Sécurité numérique en santé

TOUS CYBER VIGILANTS EN PAYS DE LA LOIRE

MÉMO

COLLECTE DES TRACES SUITE A UN INCIDENT SI D'ORIGINE MALVEILLANTE

Rédigé en partenariat avec : Gendarmerie nationale

RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité

ars Agence Régionale de Santé Pays de la Loire

e-santé Pays de la Loire

Pays de la Loire

Sécurité numérique en santé

MÉMO – Collecte des traces suite à un incident SI d'origine malveillante

[Octobre 2023]

La collecte de traces suite à un incident numérique d'origine malveillante est une action nécessaire à l'investigation et au dépôt de plainte.

OBJECTIFS

- ✓ Mettre à disposition des personnes en charge de l'investigation numérique et des forces de l'ordre des éléments techniques nécessaires.
- ✓ Déterminer le chemin d'attaque et les faiblesses exploitées pour pouvoir y remédier.
- ✓ Identifier un responsable.
- ✓ Fournir de preuves recevables pour engager une procédure.

ACTEURS CONCERNÉS

- ✓ Utilisateurs du SI
- ✓ Responsable réseau
- ✓ Responsable applicatif
- ✓ Direction des systèmes d'information
- ✓ RSSI

PRÉSERVER TOUTES LES TRACES

✓ **Déconnecter du réseau** (câble / wifi / cartes réseaux virtuelles pour les machines virtualisées) les appareils concernés pour stopper l'incident et **mettre en quarantaine les machines** et **supports de stockage amovibles** concernés (disque externe, clé USB…) ou récemment connectés aux machines concernées.

✓ **Ne pas éteindre électriquement** les appareils compromis pour éviter la perte d'informations en mémoire. Si besoin, brancher les ordinateurs portables / smartphones / tablettes sur secteur.

✓ Tenir une main courante traçant l'ensemble des actions / évènements.

✓ **Identifier** si possible le « **patient zéro** » (première machine compromise) et l'**isoler**.

✓ **Effectuer une copie complète de la mémoire** (RAM) de l'appareil ou du fichier mémoire pour une machine virtualisée (.vmem pour Virtual Machine volatile memory file ou .vmss pour Virtual machine suspend file sur une machine VMWare).

✓ Si besoin de déplacer l'appareil ou si ce dernier est inutilisable, le mettre en **état de veille prolongée** (machine physique ou virtuelle) puis attendre 15 secondes avant de retirer le câble d'alimentation de la prise de courant (machine physique uniquement). Afin de **maximiser les chances de pouvoir conserver les traces,** tout appareil en veille doit être **rebranché électriquement**. **Identifier clairement la non-disponibilité** des matériels concernés (ordinateur, disque dur externe…) pour les utilisateurs en effectuant un marquage clair sur l'appareil « **cyberattaque, ne pas éteindre / allumer / connecter l'appareil** ».

✓ **Ne pas rallumer** le poste de travail ou l'appareil compromis, **si** ce dernier est **éteint**.

✓ Prendre des **photos** ou faire des **captures d'écran d**e tout ce qui est visible.

✓ Récupérer les **fichiers de journalisation** (logs) de vos pares-feux (sans se limiter aux données présumées relatives à l'attaque), des serveurs mandataires (proxys), des postes ou serveurs touchés qui seront des éléments d'investigation.

✓ Effectuer une **copie complète** (disque dur) des machines impactées en privilégiant les copies intégrales (dite « bit à bit »). Des outils libres et gratuits tels que EWF Tools sont dédiés à l'acquisition de données pour l'investigation numérique. L'utilisation **d'un bloqueur physique** permettant d'éviter toute altération des données sur le support d'origine est **fortement recommandée**.

Vous pouvez vous faire assister d'un professionnel pour réaliser certaines actions ou pour conserver le matériel à disposition des enquêteurs. Il est aussi possible, selon les enjeux, de réaliser ces actes en présence d'un huissier de justice.

Gendarmerie nationale
RÉPUBLIQUE FRANÇAISE
ars Agence Régionale de Santé Pays de la Loire
e-santé GRADeS Pays de la Loire
Pays de la Loire

Sécurité numérique en santé

MÉMO – Collecte des traces suite à un incident SI d'origine malveillante

[Octobre 2023]

La collecte de traces suite à un incident numérique d'origine malveillante est une action nécessaire à l'investigation et au dépôt de plainte.

RECEVABILITÉ D'UNE TRACE EN TANT QUE PREUVE

✓ En plus d'un usage interne pour comprendre l'origine et le périmètre de l'incident survenu sur votre système d'information, les traces collectées peuvent constituer des **preuves à valeur juridique** en cas d'engagement d'une procédure suite à un dépôt de plainte.

✓ Pour permettre l'utilisation des traces recueillies comme éléments de preuve, il est recommandé de veiller à respecter les éléments ci-dessous :

- ✓ Les informations fournies doivent avoir été **obtenues légalement**.
- ✓ **Répertorier dans une main courante pour chaque action / évènement** :
  - ✓ Description de l'action / évènement.
  - ✓ Noter l'heure et si besoin l'écart entre l'heure de la montre et l'heure du système.
  - ✓ Indiquer le nom et la fonction de la personne ayant réalisé l'action, ainsi que ces informations pour celle à l'origine de la demande.
  - ✓ Les logiciels / applications utilisés doivent être indiqués avec leur version précise et l'horodatage de leur dernière mise à jour.
  - ✓ Calculer l'empreinte des fichiers collectés pour prouver leur intégrité (sha256 minimum : ***Get-FileHash nom_du_fichier*** sous Windows Powershell / ***sha256sum nom_du_fichier*** sous Linux).
  - ✓ Nommer et identifier clairement les appareils concernés.
  - ✓ Identifier le prestataire de service ayant fourni la donnée (le cas échéant).
- ✓ Récupérer les éléments (journaux proxy, pare-feu, WAF, IDS, EDR …) au **plus proche du moment de l'incident.**
- ✓ **Conserver** les éléments recueillis dans **un lieu sûr, sécurisé** dont l'accès est restreint et surveillé.

✓ L'ensemble de ces conditions doit être **appliqué par vos prestataires**, le cas échéant.

AUTRES ÉLÉMENTS UTILES À PARTAGER LORS DU DÉPÔT DE PLAINTE

- ✓ L'architecture du réseau informatique,
- ✓ Les mails en lien avec l'incident,
- ✓ L'organigramme de la structure,
- ✓ Les coordonnées et périmètres des différents prestataires informatiques,
- ✓ …

Gendarmerie nationale

Sources

ATTAQUES PAR RANÇONGICIELS, TOUS CONCERNÉS - COMMENT LES ANTICIPER ET RÉAGIR EN CAS D'INCIDENT ? - ANSSI 2020
Piratage d'un système informatique professionnel, que faire ? – ACYMA 2021
Réagir à une attaque informatique : 10 préconisations – DCPJ 2016

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Pays de la Loire
e-santé GRADeS Pays de la Loire
Pays de la Loire