aDvens

Security for the greater good

Infection par un ver

Méthodologie de réponse à incident

2024-10-03 | **TLP-CLEAR** | CERT aDvens - CSIRT

Advens - 38 rue des Jeuneurs - 75002 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.

- → Définir les acteurs, pour chaque entité, qui seront impliqués dans la cellule de crise. Ces acteurs doivent être référencés dans une liste de contacts tenue à jour en permanence,
- → S'assurer que les outils d'analyse sont en place, fonctionnels (EDR, antivirus, IDS, analyseurs de journaux), non compromis et à jour,
- → S'assurer d'avoir une cartographie de l'architecture réseaux,
- → S'assurer qu'un inventaire à jour des actifs est disponible,
- → Effectuer une veille de sécurité continue et informer les personnes en charge de la sécurité de l'évolution des menaces.

2. Identification

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

2.1. Détecter l'infection

Les informations provenant de plusieurs sources doivent être recueillies et analysées :

- Journaux antivirus,
- IDS/IPS,
- EDR,
- Tentatives de connexion suspectes sur les serveurs,
- Nombre élevé de comptes verrouillés,
- Trafic réseau suspect,
- Tentatives de connexions suspectes dans les pare-feux,
- Forte augmentation des appels au support,
- Charge élevée ou blocage du système,
- Volumes élevés d'e-mails envoyés.

Si un ou plusieurs de ces symptômes ont été repérés, informer le responsable de la sécurité du système d'information (RSSI/CISO), et si nécessaire, activer une cellule de crise.

2.2. Identifier l'infection

Analyse des symptômes pour identifier le logiciel malveillant, ses vecteurs de propagation et les contre-mesures.

Les pistes peuvent être trouvées auprès de :

- Bulletins du CERT,
- Contacts d'assistance externes (sociétés d'antivirus, etc.),
- Sites Web de sécurité,
- Capacités et fournisseurs de renseignement sur les menaces.

Informer le responsable de la sécurité de l'information.
Contacter le CERT national et les régulateurs si nécessaire.

Évaluer le périmètre de l'infection

Définir les limites de l'infection (c'est-à-dire : infection globale, limitée à une filiale, etc.).
Si possible, identifier l'impact financier de l'infection.

Pour plus de détails, vérifier les IRM Windows et Linux intrusion IRM-2 et IRM-3

3. Confinement

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

Les actions suivantes doivent être réalisées par les administrateurs et suivies par la cellule de gestion de crise:

3.1. Déconnexion de la zone infectée d'Internet

- Isoler la zone infectée. La déconnecter de tout réseau,
- Si le trafic critique ne peut pas être déconnecté, l'autoriser après s'être assuré qu'il ne peut pas être un vecteur d'infection ou trouver des techniques de contournement,
- Neutraliser les vecteurs de propagation. Pour se propager, le ver peut utiliser différentes techniques telles que les protocoles réseaux de partage ou des vulnérabilités présentes. Des contre-mesures, pertinentes doivent être appliquées (correctif, blocage du trafic, désactivation des appareils, etc.).

Par exemple, les outils/techniques suivants peuvent être utilisés :

- EDR,
- Outils de déploiement de correctifs (WSUS),
- GPO Windows,
- Règles de pare-feu,
- Procédures opérationnelles.

Répéter les différentes étapes sur chaque sous-zone de la zone infectée jusqu'à ce que le ver cesse de se propager. Si possible, mettre en surveillance l'infection à l'aide d'outils d'analyse (console antivirus, journaux du serveur, appels au support) en récupérant les indicateurs de compromission.

La diffusion du logiciel malveillant doit être surveillée.

3.2. Téléphone et mobile

- S'assurer que les ordinateurs portables, téléphones mobiles et les supports de stockage externes ne puissent être utilisés comme vecteur d'infection. Si possible, bloquer toutes leurs connexions.
- Demander aux utilisateurs de suivre strictement les directives et procédures.

A la fin de cette étape, l'infection devrait être contenue.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

4.1. Identifier

- Identifier les outils et les méthodes de remédiation.
- Les ressources suivantes doivent être considérées :
  - Base de données de signatures antivirus,
  - Contacts d'assistance externes,
  - Sites Web de sécurité,
  - Numérisation Yara, Loki, DFIR-ORC, ThorLite,
  - Recherche EDR.

Définir un processus de désinfection. Le processus doit être validé par une structure externe, à savoir le CERT, le SOC et/ou l'équipe de réponse à incident.

Le moyen le plus simple de se débarrasser du ver est de réinstaller entièrement la machine.

4.2. Tester

Tester le processus de désinfection pour vérifier qu'il fonctionne correctement sans endommager de service.

4.3. Déployer

Pour déployer les outils de désinfection, plusieurs options peuvent être utilisées :

- EDR,
- Windows WSUS et GPO,
- Déploiement des signatures virales d'antivirus,
- Désinfection manuelle,
- Correction des vulnérabilités.

Certains **vers** peuvent bloquer certaines des méthodes de déploiement de la remédiation. Si c'est le cas, une solution de contournement doit être trouvée.
Les progrès de la remédiation doivent être suivis par la cellule de crise.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Vérifier que toutes les étapes précédentes ont été effectuées correctement et obtenir l'approbation de la direction avant de suivre les étapes suivantes :

1. Réouverture du trafic réseau qui a été utilisé comme méthode de propagation par le logiciel malveillant,
2. Reconnexion des sous-zones entre elles,
3. Reconnexion des ordinateurs portables mobiles à la zone,
4. Reconnexion de la zone au réseau local,
5. Reconnexion de la zone à Internet.

Toutes ces démarches seront réalisées étape par étape et un suivi technique sera mis en place par la cellule de crise.

Pour plus de détails sur l'authentification et la restauration de l'infrastructure, se référer à l'IRM de compromission sur un large périmètre IRM-18.

6. Capitalisation et apprentissage

Objectif : Documenter les détails de l'incident, discuter des leçons apprises et 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 de la cellule de gestion de crise.

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 gestion des incidents doivent être définies pour capitaliser sur cette expérience.