Agir contre une campagne d'hameçonnage

*Fiche à l'attention des **responsables de la sécurité des systèmes d'information (RSSI)***

Objectifs de la campagne

La technique de **l'hameçonnage** (phishing) consiste à usurper l'identité d'un tiers légitime dans le but d'obtenir des informations sensibles pour accéder à des comptes (messagerie, VPN, administration, etc…) en vue de réaliser des actions malveillantes (spam, intrusion, fraude, etc…). Elle est basée sur l'utilisation de la messagerie électronique, de SMS et de portails Web. Une fiche de sensibilisation est disponible sur le portail **cybermalveillance.gouv.fr.**

Actions de confinement

- **Désactiver les comptes compromis.**
- **Couper toutes les sessions en cours liées aux comptes compromis** sur le webmail/IMAP/POP (sur office365 le jeton/token d'actualisation a une durée de vie de 90 jours et peut rester valide après la réinitialisation du mot de passe (https://docs.microsoft.com/fr-fr/azure/active-directory/develop/refresh-tokens); il faut l'invalider par commande powershell: https://docs.microsoft.com/fr-fr/powershell/module/azuread/revoke-azureaduserallrefreshtoken?view=azureadps-2.0).
- Si l'utilisateur a **un accès VPN alors désactiver son compte** puis vérifier qu'il n'y a pas eu de connexion suspecte, sinon couper la session et prévenir immédiatement le CERT Santé.
- Identifier s'il s'agit d'une action d'hameçonnage (l'utilisateur a donné son mot de passe à son insu). Si c'est le cas, identifier si l'action a été faite lorsque l'utilisateur était sur son lieu de travail et l'heure approximative afin d'identifier le lien malveillant pour le bloquer (firewall ou proxy) ; vérifier qu'aucun autre utilisateur ne l'a utilisé pour transmettre son mot de passe.
- Si le mot de passe n'a pas été transmis (ou s'il y a un doute), alors **isoler le poste de travail** qui pourrait avoir été compromis. Si l'utilisateur est administrateur local du poste alors il faut réinitialiser le compte de tous les utilisateurs qui ont réalisé une connexion "interactive" sur le poste (ex: rdp/connexion physique sur le poste) et vérifier les connexions VPN de ces utilisateurs. Prévenir le CERT Santé qui pourra vous aider dans l'analyse du poste (pensez à extraire tous les logs des connexions sortantes vers internet pour aider à l'analyse).
- Si le serveur de messagerie est géré par le service informatique (ex: Exchange on premise), **vérifier que le serveur est à jour des derniers patch de sécurité**. Si ce n'est pas le cas, passer l'outil MSERT sur tous les serveurs du cluster de messagerie. Si MSERT détecte un élément, alors isoler votre serveur et contacter le CERT Santé immédiatement. Dans le cas contraire, appliquer les mises à jour à l'ensemble du cluster en débutant par le serveur webmail.
- Si l'utilisateur du compte compromis avait des identifiants permettant l'accès à des ressources sur internet dans les courriels présents dans la boite, il faut **changer les mots de passe**.
- Si le mot de passe volé était ré-utilisé sur d'autres accès internet (personnels ou professionnels), alors il faut **changer le mot de passe sur l'ensemble de ces accès**.

Actions de remédiation

- **Vérifier la configuration de la boite de l'utilisateur** (sur office365, vous pouvez utiliser l'outil https://github.com/CrowdStrike/CRT) afin de vérifier qu'il n'y a pas eu de modifications illégitimes (redirection, ...).
- **Réinitialiser les mots de passe des comptes compromis**, et si possible **activer l'authentification à multi-facteurs** (attention il n'est pas possible de mettre en place de l'authentification multi-facteurs sur des protocoles dits "legacy" [IMAP, ActiveSync, SMTP, POP, ...], il est donc préférable de ne pas utiliser ces protocoles sur internet).
- Si possible, **mettre le webmail derrière le VPN**. Sinon, avec Exchange on premise, **filtrer l'accès aux adresses IP françaises**. Attention, l'activation de cette option ne permettra plus de voir rapidement si une boite a été compromise par une règle de détection simple (connexion réussie depuis une adresse IP à l'étranger = boite compromise), cependant, si vous n'avez pas les capacités pour réaliser cette détection en temps réel, il est préférable d'activer cette règle. Dans le cadre d'office 365, activer l'accès conditionnel (https://docs.microsoft.com/fr-ca/azure/active-directory/conditional-access/overview).
- Identifier **pourquoi le courriel de phishing a réussi à contourner vos protections** de messagerie et renforcer ces protections. Dans cet objectif, le CERT Santé conseille d'appliquer les recommandations présentées dans le document suivant : https://github.com/cybersante/mx_sec_conf.
- Vérifier que vous disposez d'assez de **rétention de journaux** (3 à 6 mois de préférence) sur les éléments suivants : journaux des connexions sortantes vers internet, journaux des authentifications réussies sur la connexion VPN, journaux des requêtes vers votre serveur webmail.
- Sensibiliser l'utilisateur **à ne pas communiquer ses identifiants**, ni d'ouvrir des pièces jointes suspectes.

Alerter des tiers

Phishtank & Signal Spam / @abuse du domaine émetteur des courriels.

Si la campagne provient d'une adresse légitime, **informer l'organisation concernée ou l'hébergeur du domaine.**