Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Compromission Infostealer

Endiguement

2026

InterCERT FRANCE

A qui s'adresse-t-elle ?

- Responsables de la sécurité des systèmes d'information (RSSI)
- Administrateurs du système d'information

Quand l'utiliser ?

Utiliser cette fiche lorsqu'une compromission est fortement suspectée (levée de doute en cours) ou confirmée sur un compte du système d'information par un infostealer.

À quoi sert-elle ?

L'objectif de cette fiche est de proposer les premières actions d'*endiguement* ayant pour objectif de circonscrire l'attaque. Elles tenteront de *limiter son extension et son impact* et de donner du temps aux défenseurs pour s'organiser et reprendre l'initiative.

Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie Actions d'endiguement par priorités pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante.
- La partie Actions d'endiguement par thèmes détaille les différentes actions d'endiguement possibles selon différents axes thématiques.

Si l'organisation estime avoir besoin d'aide pour réaliser ces actions d'endiguement, elle peut contacter des équipes spécialisées en réponse à incident, qu'elles soient internes ou externes : voir la partie Contacts.

SOMMAIRE

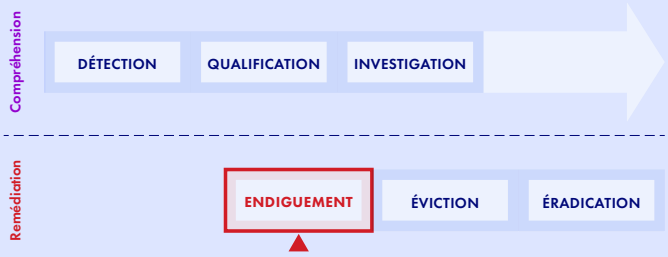
Prérequis 3

Actions d'endiguement par priorités 5

Actions d'endiguement par thèmes 6

Suite des actions 12

Annexes 13



PRÉREQUIS

Demander de l'aide

Ne jamais rester seul face à un incident. Solliciter l'aide d'un collègue afin de ne pas assumer seul la responsabilité de son traitement et de pouvoir répartir efficacement les tâches. Par exemple, une personne peut se concentrer sur l'approfondissement de la qualification de l'incident, tandis que d'autres peuvent contacter un responsable hiérarchique et le CSIRT/CERT, initier les premières mesures d'endiguement, voire paralléliser les actions prioritaires.

Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur mon système d'information soit bien lié à l'activité d'un code ou d'un acteur malveillant sur une machine du système d'information, et en avoir évalué la gravité :
Fiche précédente conseillée : Fiche réflexe - Compromission Infostealer - Qualification
Les mesures d'endiguement proposées dans cette fiche devront être appliquées en cohérence avec les conclusions de la *qualification* : le *périmètre* affecté par l'incident, son *impact* potentiel sur l'organisation, l'*urgence* à résoudre la situation, etc.
Si la qualification permet de suspecter un début de compromission système, il convient de dérouler la séquence :

- Fiche réflexe - Compromission système - Qualification
- Fiche réflexe - Compromission système - Endiguement

Si la qualification permet de suspecter un début d'incident rançongiciel, il convient de dérouler la séquence :

- Fiche réflexe - Chiffrement ou effacement en cours - Qualification
- Fiche réflexe - Chiffrement ou effacement en cours - Endiguement

Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement aient les *droits d'administration* du système d'information : réseau, système, sécurité opérationnelle.
Si le système d'information est infogéré, s'assurer de la capacité à mobiliser l'infogérant dans l'urgence.

Ouvrir une main courante

Dès le début de l'incident, ouvrir une *main courante* pour tracer tous les actions et événements survenus sur le système d'information dans un *ordre chronologique*.
Chaque ligne de ce document doit représenter une action avec au minimum trois informations :

1. La **date et l'heure** de l'action ou de l'évènement (si estimé nécessaire, ajouter le fuseau horaire UTC).
2. Le **nom de la personne** en charge de cette action ou ayant informé sur l'évènement (ou le nom du service de sécurité ayant détecté l'évènement).
3. La **description** de l'action ou de l'évènement, incluant les détails de son avancement ainsi que les comptes et machines concernés.

Ce document sera utile pour :

- Réaliser un historique du traitement de l'incident et partager les retours d'expérience.
- Piloter la coordination des actions et suivre leur état d'avancement.

- Évaluer l'efficacité des actions et leurs potentiels impacts non prévus.

Cette main courante doit être éditable et consultable par tous les intervenants. Il est déconseillé de la stocker sur le système d'information compromis, où elle serait accessible par l'attaquant. En revanche, cette main courante peut être accessible sur un partage de fichiers en ligne (cloud) ou intégrée dans le logiciel de gestion d'incident ou le SIEM si l'organisation en possède un, voire être au format papier.

Prendre en considération la présence active d'un attaquant

> ⚠ ATTENTION
>
> Dans les actions d'endiguement, il est faut éviter d'ouvrir une session interactive avec la machine suspectée compromise : connexion locale, *RDP* et *SSH* sont à minimiser, à fortiori avec un compte privilégié.

Si les actions à distance sont impossibles, autant que faire se peut :

1. Préférer les actions au travers d'un EDR.
2. Sinon, préférer une connexion locale - console physique, hors bande (*Out-of-Band*) ou d'hyperviseur - avec un compte administrateur uniquement local au système concerné.
3. En dernier recours, utiliser une connexion par le réseau qui ne met pas en danger le mot de passe des administrateurs : *Powershell Remoting* ou *Windows Remote Shell* (*WinRS*) qui permettent d'ouvrir l'équivalent d'un terminal, ou *RDP* en mode *Restricted Admin* qui n'autorise que Kerberos et n'autorise pas la mise en cache du *TGT*.

Tracer impérativement ces actions de connexion sur une machine compromise par l'infostealer dans la main courante.
Lors d'une compromission par un infostealer, il existe différents cas de détection de ce dernier sur votre système d'information :

- CAS 1 : Alerte EDR / AV / FW / Proxy d'une détection d'un infostealer (compromission en cours).
- CAS 2 : Signalement par votre équipe de CTI ou par une source externe de confiance d'une fuite d'identifiants (login/mot de passe) ou de journaux issus d'un infostealer, indiquant une compromission potentielle ou avérée.

ACTIONS D'ENDIGUEMENT PAR PRIORITÉS

Cette partie pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante :

Cas 1 : Alerte AV / EDR / Proxy

Actions	Priorité
Figer la situation *(Mesure 1)*	P0
Réinitialiser les identifiants suspectés compromis *(Mesure 2)*	P1
Réinitialiser les secrets liés à la machine infectée *(Mesure 3)*	P1
Préserver les traces sur les machines infectées *(Mesure 4)*	P1
Préserver les traces des journaux d'équipements *(Mesure 5)*	P2
Sécuriser des sauvegardes à jour *(Mesure 6)*	P2

Cas 2 : Signalement

Actions	Priorité
Figer la situation *(Mesure 1)*	P0
Préserver les traces sur les machines infectées *(Mesure 4)*	P1
Préserver les traces des journaux d'équipements *(Mesure 5)*	P1
Réinitialiser les identifiants suspectés compromis *(Mesure 2)*	P2
Réinitialiser les secrets liés à la machine infectée *(Mesure 3)*	P2
Sécuriser des sauvegardes à jour *(Mesure 6)*	P3

Dans le **CAS 1**, la compromission par un infostealer est en cours et à priori au stade de l'intrusion initiale ou de la latéralisation. Il convient de limiter les capacités de l'attaquant à contrôler le compte et machine compromis et éventuellement à réagir aux mesures d'endiguement.
Dans le **CAS 2**, la compromission par un infostealer a été confirmée et n'a pas été détectée par les moyens en place. L'attaquant a pu latéraliser et prendre la main sur une partie du système d'information. Il va être particulièrement important d'estimer les droits des différents comptes et postes impactés pour connaître les mesures d'endiguement à mettre en place. *Les traces sont particulièrement critiques pour eviter un effacement de ces dernières.*

> ⚠ ATTENTION
>
> La préservation des traces doit être une préoccupation pour tous les choix d'actions. Il conviendra de préférer les actions les altérant le moins possible, y compris dans la partie Mesure 1 - Figer la situation.

ACTIONS D'ENDIGUEMENT PAR THÈMES

Une compromission d'un compte n'est qu'une étape dans la tentative de compromission du système puis du système d'information. Un adversaire s'y est introduit et y a certainement eu une activité.
Le traitement d'un tel incident ne doit pas être limité à la suppression de codes malveillants mais doit faire l'objet de mesures complémentaires surtout au niveau des comptes et des domaines d'authentification.
Cette partie détaille les différentes mesures d'endiguement possibles selon 4 axes thématiques. Chaque *mesure* est ensuite scindée en *actions unitaires* :

- ▶ Limiter l'extension de la compromission
  - Mesure 1 - Figer la situation
  - Mesure 2 - Réinitialiser les identifiants suspectés compromis
  - Mesure 3 - Réinitialiser les secrets liés à la machine infectée
- ▶ Préserver les traces
  - Mesure 4 - Préserver les traces sur les machines infectées
  - Mesure 5 - Préserver les journaux
- ▶ Préserver les biens essentiels de l'organisation
  - Mesure 6 - Sécuriser des sauvegardes à jour

Les actions présentées dans cette partie sont regroupées par thèmes, et non par priorités ! Pour cela, se référer à la précédente partie Actions d'endiguement par priorités.

Limiter l'extension de la compromission

Dans le **CAS 1**, la compromission par un infostealer est en cours et à priori au stade de l'intrusion initiale ou de la latéralisation. Il convient de limiter les capacités de l'attaquant à contrôler le compte et machine compromis et éventuellement à réagir aux mesures d'endiguement.
Dans le **CAS 2**, la compromission par un infostealer a été confirmée et n'a pas été détectée par les moyens en place. L'attaquant a pu latéraliser et prendre la main sur une partie du système d'information. Il va être particulièrement important d'estimer les droits des différents comptes et postes impactés pour connaître les mesures d'endiguement à mettre en place. *Les traces sont particulièrement critiques pour eviter un effacement de ces dernières.*

> NOTE
>
> À la différence, de la compromission système les infostealer ne compromettent pas forcément le système. Ils visent les comptes, les identifiants, les sessions, les containers de mot de passe. Il faut garder ces points en tête lors de l'endiguement.

Mesure 1 - Figer la situation

Action 1.a : Interrompre l'activité de la machine infectée

- ▶ **Si la machine infectée ne porte pas un système a forte exigence de disponibilité**
  - ☐ Si le système compromis est une **machine virtuelle**, mettre cette machine en **pause** (snapshot).
    - ▷ Si possible, renommer la machine avec une mention "ne pas rallumer" pour éviter un redémarrage accidentel.
  - ☐ Si c'est une **machine physique** qui supporte la mise en veille, la mettre en **veille prolongée**.
  - ☐ Sinon déconnecter la machine du réseau :
    - ☐ Préférer par *isolation* utilisant un EDR.
    - ☐ Sinon par *configuration* :
      - □ En utilisant au choix : pare-feu d'infrastructure ou commutateur réseau.

- ☐ Enfin, par *déconnexion physique*.
  - ▷ Attention : penser aux réseaux sans fil vers lesquels l'équipement pourrait basculer.
- ☐ En dernier recours, si la déconnexion du réseau est impossible, *éteindre* la machine.
  - ▷ Si les outils sont disponibles, effectuer une collecte forensique avant extinction (y compris copie mémoire).

► **Si la machine ne peut être rendue indisponible**

- ☐ Procéder aux isolations réseau de l'*Action 1.b* est particulièrement important.
- ☐ Si un EDR est disponible et que la machine ne peut être arrêtée, il est possible de neutraliser un processus attaquant identifié.
  - ▷ Cette mesure ne résout pourtant pas l'incident : un outil hostile a été détecté sur le poste et potentiellement déjà utilisé pour se latéraliser vers d'autres machines.
  - ▷ Veiller à préserver les informations relatives à l'outil : condensat, voire copie du fichier.

Action 1.b : Isoler au niveau réseau les zones infectées d'Internet et/ou du reste du système d'information

► **Si possible, isoler par le réseau les zones contenant la machine infectée (réseau physique ou virtuel) en pensant à couper les flux vers et depuis Internet** :

- ☐ Couper les flux par *configuration*, si possible
  - ▷ Sur des pare-feu d'infrastructure, règles de filtrage dans les serveurs mandataires (proxy) ou d'ACL sur les équipements de niveau 2
- ☐ Sinon, procéder à une *déconnexion physique*

► **Si la machine infectée accédait à une zone particulièrement sensible (réseau industriel, SIIV...)**

- ☐ considérer un passage temporaire de ce dernier en mode isolé ("mode ilot" pour le monde industriel) déconnecté du SI bureautique, le temps de lever l'alerte.

► **Si les zones infectées sont identifiées et peuvent être concrètement isolées par le réseau d'autres zones interconnectées (systèmes industriels, filiales, partenaires, etc.)**

- ☐ Isoler ces zones peut éviter à l'incident de s'étendre davantage.

► **Dans le cas d'infrastructure infonuagique (Cloud/IaaS)**

- ☐ Fermer les réseaux et services exposés à Internet et vérifier qu'aucune interface réseau ne soit exposée sur Internet ou aux réseaux inter-clients.

L'isolation pourra être levée dès qu'il sera possible de vérifier l'innocuité des autres machines de la zone. Il peut être nécessaire de **baliser** le poste compromis pour éviter une reconnection ou une réutilisation du poste le temps des investigations.

IMPACT

Une telle action peut avoir de grands impacts sur les applications métiers dont les dépendances pourraient ne plus être accessibles. Si jamais cette action est réalisée, il faudra être vigilant aux signalements de dysfonctionnements de la part des équipes métiers des applications critiques et avoir la capacité d'effectuer un retour arrière ou de filtrer finement les flux réseau.

Mesure 2 - Réinitialiser les identifiants utilisateurs suspectés compromis

Les comptes utilisés sur un système compromis doivent être considérés comme eux-mêmes compromis. Leurs identifiants doivent être réinitialisés et leur activité faire l'objet d'une revue.
Une machine Linux peut être inscrite dans un annuaire, y compris *Windows Active Directory*, et dans ce cas, les mêmes précautions que sous système Windows s'imposent.

ATTENTION

Il ne faut pas négliger les accès que peut avoir un attaquant directement depuis l'extérieur sur le SI tels que VPN, application SaaS, application de messagerie exposée, etc. Il est important de réduire au maximum les accès des comptes compromis aux services externes puis aux services internes.

Dans certains cas, le changement du mot de passe doit être efectué 2 fois pour éviter un historique et une réutilisation.

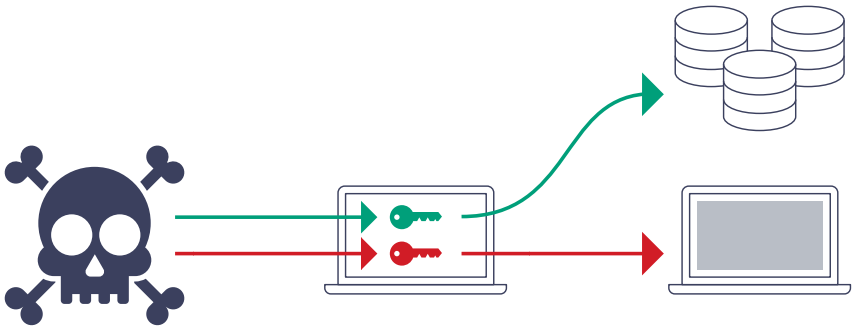


Figure 1 – Récupération d'identifiants et latéralisation

Action 2.a : Désactiver tous les comptes utilisateurs suspectés compromis

Si des comptes ont récemment été utilisés pour se connecter sur la machine compromise (depuis le dernier redémarrage) :

- ☐ Désactiver ces comptes dans l'*Active Directory* ou l'annuaire d'identité (quels que soient leurs privilèges et sensibilités).
- ☐ Prévoir une rotation d'identifiants par la suite.

Action 2.b : Désactiver tous les comptes administrateurs du domaine suspectés compromis (transit ou stockage sur la machine compromise)

- ▶ **Si ce sont des comptes individuels**
  - ☐ Les *désactiver* dans l'*Active Directory*.
- ▶ **Si c'est le compte administrateur du domaine par défaut (RID 500) ou équivalent**
  - ☐ Effectuer une *rotation de mot de passe* du compte.

> **NOTE**
>
> Considérer l'escalade vers le traitement d'une compromission du domaine Windows dans son ensemble, car l'attaquant a pu en altérer l'intégrité ou s'émettre des tickets privilégiés.

Action 2.c : Réinitialiser les comptes homonymes sur les autres machines

Si des comptes locaux homonymes aux utilisateurs interactifs de la machine compromise existent sur d'autres machines :

- ☐ Effectuer une rotation du mot de passe de ces comptes.

Action 2.d : Réinitialiser ou bloquer les comptes utilisés sur la machine infectée

Si la machine infectée contenait des identifiants de comptes permettant de s'authentifier sur d'autres machines ou applications du système d'information, comme ceux-ci :

- ☐ Changer les mots de passe ou secrets de comptes de services utilisés sur la machine infectée (attention à leur présence dans des fichiers de configuration ou scripts).
- ☐ Comptes applicatifs utilisateurs internes et externes :
  - ☐ Désactiver le compte.
  - ☐ Changer le mode de passe des comptes requis.
- ☐ Comptes privilégiés vers d'autres machines :
  - ☐ Invalider les secrets de déploiement ou de CI/CD sur les postes développeurs.
  - ☐ Changer les mots de passe des comptes requis.

> **ATTENTION**
>
> Les comptes sont présents au niveau des navigateurs, des fichiers stockants les mots de passe (word, excel, keepass ...), clef ssh,

token API ... Les gestionnaires de mot de passe sont la cible des infostealer. Ils sont particulièrement vulnérables lorsqu'ils sont déchiffrés, lorsque le mot de passe maître (passphrase) est faible ou qu'il n'est pas à jour.

Action 2.e : Révoquer les sessions des comptes utilisés sur la machine infectée

Si des comptes tels que mentionné à l'action précédente ont ouvert des sessions sur des applications web ou des systèmes :

- ☐ Déconnecter les sessions système en cours.
- ☐ Révoquer les sessions applicatives.
- ☐ Révoquer ou invalider les jetons en cours sur les applications Web et infonuagiques (*Cloud*) : OAuth, SAML...

Action 2.f : Supprimez les clés SSH des autres serveurs

Si la machine infectée contenait des clés privées SSH :

- ☐ Supprimez des *autres* serveurs les clés publiques associées des fichiers `authorized_keys`.

⚠ ATTENTION

La recherche de clés publiques SSH déployées peut être sujette à oublis :

- ► Ces clés publiques peuvent être dans `$HOME/authorized_keys`, mais aussi dans la configuration globale du système (souvent `/etc/ssh/keys`).
- ► Considérez de chercher ces clés sur tous les composants du système d'information exposant un serveur SSH en interne ou externe à l'organisation.
- ► L'ensemble des clés / certificats utilisateurs sont à considérer dans cette action.

Action 2.g : Réinitialiser les comptes cloud

Si la machine était utilisée pour accéder à des services *cloud* :

- ☐ Effectuer une rotation du mot de passe de ces comptes.
- ☐ Révoquer les sessions et tokens.
- ☐ Fiches conseillées :
  - Fiche réflexe - Compromission d'un compte de messagerie - Qualification
  - Fiche réflexe - Compromission d'un Tenant Azure - Qualification

IMPACT

Les changements de comptes de service impactent les fonctionnements applicatifs. Il convient de vérifier la disponibilité et la bonne exécution des processus métier après tout changement.

NOTE

Si un second facteur était utilisé depuis ou vers la machine compromise, considérer de suspendre le second facteur suspecté le temps de l'investigation de l'incident.

Mesure 3 - Réinitialiser les secrets liés à la machine infectée

Action 3.a : Révoquer les certificats de la machine infectée

Si la machine infectée contenait des certificats (802.1X, VPN, etc.) :

- ☐ Révoquer ces certificats.
- ☐ S'assurer de la publication de la révocation (rafraîchissement de CRL, publication sur le serveur OCSP).

Action 3.b : Réinitialiser les jetons ou clés d'API présents sur les comptes des machines compromises

Si la machine infectée contenait des identifiants applicatifs (token d'API) :

- ☐ Révoquer les jetons, et, si nécessaire, en déployer de nouveau sur d'autres instances partageant la même clé.

Action 3.c : Si la machine compromise est inscrite dans un Active Directory

- ☐ Désactiver le compte machine dans l'*Active Directory*.

Préserver les traces

> **NOTE**
> Il convient d'éviter de réinitialiser tout équipement infecté ou suspecté avant que le traitement de l'incident n'aie été clos.

Ce point est particulièrement important dans le **CAS 2**, la compromission par un infostealer a été confirmée et n'a pas été détectée par les mesures de sécurité en place. Préserver les traces dans ce cas est primordiale pour éviter de les effacer ou les perdre par rotation des journaux.

Mesure 4 - Préserver les traces sur les machines infectées

Action 4 : Préserver les traces sur les machines infectées

- ▶ **Si la machine infectée est une machine virtuelle**
  - ☐ Prendre un instantané de la machine virtuelle (déjà mise en pause) puis l'exporter sur un disque dédié hors ligne.
    - ▷ **Attention** : bien inclure l'export de la mémoire dans l'instantané quand disponible (souvent impossible dans le cadre d'hébergement cloud).
- ▶ **Sinon la machine infectée est une machine physique**
  - ☐ Effectuer un prélèvement forensique :
    - ▷ en utilisant l'EDR,
    - ▷ par un agent forensique,
    - ▷ par service d'administration,
    - ▷ en exécutant manuellement un outil de prélèvement,
    - ▷ ou manuellement directement à leur emplacement sur les machines ou équipements.

> **ATTENTION**
> Certains environnements ne permettent pas d'exécuter des outils arbitraires. Avant de lancer l'exécution d'un outil de prélèvement s'assurer que la politique de gestion de l'équipement l'autorise.

Mesure 5 - Préserver les journaux (Logs)

Action 5.a : Préserver les traces dans les journaux d'équipements

- ☐ Identifier les équipements de sécurité du système d'information :
  - ☐ pare-feu
  - ☐ passerelles VPN
  - ☐ proxy
  - ☐ console de CDN
  - ☐ console antivirus et EDR, etc.
- ☐ Exporter les journaux historiques.

- ☐ Augmenter la rétention des événements dans les journaux ou suspendre leur rotation (sur les systèmes, dans les puits de logs, dans le SIEM/XDR).
- ☐ Activer les journaux les plus complets possibles et supportables (espace disque, impact performance).

Action 5.b : Préserver les traces dans les journaux d'authentification (AD, EntraID, iCloud, Google Identity, AWS IAM, IDP, fournisseurs d'identité ou de second facteur)

- ☐ Identifier la solution de stockage des journaux d'identification sur le réseau interne, comme le domaine *Active Directory*.
- ☐ Exporter ces journaux (depuis consoles, contrôleurs de domaine, IDP, ou infrastructures cloud).
- ☐ Augmenter la rétention de ces journaux ou suspendre temporairement leur rotation.

> **REMARQUE**
>
> En plus d'être indispensable à la compréhension de l'incident, sauvegarder les éléments de preuve pourra être nécessaire pour répondre aux forces de l'ordre lors d'éventuelles poursuites judiciaires. L'analyse rapide des requêtes bloquées suite aux mesures mises en place permet de découvrir souvent des éléments pertinents.

Préserver les biens essentiels de l'organisation

Mesure 6 - Sécuriser des sauvegardes à jour

Les *sauvegardes* sont primordiales pour rétablir les services du système d'information en cas d'incident destructif : il faut les préserver en cas de suspicion d'incident majeur.
Ces sauvegardes pourront aussi servir de source de données pour l'investigation sur l'incident.

Action 6.a : Sécuriser des sauvegardes à jour

S'assurer de l'existence d'une sauvegarde récente des données accessibles depuis la machine compromise :

- ☐ Serveurs de fichiers.
- ☐ Serveurs accessibles interactivement aux utilisateurs de la machine.
- ☐ En cas de doute sur le périmètre de compromission, limiter l'accès.

Action 6.b : Valider l'accès fonctionnel aux sauvegardes

- ☐ Serveur de restauration accessible uniquement aux utilisateurs de la machine.

SUITE DES ACTIONS

A la fin de ces actions d'endiguement, la compromission devrait être contenue.
La neutralisation supposée des actions de l'attaquant ne permet pas de savoir comment le compte et la machine ont été compris, à quelle étape de l'attaque la détection a eu lieu ou l'ampleur d'autres compromissions. Seule une analyse approfondie des événements permettra de comprendre ces éléments.
En fonction de votre niveau de maturité, il est possible de réaliser des actions complémentaires telles que :

- ☐ Réinitialiser les *Machine Keys*.
- ☐ Mettre en place une collecte réseau ciblé.
- ☐ Collecter les preuves / journaux de manière recevable juridiquement (procédures de collecte et calcul d'empreintes cryptographique SHA256).

De manière générale, un incident doit être géré jusqu'à son terme avec tous les corps de métier concernés : *investigation forensique et remédiation par une équipe spécialisée, maintien d'activité, communication interne aux partenaires, dépôt de plainte et déclarations*, etc.
Pour ce faire, il est conseillé de piloter la suite de la résolution de l'incident en cohérence avec les *impacts* identifiés et demander de l'aide :

- ► Mettre en œuvre une **gestion d'incident cyber** pour piloter la résolution de l'incident.
  - Voir les annexes *Contacts* et *Déclarations*.
  - Notifier le ou les utilisateurs impactés est à prendre en compte avec les RH et la communication.

De plus, si l'incident a un *périmètre étendu* sur le système d'information, qu'il a un *impact fort* et qu'il nécessite une *résolution urgente* :

- ► Activer le dispositif de **gestion de crise cyber** de l'organisation pour piloter la résolution de l'incident et la continuité d'activité.
  - Guide conseillé : Crise cyber, les clés d'une gestion opérationnelle et stratégique

ANNEXES

Préparation

En *prévention* d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être préparée en amont, contextualisée et traduite en une *procédure interne et actionnable immédiatement* à son système d'information. Dans une situation d'urgence, elle augmentera la rapidité de la réponse, minimisera les erreurs de manipulation et permettra à une personne d'astreinte moins expérimentée de mener ces actions.
Il est également conseillé d'imprimer les fiches réflexes afin qu'elles restent disponibles en cas d'indisponibilité du système d'information. Il en va de même pour les autres documents utiles, comme la notice d'aide au dépôt de plainte ou votre annuaire de contacts.

Liens utiles

Lors d'une lecture préparatoire de cette fiche ou pour aller plus loin dans la compréhension et la mise en œuvre des notions évoquées, certains documents annexes peuvent être utiles :

- Fiche réflexe - Compromission Infostealer - Qualification
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Cyberattaques et remédiation
- Fiche réflexe - Compromission système - Qualification
- Fiche réflexe - Compromission système - Endiguement
- Fiche réflexe - Chiffrement ou effacement en cours - Qualification
- Fiche réflexe - Chiffrement ou effacement en cours - Endiguement
- Fiche réflexe - Compromission d'un compte de messagerie - Qualification
- Fiche réflexe - Compromission d'un Tenant Azure - Qualification

Contacts

La gestion d'un incident cyber implique de faire appel à des équipes spécialisées au sein de CERT/CSIRT, qui appuieront les équipes internes dans la réalisation de leurs actions de défense.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation	Se référer aux procédures internes.	Pour les organisation disposant d'une équipe de réponse à incident interne.
CERT/CSIRT externe en prestation de réponse à incident	`https://www.cybermalveillance.gouv.fr/diagnostic/accueil` `https://cyber.gouv.fr/prestataires-de-reponse-aux-incide`	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CSIRT régional	`https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux`	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations

CERT sectoriel	`https://www.cert-aviation.fr`
	`https://www.m-cert.fr`
	`https://esante.gouv.fr/produits-services/cert-sante`
		Pour les organisations du secteur de l'aviation, maritime ou santé

CERT-FR	`https://www.cert.ssi.gouv.fr/contact`	Pour les administrations et les opérateurs d'importance vitale et de services essentiels

De plus, pour les incidents complexes, une aide externe est également recommandée pour :

- Gérer la crise

- Gérer la communication interne et externe
- Augmenter les ressources humaines et capacitaires de reconstruction de votre direction informatique

Pour faciliter la mobilisation de tous ces acteurs, il est conseillé de s'appuyer sur des annuaires tenus à jour en amont et accessibles même en cas d'indisponibilité du système d'information.

Déclarations

Conjointement à la résolution de l'incident, des déclarations doivent être effectuées :

Qui ?	Comment ?	Pourquoi ?
Assureurs		Notifier son assurance cyber permet de démarrer la prise en compte de la couverture et d'identifier des prestataires que l'assureur pourra recommander ou mandater.
ANSSI	`https://www.cert.ssi.gouv.fr/contact/` `https://cyber.gouv.fr/notifications-reglementaires`	L'administration, les opérateurs d'importance vitale et de services essentiels, et toute organisation impliquant des informations classifiées, doivent déclarer leurs incidents à l'ANSSI.
Dépôt de plainte	`https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de`	Déposer plainte permet de déclencher une enquête et de dégager votre responsabilité en cas de propagation de l'attaque à d'autres victimes.
CNIL	`https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles`	Les incidents affectant des données personnelles doivent faire l'objet de déclaration à la CNIL dans un délai de 72 heures. En cas de doute, il faut faire une pré-déclaration précisant avoir subi une potentielle compromission même si aucune exfiltration de données n'a été confirmée.
Autres autorités		Une organisation d'un domaine réglementé (finance, santé, etc.) est astreinte à des obligations de déclaration spécifiques. Dans le doute, consulter le service juridique.

Préparation

En *prévention* d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être préparée en amont, contextualisée et traduite en une *procédure interne et actionnable immédiatement* à son système d'information. Dans une situation d'urgence, elle augmentera la rapidité de la réponse, minimisera les erreurs de manipulation et permettra à une personne d'astreinte moins expérimentée de mener ces actions.
Il est également conseillé d'imprimer les fiches réflexes afin qu'elles restent disponibles en cas d'indisponibilité du système d'information. Il en va de même pour les autres documents utiles, comme la notice d'aide au dépôt de plainte ou votre annuaire de contacts.

Définitions

Axes d'évaluation

- *Périmètre* : Le périmètre d'un incident désigne son étendue sur le système d'information et dans son administration.
- *Impact* : L'impact d'un incident désigne le niveau de perturbation et de dommage potentiel qu'il engendre pour l'organisation.
- *Urgence* : L'urgence d'un incident désigne la rapidité avec laquelle il faut réagir pour rétablir les activités essentielles impactées.

Compromission d'un compte de messagerie

Une *compromission d'un compte de messagerie* désigne un accès non autorisé à un compte de messagerie, par un attaquant. Ce dernier peut alors lire et envoyer des courriels à l'insu de l'utilisateur légitime du compte, et accéder à ses données.

Compromission système

Une *compromission système* est l'activité d'un code ou d'un acteur malveillant sur une machine du système d'information, résultant en sa prise de contrôle.
Faute de pouvoir qualifier précisément la prise de contrôle, dans de nombreux cas, toute activité adverse sur le système pouvant avoir donné lieu à une escalade de privilège est considérée comme une compromission. Une compromission entraîne généralement une forme de communication entre la machine compromise et un attaquant y exécutant des actions.

Degrés de gravité

- *Anomalie courante* (gravité faible) : Une anomalie courante est un incident de sécurité ne représentant pour l'instant pas de menace sérieuse pour la sécurité du système d'information et n'entraînant pas d'impact significatif sur l'activité métier. Elle nécessite tout de même d'être correctement qualifiée pour confirmer son faible degré de gravité.
- *Incident mineur* (gravité modérée) : Un incident mineur est un incident de sécurité représentant une menace limitée pour le système d'information et entraînant - ou risquant d'entraîner - un impact modéré sur l'activité métier.
- *Incident majeur* (gravité élevée) : Un incident majeur est un incident de sécurité représentant une menace sérieuse pour le système d'information et entraînant - ou risquant d'entraîner - un impact fort sur l'activité métier.
- *Crise cyber* (gravité critique) : Une crise cyber représente un incident de sécurité ayant un *périmètre étendu* sur le système d'information, un *impact fort* sur l'activité métier et nécessitant une *résolution urgente*.

Endiguer un incident

L'endiguement désigne l'ensemble des actions prises au début d'un incident de sécurité informatique destinées à en contenir l'ampleur. Elles n'ont généralement pas vocation à être prolongées durablement.

Fuite de données

Une *fuite de données*, également appelée *violation de données*, désigne un incident au cours duquel des informations confidentielles, sensibles ou protégées sont consultées, divulguées ou volées par une personne non autorisée. Cela peut concerner divers types de données, notamment des informations personnelles, financières, médicales, ou des secrets commerciaux.
Les fuites de données peuvent résulter de cyberattaques, comme le piratage ou le phishing, mais aussi d'erreurs humaines, telles que l'envoi d'informations à la mauvaise adresse e-mail ou la perte de dispositifs contenant des données sensibles. Les conséquences d'une fuite de données peuvent être graves, allant de pertes financières et d'atteintes à la réputation de l'entreprise à des problèmes juridiques et à la compromission de la vie privée des individus concernés.

Qualifier un incident

Qualifier un incident signifie :

- *Confirmer* qu'un incident de sécurité est bien en cours et si oui, déterminer précisément sa *nature*.
- *Évaluer la gravité/priorité de l'incident* en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

La qualification permettra de prendre des décisions éclairées sur la réponse à l'incident et d'allouer les ressources appropriées pour le résoudre.

FICHE RÉFLEXE

L'InterCERT France fédère aujourd'hui plus de 100 CERTs sur le territoire national, constituant ainsi la 1ère communauté de CERTs en France.

Cette fiche réflexe est issue de la coopération et du partage d'expérience de plusieurs de ces CERTs. Elle a pour objectif d'être un outil efficace lors des premières étapes de gestion de l'incident en cours, en proposant des actions concrètes pour débuter le processus de remédiation.

Vous pouvez trouver l'ensemble de ces fiches au lien suivant :
`https://www.intercert-france.fr/publications/fiches-reflexes/`

Votre expérience dans le traitement d'un incident et l'utilisation de cette fiche est précieuse. Dans le but d'améliorer sa qualité, nous vous invitons à partager vos commentaires et suggestions d'amélioration, en nous contactant à l'adresse suivante :
fichesreflexes-remediation@intercert-france.fr