



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 30 janvier 2004
N° CERTA-2004-ALE-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Obstacles à la résolution d'incidents

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-001>

Gestion du document

Référence	CERTA-2004-ALE-001
Titre	Obstacles à la résolution d'incidents
Date de la première version	30 janvier 2004
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- destruction d'éléments qui permettent de mener correctement l'analyse technique mettant en évidence le mode opératoire d'un intrus, ce qui peut souvent conduire à de nouvelles intrusions (risque technique).
- difficulté de prouver sa bonne foi vis-à-vis d'actions commises par l'intrus au moyen des systèmes compromis (risque légal).

2 Systèmes affectés

Tout système compromis, en particulier les sites WEB faisant l'objet d'une défiguration.

3 Description

La « défiguration » d'un site WEB, est une intrusion menée sur un site WEB ayant pour effet d'en modifier le contenu.

Une société a automatisé un procédé qui prévient les administrateurs des sites WEB défigurés. Le message d'alerte contient des « explications » et une référence à un site WEB qui donne des « recommandations » sur la marche à suivre :

« *What is the next step?*
« *The remediation process can be broken down into this high-level set of procedures:*
« *1) Replace the defaced message with a 'temporarily unavailable' message to retain reputation.*
« *2) Restore the original website (recommended: reload server and website in the event backdoors were installed).*
« *3) Install all appropriate security bug fixes and patches.*
« *4) Perform external security assessment to ensure all security holes and vulnerabilities are resolved.*
« *Remote Assessment [remoteassessment.com] can guide, assist and perform all of the steps listed above. Contact Remote Assessment immediately to begin the remediation process.* »¹

Ces conseils semblent être de bon sens. En pratique, ils posent de nombreux problèmes.

Le premier est qu'un tel traitement « amateur » de l'incident échappe aux équipes qui en ont officiellement la mission, qui savent adapter leur réponse au contexte de la victime bien mieux qu'un message envoyé automatiquement par un inconnu.

Le deuxième problème vient de ce que les « recommandations », si on les suit à la lettre, conduisent à :

- 1° écraser la page posée par l'intrus ainsi que les divers traces et indices associés ; l'annonce de la défiguration de votre site est déjà publiée, avec un miroir de la page concernée, sur un site consacré à cet effet ; il est donc naïf de croire qu'on protège sa réputation en mettant une page de substitution qui ne trompera personne ;
- 2° écraser les éléments permettant de comprendre ce qui a été fait par l'intrus sur le serveur ; en effet la défiguration n'est que l'aspect visible, le vrai problème comprend aussi et surtout l'intrusion dans votre système (déterminer ce que l'intrus a fait une fois dans la place : installation de *rootkits* ou autre moyens de masquer son activité, installation de porte dérobée, installation de serveurs, lecture ou modification de documents, attaques commises avec votre adresse IP, ... et toute action pouvant engager à priori votre responsabilité) ;
- 3° écraser les logiciels en place, si bien qu'on ne pourra plus affirmer lequel était vulnérable ; sans analyse approfondie qui met en évidence la vulnérabilité exploitée par l'intrus, le site risque d'être à nouveau compromis ; l'expérience montre en effet qu'une défiguration est souvent suivie de nombreuses tentatives d'intrusions ;
- 4° polluer les journaux d'événements de sécurité avec des traces qui n'ont rien à voir avec l'incident, au risque d'effacer des indices intéressants.

Sous l'apparence d'une aide qui vous est apportée, ce type de message d'alerte prodigue de mauvais conseils. Il conduit à compromettre considérablement les chances de mener à bien l'analyse qui permettra de comprendre l'intrusion dans le système de traitement automatisé de données.

4 Solution

Lorsque vous recevez un message de ce type, il convient de suivre les conseils dispensés dans la note d'information CERTA-2002-INF-002. Avant toute action sur la machine compromise, prenez contact avec votre CERT de rattachement (le CERTA pour l'administration) et/ou votre chaîne fonctionnelle de sécurité des systèmes d'information.

5 Documentation

CERTA-2003-INF-002 Les bon réflexes en cas d'intrusion sur un système d'information :

<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html>

1. littéralement : « *Que faire ensuite (après la défiguration)?* »

- « 1° *remplacer le message de la défiguration avec la mention « momentanément indisponible » dans le but de préserver votre réputation,*
« 2° *restorer le site original (il est recommandé de recharger le serveur et le site dans le cas où des portes dérobées auraient été installées),*
« 3° *installer tous les correctifs de sécurité appropriés,*
« 4° *faire une évaluation de la sécurité afin de s'assurer que tous les trous de sécurité sont bouchés.*
« *Remote assessment » peut guider, assister et réaliser toutes les étapes ci-dessus. Contactez « Remote assessment » immédiatement pour commencer le processus de reprise sur incident.*
»

Gestion détaillée du document

30 janvier 2004 version initiale.