aDvens

Security for the greater good

Usurpation de marque

Méthodologie de réponse à incident

IRM-15 | 2022-11-28 | **TLP-CLEAR** | CERT aDvens - CSIRT
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

→ La fiche IRM s'adresse aux personnes ou fonctions suivantes :
- Les **RSSI et leurs adjoints**
- Le **CERT**
- Le **SOC**
- Les **administrateurs**

Dans le cas d'un incident : Lire l'IRM et prendre des notes.
Rester calme et contacter immédiatement l'équipe de réponse à incident du secteur d'activité ou un CERT si nécessaire.

Étapes de traitement des incidents

6 étapes sont définies pour gérer les incidents de sécurité :

1. **Préparation** : Se préparer à gérer l'incident,
2. **Identification** : Détecter l'incident,
3. **Confinement** : Limiter l'impact de l'incident,
4. **Remédiation** : Supprimer la menace,
5. **Récupération** : Revenir à un état normal,
6. **Capitalisation et apprentissage** : Élaborer et améliorer les processus.

Cette IRM fournit des informations détaillées pour chaque étape. Les étapes sont issues du NIST.

Cette fiche est issue du travail collaboratif avec le **CERT-SG** de modification et de mise à jour de leurs fiches de méthodologie de réponse à incident.

Références

→ IRM CERT-SG
→ IRM CERT-aDvens

1. Préparation

Objectif : Établir des contacts, définir des procédures, recueillir des informations et se familiariser avec les outils de détection d'intrusion pour gagner du temps lors d'une attaque.

- Tenir à jour une liste de toutes les marques légitimes appartenant à l'entreprise et à ses filiales.
  Cela aidera à évaluer la situation en question et évitera d'entamer une procédure d'infraction sur une marque obsolète, un site Web légitime non lié ou un compte de réseau social,
- Établir une liste d'informations complète et fondée sur des preuves concernant les différentes marques pour faire valoir vos droits (juridique) :
  - Nom(s), noms de domaine légitimes et comptes de médias sociaux utilisés par l'entreprise et ses filiales,
  - Les mots, symboles, slogans, graphiques, etc. de l'entreprise,
  - Numéros d'enregistrement de la marque, le cas échéant, (KBIS, Numéro SIRET),
  - Les bureaux d'enregistrement des marques internationaux et fédéraux/locaux (USPTO, INPI, etc.) où les marques déposées ont été étiquetées comme telles, le cas échéant,
  - Tout autre document établissant clairement qu'une marque appartient à l'entreprise.
- Préparer des formulaires de courrier électronique d'usurpation de marque,
  - Ils seront utilisés pour chaque dossier de contrefaçon de marque, si possible en plusieurs langues.
  - Ils permettront d'accélérer les choses lors des contacts avec le bureau d'enregistrement, le fournisseur de services et toute autre partie concernée au cours de la procédure.
- Promouvoir un système central de gestion de domaine en utilisant des champs WHOIS normalisés,
- Faire la promotion d'une publicité en ligne éthique pour éviter d'apparaître dans les noms de domaine parqués,
- Préparer des processus et des modèles de demande de retrait avec l'équipe juridique,
- Avoir des processus, des experts et des technologies en place pour gérer le portefeuille de marques,
- Disposer d'un processus ou d'un référentiel centralisé pour gérer les noms de marques, les adresses IP, les domaines, les PII, les mots-clés, etc.

1.1. Interlocuteurs internes

- Maintenir une liste de toutes les personnes impliquées dans l'enregistrement de la marque dans l'entreprise, en particulier celles qui font partie des services juridiques et des relations publiques,
- Maintenir une liste de toutes les personnes accréditées/habilitées pour prendre des décisions sur les marques et les éventuelles actions en matière de contrefaçon de marque,
  - Si possible, obtenir un accord écrit qui permettant à l'intervenant de prendre ce genre de décisions.

1.2. Interlocuteurs externes

- Établir et tenir à jour une liste de contacts externes au sein des bureaux d'enregistrement et des prestataires de services impliqués dans les questions relatives aux marques.

2. Identification

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

2.1. Détection de contrefaçon de marque

- → Déploiement d'une surveillance active des enregistrements de nom de domaine via les mises à jour des zones DNS chaque fois que possible ou via des services de surveillance de marque,
- → Configurer des flux pour surveiller les noms d'utilisateur, les pages et les groupes sur les réseaux sociaux,
- → Analyser les champs "*referrer*" HTTP dans les journaux de sites Web pour identifier des téléchargements frauduleux et les redirections frauduleuse de vos sites Web,
- → Mettre en place une veille de marque avec des moteurs de recherche spécialisés,
- → Tirer parti de l'automatisation dès que possible pour déclencher des alarmes et améliorer les temps de réaction,
- → Collecte et analyse des alertes des partenaires de confiance.

2.2. Impliquer les parties appropriées

- → Dès qu'une infraction est constatée, contacter les personnes de l'entreprise qui sont habilitées à prendre une décision, si la personne n'est pas autorisée à prendre cetype de décision.

La décision d'agir sur le nom de domaine, groupe ou compte utilisateur frauduleux doit être prise dans les meilleurs délais.

2.3. Recueillir des preuves

- → Recueillir des preuves de noms de domaine, de sites Web, d'URL spécifiques (par exemple, l'URL personnalisée de Facebook), de pages, de groupes ou de détails du compte,
- → Faire une copie horodatée des éléments contrefaits (page, groupe, blog, forum, chronologie de micro-blogging, etc.) et réaliser des captures d'écran si possible.

3. Confinement

Objectif : Atténuer les effets de l'attaque sur l'environnement ciblé.

3.1. Évaluer l'impact de la contrefaçon de marque :

- → Peut-il être utilisé pour la redirection de trafic (cybersquatting, typosquatting, SEO) ?
- → Peut-il être utilisé pour du spoofing, de la contrefaçon ou du scamming (cybersquatting avec redirection vers le site de l'entreprise) ?
- → Peut-il être utilisé pour diffamer la marque ?
- → Évaluer la visibilité du composant en infraction,
  - Visibilité du site Web (classement),
  - Nombre de fans ou de followers sur les réseaux sociaux,
- → Surveiller le domaine inactif et en infraction pour détecter des signes d'activités frauduleuses.

Se référer à IRM-13-Phishing et IRM-14-Scam pour plus d'informations.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

Dans la plupart des problèmes de marque, la surveillance est généralement suffisante.
La remédiation ne doit être lancée que s'il y a un impact sur l'entreprise ou ses filiales.

4.1. Nom de domaine

- → Contacter le propriétaire du nom de domaine et le fournisseur de services d'hébergement pour les informer de l'usurpation de la marque et leur demander de supprimer le contenu frauduleux,
- → Contacter le bureau d'enregistrement du nom de domaine pour l'informer de la contrefaçon et leur demander de désactiver le nom de domaine associé ou de le transférer à l'entreprise,
- → Demander au propriétaire du nom de domaine ou au bureau d'enregistrement de rediriger toutes les requêtes DNS vers les serveurs de noms de l'entreprise si possible,
- → Si ni le propriétaire du nom de domaine, ni le bureau d'enregistrement ne donnent suite aux demandes, engager une procédure UDRP (Uniform Domain-Name Dispute-Resolution Policy).

4.2. Compte de réseau social

- → Contacter le fournisseur de services de la page, du groupe ou du compte en infraction pour l'informer de toute violation de ses politiques en matière de marques ou de ses conditions d'utilisation et lui demander de désactiver le compte en infraction,
- → Demander au fournisseur de services de transférer le compte usurpant la marque vers un compte d'entreprise existant si possible.

Dans les deux cas, envoyer des e-mails aux adresses de contact du bureau d'enregistrement ou du fournisseur de services.
Il existe généralement une adresse e-mail pour signaler les abus, les problèmes juridiques ou de droits d'auteur.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

5.1. Évaluer la fin de l'infraction

- → S'assurer que le nom de domaine, la page, le groupe ou le compte en infraction sont hors service ou redirigés vers l'entreprise,
- → Continuer à surveiller le nom de domaine, la page, le groupe ou le compte en infraction. Parfois, un site Web peut réapparaître,
- → Il est possible d'envisager d'acquérir le nom de domaine en infraction s'il est disponible à l'achat.

6. Capitalisation et apprentissage

Objectif : Documenter les détails de l'incident, discuter des leçons apprises et ajuster/améliorer les dispositifs et stratégies de défense.

Le rapport d'incident

Il doit être rédigé et mis à la disposition de toutes les parties prenantes.

Le retour d'expérience

Les thèmes du retour d'expérience doivent être décrits avec les éléments suivants :

- → Cause initiale de l'infection,
- → Actions et chronologies de chaque événement important,
- → Ce qui s'est bien passé,
- → Ce qui ne s'est pas bien passé,
- → Coût de l'incident,
- → Indicateurs de compromission.

La capitalisation

Des actions d'amélioration des processus de détection des logiciels malveillants et des intrusions sur le réseau doivent être définies pour capitaliser sur cette expérience.