



RETEX: Allo helpdesk ? J'ai besoin d'un compte

WineRump 2025

Kévin Tellier

26/09/2025

Pourquoi le vishing ?

En un mot : Moins de sensibilisation et de mécanismes de défense, plus humain

Les méthodes traditionnelles :

- **Phishing**
 - Beaucoup de sensibilisation et de mécanismes de détection
 - De + en + difficile
- **Bruteforce**
 - Succès incertain
 - Risque de lock de comptes
- **Surface externe**
 - Dépend de la surface d'exposition et des services
 - Dépend du type d'hébergement (cloud ou on-prem)
- **Physique** :
 - Résultat incertain suivant la configuration (Zero-trust, full WiFi)
 - Risque non nul de se faire flag physiquement

- Attaque ancienne, rendue populaire par certaines figures comme Kevin Mitnick
- Cible aussi bien les particuliers que les pros
 - Attaque la moins chère et délégable à des profils non-techniques
- Professionalisation récente : exemple de **Scattered Spider (UNC3944)**
 - Groupe criminel basé aux USA et UK
 - Attaques par secteur d'activité : Casinos, Retail, Companies aériennes

Prêt ?



Qui cibler ?

- **Helpdesk** : Se faire passer pour un employé et reset le mot de passe
 - Moins de cibles : Nombre réduit d'appel à étaler dans le temps (1-2 appel par jour max)
 - Facile de se procurer le numéro
- **Employé** : Se faire passer pour le helpdesk et demander à un employé de reset son mot de passe
 - Plus de cibles : On ratisse large (10+ appels par jour)
 - Plus difficile de trouver le 06 de tout le monde (quid du tel pro)

Setup technique :

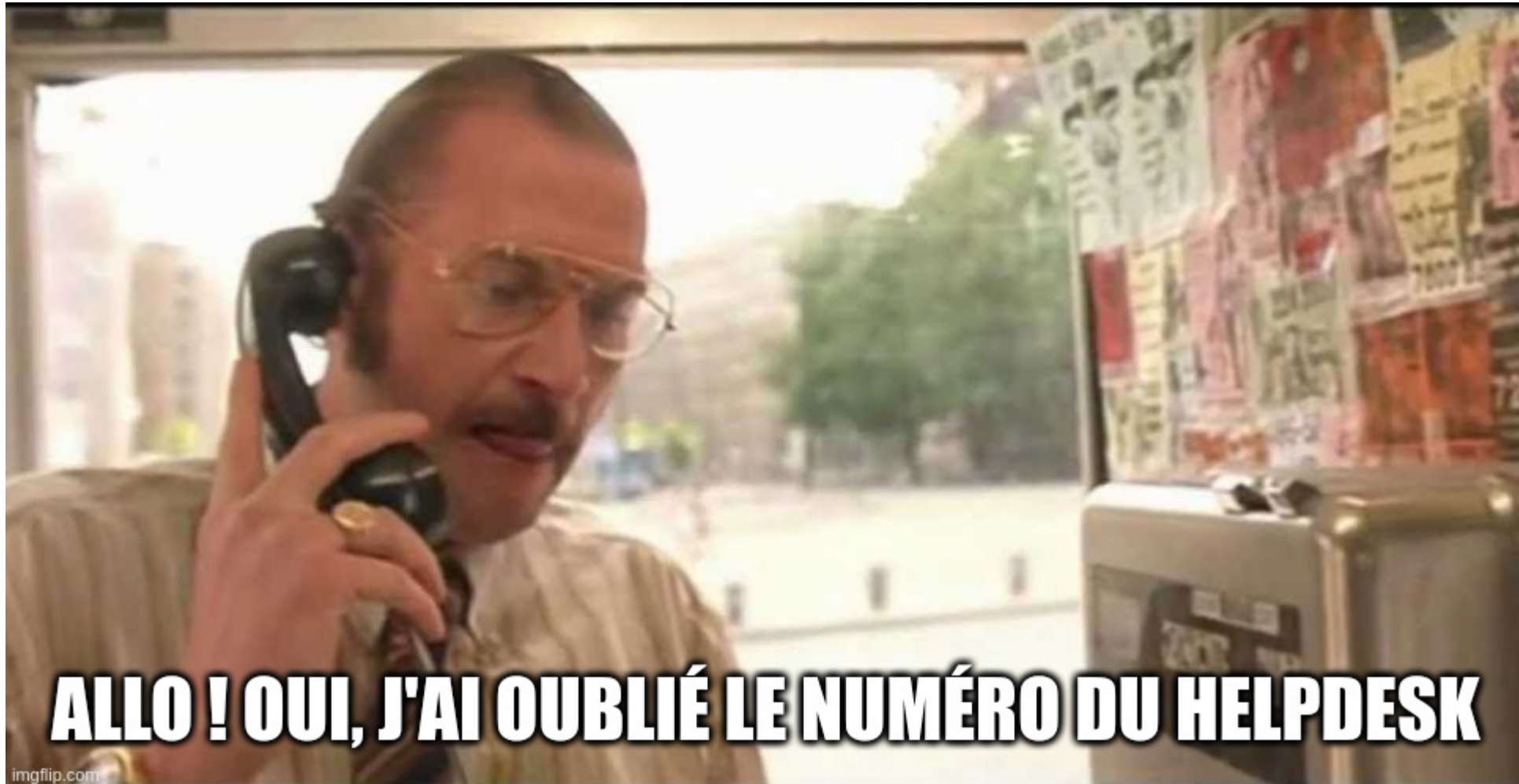
- Service de VoIP (préférer les 01) :
 - En France : Ringover, Aircall etc..
 - A l'étranger : Amazon Connect
- Préparer une VM clean avec le nécessaire d'installé (VPN, fond d'écran)

OSINT :

- Recherche d'employés
 - Apollo
 - RocketReach
 - Linkedin
- Informations à relever pour coller au personnage
 - Genre (faut que ça colle un peu à votre voix naturelle)
 - Lieu de travail
 - Collègues proches
 - Estimation de l'âge (si possible date de naissance)
- Termes propres à l'entreprise

Step 1 - Récupérer le numéro du helpdesk

Appeler le siège



Step 2 - Appeler le helpdesk

Scénario : Employé en télétravail ayant oublié son téléphone pro dans son casier au bureau. Besoin d'accéder à un document urgent.

Récolte d'informations (die and retry) :

- Procédure standard de reset de mot de passe
 - Service de reset de mot de passe
- Identifier les termes internes à l'entreprise
 - Applications internes
 - Nom des services

Step 3 - Attaquer

Utiliser les infos récupérées avant pour être cohérent

- Exploiter les biais cognitifs
 - Bais d'autorité : "Bonjour, David Richard, directeur commercial europe...."
 - Biais d'ancrage : Donner une information (comme le nom de poste) dès le début de l'appel
 - Effet de groupe : "Vôtre collègue avait changé mon mot de passe par XXX il y a 3 mois"
 - Effet d'exposition : Mentionner des noms de personnes, d'applications internes, de sites, jargon etc...

3 comptes récupérés : Accès à 0365 et accès au réseau interne via VPN



- **Des disparités géographiques**
 - 100 % de succès dans certains pays et 0% dans d'autres
- **Peu de signalement**
 - Si risque de détection : Avouer un faux exercice et demander de rester discret
- **Reset de MFA**
 - En 2 appels, moins flag

Scénario Employé - Setup

- Copier un portail de connexion type ADFS ou page de connexion Microsoft
- Acheter un nom de domaine crédible
 - entreprise-help.com
 - Typosquatting
 - application_reset_mdp-helpdesk.com
- Utiliser des numéros locaux

Scénario : "Bonjour, Kévin du helpdesk, vous vous êtes rendu récemment en Roumanie ?"

- Choisir un pays qui fait "peur"
- Lui expliquer la situation
- Authentifier l'appel : "Pouvez-vous me confirmer votre date de naissance ?"
- Rassurer la victime qu'elle n'est pas la seule dans cette situation, que c'est courant
- Inviter la victime à se connecter sur la page de phishing

- Le petit cadenas 
- Les bluffeurs : "Non mais j'ai pas rentré mon mot de passe" 
- Les gens très énervés (ils sont peu mais ça arrive)
- Un faible niveau en informatique peut être une bonne protection



- ~60% de succès (sur 74 appels décrochés)
- Le doute n'implique pas systématiquement le refus
- Nous ne sommes pas tous égaux face au Social Engineering
 - Se font avoir à 2 semaines d'intervalle sur le vishing et le smishing
 - Se font avoir 2 années d'affilé sur le même scénario

- Authentification Phishing-resistant (FIDO2, Passkeys)
- Sensibiliser les équipes (helpdesks et employés)
 - Faire des exercices réguliers
- Validation par un tiers : 4 eyes principle
 - Validation du manager direct
- Mettre en place un mécanisme de posture check et conditional access
 - Pas parfait mais c'est un +



<https://www.linkedin.com/company/synacktiv>



<https://x.com/synacktiv>



<https://bsky.app/profile/synacktiv.com>



<https://synacktiv.com>