Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

REAGIR A UN DEFACEMENT – REFLEXES

QU'EST-CE QU'UN DEFACEMENT ?

Un défacement (ou défiguration) désigne la modification non sollicitée de la présentation d'un site web, à la suite du piratage de ce site.

OBJECTIFS DE L'ATTAQUE

- Dégrader l'image du site web
- Acte politique pour diffusion d'un message.

RISQUES

- ➔ **PERTE D'IMAGE**
- ➔ **VOL DES DONNEES**
- ➔ **UTILISATION DU SERVEUR COMME VECTEUR POUR D'AUTRES ATTAQUES**

SYMPTOMES

CHANGEMENT DE LA PAGE D'ACCUEIL DU SITE INTERNET

ORIGINES

- Erreur de configuration / faiblesse de sécurisation (briques de framework, API accessibles, etc.)
- Via un site vulnérable hébergé sur la même plate-forme
- Mot de passe faible / Faiblesse du système de gestion et de stockage des mots de passe
- Absence des derniers correctifs de sécurité ou de recommandations de configuration
- Erreur de programmation
- Faille 0day

QUOI FAIRE

- **ARRETER LE SERVEUR WEB**
- **AVERTIR LE RESPONSABLE SECURITE**
- **AVERTIR LES TECHNICIENS**
- **AVERTIR LE SERVICE COMMUNICATION (SITE ACCESSIBLE PAR LE PUBLIC)**
- **DEPOSER PLAINTE AUPRES DE LA POLICE OU DE LA GENDARMERIE**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

REAGIR A UN DEFACEMENT – REFLEXES

GRAVE OU PAS ?

Le défaçage est le symptôme visible du fait qu'un attaquant a récupéré un accès au serveur et des possibilités offertes (modification des données, installation d'une porte dérobée, rebond vers d'autres machines, etc.)

LES BONNES PRATIQUES

- Installer les correctifs de sécurité du système et des logiciels
- Exporter les journaux système (prévenir effacement des traces)
- Réaliser des sauvegardes régulières
- Durcir le serveur web
- Mettre en place une politique de mots de passe forte
- Réaliser une veille régulière sur les logiciels utilisés par le serveur
- Réaliser des audits/scans de sécurité réguliers
- Installer un waf

RESSOURCES

- CERT-FR : Les défigurations de sites Web
- Recommandations pour la sécurisation des sites web
- Service d'alerte de vulnérabilités : https://vigilance.fr/

REPARER ET ENQUETER

LES PRINCIPALES ETAPES DE L'ENQUETE •

- **Acquérir les données du système**
  - Faire une copie de la mémoire vive
  - Faire une copie physique / snapshot du système (nécessite de redémarrer le système)
  - Réaliser une copie de l'image et calculer son empreinte de l'image réalisée
- **Arrêter le serveur web**
- **Identifier la source de l'intrusion**

La méthode la plus simple pour déterminer la source de l'intrusion d'un serveur web est d'analyser les accès réalisés dans les journaux d'événements. Attention la source de l'intrusion peut être autre que le serveur web (outils d'administration, serveurs d'applications, etc.). Attention, si l'attaquant a pu obtenir un accès privilégié, celui-ci a pu effacer l'ensemble de ses traces. Selon le système d'exploitation, il faut analyser les journaux d'événements issus de :

- Du serveur web (IIS, Apache, nginx)
- Des outils d'administration (ssh, vnc, rdp, etc.)
- Des applications accessibles à distance (sgbd, serveurs d'applications, etc.)
- Des serveurs frontaux si présents (reverse-proxy, cache, etc.)

- **Réinstaller le système**

La réinstallation totale à partir d'un système sain (et donc le reformatage) s'avère souvent nécessaire pour s'assurer que le système n'est plus infecté.

- **Restaurer les données**

Il est indispensable de posséder des sauvegardes, afin de permettre une reprise de l'activité dans un délai acceptable. Attention aux sauvegardes issus du système corrompu qui peuvent être infectés/corrompus.

- **Changer tous les mots de passe des accès présents sur le serveur**

Sans changement des mots de passe, l'attaquant peut ré-utiliser les accès précédemment obtenus.

- **Identifier les possibilités de rebond**

Si le serveur piraté est présent dans un réseau interne, analyser les serveurs connectés afin de déterminer si d'autres accès ont pu avoir lieu. Attention, car un des systèmes a pu être à l'origine de l'attaque.