29.05.2026

Phishing version 2.0 : comment les attaques « man in the middle » font tomber le rempart de l'authentification multifacteur (MFA)

Les cyberpirates ne cessent de perfectionner leurs méthodes de hameçonnage. En particulier, les attaques dites de « l'homme du milieu » (ou MITM pour Man in The Middle) s'avèrent redoutables. Dans ce scénario, les criminels s'interposent discrètement entre la victime et le site web légitime pour intercepter en temps réel les identifiants de connexion.

Contrairement aux sites de phishing classiques, les attaques MITM ne se contentent pas de copier une page de connexion. L'infrastructure frauduleuse permet en effet de relayer directement les données au serveur légitime et d'afficher la page web officielle. Dans ces conditions, l'intrusion passe totalement inaperçue. Même l'authentification multifacteur (MFA) peut, dans certains cas, être contournée.

Recrudescence des attaques

En Suisse, la menace liée au phishing continue de croître. Actuellement, une forme particulièrement sournoise d'hameçonnage circule : l'attaque de « l'homme du milieu » (Man in the Middle), qui fait de plus en plus appel à de nouvelles technologies d'hébergement et des infrastructures très difficiles à détecter.

Fonctionnement des attaques MITM

Souvent, l'offensive démarre par un message en apparence inoffensif : un email, un SMS ou un message WhatsApp contenant un lien vers une fausse page de connexion. Si la victime clique sur ce lien et saisit non seulement son nom d'utilisateur et son mot de passe, mais aussi son code MFA, l'infrastructure relaie en temps réel les données de connexion à la plateforme officiel, et le hacker prend le contrôle de la session.

Le piège est d'autant plus redoutable que les infrastructures font appel à des chaînes de redirection complexes et à des sites au design professionnel pour tromper les solutions de sécurité. Certaines ont même recours à des services de cloud spécialisés ou à des plateformes décentralisées pour s'assurer que les pages de phishing restent en ligne le plus longtemps possible.

Particuliers et entreprises : que faire pour se protéger ?

Si aucune protection n'est en mesure de garantir un risque zéro, il est néanmoins possible de réduire considérablement l'exposition aux attaques en adoptant les mesures de prévention suivantes :

- toujours se méfier des liens de connexion reçus par email, SMS ou messagerie instantanée
- examiner avec attention l'adresse affichée dans le navigateur
- utiliser un gestionnaire de mots de passe

- privilégier les méthodes d'authentification multifcateur telles que les solutions FIDO2 ou les passkeys lorsqu'elles sont proposées
- maintenir le système d'exploitation, le navigateur et les logiciels de sécurité parfaitement à jour
- sensibiliser et former les collaborateurs de l'entreprise

Enfin, il est recommandé de traiter avec le plus grand sérieux toute demande de connexion suspecte ou notification MFA inattendue. Si vous recevez soudainement plusieurs demandes de confirmation alors que vous ne tentez pas de vous connecter, changez immédiatement votre mot de passe et déconnectez toutes les sessions actives.

L'humain reste le dernier rempart contre les attaques

Malgré l'évolution des technologies de sécurité, l'humain reste la cible privilégiée des cybercriminels. Les attaques de phishing misent délibérément sur l'urgence, la confiance et nos automatismes. Dans ce contexte, la vigilance et une bonne dose de scepticisme demeurent vos meilleurs atouts dans votre quotidien numérique.