aDvens

Security for the greater good

Compromission large périmètre

Méthodologie de réponse à incident

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

Advens - 38 rue des Jeuneurs - 75002 Paris

Sommaire

INTRODUCTION 2
ÉTAPES DE TRAITEMENT DES INCIDENTS 2
1. PRÉPARATION 3
1.1. Les postes et serveurs 3
1.2. Les réseaux 3
1.3. Flux de l'entreprise 4
2. IDENTIFICATION 5
2.1. Détection 5
2.2. Cadrage de l'incident 5
2.3. Trouver le vecteur initial de compromission 5
3. CONFINEMENT 6
4. REMÉDIATION 7
4.1. Les postes et serveurs 7
4.2. Les réseaux 7
5. RÉCUPÉRATION 8
5.1. Les postes et serveurs 8
5.2. Les réseaux 8
6. CAPITALISATION ET APPRENTISSAGE 8

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.

Différents actions/points doivent pouvoir être effectués :

- Être en mesure de déployer une solution EDR sur les postes 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.
- Être en mesure de lancer une recherche EDR et/ou une analyse AV avec des règles explicites d'IOC afin d'obtenir les premiers indicateurs pouvant servir à la remédiation,
- Être en mesure de définir des politiques EDR en mode prévention,
- Être en mesure de bloquer les IOC liés aux activités de logiciels malveillants recueillies par la *Threat Intelligence*,
- Être en mesure de déployer et exploiter des solutions de sécurité permettant la détection et facilitant la réponse,
  - Collecter les journaux dans un SIEM,
  - Avoir la capacité d'exécuter des outils comme YARA ou DFIR-ORC (ANSSI),
- Avoir une bonne rétention des journaux et de la verbosité,
- Pouvoir définir une posture stricte face à l'agresseur,
- Préparer la stratégie de communication interne et externe,
- Détenir un processus pour définir la posture à adopter le plus rapidement possible après la détection de la compromission : *discret* ou *réaction rapide*.

Être prêt à notifier les équipes de sécurité, les forces de l'ordre et les régulateurs de secteur, si cela le nécessite pendant un incident (cellule de management de crise)

1.1. Les postes et serveurs

- Connaître les politiques de sécurité usuelles des systèmes d'exploitation,
- Détenir les politiques de profil des utilisateurs,
- S'assurer que les outils de surveillance sont à jour,
- Pouvoir établir la liste des contacts entre les équipes d'exploitation des systèmes d'information (réseau, système, sauvegarde …) et de sécurité,
- S'assurer qu'un processus de notification d'alerte est défini et connu de tous,
- S'assurer que tous les équipements sont configurés sur le même serveur de temps (serveur NTP),
- Être en mesure de connaître les fichiers qui peuvent être perdus/volés et limiter l'accès aux fichiers confidentiels,
- S'assurer que les outils d'analyse sont opérationnels (antivirus, EDR, IDS, analyseurs de journaux), non compromis et à jour.

1.2. Les réseaux

- Détenir l'architecture, la segmentation VLAN et les interconnexions (cartographie) :
  - Avoir la capacité d'isoler des entités, des régions, des partenaires ou Internet
  - Avoir la capacité d'isoler des éléments en SaaS ou dans le Cloud tout comme en On-Premise
- S'assurer qu'un inventaire des points d'accès au réseau est disponible et à jour,
- S'assurer que les équipes réseau disposent de cartes et de configurations réseau à jour,
- Rechercher et fermer régulièrement les points d'accès réseau indésirables potentiels (xDSL, Wi-Fi, Modem, …),
- S'assurer que les outils et les processus de gestion du trafic sont opérationnels,

Une bonne connaissance de l'activité réseau habituelle des postes et serveurs est nécessaire.
Un fichier la décrivant doit être créé et stocké dans un emplacement sécurisé pour la comparer efficacement à l'état actuel en cas d'incident.

1.3. Flux de l'entreprise

- Identifier le trafic et les flux de référence,
- Identifier les flux critiques pour l'entreprise (salaire, facturation, MFA, EDR ...).

2. Identification

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

Il est possible qu'il faille prévenir l'équipe juridique, les régulateurs de secteur et/ou l'équipe de sécurité au commencement de cette étape.

2.1. Détection

- Surveiller les IOCs venant de la "*Threat Intelligence*" par le SOC,
- Supervision des alertes et des journaux Antivirus, EDR, SIEM, IDS,
- Des e-mails professionnels étranges (souvent de fausses factures) contenant des pièces jointes ayant été reçus,
- Le mouvement latéral est généralement effectué, vérifier toutes les connexions au serveur AD et de partage de fichier avec des comptes privilégiés à des heures anormales de la journée,
- Nombre élevé de comptes verrouillés,
- Rechercher les activités inhabituelles ou rare de navigation sur le réseau ou sur le Web :
  - Notamment les connexions aux IP Tor I2P, aux passerelles Tor (tor2web, etc) ou aux sites de paiement Bitcoin.

Si un poste ou un serveur est identifié comme compromis, le déconnecter du réseau et le garder allumé pour pouvoir réaliser une analyse de la mémoire.

2.2. Cadrage de l'incident

Un EDR ou des outils de recherche (*Hunting*) à grande échelle comme YARA ou DFIR-ORC permettent de faire l'inventaire des machines infectées.

- Utiliser l'EDR, les journaux des terminaux, les journaux système, les outils permettant la recherche IOC à grande échelle,
- Identifier les techniques de pivot sur le réseau,
- Consulter les statistiques et les journaux des périphériques réseau,
- Identifier l'utilisation malveillante des comptes compromis,
- Identifier les serveurs de commande et de contrôle dans les journaux de pare-feu, les journaux de proxy, les journaux IDS, les journaux système, l'EDR, les journaux DNS, les NetFlow et les journaux de routeur.

2.3. Trouver le vecteur initial de compromission

- Rechercher sur les actifs exposés (en particulier ceux qui ne sont pas à jour),
- Vérifier la présence de fichiers binaires dans les profils utilisateur, **Users\Public**, **%ALLUSERSPROFILE%** ou **%APPDATA%** et **%SystemDrive%**

L'identification de la menace à l'origine de l'attaque pourrait aider lors des phases suivantes basées sur les TTPs et IOCs connus.

A l'issue de cette étape, les machines impactées et le modus operandi de l'attaque doivent être identifiés. Idéalement, la source de l'attaque aurait également dû être identifiée.
Les investigations numériques commencent à ce moment.
Il faut garder les sauvegardes en sécurité et déconnectées de la partie compromise.

3. Confinement

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

1. Si le sujet est considéré comme stratégique (accès aux ressources sensibles), une cellule de gestion de crise spécifique doit être activée.

- → S'assurer que toutes les implants des attaquants ont été identifiés avant de prendre des mesures de confinement,
- → Rester discret si c'est possible et nécessaire.

2. Si applicable à l'attaque :

- → Isolation du VLAN, des interconnexions, des entités, des régions, des partenaires/prestataires compromis ou d'internet,
- → Déconnexion de tous les ordinateurs qui ont été identifiés comme compromis du réseau,
- → Isolation possible avec l'EDR,
- → Réduction des accès internet en conservant les connexions vers EDR actives,
- → Blocage du trafic vers les C2,
- → Blocage de toute adresse IP détectée comme malveillante,
- → Désactivation des comptes compromis/créés par les attaquants,
- → Envoi des échantillons non détectés au fournisseur de sécurité des terminaux et/ou à des bacs à sable privés,
- → Envoi de l'URL malveillante non catégorisée, des noms de domaine et d'IP au fournisseur de sécurité périmétrique.

3. 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 valides.

4. Neutraliser les vecteurs de propagation. Pour se propager, l'attaquant 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 …)

Par exemple, les techniques suivantes peuvent être utilisées :

- → Outils de déploiement de correctifs (WSUS),
- → GPO Windows,
- → Règles de pare-feu,
- → Sinkhole du DNS,
- → Arrêter les services de partage de fichiers,
- → Mettre fin aux connexions ou aux processus indésirables sur les machines concernées.

5. Répéter les étapes 2 à 4 sur chaque sous-zone de la zone infectée jusqu'à ce que le fichier malveillant cesse de se propager. Surveiller l'infection à l'aide d'outils d'analyse (console antivirus/EDR, journaux du serveur, appels au support).

Appliquer des actions ad hoc en cas d'enjeu stratégique :

- → Bloquer la destination d'exfiltration ou l'emplacement distant au niveau des règles de filtrage d'internet,
- → Restreindre les serveurs de fichiers stratégiques pour rejeter les connexions des postes ou serveurs compromis,
- → Informer les utilisateurs de l'entreprise ciblés de ce qui doit être fait et de ce qui est interdit,
- → Augmenter la verbosité des journaux des postes, des serveurs et du réseau au niveau de l'environnement ciblé et stockez-les sur un serveur sécurisé distant.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

4.1. Les postes et serveurs

- → Réinitialiser tous les accès aux comptes concernés par l'incident,
- → Supprimer tous les comptes créés par les attaquants,
- → Supprimer l'accès initial utilisé par l'attaquant,
- → Supprimer les binaires utilisés par l'attaquant ayant permis une latéralisation sur le réseau,
- → Supprimer les persistances,
- → Changer le mot de passe des comptes compromis,
- → Réappliquer les bonnes configurations qui ont été modifiées par l'attaquant,
- → Opérer un durcissement du système.

4.2. Les réseaux

- → Découvrir tous les canaux de communication utilisés par l'attaquant et les bloquer sur l'ensemble des réseaux,
- → Vérifier si la configuration de sécurité est intacte : GPO, AV, EDR, Patch ...,
- → Opérer le renforcement des configurations réseaux.

Si la source a été identifiée comme un attaquant externe alors il faut prévenir l'équipe juridique et les régulateurs si nécessaire.
Si la source a été identifiée comme un attaquant interne prendre les actions appropriées et prévenir la hiérarchie et/ou les ressources humaines et/ou l'équipe juridique.

L'utilisation de la partie remédiation des IRM d'intrusion Windows (IRM-02) ou Linux (IRM-03) peuvent être utiles en fonction du cas.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Prioriser le plan de reprise en fonction du plan de reprise d'activité après l'incident (PRA / DRP - disaster recovery plan).

L'ensemble de ces étapes se fera de manière progressive avec un suivi technique.

5.1. Les postes et serveurs

S'assurer qu'aucun fichier malveillant n'est présent sur les systèmes avant de les reconnecter.

- → Les bonnes pratiques sont de réinstaller complètement un poste ou serveur compromis avec les éléments originaux,
- → Installer toutes les mises à jour sur le poste ou serveur nouvellement créé.
- → Si les solutions sont inapplicables :
  - Restaurer tous les fichiers modifiés
  - Changer tous les mots de passe du poste ou serveur (utiliser des mots de passe robuste)

5.2. Les réseaux

1. S'assurer d'un retour à la normal du trafic réseau (sécurisé)
2. Autoriser de nouveau le trafic réseau qui a pu être utilisé pour la propagation de l'attaquant
3. Reconnecter les sous-réseaux ensemble si nécessaire
4. Reconnecter les réseaux au réseaux locaux si nécessaire
5. Reconnecter les différentes zones réseaux à internet si nécessaire
   - Surveiller le trafic réseau pour identifier une potentielle reprise ou un infection encore présente,
   - Si possible, appliquer un filtrage géographique sur les pare-feux pour bloquer le trafic illégitime provenant de pays étrangers,

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.