RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Ne pas diffuser aux joueurs

DÉTAILS DU SCÉNARIO

« ATTAQUE PAR SUPPLY CHAIN »

Type d’attaque : supply-chain

(Chaine logistique informatique)

Scénario « attaque par supply chain » proposé dans le cadre du kit simulation :

Une attaque de la chaine logistique informatique se produit lorsqu'un pirate accède au réseau d'une entreprise par le biais d'un fournisseur tiers.

En l’occurrence dans le scénario proposé, des attaquants attaquent un fournisseur cloud via une mise à jour logiciel vérolée pour chiffrer les serveurs puis accèdent aux réseaux des clients de ce dernier (déploiement du rançongiciel).

Conventions d’exercice (règles et limites des simulations – à adapter) :

- Votre entité à recours à des services hébergés ;
- Déroulement de l’exercice en temps réel (pas de compression de temps).

Adaptation du chronogramme à votre entité :

Le scénario d’exercice proposé se découpe en trois phases avec une gradation des impacts. Un chronogramme d’exercice générique est fourni dans le kit planificateur/animateur. Il convient de l’ajuster en fonction de vos spécificités.

Type d'attaque : supply-chain

Définition d'une attaque par supply-chain

Menace informatique ciblant les prestataires de service et les bureaux d'études. Des attaquants prennent position sur les réseaux de prestataires afin de récupérer les données, voire d'accéder aux réseaux de leurs clients.

Contexte

Les usages numériques non maîtrisés et les faiblesses dans la sécurisation des données continuent d'offrir de trop nombreuses opportunités d'actions malveillantes. Le Cloud Computing et l'externalisation de services auprès d'entreprises de services numériques (ESN), sans clauses de cybersécurité adaptées, augmentent la surface d'attaque potentielle et représentent toujours un vecteur d'attaque indirecte d'intérêt.

Pour en savoir davantage sur l'exploitation des nouveaux usages numériques à des fins malveillantes, vous pouvez prendre connaissance du Panorama de la cybermenace 2022, réalisé par l'ANSSI. https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/

Source: Panorama de la cybermenace 2022, ANSSI.

Les différentes phases du scénario (1/4)

Compromission d'un fournisseur cloud → Propagation du rançongiciel → Divulgation de données

Phase 1 du scénario
Indisponibilité de certains services bureautiques et informatiques en nuage

- → Un de vos hébergeurs infonuagique a effectué une mise à jour vérolée du logiciel de supervision de ses hyperviseurs (machines virtuelles) ;
- → Les attaquants ont pu accéder à distance au réseau administrateur des datas centers concernés et ont pu déployé un logiciel espion (spyware) leur permettant ainsi de collecter des données stratégiques présentes sur les machines virtuelles pendant quelques mois ;
- → Chiffrement par rançongiciel des machines virtuelles de l'hébergeur ;
- → Cela a entraîné au sein de votre organisation l'indisponibilité de certains services de bureautique (tableau, traitement de texte, stockage en ligne, etc.) et d'applications Saas*.

Phase 2 du scénario
Blocage des postes informatiques et serveurs

- → A partir des données collectées par l'attaquant via l'hébergeur cloud, ce dernier a récupéré des informations d'accès à distance et des identifiant/mot de passe d'un compte administrateur de votre organisation ;
- → Avec ceux-ci, avant de déployer le rançongiciel sur les machines virtuelles de l'hébergeur (pour ne pas être repéré), l'attaquant s'est introduit sur votre réseau, a escaladé successivement ses privilèges pour prendre le contrôle d'un contrôleur de domaine et récolté des données sensibles supplémentaires.
- → Déploiement du rançongiciel sur votre/vos SI.
- → Cela a entraîné au sein de votre organisation un blocage des serveurs et postes informatiques.

Phase 3 du scénario
Divulgation de données sensibles

- → L'attaquant, par le biais du logiciel espion déployé sur les machines virtuelles de l'hébergeur et lors de son infiltration sur votre/vos SI, a pu rassembler des données stratégiques et sensibles ;
- → Pour mettre la pression sur votre organisation et encourager le paiement d'une rançon, l'attaquant met en ligne un jeu de données. Il menace de mettre en ligne davantage de données dans les prochaines heures si la rançon n'est pas payée.

*SaaS = Software as a Service (Logiciel en tant que service) > logiciels/applications directement accessibles en ligne

Les différentes phases du scénario (2/4)

Phase 1 – Panne des services bureautiques et informatiques en nuage

Contexte cyber

- Un de vos hébergeurs infonuagique (cloud) a effectué une mise à jour vérolée du logiciel de supervision de ses hyperviseurs (machines virtuelles) ;
- Lors de cette mise à jour, un logiciel espion (spyware) a été déployé par les attaquants leur permettant ainsi de collecter des données stratégiques présentes sur les machines virtuelles ;
- À partir des données récupérées, chiffrement par rançongiciel des machines virtuelles de l'hébergeur.

Impacts sur votre organisation

- Plusieurs de vos services bureautiques ainsi que d'autres services numériques s'appuyant sur ce fournisseur cloud sont indisponibles (gestion RH, paie, etc.) ;
- Les services de stockage de données en ligne sont également indisponibles.

Par convention d'exercice, les boîtes mail sont fonctionnelles.

Enjeux pour les joueurs

- Activation de la chaine d'alerte ;
- Comprendre l'origine de la défaillance et les alternatives pour continuer à travailler ;
- Répondre à la pression interne et à la pression externe relatives à l'indisponibilité des services ;
- Identifier les moyens et la coordination nécessaire avec l'hébergeur touché.

À adapter selon votre organisation : applications internes et externes indisponibles, périmètre touché, noms des départements touchés, etc.

Les différentes phases du scénario (3/4)

Phase 2 – Déploiement du rançongiciel / blocage de certains postes informatiques

Contexte cyber

- A partir des données collectées par l'attaquant via l'hébergeur cloud, ce dernier a récupéré des informations d'accès à distance et des identifiant/mot de passe d'un compte administrateur de votre organisation ;
- Avec ceux-ci, avant de déployer le rançongiciel sur les machines virtuelles de l'hébergeur (pour ne pas être repéré), l'attaquant s'introduit sur votre réseau, escalade ses privilèges successivement pour prendre le contrôle d'un contrôleur de domaine, récolte des données supplémentaires et lance le déploiement du rançongiciel sur votre/vos SI.

Impacts sur votre organisation

- Suite à l'activation du rançongiciel, plusieurs serveurs et postes informatiques sont bloqués et inutilisables ;
- La pression médiatique est forte.

Par convention d'exercice, un seul département/filiale peut être impacté par le rançongiciel.

Enjeux pour les joueurs

- Activation de la chaine d'alerte ;
- Identifier les mécanismes de continuité d'activité à activer ;
- Mettre en place la stratégie de communication de crise pour répondre à la pression médiatique.

Par convention d'exercice, l'endiguement de l'attaque ainsi que la remédiation ne sont pas à jouer.

À adapter selon votre organisation

Périmètre victime du rançongiciel, impact métiers, etc.

Les différentes phases du scénario (4/4)

Phase 3 – Divulgation de données sensibles

Contexte cyber

- L'attaquant, par le biais du logiciel espion déployé sur les machines virtuelles de l'hébergeur et lors de son infiltration sur votre/vos SI, a pu rassembler des données stratégiques et sensibles ;
- Pour mettre la pression sur votre organisation et encourager le paiement d'une rançon, l'attaquant met en ligne un jeu de données. Il menace de mettre en ligne davantage de données dans les prochaines heures si la rançon n'est pas payée.

Impacts sur votre organisation

- Fuite de données à caractère personnel ;
- La pression interne et médiatique s'accentue.

Enjeux pour les joueurs

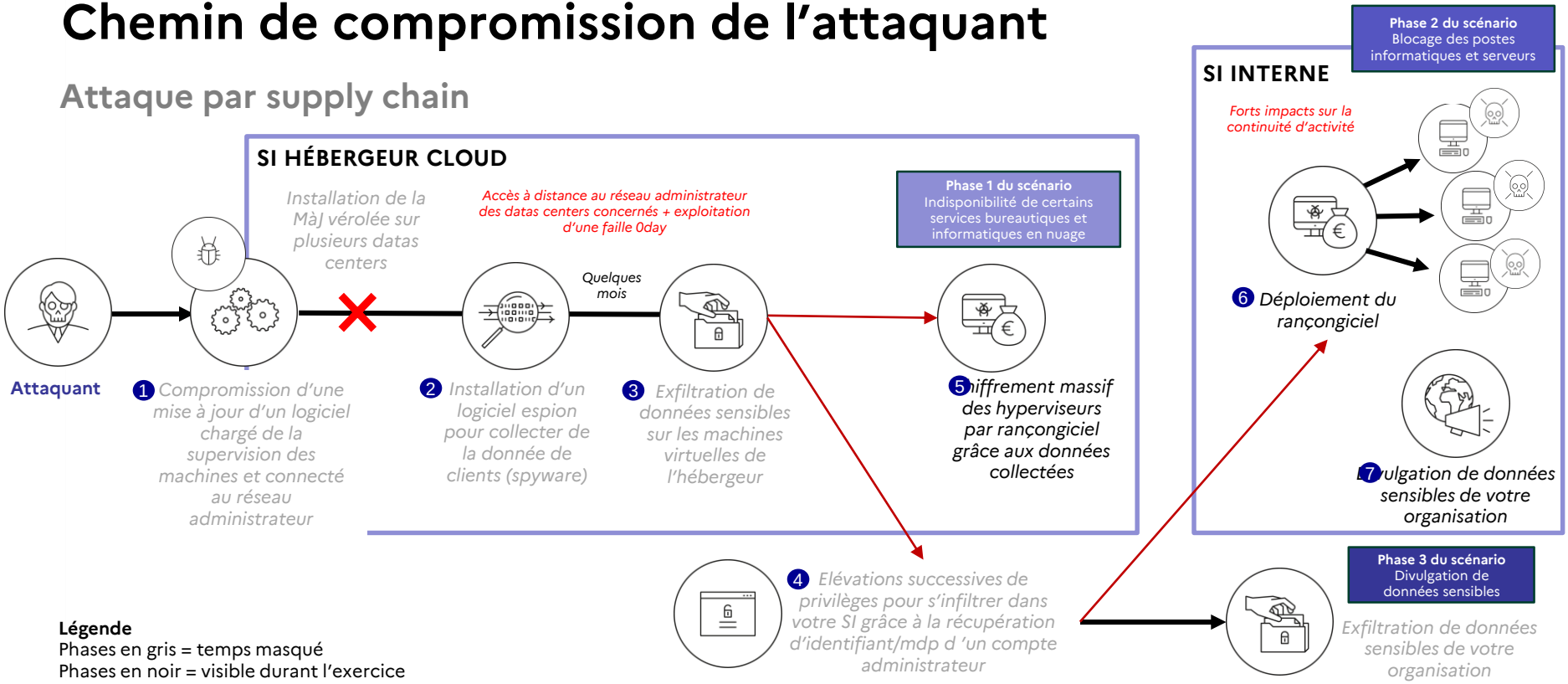
- Analyser les données et les conséquences de la fuite pour l'entité ;
- Notifier les autorités pertinentes et le public cible.

À adapter selon votre organisation

Type de données ayant fuitées, conséquences métiers, etc.

Chemin de compromission de l'attaquant

Attaque par supply chain



Légende
Phases en gris = temps masqué
Phases en noir = visible durant l'exercice