aDvens

Security for the greater good

Malware sous Windows

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.

1.1. Déployer une solution EDR sur les endpoints et les serveurs

- Cet outil est devenu l'une des pierres angulaires de la réponse aux incidents en cas de rançongiciel ou de compromission à grande échelle, facilitant les phases d'identification, de confinement et de remédiation,
- Lancer la recherche EDR et l'analyse AV avec les règles explicites d'IOC et obtenir les premiers indicateurs de progression de la correction,
- Définition des politiques EDR en mode de prévention pour éviter toute interruption inutile de l'activité.

1.2. En l'absence d'EDR

- Un accès physique au système suspect doit être accordé à l'analyste,
- L'accès physique est préféré à l'accès à distance, car le pirate pourrait détecter les investigations effectuées sur le système (en utilisant un renifleur de réseau par exemple),
- Une copie physique du disque dur peut être nécessaire à des fins d'investigation et de preuve. Enfin, si nécessaire, un accès physique pourrait être nécessaire pour déconnecter la machine suspecte de tout réseau,
- Des profils d'acquisition pour EDR ou des outils tels que FastIR, DFIR Orc, KAPE, DumpIt, FTK Imager, WinPmem doivent être préparés et testés,
- Une bonne connaissance de l'activité réseau habituelle de la machine/serveur est nécessaire :
  - Un fichier dans un emplacement sécurisé décrivant l'activité réseau permettrait une comparaison rapide des états.
- Une bonne connaissance des services usuels exécutés sur les postes peut être très utile :
  - Ne pas hésiter à demander l'aide d'un expert Windows, le cas échéant,
  - Une bonne idée est également d'avoir une liste de tous les services/processus en cours d'exécution de la machine.

1.3. Les postes et serveurs

- S'assurer que les outils de suivi sont à jour,
- Déployer Sysmon, SmartScreen et appliquer les référentiels de recommandations ANSSI et CIS,
- Établir la liste des contacts avec les équipes d'exploitation réseau et sécurité,
- S'assurer qu'un processus de notification d'alerte est défini et bien connu de tous,
- S'assurer que tous les équipements sont synchronisés avec le même serveur NTP,
- Sélectionner le type de fichiers pouvant être perdus/volés et restreindre l'accès aux fichiers confidentiels,
- S'assurer que les outils d'analyse sont en place, fonctionnels (antivirus, EDR, IDS, analyseurs de journaux), non compromis et à jour,
- Installer à partir du même master d'origine.

2. Identification

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

La famille de logiciels malveillants identifiée aura un impact sur les prochaines étapes de la réponse à l'incident. L'investigation sera plus rapide pour un logiciel potentiellement indésirable ou un mineur. La famille Stealer, Dropper ou Ransomware impliquera une analyse plus approfondie et peut conduire à un autre type d'incident (se reporter à compromission malware sur large périmètre, Ransomware, Windows Intrusion Detection ou Infection par ver si nécessaire).

Signes principaux de la présent d'un logiciel malveillant

→ Plusieurs signes pourraient suggérer que le système pourrait être compromis par des logiciels malveillants :

- EDR, HIDS, logiciel antivirus levant une alerte, incapable de mettre à jour ses signatures, s'arrêtant ou incapable d'exécuter des analyses manuelles,
- Activité inhabituelle du disque dur : le disque dur effectue d'énormes opérations à des moments inattendus,
- Ordinateur anormalement lent : ralentissements soudains et inexpliqués non liés à l'utilisation du système,
- Activité réseau inhabituelle : connexion Internet lente / performances de partage réseau médiocres à intervalles irréguliers,
- L'ordinateur redémarre sans raison,
- Les applications qui se bloquent de manière inattendue,
- Fenêtres intempestives apparaissant lors de la navigation sur le Web. (parfois même sans naviguer),
- L'adresse IP (si statique) est présente sur une ou plusieurs listes de blocage Internet,
- Les gens se plaignent d'envoi de e-mails ou de contact par messagerie instantanée, etc.

Si l'incident est considéré comme stratégique (accès aux ressources sensibles), une cellule de gestion de crise spécifique doit être activée. i.e. Compromission Large Périmètre IRM-18.

La plus part des conseils sont issue des guides du SANS Institute : posters SANS.

2.1. Acquisition de preuves

Avant d'effectuer toute autre action, s'assurer d'effectuer une capture de mémoire volatile en téléchargeant et en exécutant FTK Imager, WinPmem ou un autre utilitaire à partir d'un lecteur externe. Les données volatiles fournissent des informations précieuses et sont simples à acquérir.

2.1.1. Données volatiles

→ Les données volatiles sont utiles pour effectuer une analyse de l'historique de la ligne de commande, des connexions réseau, etc.

Utiliser l'outil winpmem ou DumpIt pour extraire la mémoire vive si possible. * Prendre une image de tri : ** Utiliser des outils comme EDR, FastIR, DFIR Orc, KAPE avec des profils préconfigurés.

Ou

→ Image de copie de disque complète :

- Avec des outils comme dd, FTKImager, etc.

Les privilèges d'administrateur sont souvent requis sur le poste à prélever ou un bloqueur en écriture (physique ou logique) pour la création d'image disque en fonction des cas.

2.1.2. Analyse de la mémoire

- Rechercher des processus malveillants,
- Examiner les DLL et les "handles" de processus,
- Vérifier les traces réseau,
- Rechercher des injections de code,
- Vérifier la présence de rootkits,
- Récupérer les processus suspects pour une analyse plus approfondie.

Si l'incident est considéré comme stratégique (accès aux ressources sensibles), une cellule de gestion de crise spécifique doit être activée. i.e. Compromission Large Périmètre IRM-18.

2.1.3. Identifier les mécanismes de persistance

La persistance peut être acquise par différentes techniques :

- Tâches planifiées,
- Remplacement de service,
- Création d'un service,
- Démarrage automatique par le biais des clefs de registres et des répertories de démarrage,
- *Hijacking* de DLL,
- Utilisation de chevaux de Troie par piégeage de librairies légitime,
- Stratégie de sécurité locale,
- Installation d'Add-in MS Office,
- Persistance au niveau du boot (altération de BIOS/UEFI/MBR)

Il est possible de considérer que les *autoruns* Microsoft soient pertinent.

2.1.4. Vérifier les journaux d'évènements

- Journaux des tâches planifiées,
- Journaux des audits de comptes (regarder des connexions aux heures non-ouvrées),
- Utilisation de compte locaux suspects,
- Service malveillant,
- Suppression des journaux,
- Journaux de connexion RDP/TSE,
- Journaux PowerShell,
- Journaux SAMBA (SMB).

2.1.5. Réaliser une frise chronologique complète

- Traiter les prélèvement pour créer une frise chronologique complète avec comme outil *Log2timeline* par exemple,
- Analyser cette frise avec *TimelineExplorer* ou *glogg* par exemple.

2.1.6. Pour aller plus loin

- Vérifier les empreintes dans des bases d'empreintes,

→ Rechercher des anomalies sur la MFT de type *Timestamping*,

→ Analyser avec des antivirus, moteur Yara ou Sigma :

- Connecter les preuves en **READ-ONLY**. Lancer un scan complet antivirus ou avec un moteur Yara pour trouver rapidement des éléments pertinents,
- Les logiciels malveillants ne seront pas détectés pour autant, c'est un premier niveau.

Si l'incident est considéré comme stratégique (accès aux ressources sensibles), une cellule de gestion de crise spécifique doit être activée. i.e. Compromission Large Périmètre IRM-18.

3. Confinement

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

L'acquisition de la mémoire et des artefacts volatils sélectifs doit être effectuée avant que les étapes suivantes aient eu lieu.

Si la machine est considérée comme critique pour l'activité de l'entreprise et ne peut pas être déconnectée, sauvegarder toutes les données importantes au cas où le pirate remarquerait l'investigation en cours et commencerait à supprimer des fichiers.

→ Si possible, isoler la machine via EDR.

OU

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

Envoyer les fichiers binaires suspects au CERT ou demander l'aide du CERT si la nature du logiciel malveillant n'est pas connu.
Le CERT devrait être en mesure d'isoler le contenu malveillant et de l'envoyer à tous.
*** Le meilleur moyen est de créer un fichier compressé et chiffré par mot de passe du binaire suspect.**

3.1. Investigation hors Ligne

Les investigations hors ligne doivent être lancées immédiatement si les premières analyses n'ont rien donné. Le système doit toujours être considéré comme compromis.

→ Inspecter les partages réseau ou tout dossier publiquement accessible avec d'autres utilisateurs pour voir si le logiciel malveillant ne s'y est pas propagé.
→ Plus généralement, essayer de trouver comment l'attaquant est entré dans le système.
- Toutes les pistes doivent être prises en compte. Si aucune preuve informatique de l'intrusion n'est trouvée, ne pas oublier qu'elle pourrait provenir d'un accès physique ou d'une complicité ou d'un vol d'informations d'un employé.

→ Appliquer les correctifs le cas échéant (système d'exploitation et applications) au cas où l'attaquant utiliserait une vulnérabilité connue.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

Ne commencer à corriger que lorsque 100% du périmètre délimité est contenu afin d'empêcher l'attaquant de lancer des actions en représailles.

Le moyen le plus simple de se débarrasser des logiciels malveillants consiste à réinstaller le poste de zéro.

→ Supprimer les fichiers binaires et les entrées de registre associées,
→ Découvrir le meilleur moyen pour supprimer le logiciel malveillant. Ils peuvent généralement être trouvés sur les sites Web des sociétés antivirus,
→ Supprimer tous les fichiers malveillants installés et les mécanismes de persistance mis en place par l'attaquant,
→ Appliquer le mode de prévention EDR pour tous les IOC (indicateurs de compromission) identifiés.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

- → Si possible, réinstaller le système d'exploitation et les applications et restaurer les données de l'utilisateur à partir de sauvegardes propres et fiables.
  - Si cela est jugé nécessaire, demander au service d'assistance informatique local de repartir d'une image disque saine.

Si l'ordinateur n'a pas été complètement réinstallé

- → Restaurer les fichiers qui auraient pu être corrompus par le logiciel malveillant, en particulier les fichiers système.
- → Modifier tous les mots de passe des comptes du système et faire en sorte que les utilisateurs le fassent de manière sécurisée.
- → Redémarrer la machine une fois tous les fichiers suspects supprimés et confirmer que le poste de travail ne présente aucun comportement inhabituel. Une analyse avec AV et EDR à jour sur tous les disques durs et la mémoire est recommandée.

Si un utilisateur est à l'origine de la compromission, un renforcement des campagnes de sensibilisation à la sécurité est à prévoir.

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.