Bypassing MFA

4/26/2024

Understanding MFA

While there are many ways to secure an account or ecosystem, the most important topic to consider is the defense in depth idea. The briefest explanation of this is not relying on a single security measure to be the only safeguard. Thinking about this in terms of securing a building, this would be like a fence around the perimeter, a lock on the front door and then a lock on each room. Understanding this will help to paint the picture that MFA is just a piece to this puzzle. There is a common misconception that if you have MFA on an account, the account is secure and safe from compromise.

First, let's take a look at the different types of MFA and the strength of these. Of course, there is the code sent either to email, SMS or through a phone call. While these are a great start, they are not very secure. As of the writing of this, attackers can spend as little as $300 for a SIM swap. This allows them to fully take over your phone number and in turn, they are now the ones receiving those calls or messages. Next up is the MFA push notification. On log in, a push request is sent to the phone with a simple is this you in which you will select yes or no. While this is slightly more secure, attackers will leverage the attack vector of push fatigue. By continuously sending a push to the user's device, it is likely that the user will get tired of receiving these and just approve them. In the same attack vector, threat actors will also use OSINT to determine when you are actively working. The thought behind this is that you are already working, and a random push might raise less suspicion. The improvement to this method is the challenge push. An example of this is the Microsoft Authenticator where it displays a 2-digit code that must be input in the application for approval. This helps prevent things like push fatigue as if the user does not have access to see the code displayed, there is not a way for them to accept the push. Moving to what is considered the most secure MFA, we will look at Password-less authentication and the FIDO2 tokens. By creating trust with a device and using the TPM, the protection is greatly increased.

Moving to the attack vectors used to bypass MFA, there are three we will talk about. While there are variations on these methods and the threat actors are constantly working on creating new ones, each method will just help to understand the risk associated with complacency in this realm. First, is by hijacking the browser cookies. There are many ways to accomplish this, but the main way would be to listen to the traffic traversing the network. While packet sniffing is the hardest to achieve due to encryption used for transporting data, it is still worth noting. In an effort to improve the reliability of this, if an attacker can get access to the DNS Cache that is used by the end user, DNS poisoning becomes possible. This allows threat actors to change where a website is directed

to, resulting in the ability to have a malicious log in page displayed. To learn more on how this can be achieved, you can check out the YouTube listed in the reference section. Finally, the use of phishing emails is the tried-and-true method for pushing the malicious login pages used to steal credentials. This allows the collection of the username, password and the secret key that is used for most MFA methods. While each of these will give the attackers access to the account for at least a period of time, the control allows them to either remove the MFA or add their own as an alternative method. Unfortunately, by adding another method as a secondary, it is not immediately seen by the end user as their primary method will still be the default.

If you are responsible for monitoring these accounts, there are a few ways to spot when an attacker has gained access to the accounts. Of course, the first thing to look for is going to be the sign-in logs. Generally speaking, you will see logins from locations that the user is not in or logins from locations where it would be impossible to get to in the time difference between sign-ins. Once this is discovered, you will want to get a full understanding of exactly what is going on which helps to define the steps to take and the paths of investigation that are needed and to start the mitigation. Of course, the first mitigation steps are to block sign-ins, revoking active sessions, changing the password, and reviewing the MFA methods will ensure that you regain control over the account. If it is a Microsoft account, checking for anomalous behavior, like e-mail blasting, mass OneDrive downloads or removals or missing data by the user are just a few examples of the scope of the compromise. The amount of investigation will depend on the license that is assigned to the tenant. Also, it is important to understand if the user has any other accounts that have been created using that email. Knowing this will ensure that you are able to recover any other stolen accounts that are tied to the email compromised. It is important to note that even if the user did not sign up for these accounts, with access to the email, attackers are also able to create these accounts which increases the likelihood of future attacks since it will now appear to come from a legitimate source.

While this is not meant to make you an expert in any of the areas covered, but instead give you a starting point in understanding MFA, Bypassing and remediation. Remember that as an IT professional, you are charged with the protection and remediation of the users that you support.

Warmest regards,

Caleb Leggett

Sources:

https://www.youtube.com/watch?v=nggQan4XZ1E

https://saaspass.com/threats/prevent-dns-cache-poisoning-attacks-with-two-factor-authentication/

https://atlantsecurity.com/phishing-examples-examples-of-fake-login-emails-and-forms/