Sensibilisation à la cybersécurité opérationnelle
Notes complémentaires

Menaces

Les **ransomwares**, logiciels permettant d'exfiltrer des données et de chiffrer les données des victimes en vue du paiement d'une rançon, et le **phishing** constituent les menaces principales actuelles. Elles sont à prendre au sérieux, car de plus en plus difficiles à détecter.

Quelques définitions

Phishing ou hameçonnage : email malveillant élaboré pour tromper le destinataire et l'inciter à charger un fichier contenant un malware ou à fournir à son auteur des informations sensibles (identifiant, mot de passe, second facteur d'authentification, données confidentielles…).

Spear phishing : Phishing ciblé sur des employé.e.s d'une organisation disposant de droits élevés.

Fraude au Président : Fraude utilisant le plus souvent les emails ou le téléphone, ciblant principalement les personnes en charge des finances dans une organisation. L'attaquant se fait passer pour un haut responsable et exerce une forte pression sur un.e employé.e pour faire transférer en urgence des fonds sur un compte à l'étranger sans respecter les procédures internes.

Smishing : Version SMS du phishing.

Vishing : Version message vocal du phishing.

Whaling : Phishing sophistiqué et ciblé sur des personne occupant des fonctions dirigeantes dans une organisation (Président, CEO, COO, CIO…).

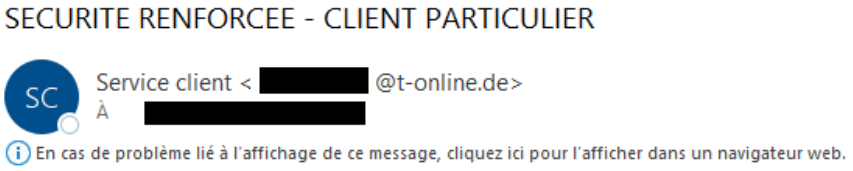
Phishing : processus

L'attaquant suscite le plus souvent la **peur** chez le destinataire du phishing en utilisant **l'urgence** ou la **menace** (suppression ou suspension de son compte, retrait d'argent, annulation ou retard de livraison, fausse facture, renvoi/licenciement, poursuites pénales, fausses accusations, notification de poursuites, etc.).
L'intelligence artificielle générative ouvre la porte aux fausses photos, vidéos ou bandes son pour renforcer la peur. Cette émotion négative pousse le destinataire à la recherche d'une solution pour la réduire ou la remplacer par une autre émotion. Dans son message, l'attaquant propose une solution raisonnable qui offrira un soulagement au destinataire. Il lui suffit d'ouvrir la pièce jointe, de cliquer sur un lien, de remplir un formulaire ou de répondre à l'email.

Phishing : indices

Les attaquants s'adaptent en permanence pour éviter les systèmes de détection et profiter de l'inattention des destinataires. Il n'existe donc pas de recette miracle pour détecter le phishing, et il est nécessaire de prêter attention à certains indices :

1. Le nom affiché (« *display name* ») ne correspond pas à l'**adresse de l'expéditeur** et peut faire croire que l'email provient de l'organisation au lieu de l'extérieur.
   Exemple (réel) : « Service client », avec une adresse d'expédition « @t-online.de » pour une prétendue société suisse.

   Le d*isplay name* est choisi par l'expéditeur et ne fournit aucune garantie sur l'identité de l'expéditeur. Attention, certains outils de messagerie masquent l'adresse de l'expéditeur et ne montrent que le d*isplay name*, ce qui ne permet pas de vérifier l'adresse. Évitez cela et configurez si possible votre outil de messagerie pour voir l'adresse réelle de l'expéditeur.

2. Le **nom de domaine** de l'expéditeur peut s'approcher d'un nom de domaine connu : « epfi.ch », « microsft.com », …

3. Le phishing, hors *spear phishing*, est envoyé à un grand nombre de personnes, souvent par vagues. Ainsi, les **formules de salutation** sont génériques (« Cher client », « Cher utilisateur », …).

4. L'attaquant utilise la **peur** pour inciter à ouvrir la pièce jointe, à cliquer sur un lien ou à remplir un formulaire. La pièce jointe peut être un fichier d'un outil de bureautique contenant une macro ou un script, ou être un exécutable ou une page web.

5. Le message peut **contenir un lien** vers un site hébergeant du contenu malveillant. Ce lien peut être masqué derrière un libellé anodin (« lien », « cliquer ici »…).

6. Le **style du message** ne correspond pas à ce qui est attendu de l'expéditeur (trop familier ou trop formel, fautes de français ou d'orthographe, tournures de phrase maladroites. etc.). Cependant, les outils d'intelligence artificielle générative sont de plus en plus utilisés par les attaquants et la qualité des messages est en constante augmentation.

7. La présence d'un **ancien logo** d'entreprise ou de l'EPFL peut être un indice de phishing.

8. La présence d'une adresse postale de l'expéditeur ne permet pas à elle seule de s'assurer que l'email est légitime.

9. La **signature** est souvent **générique** et ne permet pas de contacter l'expéditeur sans répondre à l'adresse de l'expéditeur ou en suivant ses instructions.

10. L'attaquant peut avoir compromis la boîte aux lettres de votre interlocuteur ou d'une personne en copie d'un email qui vous a été adressé, avant de tenter de s'introduire dans la conversation.
    Dans l'exemple (réel) suivant, l'attaquant a eu accès (p.ex. via une première victime) à un vrai email envoyé par Mike Walthers (nom fictif) et a acheté un nom de domaine très proche visuellement (« vvrgs » au lieu de « wrgs » ; noms fictifs) afin de détourner les échanges avec sa prochaine victime :

De : Mike Walthers <mike.walthers@vvrgs.com>
Envoyé : vendredi 30 août 2024 14:17
À : vous
Objet : TR: Votre candidature pour le stage de développement en C++

Cher Monsieur,

Je vous prie de remplir le formulaire en ligne vvrgs.com/startform afin de compléter votre dossier.

Avec nos meilleures salutations,

Mike Walthers

Water Recycling Global Solutions Limited

> **De :** Mike Walthers <mike.walthers@wrgs.com>
> **Envoyé :** jeudi 29 août 2024 9:36
> **À :** vous
> **Objet :** Votre candidature pour le stage de développement en C++
>
> Cher Monsieur,
>
> Nous avons le plaisir de vous informer que vous avez été retenu pour le stage de développement en C++ auquel vous avez postulé au sein de notre établissement. Nous nous réjouissons de vous accueillir le 10 septembre 2024 à 9 heures dans nos locaux rue du Rhône à Genève.
>
> Nous vous prions de vous munir d'une pièce d'identité afin d'établir votre badge d'accès.
>
> Avec nos meilleures salutations,
>
> Mike Walthers
>
> Water Recycling Global Solutions Limited

Phishing : autres vecteurs

Toutes les attaques de phishing ne sont pas nécessairement faites par voie email. Elles peuvent aussi être menées par SMS, voire même directement par téléphone (appel). Ce dernier moyen est en augmentation. Méfiez-vous donc aussi des appels qui engendrent **urgence** ou **peur**.

Que faire si l'on a cliqué sur le lien contenu dans l'email de phishing ?

- Informer le Help-Desk EPFL (1234@epfl.ch)
- Si le lien conduit à un formulaire, vérifier si le nom de domaine correspond à ce qu'il devrait être, et relever les anomalies : par exemple site hébergé à l'étranger pour une prétendue banque Suisse, différence d'orthographe entre le nom de domaine et le prétendu expéditeur, hébergeur peu connu… Le formulaire peut inciter à fournir des informations qui ne devraient jamais être demandées comme le code PIN de la carte de crédit. Si c'est le cas, il faut quitter immédiatement le formulaire et détruire l'email.
- Si le lien visait à télécharger un fichier sur l'ordinateur, lancer l'anti-virus pour vérifier s'il s'agit d'un malware. Il est possible de charger le fichier sur https://www.virustotal.com/gui/home/upload pour une vérification multi antivirus en ligne. Ne pas tenter d'ouvrir le fichier et le supprimer en cas de doute, puis détruire l'email.
- Si des informations personnelles (nom d'utilisateur, mot de passe) ont été saisies sur un site frauduleux, réinitialiser immédiatement l'intégralité des mots de passe (E-banking, Google, Compte EPFL, etc…)

Que faire si l'on a ouvert le fichier contenu dans l'email de phishing ?

- Informer le Help-Desk EPFL (1234@epfl.ch)
- Lancer l'anti-virus sur l'ordinateur.
- Tant qu'un doute subsiste, ne se connecter à aucun site nécessitant de saisir un mot de passe.
- En cas de comportement anormal de la machine, la réinstaller à partir d'une source sûre.

À retenir

En cas de doute :

- Ne pas cliquer sur le lien et ne pas ouvrir la pièce jointe.

- Ne jamais répondre à l'email ni appeler le numéro de téléphone proposé : contacter l'expéditeur par un autre canal et sans utiliser les informations contenues dans l'email (par exemple utiliser une ancienne facture pour trouver le numéro de contact ou le site web ; rechercher le numéro de téléphone dans l'annuaire ; se connecter à la plateforme où la commande a été faite pour voir où en est la livraison).

Il est important d'anticiper les difficultés en installant un antivirus et en le tenant le à jour, mais aussi en effectuant régulièrement des sauvegardes de ses données.