aDvens

Security for the greater good

Attaque par rançongiciel

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.

Une bonne connaissance des éléments suivants est indispensable pour une bonne réaction face à une attaque par rançongiciel :

- Des politiques de sécurité des systèmes d'exploitation,
- des politiques de profil des utilisateurs,
- Une architecture de segmentation en VLAN et interconnexions,
  - Avoir la capacité d'isoler des entités, des régions, des partenaires ou internet,
- S'assurer que les produits de sécurité des points de terminaison et périmétriques (passerelle de messagerie, caches proxy) sont à jour,
- 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 l'analyse AV avec les règles explicites d'IOC afin d'obtenir les premiers indicateurs pouvant servir à la remédiation,
  - Définir les politiques EDR en mode prévention,
- Être en mesure de bloquer les IOC liés aux activités de rançongiciel 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 du journal et de la verbosité,
- Pouvoir définir d'une posture stricte face à l'agresseur,
- Préparer la stratégie de communication interne et externe.

Si un poste ou un serveur est identifié avec un rançongiciel, il est préférable d'isoler l'équipement du réseau sans l'éteindre afin de procéder à des investigations numériques.

Étant donné que cette menace est souvent détectée par les utilisateurs, une sensibilisation du support informatique de l'entreprise à la menace rançongiciel est indispensable.

1.1. Les sauvegardes

Conserver des sauvegardes exhaustives, récentes et fiables des données des utilisateurs locaux et du réseau.

Les règles de **sauvegarde 3-2-1** peuvent être suivies : chacune de ces règles est destinée à garantir que vos données soient stockées de plusieurs manières.

1.1.1. Politique de sauvegarde

- → Au moins **trois** copies : trois copies différentes signifient trois copies différentes à des endroits différents :
  - En les stockant à différents endroits, cela réduit le risque qu'un seul événement détruise plusieurs copies.
- → Dans **deux** formats différents : utilisation d'au moins deux méthodes différentes pour stocker les données :
  - Par exemple : bandes, disques durs, services Cloud ou autres sont des formats différents.
- → Avec l'**une** de ces copies hors site : conserver une copie hors site garantit que, quoi qu'il arrive où se trouvent les données (incendie, effraction, catastrophe naturelle…) :
  - Au moins une copie est en sécurité. Avec cette règle, les services cloud ont du sens.
- → Utilisation d'un format de sauvegarde stocké hors du réseau :
  - Si un mouvement latéral se produit dans le but de chiffrer vos données, cette copie sera hors de portée.

2. Identification

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

2.1. Signes généraux de présence de rançongiciels

Certains signaux peuvent indiquer que le système est compromis par un rançongiciel :

- Surveillance des IOC de ransomware par un SOC,
- Supervision des alertes EDR,
- Des e-mails professionnels étranges (souvent de fausses factures) contenant des pièces jointes ayant été reçus,
- Un message de rançon expliquant que les documents ont été chiffrés et demandant le paiement d'une rançon s'affiche sur le bureau de l'utilisateur,
- Les gens se plaignent que leurs fichiers ne sont pas disponibles ou sont corrompus sur leurs ordinateurs ou leurs partages réseau avec des extensions inhabituelles (.abc, .xyz, .aaa, etc…),
- De nombreux fichiers sont modifiés en très peu de temps sur les partages réseau,
- Publication d'informations sur les sites Web ou les forums des opérateurs de rançongiciels,
- Des mouvements latéraux sont effectués :
  - Vérifier de toutes les connexions au serveur AD et partage de fichiers avec des comptes privilégiés à des heures anormales de la journée,
- Rechercher des activités inhabituelles 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,
- Rechercher de connexions rares.

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 par le rançongiciel.
- L'identification de l'accès initial et du pivot utilisé par les attaquants est la priorité, comme lors d'une compromission sur un large périmètre (IRM-18). Cela permet d'établir les phases suivantes de la réponse à incident.

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

L'identification de la compromission du réseau par les rançongiciel présente de nombreuses similitudes avec la compromission sur un large périmètre (IRM-18).
La plupart du temps, la décision de réaction doit être prise plus rapidement dans les cas de rançongiciel. Pour plus de détails sur la compromission sur un large périmètre, se référer à IRM-18.

3. Confinement

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

- → Faire une déclaration publique dès que possible sur la base du modèle de communication élaboré lors de la phase de préparation,
- → Suivre la posture définie dans la phase de préparation,
- → Envoyer des échantillons non détectés aux fournisseur de sécurité des postes/serveurs et/ou à des bacs à sable privés,
- → Envoyer de l'URL malveillante non catégorisée, des noms de domaine et de l'IP au fournisseur de sécurité périmétrique,
- → Bloquer du trafic vers les C2 (serveur Command And Control),
- → Bloquer d toute adresse IP détectée comme utilisée par des attaquants,
- → Isoler les VLAN, interconnexions, entités, régions, partenaires compromis ou internet,
- → Désactiver les comptes compromis/créés par des attaquants,
- → Déconnecter de tous les ordinateurs détectés comme compromis du réseau :
  - Une isolation par l'EDR est conseillée ainsi que la fermeture des liaisons internet en gardant les connexions EDR actives,
- → Si certaines isolations ne sont pas possibles, déconnecter et supprimer les partages de fichier des postes ou serveurs impactés :
  - exemple sous Windows : `net use x: \\unc\path /DELETE`.

Surveiller le site internet de l'acteur de rançongiciel pour rechercher une fuite d'information qu'il revendiquerait et/ou diffuserait grâce à l'attaque.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

- → Supprimer l'accès initial utilisé par l'attaquant,
- → Supprimer les binaires utilisés par l'attaquant pour se déplacer (latéralisation) sur le réseau,
- → Supprimer tous les comptes créés par des attaquants,
- → Remédier aux changements de configuration effectués par l'attaquant,
- → Opérer un renforcement de la configuration des systèmes et du réseau.

Pour plus de détails voir l'IRM-18, compromission sur un large périmètre.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

- → Mettre à jour les signatures antivirus pour les binaires malveillants identifiés pouvant être bloqués,
- → S'assurer qu'aucun fichier binaire malveillant n'est présent sur les systèmes avant de les reconnecter,
- → S'assurer que le trafic réseau est revenu à la normale,
- → Restaurer les documents de l'utilisateur à partir des sauvegardes.

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 feront de manière progressive avec un suivi technique.

Il faudra vérifier que les sauvegardes ne sont pas compromises :

- → Ne restaurer qu'à partir d'une sauvegarde sûre ainsi que depuis des postes ou serveurs vérifiés,

ou bien

- → Restaurer l'image originale du poste ou du serveurs avec une nouvelle installation,
- → Réinitialiser les informations d'identification, y compris les mots de passe (en particulier pour les administrateurs et les autres comptes privilégiés),
- → 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,
- → Maintenir une surveillance des sites Web des acteurs de la menace de rançongiciel et d'internet pour déterminer s'il existe une publication de données liée à la compromission (fuite de données).

Pour plus de détails voir l'IRM-18, compromission sur un 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.