Numéro
Février 2015

Lettre SSI du haut fonctionnaire de défense et de sécurité

vigi@net

Vigilance pour internet et les systèmes d'information

Vigi@net

Responsable de la publication :
Frédéric Guin

Comité éditorial :
Frédéric Morinière, Josiane Guilhot-Mahler, Benoît Moreau

Contacts :
hfds@education.gouv.fr
ou
hfds@recherche.gouv.fr

Retrouvez ce numéro sur le portail du ministère : pléiade

https://www.pleiade.education.fr
(nécessite une authentification)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR ET
ET DE LA RECHERCHE

Ce numéro est consacré aux attaques informatiques en défiguration ayant fait suite aux attentats «Charlie » et qui continuent épisodiquement. Bien que les revendications des pirates ne concernent pas directement les missions du ministère au sens large, de nombreux sites de la communauté ont été piratés. Ce phénomène illustre bien qu'aucun site n'est à l'abri, quel qu'en soit l'intérêt stratégique, et que la cyber sécurité doit être considérée globalement.

Cyber attaques coordonnées « je ne suis pas Charlie »

Suite aux attentats « Charlie », un mouvement contestant l'élan de solidarité nationale est apparu et utilise Internet pour sa propagande. Il encourage ses partisans à mener des attaques informatiques, notamment des défigurations*, dans le cadre d'un cyber djihad avec un paroxysme qui avait été annoncé pour le 15 janvier 2015.

L'objectif de ces attaques étant de donner une visibilité médiatique à leurs messages, les défigurations sont revendiquées sur les réseaux sociaux, notamment sur twitter avec le mot clé « #OpFrance ». Elles sont globalement d'un niveau technique faible et touchent les sites les plus fragiles, contrairement à ce que veulent laisser penser les revendications parfois fantaisistes. Par exemple, la compromission d'une base de données personnelles avait été annoncée, alors que les informations publiées étaient tirées d'un annuaire public.

Aujourd'hui près de 1000 sites web de la communauté du ministère ont été défigurés par des attaquants afin de faire afficher des revendications telles que « Je ne suis pas Charlie ». Les sites étaient de moyenne importance et les conséquences opérationnelles ont été très limitées.

**** Les attaques en défiguration et leurs implications sont détaillées dans l'article ci-après.***

Ces attaques font parties d'une manœuvre médiatique de guerre de l'information plus que de guerre des systèmes d'information. Cependant, bien que les impacts opérationnels dans ce contexte soient faibles, il ne faut pas minimiser l'importance des fragilités constatées.

Les attaques en défiguration ou défacement

Attaques en défiguration : elles consistent en une modification d'un site web par un tiers non autorisé, un pirate. L'objectif étant souvent d'utiliser la notoriété du site afin d'afficher et diffuser un message (cf. illustration), elles sont le plus souvent visibles. Cependant elles peuvent aussi être « invisibles »**,** c'est-à-dire sans changement d'apparence, afin d'y introduire un virus qui tentera d'infecter discrètement les internautes navigant sur le site.

Qu'est-ce que cela implique : le fait qu'un tiers non autorisé puisse modifier l'apparence d'un site web montre la présence d'une vulnérabilité ; une sorte de porte dérobée, lui permettant d'agir en contournant les mesures de protection en place.

Par analogie, une défiguration visible est comparable à un graffiti sur un mur à l'intérieur d'un musée censé être fermé.

Quelles réactions après l'incident : les modifications impactant le plus souvent des fichiers sauvegardés, il suffirait de remettre les anciens pour que le site retrouve son état initial. Cependant, cela ne permettrait pas de « refermer la porte dérobée » et donc d'empêcher que cela ne se reproduise. Il convient donc de prendre le temps d'étudier l'attaque et de corriger la vulnérabilité.

Il suffirait de repeindre le mur du musée pour que le message ne soit plus lisible par les visiteurs. Cependant il s'agira de trouver comment l'auteur a pu pénétrer pour éviter que cela ne se reproduise et éviter une situation plus alarmante la fois suivante, comme le vol ou la dégradation d'une œuvre d'art.

Les conséquences : les impacts sont multiples et peuvent notamment ternir l'image de l'entité détentrice du site. En effet, dans certains cas l'internaute pourrait croire que le message affiché est légitime, et dans d'autres cas, s'il a conscience qu'il s'agit d'une attaque, il pourrait perdre confiance dans la sécurité de l'entité dans son ensemble. Les impacts peuvent aussi être opérationnels et financiers, liés par exemple au coût de la correction du site et à la durée d'interruption, le temps que la nouvelle version soit disponible.

Si le graffiti annonçait une menace terroriste dans le musée, il est probable que certains visiteurs hésiteraient à y venir. De plus, le défaut de sécurité pourrait faire hésiter des collectionneurs à lui confier des œuvres. La fermeture du musée le temps d'enquêter, de vérifier les portes et de repeindre les murs entrainerait à la fois un manque à gagner et des dépenses imprévues en expertise et en travaux.

Les mesures préventives

Adapter l'architecture : les sites web étant particulièrement exposés aux attaques, il convient de limiter les informations sensibles qui pourraient s'y trouver et de ne laisser que ce qui est nécessaire.

Le musée n'expose au public que les œuvres clairement identifiées avec des mesures de sécurité adaptée, et entrepose toutes les autres dans des zones aux accès restreints.

Appliquer les mises à jour : elles contiennent des correctifs pour des vulnérabilités et doivent être appliquées pour « refermer les portes dérobées » avant qu'un pirate ne les utilise.

Le musée s'assure quotidiennement que les accès sont bien fermés et entretient régulièrement les portes.

Prévoir la journalisation : afin de pouvoir comprendre les attaques, il est nécessaire d'avoir des éléments à analyser et notamment les journaux de connexion permettant de retracer l'activité du pirate et d'identifier la vulnérabilité utilisée.

Le musée enregistre plusieurs heures de vidéosurveillance permettant de retracer le parcours d'un individu depuis le lieu du méfait à l'ouverture utilisée pour entrer.

Réaction et remédiation : en cas d'incident, en fonction du site concerné et de la teneur de la défiguration, les réactions peuvent varier. Le responsable en capacité de décider doit être connu et joignable et les moyens d'actions doivent avoir été prévus et testés.

Le directeur du musée, ou le responsable identifié, doit être joignable pour décider des actions, comme par exemple de fermer une salle au public avec des moyens identifiés (portes, gardiens, barrières …).

Plus de recommandations techniques sont disponibles sur les pages de l'intranet du ministère pléiade, sur les sites des RSSI (EN, ESR) et sur le site de l'ANSSI.