Agir contre une campagne de courriels contenant un maliciel

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

Objectifs de l'attaque

Compromettre des environnements utilisateur, en vue de s'infiltrer plus en profondeur dans un système d'information.

Mesures de détection

- **Surveiller l'espace de quarantaine de la messagerie** qui peut permettre d'identifier des campagnes de maliciels en cours.
- **Mettre en place un module sur le client de messagerie** permettant de remonter les courriels suspects au responsable sécurité (avec l'entête et tous les éléments nécessaires).
- **Surveiller les journaux du proxy** (blocage urlhaus, téléchargements suspects, url complexe accédée sans aucun « referer »...).
- **Surveiller quotidiennement les flux anormaux** de réception et d'envoi de courriels, par exemple le « top 20 » des courriels les plus diffusés en réception et en émission, les stats de supervision de la congestion de la file d'attente et les stats DMARC (usurpation du nom de domaine).
- **Surveiller les alertes antivirus des postes en lien avec des fichiers provenant d'internet** (emplacement de téléchargement, emplacement courriel).

Actions de confinement

- **Isoler le poste potentiellement infecté du réseau** en le laissant allumé afin d'effectuer des captures en vue d'une analyse forensique (allumé pour la RAM).
- **Désactiver** le compte des utilisateurs compromis.
- **Si l'utilisateur a un accès VPN,** alors désactiver le compte et vérifier qu'il n'y a pas de connexion suspecte, sinon couper la session et prévenir immédiatement le CERT Santé.
- **Vérifier que les sauvegardes sont intègres** et les isoler du réseau jusqu'à la fin de l'investigation (bien isoler le réseau où se trouve réellement vos sauvegardes - ex: SAN/NAS)
- **Vérifier la console antivirus du parc**. S'il y a des détections sur des serveurs, alors contacter immédiatement par téléphone le CERT Santé ou le CERT-FR.
- **Couper toutes les sessions des utilisateurs compromis** en cours 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).
- I**dentifier si l'utilisateur a ouvert le fichier malveillant**. Il faut identifier si l'action a été faite lorsqu'il était connecté au SI, ainsi que l'heure approximative, afin d'identifier les connexions malveillantes du maliciel pour les bloquer (logs firewall, proxy) et vérifier qu'aucun autre poste n'a communiqué vers ces adresses.
- Si l'utilisateur a potentiellement **ouvert le fichier,** il faut **réinitialiser les comptes de tous les utilisateurs** qui ont réalisé une connexion sur le poste et vérifier les connexions VPN pour ces utilisateurs. Si un compte administrateur du domaine avait préalablement réalisé une connexion sur le poste alors en informer immédiatement le CERT Santé.
- **Si l'utilisateur conserve des identifiants sur son poste**, il est impératif de **changer les mots de passe**

Alerter des tiers

Phishtank & Signal Spam / @abuse du domaine émetteur des courriels.
Si l'attaque provient d'une adresse légitime, **informer l'organisation concernée ou l'hébergeur du domaine.**

Agir contre une campagne de courriels contenant un maliciel

Récolte d'artefacts en vue d'une investigation

Si l'environnement informatique ou le compte d'un utilisateur a fait l'objet d'une **compromission** (ou s'il y a **suspicion de compromission**) par le biais d'une pièce jointe contenant du code malveillant, ou un lien qui mène vers du contenu malveillant, vous pouvez contacter le CERT Santé pour vous aider à traiter l'incident.

Les pièces numériques à transmettre au CERT Santé sont les suivantes :

- **Copie du courriel malveillant reçu** par le/les utilisateur(s) (**EML** ou **PST** pour analyse (pas de transfert du mail), le message d'origine reçu par l'utilisateur) **avec les pièces jointes associées** ;
- **Si le poste est nomade** et est utilisé pour se connecter à d'autres SI, **veillez à le signaler lors de votre déclaration d'incident** et à indiquer où ce poste était connecté lors de la compromission ;
- **Journaux des connexions sortantes vers internet** sur une durée de 30 jours minimum comprenant la date de l'incident ;
- Indiquer les actions de confinement réalisées selon la liste ci-dessus ;
- **Journaux de l'antivirus de l'ensemble du parc** si possible sur 30 jours minimum ;
- **Journaux d'authentification des connexions VPN** sur 30 jours si l'utilisateur dispose d'un tel accès.

Pour se prémunir - Démarche de durcissement

Afin d'entamer une démarche de durcissement de la sécurité de votre infrastructure, le CERT Santé conseille d'appliquer les recommandations présentées dans le document suivant : https://github.com/cybersante/mx_sec_conf

Le CERT Santé met à disposition un outil de test en ligne de la sécurité de la messagerie. La demande d'accès au service est à réaliser par mail à cyberveille@esante.gouv.fr. Ce service a pour but d'identifier les améliorations à apporter dans la configuration des règles de sécurité de la messagerie pour réduire le risque de manipulation de contenus malveillants par les utilisateurs.
Il permet de vérifier que la politique de contrôle des messages et de leur contenu a pris en compte les principales menaces issues de l'émetteur, de métadonnées du message (en-tête, encodage, découpage en plusieurs parties, …), d'une pièce jointe (spam, virus, …), d'une URL (hameçonnage), ainsi qu'une multitude d'autres tests.