Procédure en cas d’attaque cyber

Pour signaler une attaque et savoir quoi faire :

* **CERT-FR :** **Centre gouvernemental de veille, d’alerte et de réponse aux attaque informatiques**

*Le CERT-FR traite sur le plan technique les incidents concernant l’administration et les opérateurs d’importance vitale et de services essentiels.****Le CERT-FR n’est pas un service de justice ou de police recevant des plaintes.***

Tél : 01 71 75 84 68 (permanence 7j/7, 24h/24)

Mail : [cert-fr.cossi@ssi.gouv.fr](mailto:cert-fr.cossi@ssi.gouv.fr)

* **Formulaire assistance victime de Cybermalveillance :**

Site : <https://www.cybermalveillance.gouv.fr/diagnostic/profil>

* **Contacts régionaux ANSSI :**

Mail : [nouvelle-aquitaine@ssi.gouv.fr](mailto:nouvelle-aquitaine@ssi.gouv.fr)

Pour déposer plainte :

* **Contact cyber Police Nationale :**

Mail : [cybermenaces-bordeaux@interieur.gouv.fr](mailto:cybermenaces-bordeaux@interieur.gouv.fr)

* **Contact cyber Gendarmerie Nationale :**

Mail : [sécurité-economique-nouvelleaquitaine@gendarmerie.gouv.fr](mailto:sécurité-economique-nouvelleaquitaine@gendarmerie.gouv.fr)

* **BP Serres-Castet :** 05 59 33 52 20  
  **COB Lescar :** 05 59 77 61 30  
  **PJ de Bayonne :** 05 59 46 23 12

Les bons réflexes :

**Déconnecter la machine du réseau**

Déconnecter du réseau la machine compromise (ou les machines) permet de stopper l’attaque si elle est toujours en cours. S’il était toujours connecté à la machine, l’intrus n’a plus de contrôle sur celle-ci et ne pourra donc pas surveiller ce que vous faites et/ou modifier des fichiers. **En revanche, maintenez la machine sous tension et ne la redémarrez pas, car il serait alors impossible de connaître les processus qui étaient actifs au moment de l’intrusion.** Vous risqueriez de provoquer une modification sur le système de fichiers et de perdre de l’information utile pour l’analyse de l’attaque.

**Prévenir le responsable sécurité**

Prévenez immédiatement le responsable sécurité et votre hiérarchie qu’une intrusion a été detectée. Prévenez-les de préférence par téléphone ou de vive voix, car l’intrus est peut-être capable de lire les courriers électroniques échangés, depuis une autre machine du réseau.

Le responsable sécurité doit être clairement identifié par tous les administrateurs système/réseau avant que l’incident de sécurité ne soit déclaré. C’est la base de toute procédure de réaction sur incident de sécurité.

**Prévenir le CERT dont vous dépendez**

En France, le CERT dont dépendent les administrations est le CERTA. Il peut être contacté :

* par courrier électronique : cert-fr.cossi@ssi.gouv.fr ;
* par téléphone : 01-71-75-84-68 ;
* par fax : 01-84-82-40-70.

Pour en savoir plus sur les CERTs (Computer Emergency Response Team), vous pouvez consulter la page de présentation :

<http://www.cert.ssi.gouv.fr/cert-fr/certfr.html>

**Faire une copie physique du disque**

Attention la copie physique d’un disque dur est une opération très délicate.

**Pourquoi faire une copie du disque ?**

D’une part, en l’absence de copie, l’altération des données provoquée par l’analyse rendrait inefficace toute procédure judiciaire, si vous souhaitiez mener cette démarche. D’autre part, même si aucune action judiciaire n’est envisagée, vous pourrez tout de même avoir besoin dans le futur d’une copie exacte du système tel qu’il était au moment de la découverte de l’intrusion.

**Pourquoi faire une copie physique – du disque ?**

Une simple sauvegarde de fichiers ne fournit pas l’intégralité des informations contenues sur le disque, il est donc important de procéder à une copie de bas niveau du disque, y compris des secteurs non occupés.

**Comment faire un copie physique du disque ?**

Sur un système Unix, vous pouvez utiliser la commande dd pour procéder à la copie exacte du disque. Sur un système Windows, il n’existe pas de telle commande sur le système d’exploitation, mais de nombreuses applications sont disponibles pour effectuer la même opération.

 Si vous n’avez jamais utilisé ce type de commandes ou d’outils, ne le faites pas dans l’urgence car vous risqueriez de détruire toutes les traces. Faites appel à votre CERT pour plus de détails sur la façon de procéder.

Attention : l’image produite ne doit en aucun cas être stockée, même temporairement, sur le disque à étudier.

**Rechercher les traces disponibles**

Un équipement n’est jamais isolé dans un système d’information. S’il a été compromis, il doit exister des traces dans d’autres équipements sur le réseau (gardes-barrière, routeurs, outils de détection d’intrusion, etc…). C’est pourquoi il est utile de rechercher des traces liées à la compromisssion dans tout l’environnement, les copier, les dater et les signer numériquement.

### Remarque importante

Si vous avez pu déterminer l’origine probable de l’intrusion, n’essayez pas d’entrer en contact directement avec l’administrateur de la machine dont semble provenir l’attaque. Vous risqueriez en effet de communiquer avec le pirate et de lui fournir des informations importantes sur ce que vous savez de lui.

De toute façon, le taux de réussite pour contacter l’administrateur de la machine source sera beaucoup plus élevé si c’est un CERT qui s’en charge. Il y a plusieurs raisons à cela :

1. les CERTs disposent de nombreux outils, de contacts et de correspondants, ce qui leur permet de contacter plus rapidement la personne adéquate ;
2. les messages à entête d’un CERT sont en général pris plus au sérieux que les messages de particuliers ;
3. les CERTs représentent une autorité neutre qui permet d’entamer si nécessaire un dialogue constructif, sans accusation abusive d’un côté ou de l’autre.

Pour se faire aider par un prestataire en réponse aux incidents :

Site de la liste des prestataires : <https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/>