ATTAQUES ET VULNÉRABILITÉS

INGÉNIERIE SOCIALE

INGÉNIERIE SOCIALE ?

- **L’ingénierie sociale** est l’art d’amener les gens à fournir des informations a priori non-invasive ou sans importance (voire à leur faire exécuter des actions), pour récolter petit à petit des informations
  - en gagnant leur confiance
  - et en réduisant leurs défenses
- Cette technique est souvent combinée avec d’autres pour finalement atteindre la cible (données…)

TECHNIQUES D’INGÉNIERIE SOCIALE

- Toutes la série de techniques présentées ici font partie de la catégorie « ingénierie sociale » ou y sont étroitement associées

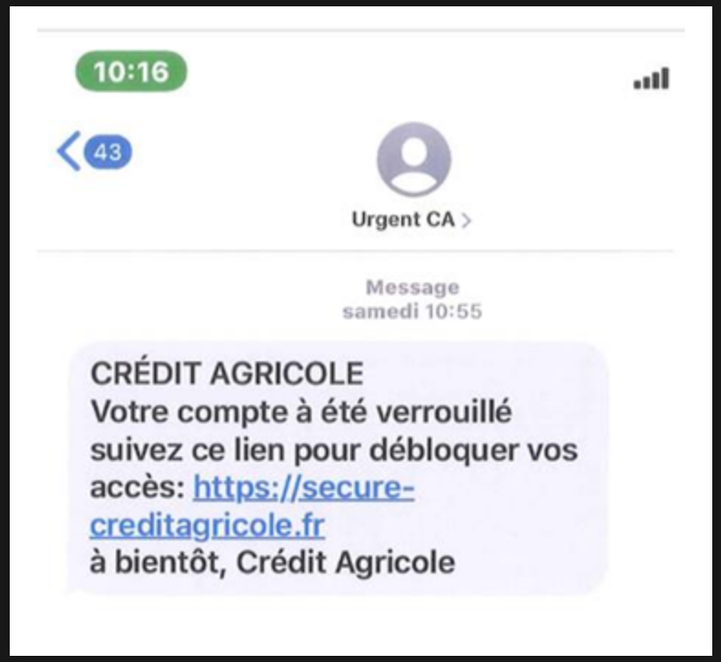
HAMEÇONNAGE

- *Objectif* : obtenir des **informations importantes** (identifiant, mots de passe, infos de carte de crédit…)
- *Moyen principal* : faire remplir à la cible ces informations sur un site web contrefait
- Vecteurs d’attaque :
  - email (souvent combiné avec *spoofing*)
  - messagerie instantanée
  - SMS (*Smishing*)

SMISHING

- *SMS Phishing* : hameçonnage par SMS
- Notamment très populaire pour les cibles plus jeunes
  - un jeune de 18-24 ans envoie et reçoit environ 4000 messages par mois (2020)

SMISHING - EXEMPLE



VOLUME = EFFICACITÉ

- Les techniques précédentes ont un taux de réussite souvent très faible
- Pour être efficace, les attaquants misent sur l’envoi en masse
- Ex : supposons un taux de réussite d’une campagne de *phishing* à 0,01 % (seule 1 personne sur 10000 se fait avoir)
  - envoi de 10 millions de messages (*spamming*)
  - résultat : 1000 victimes, largement suffisant pour rendre la campagne rentable
- D’autres techniques sont plus ciblées et misent beaucoup moins sur la quantité

VISHING

- *Voice Phishing* : hameçonnage par téléphone
- Les attaques de type *vishing* fonctionnent bien lorsque l'organisation dispose de plusieurs départements relativement dispersés (informatique, commercial, RH…)
  - entre en contact avec un service
  - récolte des informations « insignifiantes »
  - appelle plus tard un autre service et utilise les infos récoltées pour gagner la confiance

HAMEÇONNAGE CIBLÉ

- Comme le *phishing*, mais des recherches spécifiques ont été faites sur la cible
- Le message, sur le fond et sur la forme, paraît provenir d’un expéditeur de confiance
- Potentiellement très difficile à détecter car forgé pour tromper tous les « radars à *phishing* » qui nous alertent habituellement, que l’on soit formé ou pas

FRAUDE AU PRÉSIDENT

- *Whaling* (« chasse à la baleine »)
- *Phishing* en se faisant passer pour un dirigeant haut placé dans l’organisation
- Cible notamment les employés qui ont des accès privilégiés
  - ⇒ transfert d’argent
  - ⇒ divulgation d’informations comptables ou financières

FRAUDE AU PRÉSIDENT - EXEMPLE

- 10 février 2022 : une comptable de la société de production Les Films Worso (Paris) reçoit un e-mail de sa directrice
- La directrice annonce qu'elle compte procéder à une offre publique d'achat à hauteur de 5 millions €
- La comptable est ensuite contactée par un avocat qui se présente au nom de la gérante de la société, afin de finaliser l'offre de rachat ; il lui demande la discrétion afin que la transaction puisse se faire sans encombre
- La comptable effectue par la suite 8 virements bancaires sur des comptes en Croatie pour un montant total de 2,5 millions…

DUMPSTER DIVING

- Fouille de poubelles !
- Tout type de document important doit être détruit avant d’être jeté
  - identifiants de connexion
  - données personnelles/sensibles
  - données administratives/comptables
  - …

SHOULDER SURFING

- « Espionnage par dessus l’épaule »
- On essaie typiquement de récupérer des identifiants de connexion en regardant l’écran et le clavier de la cible
- Contre-mesures :
  - mots de passe masqués
  - filtres de confidentialité

PHARMING

- « Dévoiement » en français
- Rediriger le trafic destiné à un site web vers un site malveillant
  - empoisonnement DNS
  - injection de fichier *hosts*
- Généralement utilisé pour *credential harvesting*

RÉCOLTE D’IDENTIFIANTS DE CONNEXION

- Identifiants de connexion = login + mot de passe
- On parle ici d’un grand nombre d’identifiants, et généralement pas d’une attaque ciblée
- De nombreuses techniques d’ingénierie sociale sont utilisées, notamment associées au *spamming*
- Différents types d’attaques techniques peuvent également être efficaces pour attaquer des sites ou des réseaux entiers
- Les identifiants sont ensuite revendus sur le *Darknet Market* ou utilisés en *credential stuffing*

CREDENTIAL STUFFING

- Tentative d’utilisation en masse d’identifiants de connexion
  - généralement obtenus par *credential harvesting* ou sur le *Darknet*
- On essaie chaque couple id/mdp sur un grand nombre de sites

TAILGAITING

- Profiter de l’entrée authentifiée d’une personne (grille, badge…) à un bâtiment ou une zone restreinte pour entrer avec elle
  - les gens veulent aider et être polis !
  - les ingénieurs sociaux le savent !
- Il faut apprendre aux usagers à refuser poliment l’accès commun, en rappelant qu’un système de badge permet :
  - de s’assurer que les personnes présentes sont autorisées
  - **mais aussi** de savoir qui est dans le bâtiment en cas de sinistre

PREPENDING

- Ajout de mentions (`@patrice`) sur les réseaux sociaux
  - tweets, forums, IM, commentaires de publication…
  - entraîne une augmentation immédiate du niveau d’engagement et d’intérêt de la cible
  - semble personnel mais souvent automatisé (+ IA)
- De plus en plus utilisé sous forme de messages privés (Discord !)

USURPATION D’IDENTITÉ

- *Identity fraud* ou *identity theft*
- Se faire passer pour quelqu’un d’autre sur un système ou auprès de quelqu’un
- Obtenue par différentes techniques, pas seulement l’ingénierie sociale :
  - vol d’identifiant / récolte d’identifiants
  - malware
  - capture de paquets et *replaying* sur un réseau…

ATTAQUE DE POINT D’EAU

- *Watering Hole Attack*
- Cible les sites que les utilisateurs d’une organisation spécifique utilisent régulièrement
  - le site est piégé par l’attaquant
  - tous ceux qui le visitent sont infectés
  - le compte pro ou personnel de la victime est alors compromis (l’attaquant a des accès)
- Le malware en question peut avoir différents objectifs (vol de données, scan de vulnérabilités, exploits, porte dérobée, mouvement latéral…)

TYPOSQUATTAGE

- *Typosquatting* ou *URL Hijacking*
- S’appuie sur le fait que les usagers font fréquemment des erreurs en tapant une URL (erreurs de frappe ou autre)
  - ex : `goggle.com`, `creditmutuel.org`, `disqord.com`…
- L’attaquant enregistre (achète) tous les noms de domaines proches du site cible qui sont libres
- La page affichée est une copie de la page d’accueil du site original
- Objectifs : *credential harvesting*, revenus de publicité…

SÉCURITÉ PHYSIQUE

- Protection physique des équipements et des accès : fondamental
  - vandalisme, vol, sabotage
- Accès à un appareil (mobile, station…) ?
  - implique **accès à ses données**
  - voire au **réseau d’entreprise**

CONSÉQUENCES POTENTIELLES

- Entreprises : 70 % atteintes de compromission de données sur l’année passée (dont **66 % dues à accès physiques non autorisés**)
- *Quoi ?*
  - surtout documents papier et ordinateurs portables
- *Où ?*
  - bureaux et véhicules
- *Comment ?*
  - principalement et évidemment par ***social engineering***

SÉCURITÉ PHYSIQUE - BONNES PRATIQUES

- Mise sous clé des équipements et documents importants
- Retirer immédiatement les documents imprimés
- Détruire les documents inutiles

SÉCURITÉ DES LAPTOPS

- Même niveau de sécurité que votre portefeuille
- Ne pas le laisser traîner dans des endroits douteux
- Cadenas pour portables
- Au minimum, verrouiller la session
- Attention aux regards indiscrets
  - réduire luminosité
  - utiliser un filtre

EFFICACITÉ DE L’INGÉNIERIE SOCIALE

- L’efficacité des techniques d’ingénierie sociale reposent sur quelques principes :
  - autorité
  - intimidation
  - consensus / acceptation sociale
  - familiarité / attachement
  - confiance
  - caractère d’urgence / peur

PRINCIPE D’AUTORITÉ

- L’attaquant paraît savoir de quoi il parle, et / ou a des connaissances certaines de l’organisation / du projet en cours…
- La position d’autorité se gagne en utilisant :
  - du jargon technique
  - des mots-clés actuellement populaires dans l’organisation (*buzzwords*)
  - des connaissances de systèmes ou d’applications spécifiques
- Ces connaissances sont acquises petit à petit (*vishing*…)
- La position d’autorité va alors en général être utilisée pour obtenir une information plus importante

PRINCIPE D’INTIMIDATION

- Certains principes (autorité, confiance…) permettent ensuite d’imposer des choses à la cible
  - menace d’actions négatives notamment
  - souvent combiné au principe d’urgence

CONSENSUS / ACCEPTATION SOCIALE

- Une personne agit plus facilement quand elle pense être en accord avec la majorité
  - cela peut lui faire prendre des choix qu'elle ne prendrait pas en temps normal
- Cf expérience de Asch : `dailymotion.com/video/x738r9`

FAMILIARITÉ / ATTACHEMENT

- Repose sur le fait que les gens achètent et utilisent des choses qu’ils connaissent et apprécient déjà
- C’est le même principe avec les personnes : on a plus tendance à se rapprocher des gens qui ont l’air plus « comme nous », ou en tout cas qui sont perçus comme tel
  - et on sera plus disposés à leur révéler des informations, à leur tenir la porte, etc.

CONFIANCE

- Évidemment, on va plus facilement agir / répondre lorsque l'on a confiance en la personne qui demande
  - base du bon commercial : acquérir la confiance du client est essentiel
- Moyens :
  - principes de familiarité et d'autorité
  - *name dropping*
  - *shoulder surfing*
  - *dumpster diving*
  - tout ce qui peut avoir l'air de dire : « je fais partie du *gang* »

PEUR / URGENCE

- On force la cible en lui faisant croire qu'ils doivent agir rapidement
- Par incitation négative : non-action ⇒ punition
  - *votre compte va être fermé*
  - *vous passerez à 19 % d'intérêts de remboursement mensuels avec effet immédiat*
- Mais aussi par incitation positive : action ⇒ récompense
  - *cette offre expire ce soir !*
- Tout ce qui doit être résolu dans l'urgence est suspect