NEED TO KNOW NEWSLETTER | NOVEMBER 2022

Multi-factor authentication (MFA) fatigue

MFA fatigue attacks are on the rise

In this month's newsletter, we highlight a growing form of attack: MFA fatigue. Just as MFA has become more widely used, attackers have found a way to get around MFA push notifications. This identity-based attack is designed to remove security barriers and is sure to put companies and individuals on high alert.

What is MFA fatigue?[1]

MFA fatigue, also known as MFA bombing or prompt spamming, is an attack that bombards a user's authentication app with multiple push notifications. If the prompt is verified by the user, the hacker gains access to an account or device.

How does the attack work?

- The attacker has already gained some credentials, like usernames and passwords, possibly through a phishing email
- The attacker uses these stolen credentials to log into a protected account that uses an MFA push notification to verify
- The attacker requests the verification repeatedly, waiting for the user to verify
- The user gets frustrated with the number of push notifications they receive and gives in and verifies the request
- The attacker now has full access to the account

Authentication and identity provider Okta states: "The issue here is not user behavior or weak MFA, but a lack of systems that are designed to thwart these kinds of attacks before they gain traction."

Safety tips

- Know what to look for: Become familiar with MFA attacks, so you feel prepared if you encounter one
- Know how to react: If you think you are being attacked, report the situation to the proper team and immediately change your password(s)
- Stay alert: With the amount of logging in and out each day, security can easily slip your mind!
- Stay engaged so you can be ahead of the hackers

Attacks making headlines

CashApp — Insider threat[2]

In April 2022, a disgruntled former employee hacked into CashApp's servers. They managed to access customer data, stock trading records, valuable financial information and much more.

Uber — Social Engineering[3]

In September 2022, an 18-year-old hacker deceived their way into one of the largest ride-share companies. Uber stated that the hacker got a contractor's login information and bypassed the company's two-factor authentication.

Nvidia — Ransomware[4]

In March 2022, the hacking group Lapsus$ claimed responsibility for holding Nvidia's proprietary data hostage. The widely used US computer chip-making company hired a group of cybersecurity experts to help respond to the large attack.

Hook, line and phished — phishing attacks rise over 60% in 2022

Phishing is one of the most common methods of cybercrime. According to the Interisle Consulting Group, phishing has risen 61% in the last year. No company or individual is safe from receiving a phishing email.

Cryptocurrency companies are now on high alert, as their field is being phished more and more. Interisle found the increase to be over 250% year-to-year for these companies. Hackers are targeting wallets and exchanges at a rate so high that it seems no one is safe.

For more information on the rise of phishing emails, see here.

[1] https://www.okta.com/blog/2022/09/mfa-fatigue-growing-security-concern/
[2] https://ermprotect.com/blog/top-10-data-breaches-so-far-in-2022/
[3] https://www.bu.edu/articles/2022/what-you-need-to-know-about-uber-data-breach/
[4] https://techcrunch.com/2022/03/01/nvidia-hackers-leak-ransomware/

E-TECH