ultraviolet

THREAT REPORT:

MFA Bypass and Exploitation – Attackers Keep Pushing

Services Performed By:
UltraViolet Cyber
Meredith Glass
(443) 351-7630
info@uvcyber.com

Published Date:
June 26, 2024

Contents

1 Executive Summary

MFA Bypass remains a popular and effective technique used in credential access and compromise of user accounts. Cisco Talos reports exploitation of MFA weaknesses involved in roughly 50% of engagements carried out during its Q1 2024 investigations carried out by Talos IR. While proper implementation of MFA remains a crucial component in securing accounts against compromise, techniques continue to evolve amongst attackers and what remains important is for users and those responsible for defense and security to be aware of possible attack methodologies and best practices to prevent them.

2 Technical Analysis

Some of the types of attacks that can be carried out targeting MFA can be broadly grouped into some of the following categories:
-Exploitation/theft of authentication tokens; this can involve session reuse/replay from an authenticated session, obtaining static backup tokens included with authentication app platform, exploiting token onboarding processes where emails sent to newly onboarded users contain URLs requiring interaction to pair phone/user identity in the MFA server but also contain the cryptographic seed for user MFA token generation (guarded only by a short PIN code) which allows for brute-force and replication of any user's MFA token in the network, etc.
-Session hijacking (also known as cookie stealing); theft of client-side session cookies, encrypted on Windows systems using DPAPI, with any domain-joined environment maintaining a domain-wide backup key that has full access to decrypt any data blob without local admin privileges (key isn't rotated); user's browser cookies and passwords can be readily decrypted and access to domain keys achieved
-SIM Swapping/Cloning/Hacking; compromise of a user's mobile device in this fashion gives full phone number control and access to SMS-generated OTPs
-Social engineering/phishing/vishing; convincing users to click malicious links, divulge OTPs or generated codes, divulge personally identifiable information, etc., this broad group of techniques continues to be a successful avenue for attackers to gain unauthorized access
-Brute-force of MFA and 'push spray'; attackers may attempt to simply brute-force temporary pins (or passwords lacking length and complexity), or they may already have a user's password and send push requests repeatedly in hopes that the victim will respond to/accept the push notification and grant the attacker access; the success of push spraying seems to relate to attempts made during active business hours, e.g. times where push notifications would be likely to happen for users and be inconspicuous

3 What UltraViolet Cyber is Doing

- Monitoring all platforms for suspicious access attempts, excessive AD login attempt activity, MFA failures and the like, reporting promptly to customers on any activity that may be unauthorized or malicious
- Reviewing email messages containing potentially malicious URLs to determine potential threats and identify possible trends amongst techniques, domains or tools used for attempted account compromise

4 What Customers Can Do

- Enforce strong password policies throughout all systems for which credentialed access is required
- Educate users on the potential for phishing attempts revolving around MFA or credential information divulgement, reminding users to investigate any email link sent, regardless of how legitimate or known the potential sender may be, to ensure no redirects are occurring to malicious pages, domains or web applications
- Use best practices for onboarding users with MFA and have protections in place to prevent access to/compromise of MFA servers within the organization by attackers

5 References

Burton, Hazel. “How Are Attackers Trying to Bypass MFA?” Cisco Talos Blog, 18 June 2024, blog.talosintelligence.com/how-are-attackers-trying-to-bypass-mfa/. Accessed 26 June 2024.

Chipeta, Catherine. “6 Ways Hackers Can Bypass MFA + Prevention Strategies | UpGuard.” Www.upguard.com, 9 Sept. 2022, www.upguard.com/blog/how-hackers-can-bypass-mfa.

Hoffman, Nicole. “Talos IR Trends: BEC Attacks Surge, While Weaknesses in MFA Persist.” Cisco Talos Blog, 25 Apr. 2024, blog.talosintelligence.com/talos-ir-quarterly-trends-q1-2024/.

Nahari, Shay. “Best Defense? Our Red Team Lead Reveals 4 MFA Bypass Techniques.” Www.cyberark.com, 8 June 2021, www.cyberark.com/resources/threat-research-blog/mfa-bypass-techniques-from-red-team-research.

Sheth, Hitesh. “Top 5 Techniques Attackers Use to Bypass MFA.” Www.darkreading.com, 5 Aug. 2021, www.darkreading.com/endpoint-security/top-5-techniques-attackers-use-to-bypass-mfa.

Wright, Rob. “CrowdStrike Details New MFA Bypass, Credential Theft Attack | TechTarget.” Security, 26 Apr. 2023, www.techtarget.com/searchsecurity/news/365535760/CrowdStrike-details-new-MFA-bypass-credential-theft-attack. Accessed 26 June 2024.