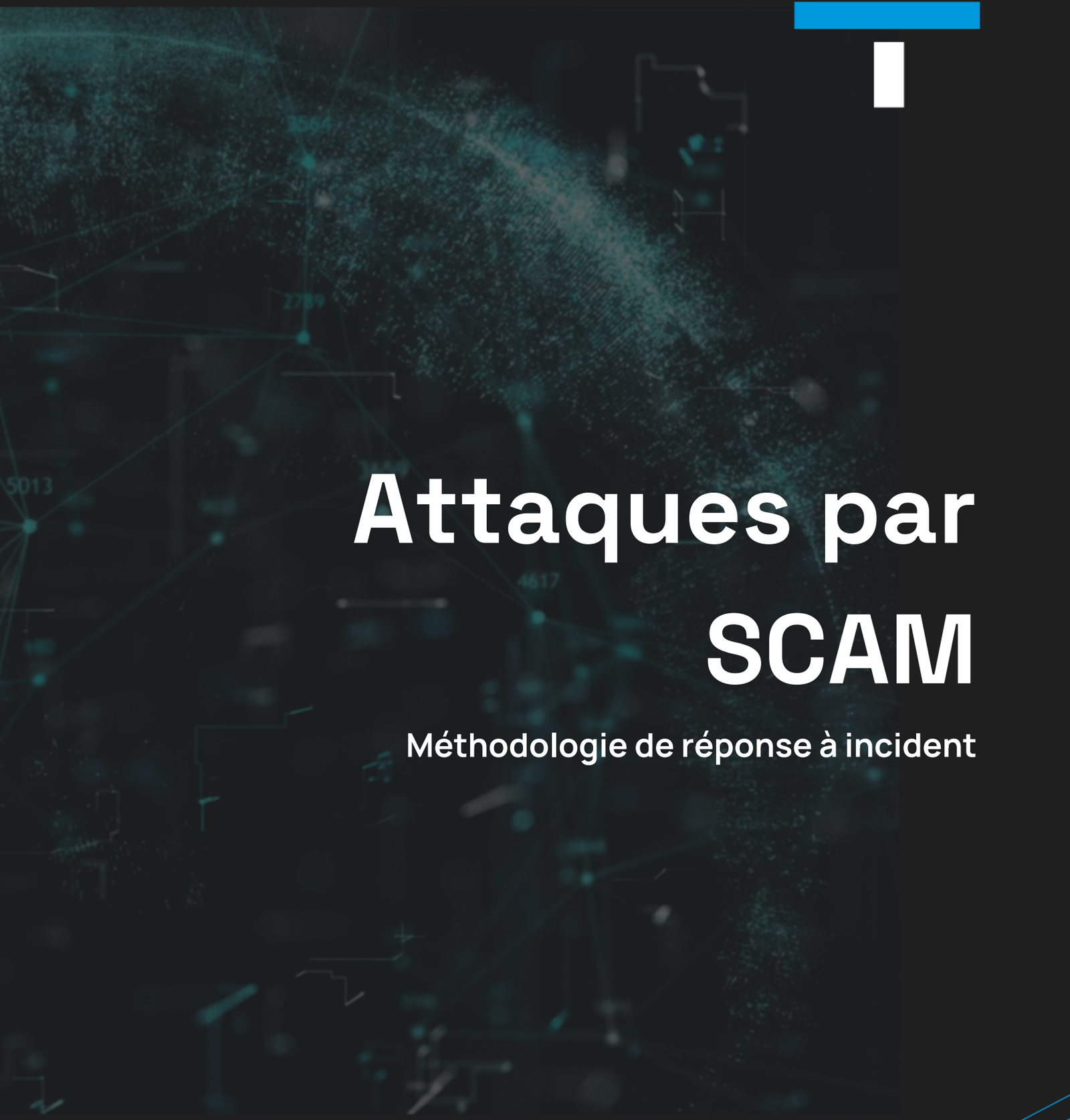
aDvens

Security for the greater good



Attaques par SCAM

Méthodologie de réponse à incident

IRM-14 | 2022-11-30 | **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.

- Créer une liste de tous les domaines légitimes appartenant à l'entreprise. Cela aidera à évaluer la situation et évitera de lancer une procédure de retrait sur un site Web légitime oublié,
- Préparer une page Web hébergée sur l'infrastructure, prête à être publiée à tout moment, pour avertir les clients d'une attaque de SCAM en cours,
  - Préparer et tester une procédure de déploiement.
- Préparer des modèles de demande de retrait des sites par courriel,
  - Ils seront utilisés pour chaque cas de SCAM, si possible, en plusieurs langues. Le processus de retrait sera accéléré lorsque les tentatives seront effectuées pour pour joindre la société d'hébergement.
- Avoir plusieurs moyens pour être joint à temps (24/7 si possible) :
  - Adresse e-mail facile à retenir pour tous (ex : sécurité@entreprise),
  - Formulaires Web sur le site Web de l'entreprise (l'emplacement du formulaire est important, pas plus de 2 clics de la page principale),
  - Compte Twitter visible.
- Déployer DKIM, DMARC et SPF sur toute la chaîne de messagerie,

1.1. Les contacts

- Maintenir une liste de toutes les personnes accréditées pour prendre des décisions sur la cybercriminalité et les actions éventuelles concernant le SCAM,
  - Si possible, avoir un contrat avec un processus validé.
- Établir et tenir à jour une liste de contacts de retrait dans :
  - Sociétés d'hébergement,
  - Sociétés d'enregistrement,
  - Fournisseurs de messagerie.
- Établir et maintenir des contacts avec des CERT à travers le monde qui pourraient être en mesure d'apporter leur aide.

1.2. Sensibiliser les clients

Ne pas attendre les incidents de SCAM pour communiquer avec les clients.

- Sensibiliser à la fraude par SCAM (419 scam ...),
- Expliquer ce qu'est un SCAM et s'assurer que les utilisateurs savent qu'aucune demande d'informations d'identification / bancaires par e-mail ou par téléphone ne leur sera demandée.

2. Identification

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

Disposer d'un équipement d'entreprise dédié pour s'identifier ou échanger avec l'arnaqueur, ne pas utiliser pas d'équipement personnel.

2.1. Détection d'un SCAM

- Surveiller de près tous les points de contact (e-mail, formulaires web, etc.),
- Surveiller les domaines typosquattés et le contenu publié sur ces derniers,
  - Rassembler les informations de contact et d'abus en cas de besoin.
- Surveiller les comptes de réseaux sociaux usurpant le top management ou la marque de l'entreprise,
- Déployer des pièges pour le SPAM et collecter les SPAMS de partenaires ou tiers,
- Déployer une surveillance active des sites de référencement des arnaques, comme 419 scam par exemple,
- Surveiller toutes les listes de diffusion spécialisées ou tous flux RSS/Twitter, qui pourraient signaler des courriels frauduleuses.

L'utilisation d'un système de surveillance automatisé pour toutes ces sources est conseillé, afin que chaque détection déclenche une alerte pour une réaction instantanée.

2.2. Impliquer les acteurs appropriés

- Dès qu'une campagne d'escroquerie est détectée, contacter les personnes de l'entreprise habilitées à prendre une décision,
- La décision d'agir sur l'adresse e-mail frauduleuse doit être prise dans les meilleurs délais, en quelques minutes.

2.3. Recueillir des preuves

- Récupérer des échantillons des e-mails frauduleux envoyés par les fraudeurs :
  - Collecter les entêtes des e-mails en plus de leur contenu,
  - Collecter plusieurs courriels, si possible, pour vérifier l'adresse IP réelle de l'expéditeur,
  - Les investigations seront facilitées si la campagne est envoyée depuis une machine ou depuis un botnet.

En cas de difficultés de collecte d'informations, vérifier http://spamcop.net/fom-serve/cache/19.html

3. Confinement

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

- → Diffuser le contenu frauduleux des e-mails sur les sites Web/partenaires/outils de signalement de spam/fraude,
- → Communiquer vers les utilisateurs et les clients,
- → Ajouter les URL dans le Blackhole DNS, les proxies et la liste de blocage des éléments de protection périmétriques (pare-feu par exemple),
- → Déployer la page d'alerte ou d'avertissement avec les informations sur l'attaque frauduleuse en cours si l'entreprise est touchée.

En cas de hameçonnage récurrent (une fois par semaine), ne pas toujours déployer un message d'alerte mais plutôt une page de phishing très informative pour sensibiliser.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

- → Si les pages frauduleuses sont hébergées sur un site Web compromis, essayer de contacter le propriétaire du site Web,
  - Expliquer clairement la fraude au propriétaire, afin qu'il prenne les mesures appropriées,
  - Supprimez le contenu frauduleux, et surtout améliorer la sécurité sur celui-ci, afin que le fraudeur ne puisse pas revenir en utilisant la même vulnérabilité.
- → Dans tous les cas, contacter également l'hébergeur du site,
  - Envoyer un courriel aux adresses de contact de l'hébergeur (en général il y a un abuse@hostingcompany) puis avoir quelqu'un au téléphone, pour accélérer les choses,
- → Contacter la société d'hébergement de messagerie pour fermer les comptes frauduleux. Ne pas oublier de transmettre une copie du courriel malveillant,
- → Contacter l'équipe d'abus du réseau social pour fermer les comptes frauduleux,
- → Bloquer l'échange de courriel avec l'entreprise ou la personne,

Si il n'a pas de réponse ou si aucune mesure n'est prise, ne pas hésiter à rappeler et à envoyer des e-mails régulièrement,

Si le retrait est trop lent, contacter le CERT local du pays qui pourrait aider à éliminer la fraude , en expliquant les problèmes rencontrés.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

5.1. Évaluer la fin de l'incident

- → S'assurer que les pages et/ou l'adresse e-mail frauduleuses sont hors ligne,
- → S'il existe un site Web frauduleux associé à la fraude, continuer à le surveiller,
- → À la fin d'une campagne de SCAM, supprimer la page d'avertissement associée du site Web de l'entreprise.

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.