


## Challenge 1 : Analyse d'un email frauduleux

**Contexte** : Kermit la Grenouille a reçu une plainte de Peggy, une de ses amies, suite à un incident de phishing dans lequel elle a reçu un email prétendant venir de Kermit, lui offrant une opportunité de "gagner une journée avec lui". Cependant, après avoir suivi le lien dans le message, elle a découvert que tous ses mots de passe étaient désormais visibles publiquement.



 **Objectif de l'analyse** : L'objectif principal de cette mission est de procéder à une analyse approfondie du mail suspect que Peggy a reçu, en vue de comprendre l'attaque dont elle a été victime et d'identifier les risques associés à cette tentative de phishing. Vous devrez évaluer si l'email correspond à une attaque de spear-phishing<sup>1</sup> et de spoofing<sup>2</sup>, et déterminer les serveurs ainsi que les adresses IP malveillantes impliquées. Il sera également essentiel d'examiner le type de stealer<sup>3</sup> déployé dans cette attaque, de comprendre son fonctionnement, d'identifier son origine et d'analyser ses mécanismes d'exfiltration de données.

### Livrable attendus (Optionnel)

- Rapport d'analyse détaillée sur l'attaque, le type de phishing, et les techniques utilisées par le Redline Stealer.
- Liste des serveurs malveillants et des adresses IP associées à l'attaque, y compris des liens vers les bases de données de reconnaissance des menaces comme [AbuseIPDB](#) ou [Cisco Talos](#).
- Recommandations de sécurité pour Peggy, y compris des actions à prendre immédiatement pour sécuriser ses comptes et éviter une future compromission.
- Plan de prévention pour des utilisateurs professionnels ou pour d'autres victimes potentielles, visant à renforcer les mesures de sécurité contre le phishing et les malwares.

### Fil rouge (Si besoin d'aide)

#### Analyse de l'email et identification du type de phishing :

- a. Décrypter l'email reçu par Peggy, en identifiant les éléments spécifiques qui indiquent un spear-phishing ciblé et une usurpation d'identité (spoofing).
- b. Examiner les en-têtes de l'email pour vérifier si des techniques de falsification des informations d'expéditeur ont été utilisées (spoofing), et analyser les liens et pièces jointes pour identifier les comportements suspects.

#### Identification des serveurs et adresses IP malveillantes :

- c. Rechercher les adresses IP malveillantes et les serveurs SMTP utilisés pour l'envoi de l'email, en s'appuyant sur les en-têtes de l'email et les rapports d'IP associées à des activités de phishing ou de malware.

- d. Analyser les domaines malveillants dans les en-têtes pour déterminer leur origine et leur lien potentiel avec des campagnes de phishing et de vol de données.

Analyse du stealer (Redline Stealer) :

- e. Identifier le stealer utilisé dans cette attaque, en particulier s'il s'agit du Redline Stealer, un malware conçu pour voler des informations sensibles comme des mots de passe et des informations bancaires.
- f. Comprendre comment ce malware s'installe sur le système de la victime, comment il exfiltre les données volées, et identifier les serveurs de commande et de contrôle (C&C) utilisés pour la transmission des données.
- g. Analyser la façon dont ce type de malware pourrait éviter les systèmes de détection classiques (comme les antivirus) et comment il persiste dans le système de la victime.

Impact de l'attaque sur la victime :

- h. Évaluer les conséquences sur Peggy, notamment l'exposition de ses mots de passe et autres informations personnelles sensibles.
- i. Identifier les risques associés à la compromission de ces données, y compris le vol d'identité, la fraude bancaire, et l'accès non autorisé à ses comptes en ligne.

Recommandations pour éviter de futures attaques :

- j. Proposer des mesures pour protéger la victime (Peggy) et d'autres utilisateurs contre des attaques similaires, telles que la mise à jour des mots de passe, l'activation de l'authentification à deux facteurs, et la mise en place de systèmes de détection de phishing.
- k. Développer des pratiques de sécurité à long terme, y compris la formation des utilisateurs sur les dangers des emails de phishing et la mise en place de filtres anti-phishing plus robustes pour les entreprises.

*Spear-phishing<sup>1</sup>*: Le spear-phishing est une attaque ciblée où un pirate envoie un e-mail ou un message personnalisé pour tromper une personne et lui faire révéler des informations sensibles.

*Spoofing<sup>2</sup>*: Le spoofing est une technique où un pirate usurpe une identité, comme une adresse e-mail ou un numéro de téléphone, pour tromper une personne ou un système.

*Stealer<sup>3</sup>*: Un stealer est un logiciel malveillant conçu pour voler des données sensibles, comme des mots de passe ou des informations bancaires, sur l'ordinateur d'une victime.