LES ATTAQUES PHISHING

EL ITAOUI Reina HASSAN Youssef

M1 AMSD, Université Paris Cité - UFR des Sciences Fondamentales et Biomédicales

LES ATTAQUES PHISHING

Devenues l'une des menaces les plus courantes pour la (Figure 1), les attaques par phishing (ou hameçonnage) sont des tentatives frauduleuses d'obtenir des informations sensibles, telles que les mots de passe, les informations de carte de crédit et d'autres informations personnelles.

Figure 1. Les cyberattaques les plus communes, selon Statista.

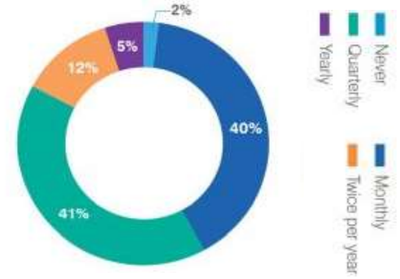

Figure 3. La fréquence des formations selon IT for business.

LES TYPES D'ATTAQUES PHISHING

Phishing par courriel : Envoi d'un courriel frauduleux à un utilisateur, prétendant être une source de confiance et demandant des informations sensibles.
Phishing par clonage de site web : Création d'un site web qui ressemble à un site légitime.réputé et qui demande aux utilisateurs de saisir leurs informations personnelles.
Phishing par SMS : L'envoi de SMS frauduleux qui demandent aux utilisateurs de saisir leurs informations personnelles en cliquant sur un lien.
Phishing de médias sociaux : Utilisation des plateformes de médias sociaux pour diffuser des messages frauduleux, comme des liens menant à des sites web malveillants.
Phishing d'assistance technique : L'attaquant se fait passer pour un représentant de l'assistance technique d'une entreprise ou d'un fournisseur de services, et demande aux utilisateurs de fournir des informations sensibles.

L'IMPACT SUR LE MONDE INDUSTRIEL

- **Fuite de données sensibles : Compromis** de la sécurité des informations sensibles et la **vie privée** des clients et des employés, c'est l'impact le plus commun (Figure 2)
- **Dommages à la réputation** et **chiffres d'affaires** des entreprises grâce à l'impact négatif sur la confiance des clients et la fidélité à l'entreprise
- **Coûts supplémentaires** comme les entreprises mettent en place des politiques de gestion des conséquences, notamment de restauration des systèmes de sécurité

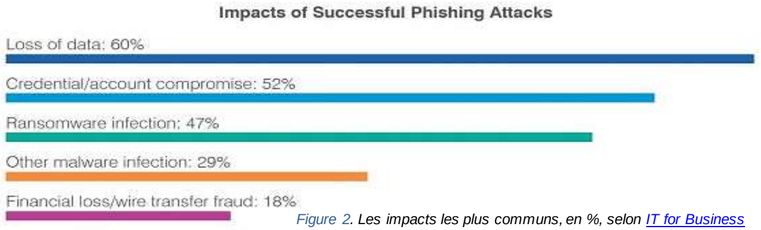

Figure 2. Les impacts les plus communs, en %, selon IT for Business

L'IMPACT SIGNIFICATIF SUR LA VIE DES UTILISATEURS

- Les utilisateurs peuvent être incités à fournir leurs informations bancaires ou financières à des escrocs, ce qui peut entraîner une **perte de fonds**.
- Les informations personnelles et sensibles peuvent être volées par les criminels, compromettant la sécurité et **la vie privée** des utilisateurs.
- Les utilisateurs peuvent télécharger involontairement des logiciels malveillants qui peuvent endommager leur ordinateur et compromettre leur **sécurité**.
- Les utilisateurs reçoivent des courriels, des appels et des messages **spam** frauduleux.

DES PRATIQUES DE SÉCURITÉ EN LIGNE

- Mettre en place **l'authentification à deux facteurs (2FA)**
- Ne **jamais fournir** des informations personnelles à des sources inconnues/réseaux **publics**
- Suivre des **sessions de formation** à propos des méthodes courantes de phishing (Figure 3)
- Utiliser et mettre à jour des logiciels antivirus et antimalware
- Utiliser des **mots de passe** forts et uniques
- **Vérifier les URL** (https) et les certificats de sécurité des sites web
- Rester attentif envers les courriels/messages

Figure 4. Le phishing en quelques chiffres selon AltoNeo.

DES TECHNOLOGIES DE SÉCURITÉ EN LIGNE

- **L'authentification à deux facteurs (2FA)** pour les employés et leur formation sur les méthodes courantes utilisées par les attaquants de phishing
- **La validation de domaines** et des **certificats SSL**
- La mise en place de **politiques de sécurité** et la **surveillance régulière** des activités
- L'implémentation des **algorithmes de filtrage**
- L'installation des **logiciels de sécurité** sur tous **les ordinateurs de l'entreprise** (Figure 4)

PERSPECTIVES À LONG TERME

Les **algorithmes de l'IA et de l'apprentissage machine** peuvent aider à détecter et à prévenir les attaques plus rapidement
La migration des systèmes d'entreprise vers le **cloud computing** offre des opportunités pour les attaquants, mais protège aussi les données grâce à la centralisation.
La sécurité **basée sur les comportements** peut aider à identifier les activités anormales dans les réseaux et à prendre des mesures pour les empêcher.
Les **réglementations** sur la protection des données encouragent les entreprises à adopter des pratiques de sécurité plus rigoureuses pour protéger les informations sensibles.

DÉFIS FUTURS

- Le développement de **nouvelles techniques** de phishing
- L'utilisation de la messagerie instantanée et les **réseaux sociaux**
- La **connaissance insuffisante** de la sécurité en ligne
- La **prolifération des objets connectés**, tels que les appareils domestiques intelligents

NOTRE MODÈLE DE DÉTÉCTION DE PHISHING

Notre modèle **détecte les liens malveillants** et identifie leurs **caractéristiques importantes** (Figure 5) grâce à une comparaison de 500 liens de phishing et 500 liens légitimes, et donc peut être utilisé pour reconnaître et **éviter les attaques**.
Les **caractéristiques détectées** sont les suivantes : présence d'une adresse IP, présence d'un caractère "@" dans l'URL, existence d'un préfixe ou suffixe dans l'URL, présence d'un enregistrement DNS, longueur de l'URL, possibilité de cliquer avec le bouton droit de la souris et capacité de redirection du site. Ces facteurs peuvent désormais être utilisés pour entraîner les modèles de ML qui **identifient les liens de** phishing avec une **bonne précision**. Nous avons créé trois modèles en utilisant les algorithmes de régression logistique, forêt aléatoire et KNN. L'efficacité des modèles a été évaluée en utilisant **le score AUC** et le meilleur score a été obtenu par le modèle de **régression logistique** (Figure 6- ROC Curve).
Tout est clairement expliqué dans nos **jupyter notebooks sur GitHub.**

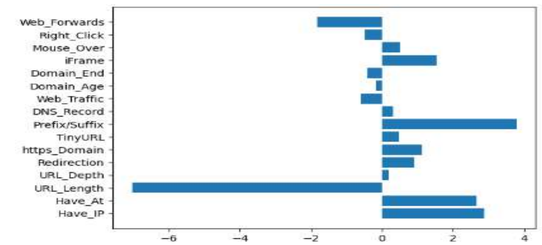

Figure 5. Importance des caractéristiques

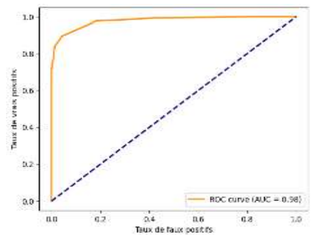

Figure 6. ROC Curve

VICTIMES DE PHISHING, QUE FAIRE ?

- **Contacter l'organisme** concerné pour confirmer le message ou l'appel reçu
- Faire **opposition** immédiatement auprès de votre organisme bancaire ou financier
- Conserver les **preuves** et le **message** d'hameçonnage reçu
- **Déposer plainte** au commissariat de police ou à la brigade de gendarmerie
- Si vous êtes un particulier, contacter une association de France Victimes au **116 006**
- **Changer** immédiatement **vos mots de passe** compromis
- **Signaler** tout message ou site douteux à Signal Spam, PHAROS, ou au 33 700
- **Signaler** l'adresse d'un site d'hameçonnage à **Phishing Initiative** qui bloquera l'adresse
- **Contacter** la **plateforme** Info Escroqueries **du ministère de l'Intérieur** pour être conseillé

RGPD ET CNIL

Le Règlement Général sur la Protection des Données (**RGPD**) exige que les entreprises prennent les **mesures nécessaires** pour protéger les données personnelles, se conformant aux directives de la CNIL, Commission Nationale de l'Informatique et des Libertés. La collaboration avec la CNIL est essentielle pour s'assurer que les pratiques sont conformes aux réglementations, notamment en ce qui concerne la **prévention du phishing**.
En cas **de violation de données**, les entreprises sont tenues de **signaler** l'incident dans les 72 heures suivant sa découverte avec les **sanctions pour non-conformité** pouvant atteindre jusqu'à 4% du chiffre d'affaires annuel mondial d'une entreprise.