E-BOOK

Tous les MFA **ne se valent pas**

Pourquoi un MFA moderne est plus sûr que les SMS ou les applications d'authentification mobile

yubico

Les méthodes MFA classiques comme les SMS, les mots de passe à usage unique et les notifications push n'arrêtent pas les cybermenaces actuelles.

Les attaques par phishing sont en hausse, mais toutes les formes d'authentification multi-facteurs (MFA) ne résistent pas au phishing. L'Histoire montre que les formes plus anciennes de MFA ont été compromises à maintes reprises, car les pirates peuvent facilement les contourner en utilisant le phishing, les malwares, les ransomwares, les échanges de cartes SIM et les attaques de type Attacker-in-the-middle.

> « N'importe quel MFA vaut mieux qu'un nom d'utilisateur et un simple mot de passe, mais la plupart des MFA sont encore vulnérables au phishing. Il n'a pas fallu longtemps pour réaliser que nous avions besoin d'une authentification plus forte et à l'épreuve du phishing pour tous les employés. »

Daniel Jacobson
Directeur des systèmes d'information, Datadog

En savoir plus:
yubi.co/datadog

Risque de piratage de compte
350 000 tentatives de piratage

- **0 %** Clé de sécurité FIDO (YubiKey)
- **10 %** Message sur appareil
- **24 %** Code SMS
- **21 %** E-mail secondaire
- **50 %** Numéro de téléphone

Résultats du déploiement de la YubiKey par rapport à une application mobile avec mot de passe à usage unique

- **0** Compte piraté
- **4x** Plus rapide à se connecter
- **92%** De recours en moins à l'assistance
- **0** Compte verrouillé
- **50m+** De retour sur investissement

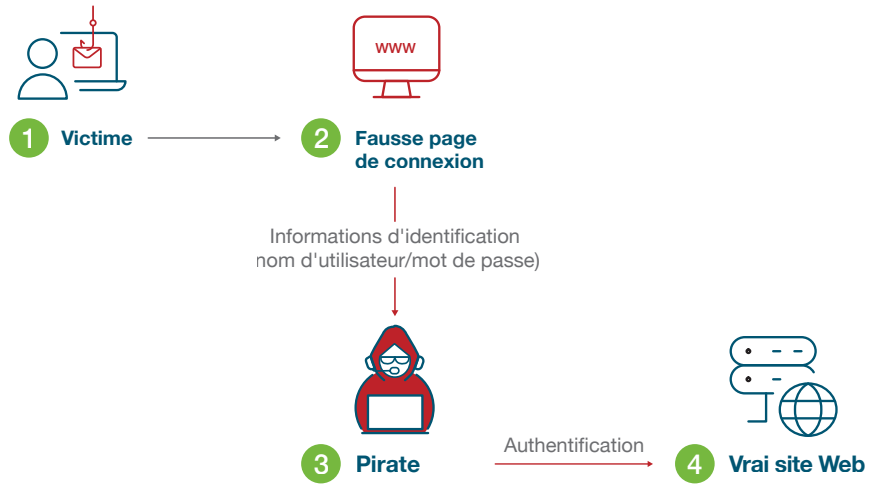
Google Research

Les clés de sécurité : des deuxièmes facteurs cryptographiques pratiques pour le Web d'aujourd'hui

yubico

Examinons un exemple d'attaque par phishing permettant de contourner les SMS et d'autres MFA logiciels.

Description d'une attaque par phishing



Étape 1

- En haut à gauche, nous avons notre victime. Appelons-le Joe.
- Joe reçoit un faux lien URL de la part d'un pirate, envoyé par e-mail ou sur les réseaux sociaux.

Étape 2

- Joe clique sur un lien qui le redirige vers un faux site imitant le vrai site Web.
- Sur le faux site, Joe saisit ses informations d'identification (nom d'utilisateur/mot de passe), en pensant se connecter au vrai site.

Étape 3

- Le pirate, via la fausse page de connexion, récupère les informations d'identification de Joe.

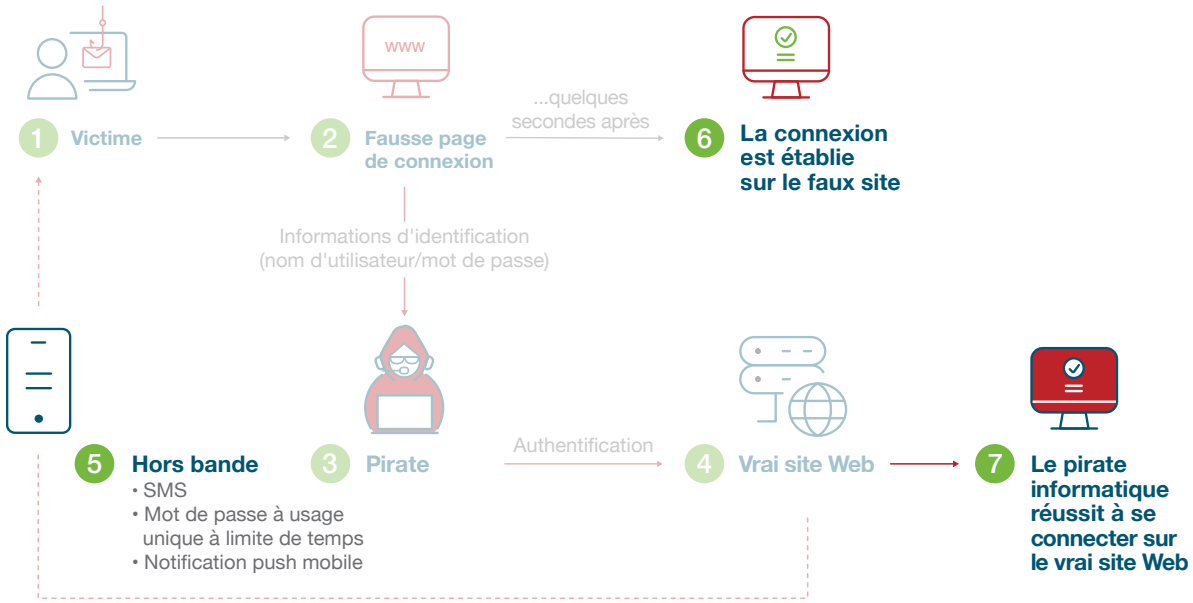
Étape 4

- Le pirate renseigne ensuite les informations d'identification sur le vrai portail Web client/la vraie page de connexion/le vrai site Web (serveur réel).

yubico

Examinons un exemple d'attaque par phishing permettant de contourner les SMS et d'autres MFA logiciels.

Description d'une attaque par phishing



Étape 5

- Toutefois, le compte de Joe peut être piraté même si une authentification à deux facteurs ou multi-facteurs est en place, comme les SMS.
- Le vrai site Web déclenche l'envoi du code SMS sur le téléphone de Joe.

Étape 6

- Peu après, Joe saisit le code sur le faux site et croit s'être connecté au bon endroit.

Étape 7

- Le pirate récupère maintenant le code SMS saisi par Joe et le saisit sur le vrai site Web, se connectant avec succès.
- Le pirate peut même aller plus loin.
- Le pirate peut mettre à jour le mot de passe sur le compte et le numéro de téléphone portable de Joe, verrouillant ainsi totalement l'accès de Joe.

yubico

Pourquoi et comment un MFA moderne résistant au phishing fait cesser les piratages de comptes

Il a été prouvé que le MFA moderne résistant au phishing, proposé uniquement via le protocole FIDO ou les cartes à puce/cartes PIV, met fin aux piratages de comptes. Les clés de sécurité matérielles, telles que la YubiKey, prennent en charge plusieurs protocoles d'authentification, notamment FIDO U2F, FIDO2 et les cartes à puce/cartes PIV, ce qui les rend vraiment résistantes au phishing et offrent une grande tranquillité d'esprit. Les YubiKeys sont spécialement conçues pour la sécurité et la prise en charge des passkeys associées aux périphériques, garantissant ainsi la conformité aux standards d'authentification de niveau 3 (AAL3).

Vous vous demandez pourquoi il vaut mieux transporter un objet de plus ? Ne laissez pas le côté matériel vous tromper ! La YubiKey est une solution puissante de nouvelle génération qui protégera votre identité numérique en ligne et bloquera les cybermenaces modernes et les piratages de comptes.

fido™ ALLIANCE | simpler stronger authentication

En étroite collaboration avec les leaders d'opinion d'Internet, Yubico a conçu et créé un ensemble de nouvelles fonctionnalités d'authentification qui mettent fin aux attaques par phishing et Man-in-the-middle à grande échelle. Ces fonctionnalités sont devenues la base des standards FIDO/WebAuthn.

« La clé de sécurité fait figure de référence en matière d'authentification, c'est un objet que vous possédez physiquement. Pour moi, la YubiKey était l'unique option. Je n'ai pas cherché ailleurs.»

Brent Deterding
CISO, Afni

En savoir plus
yubi.co/afni

Découvrez la magie derrière la YubiKey.

Matériel doté d'un chiffrement puissant

- Tout logiciel téléchargé sur un ordinateur ou un téléphone est vulnérable aux malwares et aux pirates.
- Outre les cartes à puce, la plupart des systèmes d'authentification reposent sur des serveurs centralisés sur lesquels sont stockées des informations d'identification qui peuvent être piratées.
- La YubiKey renforce considérablement la sécurité en stockant les codes secrets de chiffrement sur une puce sécurisée distincte, sans connexion à Internet, et en utilisant une cryptographie à clé publique forte où seule la clé publique est stockée sur le serveur.

Clés liées à l'origine

- Une fois qu'un utilisateur a enregistré une YubiKey auprès d'un service, elle est liée à cette URL spécifique et les informations d'identification enregistrées ne peuvent pas être utilisées pour se connecter à un faux site Web,ce qui fait de la YubiKey une défense efficace contre les attaques par phishing.

Présence de l'utilisateur

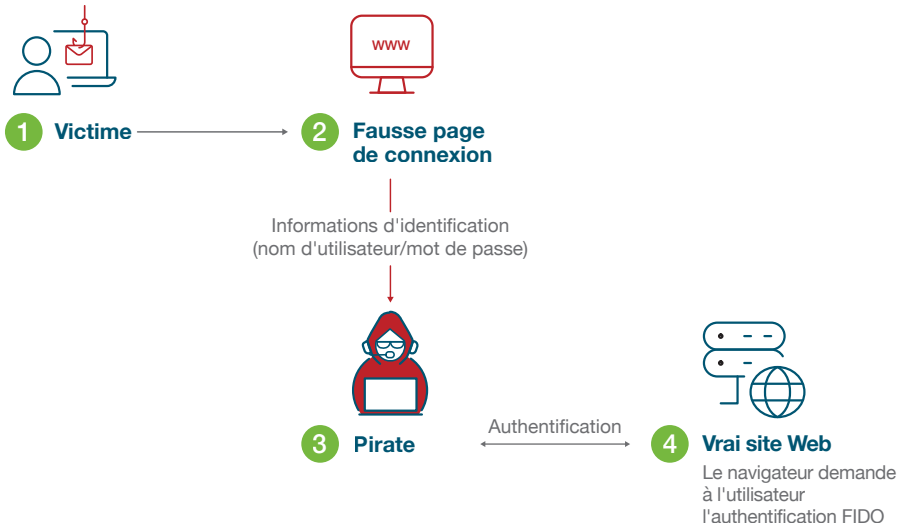
- De nombreuses solutions d'authentification exposent les vulnérabilités par le biais d'attaques à distanceaprès l'authentification du périphérique.
- Le capteur tactile de la YubiKey vérifie que l'utilisateur est bien un humain et que l'authentification est effectuée intentionnellement. La YubiKey vérifie également que l'authentification n'est pas déclenchée à distance par un pirate ou un cheval de Troie.

De nombreuses applications, des secrets bien gardés

- Enfin, les YubiKeys s'authentifient via le standard ouvert FIDO, ce qui permet d'accéder à des milliers d'applications et de services, offrant une sécurité et une confidentialité élevées à grande échelle, aussi bien au travail que dans votre vie privée.

C’est ce qui aurait pu se passer si Joe disposait d’un MFA résistant au phishing ...

Mettez fin aux piratages de comptes grâce à un MFA moderne et résistant au phishing



Étape 1

- Le pirate envoie à Joe un e-mail redirigeant vers un faux site Web/une fausse page de connexion.

Étape 2

- Joe envoie ses informations d’identification (nom d’utilisateur/mot de passe).

Étape 3

- Le pirate, via la fausse page de connexion, collecte les informations d’identification et les soumet sur un vrai portail Web client/une vraie page de connexion/un vrai site Web (serveur réel).

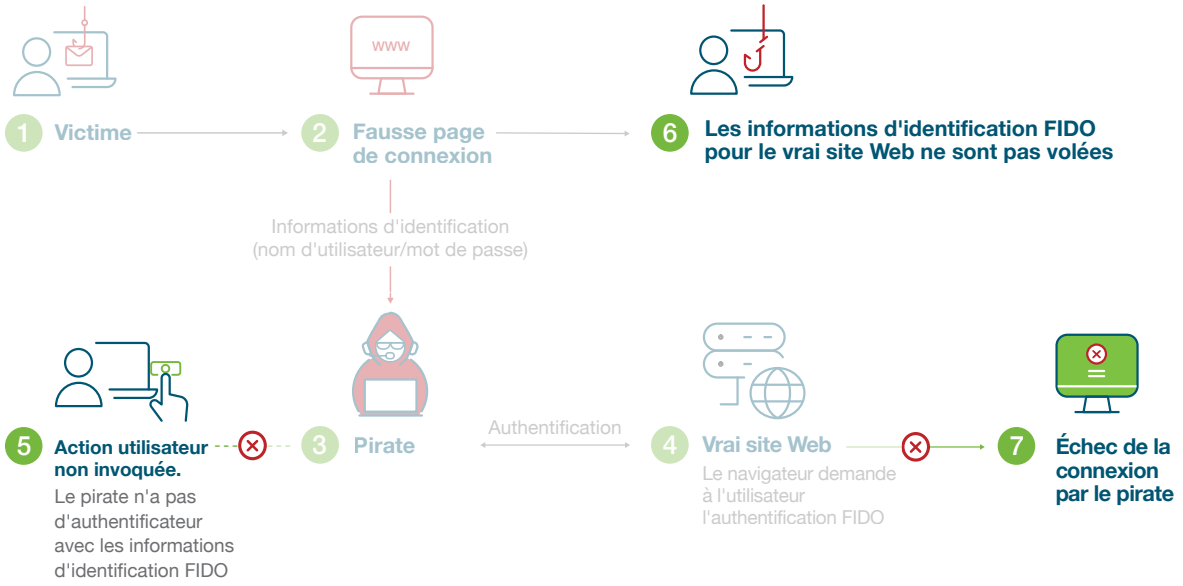
Étape 4

- Le vrai portail Web client fait appel au MFA (FIDO)... ce qui signifie que le navigateur demande une authentification FIDO.
- Joe doit utiliser une clé de sécurité (au lieu de recevoir un SMS ou d’utiliser une application d’authentification mobile).

yubico

C’est ce qui aurait pu se passer si Joe disposait d’un MFA résistant au phishing ...

Mettez fin aux piratages de comptes grâce à un MFA moderne et résistant au phishing



Étape 5

- Joe insère la YubiKey (ou utilise une méthode similaire/proche...NFC, BLE, USB).

Étape 6

- Le vrai site Web et la clé de sécurité FIDO ont un lien secret. Ainsi, lorsqu’un utilisateur utilise une clé de sécurité FIDO, la clé de sécurité comprend qu’un faux site Web demande des informations.
- Le système ne permet pas à l’utilisateur/au processus d’authentification de poursuivre et l’attaque par phishing est déjouée !
- L’authentification FIDO échoue sur le site Web car il existe une relation de confiance entre la clé FIDO et le vrai site Web.

Étape 7

- Le pirate ne parvient pas à se connecter au compte de Joe et son compte reste sécurisé.

En résumé : on peut tromper l’utilisateur, **mais pas la YubiKey !**

yubico

Comment passer à un MFA résistant au phishing à grande échelle

Planification

Définissez clairement les cas d'utilisation en déterminant les groupes d'utilisateurs concernés

Validation

Confirmez le processus avec un petit groupe d'utilisateurs avant un déploiement plus large

Integration

Assurez-vous que les applications et services clés sont prêts pour la YubiKey

Lancement

Distribuez les clés aux utilisateurs via des services de livraison clé en main ou des partenaires de distribution

Adoption

Favorisez leur adoption grâce à une formation et une assistance sur les bonnes pratiques

Mesure

Établissez des rapports relatifs à l'incidence sur la sécurité et la valeur commerciale

Vous pensez qu'il est difficile d'adopter des clés de sécurité matérielles ? Encore une fois, Yubico couvre vos arrières. Les entreprises modernes se tournent vers une sécurité sous forme d'abonnement dans le monde entier. Grâce à des économies, des dépenses prévisibles, des mises à niveau YubiKey flexibles et une livraison clé en main aux adresses professionnelles et personnelles, YubiEnterprise Subscription peut vous aider à passer plus rapidement à une authentification moderne et une protection rapide pour tous vos utilisateurs.

yubico

Contactez-nous
yubi.co/contact

En savoir plus
yubi.co/bpg-mfa

À propos de Yubico

Yubico (Nasdaq First North Growth Market Stockholm : YUBICO) est l'inventeur de YubiKey, une clé de sécurité matérielle de référence en matière d'authentification multi-facteurs (MFA) résistante au phishing. Les solutions de Yubico offrent expertise de déploiement et flexibilité opérationnelle, car les YubiKeys fonctionnent avec des centaines d'applications et de services d'entreprise et grand public.

Yubico est l'un des créateurs et principaux contributeurs de standards d'authentification ouverts FIDO2/passkey, WebAuthn et FIDO Universal 2nd Factor (U2F), et un pionnier de l'authentification par passkeys matérielles moderne et sécurisée à grande échelle, avec des clients dans plus de 160 pays.

Pour en savoir plus, rendez-vous sur : www.yubico.com.

yubico