacks-are-on-the-rise-how-to-defend-against-them.html](https://www.csoonline.com/article/3674156/multi-factor-authentication-fatigue-attacks-are-on-the-rise-how-to-defend-against-them.html)



for MFA.³ These gaps can be exploited by attackers, who are constantly innovating and evolving their tactics to compromise networks.

As technology advances, so too does the sophistication of cyber attacks. In recent years, the rise of advanced artificial intelligence (AI) and machine learning techniques has allowed threat actors to bypass MFA mechanisms by creating synthetic media through the use of Adversary-in-the-Middle (AiTM) techniques. MFA has been widely adopted as a security measure to prevent unauthorized access to sensitive information, accounts, and systems. However, the use of AI-based deepfake technology by attackers has introduced new risks to MFA systems that rely on biometric or behavioral data.

The creation of synthetic media to deceive biometric and behavioral data-based multi-factor authentication systems is a growing threat to organizational security. Synthetic media can deceive MFA systems that rely on voice, face, or behavior recognition, allowing attackers to gain access to sensitive information, accounts, and systems despite the presence of MFA. Attackers use social engineering techniques like phishing and vishing to collect data from users, which is then used to generate realistic audio and video content for use in the attacks. As a result, this trend is a significant threat to the security of organizations and their data.

Recommendations

- In response to this growing threat, ZeroFox recommends additional security measures, such as behavioral biometrics, which uses machine learning algorithms to analyze a user's unique behavioral patterns to confirm their identity.
- ZeroFox Intelligence recommends implementing phishing-resistant MFA methods that support Fast ID Online v2.0 (FIDO2) and certificate-based authentication in conjunction with a broader Zero Trust initiative.
- Users are also advised to use strong passwords and regularly change them, avoid clicking on suspicious links, and report any suspected phishing or vishing attempts to their IT security team.
- It is crucial for users to remain vigilant, stay up-to-date with emerging threats, and implement effective security measures to safeguard their personal and organizational data.
- ZeroFox recommends remaining vigilant and denying MFA requests not triggered explicitly by logging in or requesting device enrollment. These requests are typically immediate and should not randomly appear throughout the day.

³ [hXXps://securityboulevard\[.\]com/2023/02/threat-actors-turn-to-aitm-to-bypass-mfa/](https://securityboulevard.com/2023/02/threat-actors-turn-to-aitm-to-bypass-mfa/)



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.