
FICHE RÉFLEXE

Compromission Infostealer Qualification

2026



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 par un infostealer est suspectée ou confirmée sur un poste.

A quoi sert-elle ?

L'objectif de cette fiche est de proposer une *aide à la qualification* d'un signalement de compromission par Infostealer. Les différentes actions proposées aideront à :

- ▶ *Confirmer* qu'un incident de sécurité est bien en cours, et qu'un ou plusieurs systèmes sont compromis.
- ▶ Évaluer la *gravité* de l'incident en évaluant le *périmètre affecté*, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

Comment l'utiliser ?

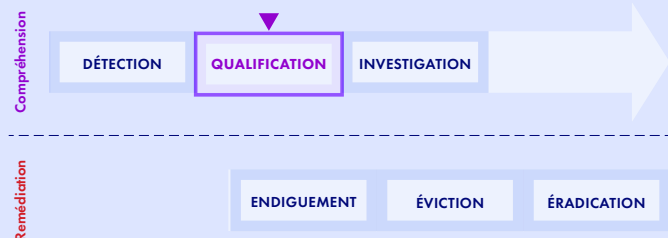
Deux parties principales composent cette fiche :

- ▶ La partie *Conclusions attendues de la qualification* correspond aux questions auxquelles la qualification devra répondre.
- ▶ La partie *Méthode d'évaluation pas à pas* correspond à la méthodologie pour aider à y répondre.

Cette fiche doit être exécutée en *temps court*. Pour cela, fixer un *temps contraint* selon l'urgence pressentie (ex : 30 minutes, 1 heure au maximum) et ne pas rechercher l'exhaustivité des réponses : des *réponses approximatives* et des réponses "*je ne sais pas répondre*" sont acceptables dans un premier temps. Par la suite, une qualification plus approfondie se fera sûrement, avec plus de recul ou l'appui d'une équipe spécialisée en réponse à incident.

SOMMAIRE

Prérequis	3
Conclusions attendues de la qualification	5
Méthode d'évaluation pas à pas	7
Suite des actions	14
Annexes	15





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.

Disposer des personnes nécessaires

S'assurer que les personnes qui effectueront la qualification de l'incident aient les accès nécessaires au système d'information :

- ▶ Les accès à l'administration et au monitoring du système d'information.
- ▶ Les accès aux équipements de sécurité du système d'information.
- ▶ La connaissance des priorités métier de l'organisation.
- ▶ L'annuaire de contacts d'urgence.

Ces personnes peuvent être internes ou externes à l'organisation. 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.

Avoir pris connaissance des actions déjà entreprises

Avoir pris note des personnes ayant déjà agi en réponse à l'incident en cours et des actions qu'elles ont déjà entreprises sur le système d'information. Commencer à reporter ces notes d'intervention dans la main courante.



Prendre en considération la présence active d'un attaquant

IMPORTANT

Un Infostealer est un outil malveillant qui va compromettre la machine et l'ensemble des comptes liés à cette machine. La charge malveillante va également s'intéresser aux fichiers de données des gestionnaires de mots de passe, aux mots de passe enregistrés dans les navigateurs et aux sessions de navigation actives (cookies). Le périmètre de compromission n'est pas limité à la machine infectée, et il faut prendre en compte l'ensemble des domaines d'authentification des comptes présents. Il faut également identifier l'ensemble des comptes qui se seraient connectés sur le poste ou serveur depuis son dernier redémarrage.

Dans les actions d'endiguement, il est important d'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 ou un logiciel de gestion à distance n'ouvrant pas de session sur le système (type RMM).
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 dans la main courante.



CONCLUSIONS ATTENDUES DE LA QUALIFICATION

Cette section présente les conclusions attendues des évaluations, qui permettront de qualifier l'incident. La section suivante détaillera les questions et actions à mener pour guider ces évaluations étape par étape. La partie suivante présentera des actions détaillées pour guider pas à pas ces évaluations.

Évaluer l'incident

Mesure 1 - Identifier le système concerné

- La nature des informations transmises permet-elle d'identifier avec confiance le système compromis par l'Infostealer ?

Mesure 2 - Confirmer l'incident de type compromission par infostealer

- L'incident de type compromission par Infostealer est-il confirmé, est-il un faux positif ou nécessite-t-il des investigations complémentaires ?

Mesure 3 - Évaluer le périmètre de l'incident

- L'incident est-il circonscrit à une partie du système d'information identifiable ?
- Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ?
- Les autres systèmes d'information interconnectés avec celui de l'entreprise sont-ils en risque ?

Mesure 4 - Évaluer l'impact de l'incident

- Quelles activités métiers essentielles sont-elles ou peuvent-elles être perturbées ?
- Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?

Mesure 5 - Évaluer l'urgence à résoudre l'incident

- L'attaque est-elle en cours ? Y a-t-il urgence à la contenir immédiatement ?
- Quelles sont les activités essentielles potentiellement perturbées, pour lesquelles des mesures préventives de maintien d'activité doivent être envisagées ?
- L'activité détectée est-elle récente et sujette à évolution ou ancienne et stable ?
- L'incident est-il à risque de généralisation imminente (forte connectivité, atteinte à une fonction de sécurité) ?

Qualifier l'incident

Conclure quant à la gravité de l'incident

- La compromission d'une machine appartenant au système d'information est-elle confirmée ?
 - Si elle ne l'est pas, y a-t-il un risque de machine réellement compromise mais non identifiée ?
- L'incident est-il circonscrit sur mon système d'information, ou est-il étendu ?
- L'incident présente-t-il un impact fort pour mon activité métier et le fonctionnement de mon système d'information ?
- L'incident est-il urgent à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?



Au final, quelle *gravité* représente cet incident de sécurité ?

1. Anomalie courante
2. Incident mineur
3. Incident majeur
4. Crise cyber



MÉTHODE D'ÉVALUATION PAS À PAS

Cette partie détaillera des actions qui aideront à conduire les évaluations et à aboutir à la qualification de l'incident.

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.

Vous avez reçu une notification vous signifiant que vous étiez compromis par un Infostealer.

Que celle-ci soit une détection interne, ou un signalement d'un tiers, il faut en évaluer la pertinence et la gravité.

Les informations relatives à une compromission par Infostealer sont généralement de 4 natures différentes :

1. Adresse réseau : adresse IP, nom d'hôte qualifié (FQDN). L'adresse peut être celle d'un équipement relai plutôt que directement la machine compromise (pare-feu, proxy, serveur DNS).
2. Nom de machine : nom Windows ou Unix d'une machine sans le domaine DNS ou *Active Directory*.
3. Nom de compte et mot de passe : adresse mail ou compte de l'entreprise avec ou sans le mot de passe, en clair ou chiffré.
4. Alerte de sécurité : alerte remontée par un capteur système comme un EDR, ou un événement système supervisé dans un SIEM.



NOTE

Dans un premier temps, il est possible de n'avoir qu'une seule des 4 natures d'information ci-dessus.

Évaluer l'incident

Mesure 1 - Identifier le système concerné

Action 1.a : Confirmer la validité du signalement (cas 2)

Les erreurs de signalement étant fréquentes et source de perte de temps considérables, il est nécessaire de le confirmer :

- L'architecture et la configuration du système concerné permettent-elles de valider l'évènement à la date signalée ? (date trop ancienne ou réforme du système d'information entre temps)
- L'horodatage est-il cohérent avec le reste du signalement ?
- Le fuseau horaire de l'horodatage du signalement est-il compréhensible ?
- Le système était-il en production aux dates et heures d'activité signalées ?
- Est-ce une réutilisation de combolist (utilisation d'ancienne informations mélangées donnant l'impression d'une nouvelle fuite de données) ?
- La cohérence entre le compte, le poste et le mot passe est-elle réelle pour l'organisation ? Date de dernier changement du mot de passe ?
- Les informations techniques signalées correspondent elles au système (versions de système d'exploitation, ou type de compromission pouvant être incohérents) ?
- Est-ce que le signalement correspond à un incident déjà traité ? Changement d'un mot de passe prévisible et facilement extrapolable (exemple : incrément d'entier, ponctuation) ?

Action 1.b : Identifier le système concerné (cas 1 et 2)

- ▶ **L'alerte vient d'un outil détection ou SOC interne**
 - Quel est l'indicateur qui a déclenché l'alerte ?
 - Les informations fournies par l'outil de détection permettent-elles d'identifier la machine compromise de façon sûre ?
- ▶ **A partir d'une adresse réseau**
 - L'adresse IP est-elle connue comme attribuée (DHCP, reverse-DNS, annuaire, CMDB, inventaire, etc.) ?
 - Le sous-réseau IP concerné fait-il partie des adresses (internes ou externes) utilisées sur le SI ?
 - Si l'adresse IP fait partie d'un pool DHCP, peut-on retrouver la machine portant l'adresse au moment de l'activité signalée ?



- Si l'adresse est publique sur Internet, la machine peut-elle être associée à l'organisation (bannières, certificats TLS, services hébergés, etc.)
- Le signalement pointe-t-il vers une machine susceptible d'en masquer plusieurs (Routeur, Proxy, Serveur DNS, Pare-feu, NAT, etc.) ?
 - Les informations du signalement permettent-elles d'identifier la machine derrière ce relais ?
 - Les journaux de l'équipement permettent-ils d'identifier les systèmes masqués ?

► **Sur la base d'un nom de machine**

- La machine existe-t-elle dans un annuaire centralisé (*Active Directory*, orchestrateur, MDM) ?
- La machine pourrait-elle être hors gestion centralisée (Workgroup, poste associé à une application métier, machine virtuelle hors domaine, instances de développement, prestataires externes, VDI, etc.) ?

► **Depuis un nom de compte et mot de passe**

- Le compte existe-t-il dans l'annuaire centralisé (*Active Directory*, *SambaAD*, *OpenLDAP*) ?
- Le mot de passe est-il cohérent avec les politiques de mot de passe appliquées dans l'organisation ?
- Le compte a-t-il des privilèges ?

► **Option : Depuis un poste personnel ou BYOD (mauvaise pratique)**

- Le poste appartient-il à une personne de l'entreprise ? (VIP / VSP)
- Le compte a-t-il des droits particuliers et est-il lié à la personne à qui appartient le poste ?
- Le poste / compte est-il celui d'un partenaire (infogéreur, TMA, etc.) ?

Action 1.c : Recueillir les informations élémentaires de configuration système (cas 1 et 2)

- Le système visé par le signalement peut-il être identifié ? Si oui :
 - Quel est le système d'exploitation opérant le système signalé ?
 - Quel est le niveau de version et d'installation de correctif déployé sur ce système ?
 - Est-ce que le système est relié à un système de synchronisation horaire (NTP) ?
 - Quelles applications métiers sont installées sur ce système ?
 - Y a-t-il présence d'un logiciel dans un niveau de version susceptible d'être vulnérable à une faille activement exploitée ?
 - ▷ CISA KEV catalogue de vulnérabilités exploitées
 - Y a-t-il présence d'un logiciel avec une version vulnérable exposée ?

Action 1.d : (Conclure) Confirmer l'identification du système

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

- La nature des informations transmises permet-elle d'identifier avec sûreté le système compromis par l'infostealer ?

Mesure 2 - Confirmer l'incident de type compromission par Infostealer

Confronter les informations du signalement aux informations observables du système d'information doit permettre de confirmer l'incident de type compromission par Infostealer :

Action 2.a : Si la détection est un flux réseau

- Le flux est-il observé dans les journaux d'infrastructure réseau
 - pare-feu,
 - DNS,
 - serveurs mandataires (proxy),
 - traces de flux (NetFlow/IPFIX),
 - console de CDN (type Cloudflare, Akamai, etc.) ?
- Le flux est-il détecté par une sonde réseau (IDS) ?
- La supervision réseau montre-t-elle des accès inhabituels ?
- Connexion de nature ou de destination Internet inhabituelle sur les serveurs mandataires
 - vers des sous-réseaux IP dédiés à l'hébergement de VPS,
 - flux vers des infrastructures TOR,



- Adresses IP de VPN,
- Ports inhabituels.
- Connexion de source inhabituelle (pays, système)
- Initiation de connexions internes, réussies ou non, vers des services inhabituels ou rares
 - dans les journaux de connexion des machines distantes
 - dans les journaux de pare-feu systèmes
 - comportements à rechercher :
 - ▷ tentatives de montage réseau,
 - ▷ balayage réseau (scan),
 - ▷ tentative de connexions interactives (RDP, SSH, etc.)
- Des alertes de blocages de flux sont-elles associées à la machine ?
 - tentative de connexion,
 - et tentatives d'établissement de tunnels VPN,
 - résolution DNS vers des domaines suspects ou caractéristiques de tunnels (entrées DNS au nom long et complexe).

Action 2.b : Si la détection est au niveau du système ou comportement illégitime

- Un EDR permet-il de vérifier la présence du code sur la machine ?
- Une alerte antivirus est-elle visible (console, journaux et événements système) ?
- Exécution de commandes inhabituelles (LOLBin, Powershell) ?
- Collecte de données dans les navigateurs ?
- Collecte de données de type coffre fort de mot de passe (*.kdbx, 1password.sqlite, bitwarden\data.json) ?
- Collecte de portefeuilles de crypto-monnaie ?
- Collecte des configuration de clients FTP, clefs SSH ?
- Collecte de boîtes aux lettres ?

Action 2.c : Utilisation illégitime de compte utilisateur

Rechercher les traces d'un usage illégitime du compte utilisateur qui pourrait avoir été compromis. Ces traces peuvent être retrouvées dans les journaux système localement ou dans un puit de logs.

Si l'attaque est en cours (CAS 1), il se peut que les connexions ne soient pas encore réalisées. Les infostealers testent souvent leurs accès dès récupérations des informations.

Si l'incident provient d'un signalement (CAS 2), il se peut que les connexions et actions illégitimes datent de plusieurs jours et soient encore actives.

- Connexion d'un compte inhabituel sur le système compromis (VPN, Messagerie, RDS, ...)
- Usage anormal d'un compte sur ou depuis le système compromis (ex : compte de service ou compte machine ouvrant des connexions interactives)
- Connexion à l'application de messagerie ?
- Tentative de connexion / connexion depuis des pays non conformes / voyage impossible pour le compte compromis ?

Action 2.d : Journaux d'infrastructure nuagique (cloud)

Quand la machine compromise est hébergée sur une infrastructure nuagique, différents types de journaux permettent d'identifier d'éventuelles activités suspectes autour du système. Ces actions sont en complément de celles effectuées au niveau réseau (2.a) et système (2.b)

Si l'attaque est en cours (CAS 1), il se peut que les actions ne soient pas encore réalisées. Les Infostealers testent souvent leur accès dès récupérations des informations. La persistance ou les modifications sont souvent identifiables post-exploitation.

Si l'incident provient d'un signalement (CAS 2), il se peut que les actions illégitimes datent de plusieurs jours et/ou soient encore actives.

- Changements d'attributs des objets associés au système compromis
- Changement de groupes ou d'utilisateurs disposant de droits sur le système compromis
- Changement de MFA ou d'OTP pour le compte utilisateur compromis ainsi que les accès conditionnels
- Connexion et changement sur des applications non supervisées (SaaS connecté à l'IDP eg. EntraID)

Action 2.e : (Conclure) Confirmer l'incident de type compromission par Infostealer

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

- L'incident de type compromission par Infostealer est-il confirmé, est-il un faux positif ou nécessite-t-il des investigations complémentaires ?



Mesure 3 - Évaluer le périmètre de l'incident

Action 3.a : Identifier la fonction de la machine suspectée

- Postes de travail ?
- BYOD / Perso ?
- Prestataire externe ?
- Serveurs applicatifs ?

- Serveurs de stockage ?

- Hyperviseurs ?
- Machines virtuelles ?
 - Sur quel hyperviseur ?
- Machines physiques ?
- Appliance en boîte noire (équipements réseau et de stockage sans console système interactive) ?
- La machine est-elle exempte de certaines mesures de sécurité (Machine de développement, En zone industrielle, Legacy) ?
- L'équipement est-il un IOT ?

Action 3.b : Identifier la connectivité de la machine

- Internet :
 - La machine expose-t-elle des services sur Internet ?
 - La machine peut-elle initier des connexions vers Internet ? Si oui, est-ce via un proxy ?
- Interconnexions :
 - La machine peut-elle monter des connexions vers des systèmes de partenaires ou clients ?
 - La machine reçoit-elle des connexions de partenaires, clients ou utilisateurs distants ?
 - La machine peut-elle servir de pont entre le réseau local et des réseaux plus sensibles ?
 - La machine dispose-t-elle de connexions sans fil (Wifi, Bluetooth, Zigbee, Cellulaire, etc.) ?
 - La machine a-t-elle des accès sur d'autres systèmes d'information de l'organisation : autres tenants cloud, autres sites, filiales, etc.

Action 3.c : Identifier le nombre de machines compromises

- Le signalement ou la détection pointent-ils vers plusieurs machines ?
- Si le système compromis était derrière un relais (routeur, proxy, pare-feu...)
 - Les anomalies détectées sur la machine compromise existent-elles sur d'autres machines ?

Action 3.d : Identifier les accès des comptes compromis

L'objectif de cette action est de définir les accès des comptes initiaux du signalement. L'action suivante permettra de faire une estimation à partir des comptes potentiellement compromis en plus des comptes du signalement.

ATTENTION

Il est important de vérifier que des comptes d'administration ou d'assistance ne se sont pas connectés depuis le dernier redémarrage du poste ou serveur. Les comptes de développement et de CI/CD permettent de plus en plus d'actions et d'accès à un ensemble critique de données et applications.

- Métier :
 - Le compte peut-il se connecter à des données critiques métiers ?
 - Le compte permet-il de modifier des configurations des applications métiers ?
 - Le compte a-t-il des capacités de sauvegarde ou d'extraction des données métiers ?
 - Le compte peut-il se connecter à des serveurs de type ERP, bases de données relevant du RGPD, DORA, etc. ?
 - Le compte est-il celui d'un prestataire de l'organisation ?
 - Le compte est-il celui d'un développeur de l'application métier ?
- Utilisateur :



- Comptes ayant accès ou ayant eu accès à la machine
- Données sur la machine (documents, secrets, coffre-forts de mots de passe)
- Certificats
- Administration :
 - Le compte est-il administrateur du domaine ?
 - Le compte est-il administrateur d'infrastructure nuagique ?
 - Le compte a-t-il des droits sur les hyperviseurs, les sauvegardes ou les équipements réseaux ?
 - Le compte est-il administrateur des systèmes métiers ?
 - Le compte est-il administrateur local des postes bureautiques et serveurs de fichiers ?
 - Un compte d'administration ou d'assistance s'est-il / se sont-ils connectés sur ce poste / serveur depuis son dernier redémarrage ?

Action 3.e : Evaluer le nombre de comptes compromis

Le but de cette action est à partir des comptes initiaux compromis, statuer sur le nombre potentiel de comptes et postes compromis. Un poste / serveur peut avoir accès à de nombreux comptes par différents moyens : coffre-fort de mots de passe, enregistrements dans le navigateur, token de session, ancienne connexion d'assistance ou d'un administrateur sans protection des clefs, clefs SSH, certificats, etc.

- Estimer le nombre de compte compromis ou potentiellement compromis depuis le poste
- Estimer le nombre de compte compromis ou potentiellement compromis depuis le signalement

Action 3.f : (Conclure) Évaluer le périmètre de l'incident

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

- L'incident est-il circonscrit à une partie du système d'information identifiable ?
- Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ? Quel est le nombre de compte potentiellement compromis ?
- Les autres systèmes d'information interconnectés avec celui de l'entreprise sont-ils en risque ?
- Si la machine est isolée, d'autres éléments permettent-ils d'identifier la source de sa compromission (autres systèmes compromis, supports USB contaminés) ?

Mesure 4 - Évaluer l'impact de l'incident

Action 4.a : Évaluer niveau de compromission pouvant résulter de la prise de contrôle des comptes

- Des comptes d'administration globaux (administrateur du domaine ou administrateur équivalent à pouvoir agir sur la totalité du SI) se sont-ils récemment connectés sur la machine et surtout depuis le dernier reboot ?
- Les comptes compromis ont-ils des fonctions spécifiques (synthèse du point 3.d et 3.e) ?
 - Au niveau métier
 - Au niveau du Système d'Information
 - Au niveau RH
 - Au niveau financier
- Les comptes compromis permettent-ils des connexions Nuagiques ?
 - Nuage propre à l'entité
 - Nuage d'un tiers
- La machine porte-t-elle une fonction de sécurité ?
 - Gestion des identités et accès (Contrôleur de domaine, annuaire, IDP, etc.)
 - Gestion des mises à jour
 - Gestion de configurations et déploiement (SCCM, Orchestrateur, etc.)
 - Console de contrôle d'une fonction vitale (EDR, sauvegarde)
 - Gestion de secrets : IGC (Autorités de Certification), coffre-fort de mots passe, serveur de déchiffrement de disque automatisé
 - Hyperviseur
 - La machine donne-t-elle accès à des services critiques ?
 - Poste d'administration
 - Serveur de rebond d'administration (bastion)
 - Postes (PC, tablettes, IHM intégrées, VDI) de maintenance et d'ingénierie d'OT
- La machine porte-t-elle ou contribue-t-elle significativement à une activité vitale ?



Action 4.b : Évaluer les impacts potentiels sur l'activité métier

- Quelles activités métiers sont concernées par la machine ou les comptes suspectés, à usage interne ou externe ?
- Quelles activités potentiellement perturbées sont vitales pour l'organisation ?
 - Si votre organisation possède un BIA (Business Impact Analysis), ces activités y ont-elles été analysées ?
- Parmi les activités potentiellement perturbées, certaines provoquent-elles un risque identifié pour l'organisation ?
 - Importante perte financière ?
 - Risque réputationnel ?
 - Risque de perte de clientèle et d'opportunité ?
 - Risque sur les personnes ?
 - Fuite ou perte d'informations métiers critiques (base clients, conceptions, prospects, etc.)
- La machine ou les services auxquels peut se connecter le compte suspecté, est-elle soumise à un engagement de disponibilité (SLA) ?

Action 4.c : Évaluer les impacts réglementaires

- Le système d'information affecté par ce compte est-il soumis à une réglementation particulière (OSE, OIV, NIS2, etc.) ?
- Peut-on savoir si le système d'information affecté par ce compte stocke des données sensibles ?
 - données classifiées
 - données personnelles (RGPD) ou RH
 - données à statut protégé : de santé, financières, recherche, etc.
 - données soumises à engagement contractuel ou réglementaire

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

Action 4.d : (Conclure) Évaluer l'impact potentiel de l'incident

- Quelles activités métiers essentielles sont-elles ou peuvent-elles être perturbées ?
- Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?

Mesure 5 - Évaluer l'urgence à résoudre l'incident

En fonction du cas et de l'origine de la détection d'un Infostealer, l'urgence à résoudre l'incident ne sera pas la même.

Dans le CAS 1, l'attaque est en cours.

Dans le CAS 2, l'attaque a déjà eu lieu et des étapes supplémentaires ont potentiellement déjà été réalisées.

Action 5.a : Évaluer l'urgence métier à résoudre l'incident

Pour chacune des activités vitales impactées identifiées précédemment :

- Existe-t-il une procédure de continuité d'activité en mode nominal ?
- Existe-t-il une procédure de maintien d'activité en mode dégradé (PCA/PRA) ?
- Existe-t-il une échéance et importante qui pourrait être affectée par l'incident ?
 - Évènements proches, contrats, livraison, date de déclenchement d'action financière, etc.
- La nature des données accédées nécessite-t-elle un traitement urgent (eg. RGPD) ?
 - impact potentiel sur l'organisation,
 - données sensibles internes,
 - engagement de réaction vis-à-vis de tiers...

Action 5.b : Évaluer à quel point l'information est récente

- Le signalement est-il à propos d'une détection récente (cela ne provient pas d'une combolist) ?
- Si oui, l'activité détectée est-elle récente ou peut-elle être détectée dans le passé ?

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :



Action 5.c : (Conclure) Évaluer l'urgence à résoudre l'incident

- Quelles sont les activités essentielles potentiellement perturbées pour lesquelles des mesures préventives doivent être envisagées ?
- L'activité détectée est-elle récente et donc sujette à évolution, ou ancienne et stable ?
- L'incident est-il à risque de généralisation imminente (forte connectivité, atteinte à une fonction de sécurité) ?
- Est-ce qu'il existe un engagement ou une contrainte à traiter dans l'urgence ?

Qualifier l'incident

Conclure quant à la gravité que représente l'incident de sécurité pour mon organisation, en prenant en compte le périmètre affecté, l'impact potentiel sur le fonctionnement de l'organisation et l'urgence à le résoudre :

- La compromission d'une machine appartenant au système d'information est-elle confirmée ?
 - Si elle ne l'est pas, y a-t-il un risque de machine réellement compromise mais non identifiée ?
- L'incident est-il circonscrit sur mon système d'information, ou est-il étendu ?
- L'incident est-il susceptible de créer un impact fort pour mon activité métier et le fonctionnement de mon système d'information ?
- L'incident est-il urgent à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?
- Au final, quelle gravité représente cet incident de sécurité ?
 1. Anomalie courante
 2. Incident mineur
 3. Incident majeur
 4. Crise cyber



SUITE DES ACTIONS

Si l'incident de compromission système est confirmé alors, en cohérence avec le *périmètre de compromission* évalué :

- ▶ Mettre en œuvre des **mesures d'endiguement** pour contenir l'attaque.
 - Fiche suivante conseillée : Fiche réflexe - Compromission Infostealer - Endiguement

Parallèlement, piloter la suite du traitement de cet incident et demander de l'aide pour résoudre l'incident, en cohérence avec les *impacts* identifiés :

- ▶ Mettre en œuvre une **gestion d'incident cyber** pour piloter la résolution de l'incident.
 - Voir les annexes *Contacts* et *Déclarations*.

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

La compromission par un Infostealer est proche d'une compromission système, les fiches de qualification et endiguement de compromission système peuvent être utilisées :

- ▶ Fiche similaire - Qualification : Fiche réflexe - Compromission système - Qualification
- ▶ Fiche similaire - Endiguement : Fiche réflexe - Compromission système - Endiguement



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 - Endiguement
- ▶ 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

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-incidents	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 1^{ère} 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 débiter 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



CC BY-NC-SA 4.0