aDvens

Security for the greater good

Malware sur smartphone

Méthodologie de réponse à incident

IRM-09 | 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.

Le service d'assistance mobile doit avoir un processus défini en cas d'infection suspectée par un logiciel malveillant : remplacer le smartphone de l'utilisateur par un nouveau et isoler l'appareil suspect pour l'analyse forensique.

Une bonne connaissance de l'activité habituelle du smartphone est appréciée (outils par défaut et extra fonctionnant dessus). Un expert en support smartphone peut être utile pour aider l'analyste.

Il est recommandé de

- → Activer la journalisation (MDM, liste d'applications ou autre),
- → Installer des applications antivirus/de sécurité sur un smartphone,
- → Configurer un VPN pour analyser l'activité du réseau.

Pour l'investigation

- → Sur Android :
  - Activer les options du développeur avec le débogage USB (attention, cela pourrait être un risque, les installations de charge USB publiques par exemple) ou avoir un processus pour l'activer,
  - Déverrouiller les options OEM si possible,
- → Tester les routines d'extraction à l'avance pour s'assurer qu'elles sont compatibles avec les preuves.

2. Identification

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

Principaux points de notification pour smartphone suspect

- → Les applications antivirus/de sécurité déclenchent des alertes,
- → Vérifier s'il n'y a pas d'anomalie dans les droits accordés aux applications,
- → Activité anormale du système, fonctionnement anormalement lent,
- → Activité réseau anormale, connexion Internet lente,
- → Le système redémarre ou s'arrête sans raison,
- → Les applications se bloquent/ redémarrent de manière inattendue,
- → L'utilisateur reçoit un ou plusieurs messages contenant des caractères inhabituels (SMS, MMS, messages Bluetooth, etc.),
- → Augmentation de la facture de téléphone ou de l'activité Web,
- → Appels vers des numéros de téléphone inconnus ou à des heures/jours inhabituels,
- → Une surveillance doit être effectuée pour vérifier une facture ou une activité réseau inhabituelle.

Interroger l'utilisateur sur ses habitudes d'utilisation du smartphone : sites internet habituels, les applications externes installées…

3. Confinement

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

Demander à l'utilisateur de fournir ses informations d'identification pour accéder au smartphone, notamment

- → Le code PIN de la carte SIM,
- → Le mot de passe smartphone,
- → L'identifiant/mot de passe iCloud,
- → Les identifiants Google Play,
- → Le mot de passe des sauvegardes …

Ne pas éteindre le téléphone.

- → S'assurer que l'utilisateur dispose d'un appareil de remplacement à utiliser pendant l'investigation.
- → Sauvegarder les données du smartphone en créant un système de fichiers physique, une sauvegarde logique ou une acquisition manuelle.
- → Mettre le téléphone dans un sac faraday si disponible.

Après l'acquisition, retirer la batterie (si possible) ou mettre le téléphone en mode avion pour bloquer toute activité (WiFi, Bluetooth, etc.).

Actions supplémentaires

- → Retirer la carte SIM pour effectuer une analyse supplémentaire en dehors du smartphone,
- → Effectuer une analyse antivirus ou de sécurité de la sauvegarde ou des fichiers collectés sur une station d'analyse dédiée,
- → Effectuer une analyse forensique de base applicable au cas de l'incident.

Des outils spécifiques doivent être utilisés par l'équipe de réponse aux incidents pour mener une investigation sur le smartphone.
Utiliser une solution d'investigation numérique dédiée pour analyser les données collectées ou le smartphone (Cellebrite, XRY, Oxygen, Axiom, Andriller, etc.)

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

- → Supprimer la menace identifiée du smartphone,
  Ou
- → Effacer de manière sécurisée le smartphone infecté puis le réinitialiser matériellement / logiciellement avec les paramètres d'usine et un micrologiciel vierge,

- → Réinsérer la carte SIM dans le smartphone.

Signaler toutes les applications malveillantes identifiées encore disponibles sur les *marketplaces* (Google / Apple par exemple) pour suppression.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

- → Réinstaller sélectivement les données et les applications enregistrées à partir de leur sauvegarde.

Envisager de conserver l'appareil pendant une période de quarantaine supplémentaire afin d'effectuer les contrôles de sécurité appropriés.

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.