aDvens

Security for the greater good

Intrusion sous Windows

Méthodologie de réponse à incident

2024-08-22 | **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 la liste de contact des personnes concernées et impliquées dans la résolution de l'incident, définir les procédures, recueillir les informations pertinentes pour ne pas perdre de temps durant la réponse à incident.

- Déployer une solution logicielle de type EDR, de détection et de réponse sur les terminaux, les postes de travail et les serveurs :
  - Cet outil est devenu l'une des pierres angulaires en réponse à incident dans la gestion d'un incident de type rançongiciel ou sur un système d'information compromis sur un large périmètre, facilitant les étapes d'identification, de confinement et de remédiation,
  - Lancer des recherches à l'aide de l'EDR et des analyses antivirales, en spécifiant des indicateurs de compromission ciblés (IOC), et suivre la progression de la compromission et de sa remédiation,
  - Configurer les stratégies de l'EDR sur le mode Prévention.

En l'absence de solution logicielle EDR, un accès physique au système suspect doit être accordé à l'analyste forensique. Un accès physique est préférable à un accès à distance, l'attaquant pouvant détecter les investigations effectuées à distance sur le système (à l'aide d'un logiciel d'analyse réseau par exemple).

- Une copie physique (binaire) du disque de données ou support de stockage peut être nécessaire pour les investigations forensiques et à titre de preuve. Une intervention en local sur le système suspect doit être envisagée pour le déconnecter de tous les réseaux.
- Des profils d'acquisition et de collecte pour l'EDR ou des outils logiciels comme FastIR, DFIR Orc, ou KAPE doivent être préparés.
- Il est nécessaire de disposer d'une base de connaissance sur l'activité réseau usuelle et normale du système compromis. Le fichier stocké dans un endroit sûr doit décrire l'activité habituelle des ports réseau afin d'être comparer à l'état actuel lors de l'incident.
- Il est nécessaire de disposer d'une base de connaissance sur les services habituellement utilisés sur les systèmes. Demander au besoin l'aide d'un expert Windows :
  - La construction d'une cartographie de tous les services et processus présents est conseillée.

Préparer un plan de notification pour la déclaration des abus aux services concernés, aux services d'application de la loi, et aux services régulateurs ou de répression si nécessaire au cours d'un incident (gestion de crise cellulaire).

Dans un environnement d'entreprise de grande importance, travailler avec des postes de travail installés et configurés à l'identique depuis le même support d'installation personnalisé représente un avantage indéniable. Il est nécessaire de disposer de la cartographie de tous les processus/services/applications exécutés sur les postes. Dans un environnement maitrisé où les utilisateurs ne sont pas autorisés à installer des logiciels, il faut considérer tout processus/service/application inhabituel comme suspect.

Plus le fonctionnement nominal et usuel d'un poste de travail est connu et maitrisé, plus il sera facile de détecter une activité malveillante sur celui-ci.

1.1. Les terminaux, postes de travail et serveurs

- S'assurer que les outils d'administration, de suivi et de supervision sont à jour.
- Établir une liste de contact avec les équipes d'exploitation réseau et de sécurité.
- S'assurer qu'un processus de notification d'alerte est défini et bien connu de tous.
- S'assurer que tous les équipements sont configurés sur le même serveur de temps NTP.
- Décider quels types de fichier peuvent être perdus/volés et restreindre l'accès aux fichiers confidentiels.
- S'assurer que les outils d'analyse et solutions de sécurité sont déployés et fonctionnels (Antivirus, EDR, IDS, analyseurs de journaux), ne sont pas compromis ou corrompus et sont à jour.
- Installer les postes et serveurs à partir du même support d'installation personnalisé.

2. Identification

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

2.1. Acquisition de preuves

(A propos des données volatiles)
Avant de mettre en oeuvre toute autre action, s'assurer d'avoir effectuer une capture de la mémoire volatile en téléchargeant et en exécutant FTK Imager, WinPmem ou un autre utilitaire à partir d'un support amovible externe.
Les données volatiles présentes en mémoire fournissent des informations forensiques précieuses et sont directement accessibles pour acquésition.

2.1.1. Données volatiles

→ Les données volatiles sont utiles pour effectuer une analyse de l'historique des lignes de commande exécutées, des connexions réseau, etc. Si possible, il est conseillé d'utiliser l'outil "*Volatility*".

2.1.2. Outil de collecte

→ Utiliser des outils comme un EDR, FastIR, DFIR Orc ou KAPE avec des profils d'utilisation pré-configurés.

2.1.3. Copie de disque

→ Réaliser une image disque complète à l'aide d'outils comme dd, FTKImager, Etc.

Les privilèges d'administrateur seront peut-être nécessaires sur le poste de travail ou le serveur pour réaliser un prélèvement avec un outil de collecte.
De plus, pour effectuer une copie de disque, l'utilisation d'un bloqueur d'écriture ou d'un copieur-bloqueur d'écriture est fortement recommandée.

2.2. Analyse de la mémoire

→ Rechercher la présence de processus malveillants,
→ Examiner les fichiers de librairie DLL et la hiérarchie des processus,
→ Vérifier les artefacts réseau,
→ Rechercher l'injection de code,
→ Vérifier la présence de rootkits,
→ Récupérer une copie des processus suspects pour une analyse plus approfondie.

Si l'incident est considéré comme stratégique (accès à des ressources sensibles), une cellule de gestion de crise spécifique doit être activée (cf. IRM 18 Compromission large périmètre). log2timeline

2.3. Identifier les mécanismes de persistance

La persistance peut être permise à l'aide de différents mécanismes, notamment :

- Tâches planifiées,
- Remplacement de service,
- Création de service,
- Clés de registre de démarrage automatique et dossier de démarrage,
- Détournement de l'ordre de recherche des fichiers de librairie DLL,
- Infection de fichiers de librairie système légitimes par un cheval de Troie,
- Stratégie de groupe locale,
- Complément ou extension Microsoft Office,
- Persistance au pré-démarrage (Altération du BIOS/UEFI/MBR).

2.4. Vérifier les journaux d'événements

- Journal des tâches planifiées (création et exécution),
- Événements de connexion de compte (vérifier les connexions hors bureau),
- Compte local suspect,
- Services malveillants,
- Effacement de journaux d'événements,
- Journaux RDP/TSE,
- Journaux Powershell,
- Journaux SMB.

2.5. Chronologie des événements

- Collecter les preuves et générer une frise chronologique des événements à l'aide d'outils comme Log2timeline,
- Analyser la frise chronologique des événements avec *TimelineExplorer* ou *glogg*.

2.6. Pour aller plus loin

- Recherches d'empreintes numériques,
- Recherche d'anomalies dans les entrées MFT et les horodatages,
- Analyse antivirale/YARA/SIGMA :
  - Accéder aux preuves collectées en mode lecture seule,
  - Exécuter une analyse antivirale ou à l'aide de plusieurs règles Yara et Sigma pour une détection rapide.

Si l'incident est considéré comme stratégique (accès à des ressources sensibles), une cellule de gestion de crise spécifique doit être activée (cf. IRM 18 Compromission large périmètre).

La plupart des conseils fournis dans ce chapitre sont inspirés des posters du Sans Institute : https://www.sans.org/posters
Pour de meilleurs résultats, il est préférable d'utiliser plusieurs de ces outils plutôt qu'un seul.

3. Confinement

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

S'assurer que tous les implants des attaquants ont été identifiés avant de prendre des mesures de confinement.
Être discret si nécessaire et possible.

L'acquisition d'artefacts spécifiques volatiles et en mémoire doit être réalisée avant la mise en oeuvre des étapes suivantes :

- Si la machine est considérée comme critique pour l'activité de l'entreprise et qu'elle ne peut pas être déconnectée, sauvegarder de toutes les données importantes au cas où l'attaquant remarquerait qu'une investigation est en cours et effacerait des fichiers,
- Si possible, isoler la machine à l'aide de l'EDR,

Ou

- Si la machine n'est pas considérée comme critique pour l'entreprise et qu'elle peut être déconnectée du réseau, l'éteindre brutalement en retirant sa prise d'alimentation. S'il s'agit d'un ordinateur portable avec une batterie intégrée, appuyer simplement sur le bouton "off" pendant quelques secondes jusqu'à ce que l'ordinateur s'éteigne.

Des investigations hors ligne doivent être lancées immédiatement si les analyses sur le poste n'ont donné aucun résultat, mais que le système est toujours suspecté d'être compromis :

- Inspecter les partages réseau ou tout dossier accessible par tout le monde et partagé avec d'autres utilisateurs pour identifier si le logiciel malveillant s'y est propagé,
- Plus généralement, essayer de trouver comment l'attaquant a pu accéder au système. Toutes les pistes doivent être prises en compte. Si aucune trace d'intrusion n'est visible, ne jamais oublier que l'attaquant ait pu accéder physiquement au poste ou bénéficier d'une complicité ou du vol d'informations d'un.e employé.e' de l'entreprise,
- Si possible, appliquer les correctifs, pour empêcher le même type d'intrusion, au cas où l'attaquant utiliserait une vulnérabilité corrigée connue.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque et éviter d'être de nouveau attaqué.

Ne commencer à corriger que lorsque l'intégralité du périmètre délimité est contenu ou isolé afin d'empêcher l'attaquant de prendre des mesures de répression.

Si le système a été compromis :

- → Le moyen le plus simple pour se débarrasser d'un logiciel malveillant est de réinstaller entièrement le poste de travail ou le serveur,
- → Supprimer temporairement tous les accès des comptes impliqués dans l'incident,
- → Supprimer tous les fichiers malveillants installés et les mécanismes de persistance mis en place par l'attaquant,
- → Appliquer le mode de prévention de l'EDR pour tous les indicateurs de compromission (IOC) identifiés.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Peu importe jusqu'où l'attaquant a pu accéder sur le système et la connaissance apprises sur l'attaque mise en oeuvre, à partir du moment où un système a été compromis, la meilleure pratique consiste à **réinstaller complètement le système à l'aide du support d'installation d'origine et à appliquer toutes les mises à jour de sécurité.**

Dans le cas où cette solution ne peut pas être appliquée :

- **Modifier tous les mots de passe des comptes du système** et faire en sorte que les utilisateurs le fassent de manière sécurisée,
- **Restaurer tous les fichiers** ayant pu être modifiés par l'attaquant (par exemple : svchost.exe)

Pour plus de détails sur l'authentification et la restauration d'une infrastructure, se référer à l'IRM-18 Compromission large périmètre

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.