TRAVAUX PRATIQUES – FILIÈRE INFRASTRUCTURE DIGITALE

M209 – S’initier aux fondamentaux de la cybersécurité

45 heures

SOMMAIRE

S’initier aux fondamentaux de la cybersécurité

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

IDENTIFIER LA TERMINOLOGIE LIÉE À LA CYBERSÉCURITÉ

Dans ce module, vous allez :

- Réaliser des recherches sur les classes d'attaque
- Préparer une communication pour un incident de sécurité

12 heures

ACTIVITÉ 1

Réaliser une recherche sur les dernières attaques par rançongiciel

Compétences visées :

- Distinguer les classes d’attaques
- Se familiariser avec la recherche internet
- S’initier au threat hunting

Recommandations clés :

- Les compétences pratiquées dans cette activité sont de plus en plus demandées
- Les prérequis pour ce type d’activités sont aussi techniques que fonctionnels

5 heures

CONSIGNES

Pour le formateur :

- Il n'y pas qu'une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices
- Le corrigé est pour orienter l'apprenant à chercher plus et challenger les propositions
- Il est recommandé de consacrer un temps pour une présentation orale des résultats et des questions/réponses où l'objectif est de challenger les propositions

Pour l'apprenant :

- L'intérêt de chaque activité est le processus de recherche et d'analyse des résultats
- Durant la présentation des autres apprenants, il faut challenger leurs propositions et poser des questions pour clarifier la compréhension
- Le support de réponse est une présentation power point
- Utiliser des sites fiables et sécurisés

Conditions de réalisation :

- Une connexion internet
- Le guide théorique
- Un minimum de compréhension de l'anglais facilitera la recherche et donnera plus d'options

Critères de réussite :

- Définition claire de la cybersécurité
- Compréhension correcte des objectifs de la cybersécurité

Activité 1

Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Exercices

Dans cet exercice, vous êtes l'expert technique sécurité dans votre organisation. Dans le contexte du conflit entre la Russie et l'Ukraine, les médias parlent beaucoup des attaques subies ransomware (rançongiciel) par plusieurs entreprises. Votre management s'inquiète et souhaite avoir plus d'informations sur ces attaques et les cyberattaques en général. Votre manager vous demande de préparer une présentation en traitant les points suivants :

1. Enumérer les types de cyberattaques et les expliquer brièvement.
2. Définir les attaques par rançongiciel.
3. Documenter 3 attaques par rançongiciel connues (années, impacts, groupes, méthodes, vulnérabilités, etc.).
4. Présenter un scénario plausible d'attaque par rançongiciel en détaillant au maximum, pour chaque étape, les pratiques et les outils mis en œuvre.
5. Préparer 2 possibles contre-mesures de sécurité pouvant complexifier une attaque par rançongiciel.

PARTIE 1

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

1. Enumérer les types de cyberattaques.

Attaques DoS et DDoS

- Une attaque par déni de service (DoS) est conçue pour submerger les ressources d'un système au point où il est incapable de répondre aux demandes de service légitimes. Une attaque par déni de service distribué (DDoS) est similaire en ce sens qu'elle cherche également à drainer les ressources d'un système. Une attaque DDoS est initiée par un vaste éventail de machines hôtes infectées par des logiciels malveillants contrôlées par l'attaquant. Celles-ci sont appelées attaques de « déni de service » car le site victime est incapable de fournir un service à ceux qui souhaitent y accéder.
- Avec une attaque DoS, le site cible est inondé de requêtes illégitimes. Comme le site doit répondre à chaque requête, ses ressources sont consommées par toutes les réponses. Cela rend impossible pour le site de servir les utilisateurs comme il le fait normalement et entraîne souvent un arrêt complet du site.
- Les attaques DoS et DDoS sont différentes des autres types de cyberattaques qui permettent au pirate soit d'obtenir l'accès à un système, soit d'augmenter l'accès dont il dispose actuellement. Avec ces types d'attaques, l'attaquant bénéficie directement de ses efforts. Avec les attaques réseau DoS et DDoS, en revanche, l'objectif est simplement d'interrompre l'efficacité du service de la cible. Si l'agresseur est embauché par un concurrent commercial, il peut bénéficier financièrement de ses efforts.

PARTIE 1

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

Attaques de phishing

- Une attaque de phishing se produit lorsqu'un acteur malveillant envoie des e-mails qui semblent provenir de sources fiables et légitimes dans le but d'obtenir des informations sensibles de la cible. Les attaques de phishing combinent l'ingénierie sociale et la technologie et sont ainsi appelées parce que l'attaquant «pêche» en fait d'accéder à une zone interdite en utilisant «l'appât» d'un expéditeur apparemment digne de confiance.
- Pour exécuter l'attaque, l'acteur malveillant peut envoyer un lien qui vous amène à un site Web qui vous trompe ensuite en téléchargeant des logiciels malveillants tels que des virus ou en donnant à l'attaquant vos informations privées. Dans de nombreux cas, la cible peut ne pas se rendre compte qu'elle a été compromise, ce qui permet à l'attaquant de poursuivre d'autres personnes dans la même organisation sans que personne ne soupçonne une activité malveillante.

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

Logiciels de rançon

- Avec les rançongiciels, le système de la victime est retenu en otage jusqu'à ce qu'elle accepte de payer une rançon à l'attaquant. Une fois le paiement envoyé, l'attaquant fournit alors des instructions sur la façon dont la cible peut reprendre le contrôle de son ordinateur. Le nom "ransomware" est approprié car le malware demande une rançon à la victime.
- Lors d'une attaque par rançongiciel, la cible télécharge un rançongiciel, soit à partir d'un site Web, soit à partir d'une pièce jointe à un e-mail. Le logiciel malveillant est écrit pour exploiter des vulnérabilités qui n'ont pas été résolues par le fabricant du système ou l'équipe informatique. Le rançongiciel crypte ensuite le poste de travail de la cible. Parfois, les rançongiciels peuvent être utilisés pour attaquer plusieurs parties en refusant l'accès à plusieurs ordinateurs ou à un serveur central essentiel aux opérations commerciales.
- Affecter plusieurs ordinateurs est souvent accompli en n'initiant la captation des systèmes que des jours, voire des semaines après la pénétration initiale du logiciel malveillant. Le logiciel malveillant peut envoyer des fichiers AUTORUN qui vont d'un système à un autre via le réseau interne ou des lecteurs Universal Serial Bus (USB) qui se connectent à plusieurs ordinateurs. Ensuite, lorsque l'attaquant lance le cryptage, il fonctionne simultanément sur tous les systèmes infectés.

Les attaques par rançongiciel

Corrigé

Attaque par mot de passe

- Les mots de passe sont l'outil de vérification d'accès de choix pour la plupart des gens, donc déterminer le mot de passe d'une cible est une proposition attrayante pour un pirate informatique. Cela peut être fait en utilisant quelques méthodes différentes. Souvent, les gens conservent des copies de leurs mots de passe sur des morceaux de papier ou des notes autocollantes autour ou sur leur bureau. Un attaquant peut soit trouver le mot de passe lui-même, soit payer quelqu'un à l'intérieur pour l'obtenir pour lui.
- Un attaquant peut également tenter d'intercepter les transmissions réseau pour récupérer des mots de passe non chiffrés par le réseau. Ils peuvent également utiliser l'ingénierie sociale, qui convainc la cible de saisir son mot de passe pour résoudre un problème apparemment "important". Dans d'autres cas, l'attaquant peut simplement deviner le mot de passe de l'utilisateur, en particulier s'il utilise un mot de passe par défaut ou un mot de passe facile à retenir tel que "1234567".
- Les attaquants utilisent également souvent des méthodes de force brute pour deviner les mots de passe. Un piratage de mot de passe par force brute utilise des informations de base sur l'individu ou son titre de poste pour essayer de deviner son mot de passe. Par exemple, leur nom, date de naissance, anniversaire ou d'autres détails personnels mais faciles à découvrir peuvent être utilisés dans différentes combinaisons pour déchiffrer leur mot de passe. Les informations que les utilisateurs mettent sur les réseaux sociaux peuvent également être exploitées dans un piratage de mot de passe par force brute. Ce que l'individu fait pour le plaisir, les passe-temps spécifiques, les noms d'animaux de compagnie ou les noms d'enfants sont parfois utilisés pour former des mots de passe, ce qui les rend relativement faciles à deviner pour les attaquants par force brute.

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

Attaques Web

- Les attaques Web font référence aux menaces qui ciblent les vulnérabilités des applications Web. Chaque fois que vous entrez des informations dans une application Web, vous lancez une commande qui génère une réponse. Par exemple, si vous envoyez de l'argent à quelqu'un à l'aide d'une application bancaire en ligne, les données que vous saisissez indiquent à l'application d'accéder à votre compte, de retirer de l'argent et de l'envoyer sur le compte de quelqu'un d'autre. Les attaquants travaillent dans le cadre de ce type de requêtes et les utilisent à leur avantage.
- Certaines attaques Web courantes incluent l'injection SQL et les scripts intersites (XSS), qui seront abordés plus loin dans cet article. Les pirates utilisent également des attaques de falsification de requête intersite (CSRF) et la falsification de paramètres. Dans une attaque CSRF, la victime est amenée à effectuer une action qui profite à l'attaquant. Par exemple, ils peuvent cliquer sur quelque chose qui lance un script conçu pour modifier les identifiants de connexion pour accéder à une application Web. Le pirate, armé des nouveaux identifiants de connexion, peut alors se connecter comme s'il était l'utilisateur légitime.
- La falsification des paramètres consiste à ajuster les paramètres que les programmeurs implémentent en tant que mesures de sécurité conçues pour protéger des opérations spécifiques. L'exécution de l'opération dépend de ce qui est entré dans le paramètre. L'attaquant modifie simplement les paramètres, ce qui lui permet de contourner les mesures de sécurité qui dépendaient de ces paramètres.
- Pour éviter les attaques Web, inspectez vos applications Web pour rechercher et corriger les vulnérabilités. Une façon de corriger les vulnérabilités sans affecter les performances de l'application Web consiste à utiliser des jetons anti-CSRF. Un jeton est échangé entre le navigateur de l'utilisateur et l'application Web. Avant l'exécution d'une commande, la validité du jeton est vérifiée. S'il vérifie, la commande passe - sinon, elle est bloquée. Vous pouvez également utiliser les drapeaux SameSite, qui autorisent uniquement le traitement des demandes provenant du même site, rendant tout site construit par l'attaquant impuissant.

Les attaques par rançongiciel

Corrigé

Menaces internes

- Parfois, les acteurs les plus dangereux viennent de l'intérieur d'une organisation. Les personnes se trouvant à l'intérieur d'une entreprise représentent un danger particulier car elles ont généralement accès à une variété de systèmes et, dans certains cas, à des privilèges d'administrateur qui leur permettent d'apporter des modifications critiques au système ou à ses politiques de sécurité.
- De plus, les personnes au sein de l'organisation ont souvent une compréhension approfondie de son architecture de cybersécurité, ainsi que de la façon dont l'entreprise réagit aux menaces. Ces connaissances peuvent être utilisées pour accéder à des zones restreintes, modifier les paramètres de sécurité ou déduire le meilleur moment possible pour mener une attaque.
- L'un des meilleurs moyens de prévenir les menaces internes dans les organisations consiste à limiter l'accès des employés aux systèmes sensibles à ceux qui en ont besoin pour accomplir leurs tâches. De plus, pour les quelques privilégiés qui ont besoin d'un accès, utilisez MFA, ce qui les obligera à utiliser au moins une chose qu'ils connaissent en conjonction avec un élément physique dont ils disposent pour accéder à un système sensible. Par exemple, l'utilisateur peut avoir à entrer un mot de passe et insérer un périphérique USB. Dans d'autres configurations, un numéro d'accès est généré sur un appareil portable auquel l'utilisateur doit se connecter. L'utilisateur ne peut accéder à la zone sécurisée que si le mot de passe et le numéro sont corrects.
- Bien que la MFA n'empêche pas toutes les attaques à elle seule, elle permet de déterminer plus facilement qui est à l'origine d'une attaque - ou d'une tentative - en particulier parce que relativement peu de personnes ont accès aux zones sensibles en premier lieu. Par conséquent, cette stratégie d'accès limité peut avoir un effet dissuasif. Les cybercriminels au sein de votre organisation sauront qu'il est facile d'identifier l'auteur en raison du nombre relativement restreint de suspects potentiels.

Les attaques par rançongiciel

Corrigé

Menaces internes

- Parfois, les acteurs les plus dangereux viennent de l'intérieur d'une organisation. Les personnes se trouvant à l'intérieur d'une entreprise représentent un danger particulier car elles ont généralement accès à une variété de systèmes et, dans certains cas, à des privilèges d'administrateur qui leur permettent d'apporter des modifications critiques au système ou à ses politiques de sécurité.
- De plus, les personnes au sein de l'organisation ont souvent une compréhension approfondie de son architecture de cybersécurité, ainsi que de la façon dont l'entreprise réagit aux menaces. Ces connaissances peuvent être utilisées pour accéder à des zones restreintes, modifier les paramètres de sécurité ou déduire le meilleur moment possible pour mener une attaque.
- L'un des meilleurs moyens de prévenir les menaces internes dans les organisations consiste à limiter l'accès des employés aux systèmes sensibles à ceux qui en ont besoin pour accomplir leurs tâches. De plus, pour les quelques privilégiés qui ont besoin d'un accès, utilisez MFA, ce qui les obligera à utiliser au moins une chose qu'ils connaissent en conjonction avec un élément physique dont ils disposent pour accéder à un système sensible. Par exemple, l'utilisateur peut avoir à entrer un mot de passe et insérer un périphérique USB. Dans d'autres configurations, un numéro d'accès est généré sur un appareil portable auquel l'utilisateur doit se connecter. L'utilisateur ne peut accéder à la zone sécurisée que si le mot de passe et le numéro sont corrects.
- Bien que la MFA n'empêche pas toutes les attaques à elle seule, elle permet de déterminer plus facilement qui est à l'origine d'une attaque - ou d'une tentative - en particulier parce que relativement peu de personnes ont accès aux zones sensibles en premier lieu. Par conséquent, cette stratégie d'accès limité peut avoir un effet dissuasif. Les cybercriminels au sein de votre organisation sauront qu'il est facile d'identifier l'auteur en raison du nombre relativement restreint de suspects potentiels.

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

Attaque de logiciels malveillants (Malware)

- Le malware est un terme général pour les logiciels malveillants, d'où le "mal" au début du mot. Les logiciels malveillants infectent un ordinateur et modifient son fonctionnement, détruisent des données ou espionnent l'utilisateur ou le trafic réseau lors de son passage. Les logiciels malveillants peuvent soit se propager d'un appareil à un autre, soit rester en place, n'affectant que son appareil hôte.
- Plusieurs des méthodes d'attaque décrites ci-dessus peuvent impliquer des formes de logiciels malveillants, notamment les attaques MITM, le phishing, les ransomwares, l'injection SQL, les chevaux de Troie, les attaques au volant et les attaques XSS.
- Lors d'une attaque de logiciel malveillant, le logiciel doit être installé sur l'appareil cible. Cela nécessite une action de la part de l'utilisateur. Par conséquent, en plus d'utiliser des pare-feu capables de détecter les logiciels malveillants, les utilisateurs doivent être informés des types de logiciels à éviter, des types de liens qu'ils doivent vérifier avant de cliquer, ainsi que des e-mails et des pièces jointes avec lesquels ils ne doivent pas interagir.

Activité 1

Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

2. Définir les attaques par rançongiciel.

- Les rançongiciels sont une classe spécialisée de logiciels malveillants : les logiciels de rançon sont utilisés pour infecter autant de systèmes que possible, cryptant les données sur les appareils et les retenant contre une rançon. Si les victimes paient les attaquants dans un délai défini (généralement via une crypto-monnaie comme le Bitcoin), les données sont théoriquement restituées.
- Les rançongiciels se propagent généralement en exploitant les vulnérabilités connues des logiciels couramment installés (par exemple, le système d'exploitation Microsoft Windows). Il peut se propager extrêmement rapidement une fois qu'une infection commence et peut exiger des millions de dollars en rançon. Le but d'une attaque par rançongiciel est d'infecter autant de systèmes que possible, puis de rendre le plus de données inaccessibles possible en les cryptant avec une clé connue uniquement de l'attaquant. Une fois l'attaque terminée, le malware affiche généralement une fenêtre qui ressemble à ceci :

PARTIE 1

Activité 1

Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

- L’image dans la slide précédente est la fenêtre qui donne aux victimes le délai et les instructions sur la façon de payer, ainsi qu'un aperçu de ce qui est exactement arrivé à leurs données. L'exemple provient du célèbre rançongiciel **Wannacry** (https://fr.wikipedia.org/wiki/WannaCry).
- Avec la rançon payée, le logiciel malveillant peut ou non décrypter les données et s'autodétruire, en fonction entièrement du bon vouloir des attaquants.

PARTIE 1

Activité 1

Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

3. Documenter 3 attaques par rançongiciel connues (années, impacts, groupes, méthodes, vulnérabilités, etc.)

- Nous pouvons citer : Wannacry, Petya, lockbit

Wannacry

- WannaCry est un exemple de crypto ransomware, un type de logiciel malveillant (malware) utilisé par les cybercriminels pour extorquer de l'argent. Pour ce faire, les ransomwares cryptent des fichiers précieux, de sorte que vous ne pouvez pas les lire, ou en vous bloquant l'accès à votre ordinateur, de sorte que vous ne pouvez pas les utiliser.
- Les rançongiciels qui utilisent le cryptage sont appelés crypto ransomwares. Le type qui vous empêche d'accéder à votre ordinateur est appelé rançongiciel de casier.
- Comme d'autres types de crypto-ransomwares, WannaCry prend vos données en otage, promettant de les restituer si vous payez une rançon. WannaCry cible les ordinateurs utilisant Microsoft Windows comme système d'exploitation. Il crypte les données et exige le paiement d'une rançon dans la crypto-monnaie Bitcoin pour son retour.
- L'attaque du rançongiciel WannaCry était une épidémie mondiale qui a eu lieu en mai 2017. Cette attaque de rançongiciel s'est propagée sur des ordinateurs exécutant Microsoft Windows. Les fichiers de l'utilisateur ont été retenus en otage et une rançon Bitcoin a été exigée pour leur retour.

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

Le fonctionnement de **WannaCry** ?

- Les cybercriminels responsables de l'attaque ont profité d'une faiblesse du système d'exploitation Microsoft Windows en utilisant un hack qui aurait été développé par la National Security Agency des États-Unis. Connu sous le nom d'**EternalBlue** (discuté dans la compétence suivante), ce hack a été rendu public par un groupe de hackers appelé les Shadow Brokers avant l'attaque **WannaCry**.
- Microsoft a publié un correctif de sécurité qui protégeait les systèmes des utilisateurs contre cet exploit près de deux mois avant le début de l'attaque du rançongiciel **WannaCry**. Malheureusement, de nombreuses personnes et organisations ne mettent pas régulièrement à jour leurs systèmes d'exploitation et ont donc été exposées à l'attaque.
- Ceux qui n'avaient pas exécuté de mise à jour Microsoft Windows avant l'attaque n'ont pas bénéficié du correctif et la vulnérabilité exploitée par **EternalBlue** les a laissés ouverts aux attaques.
- Lorsque cela s'est produit pour la première fois, les gens ont supposé que l'attaque du rançongiciel **WannaCry** s'était initialement propagée par le biais d'une campagne de phishing (une campagne de phishing est l'endroit où des spams contenant des liens ou des pièces jointes infectés incitent les utilisateurs à télécharger des logiciels malveillants). Cependant, **EternalBlue** était l'exploit qui a permis à **WannaCry** de se propager et de se propager, **DoublePulsar** étant la "porte dérobée" installée sur les ordinateurs compromis (utilisés pour exécuter **WannaCry**).

PARTIE 1

Activité 1

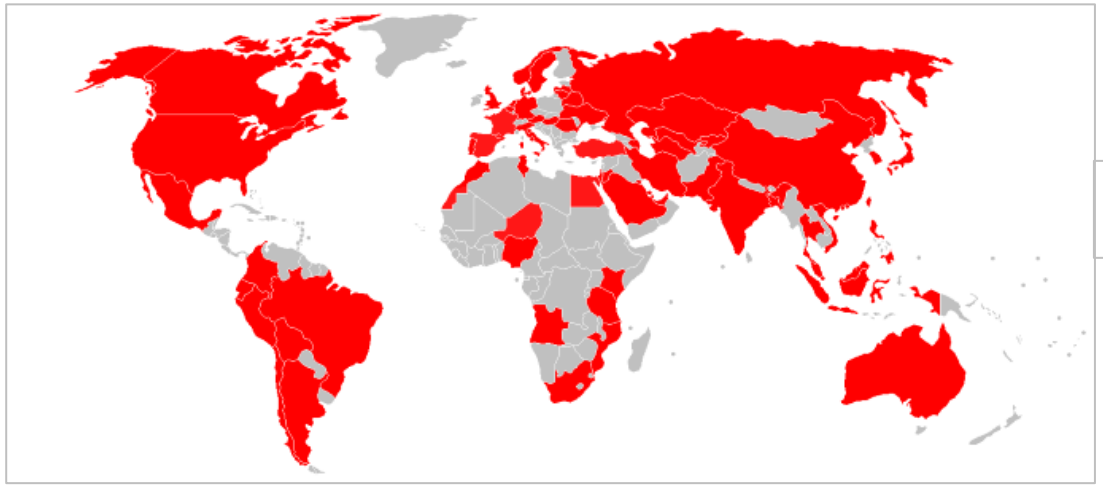
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

L'impact de l'attaque **WannaCry**

- L'attaque du rançongiciel **WannaCry** a touché environ 230 000 ordinateurs dans le monde. L'une des premières entreprises touchée a été la société espagnole de téléphonie mobile **Telefónica**. Le 12 mai, des milliers d'hôpitaux et de cabinets médicaux du NHS à travers le Royaume-Uni étaient touchés.
- Un tiers des fiducies hospitalières du NHS ont été touchées par l'attaque. De manière terrifiante, des ambulances auraient été détournées, laissant les personnes nécessitant des soins urgents dans le besoin. On a estimé que cela coûterait au NHS 92 millions de livres sterling après l'annulation de 19 000 rendez-vous à la suite de l'attaque.
- Alors que le rançongiciel se répandait au-delà de l'Europe, les systèmes informatiques de 150 pays étaient paralysés. L'attaque du rançongiciel **WannaCry** a eu un impact financier substantiel dans le monde entier. On estime que ce cybercrime a causé 4 milliards de dollars de pertes dans le monde.



Régions initialement affectées par l'attaque ***WannaCry*** entre samedi 13 et dimanche 14 mai 2017

PARTIE 1

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Petya et PetyaWrap

- Comme WannaCry, PetyaWrap est un ver informatique, ce qui signifie qu'il peut se propager tout seul. PetyaWrap peut se copier sur votre réseau, puis lancer automatiquement ses nouvelles copies sans attendre que les utilisateurs ne lisent les e-mails, ouvrent les pièces jointes ou téléchargent les fichiers via des liens Web.
- PetyaWrap chiffre vos fichiers de manière à ce que seuls les attaquants connaissent la clé de déchiffrement, vous ne pouvez donc pas déchiffrer les fichiers sans leur aide. Avoir diffusé et brouillé vos données, PetyaWrap fait la même chose que le malware Petya d'origine - il brouille votre disque au niveau du secteur, de sorte que vous ne puissiez pas du tout accéder à votre lecteur C:, même si vous branchez le disque sur un autre ordinateur.

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

Le fonctionnement **PetyaWrap**

- Tout d'abord, il copie **WannaCry** en essayant d'exploiter une paire de failles de sécurité Windows critiques qui ont été volées à l'Agence américaine de sécurité nationale (**NSA**) et divulguées par une équipe de piratage appelée Shadow Brokers. (La principale vulnérabilité utilisée est communément connue sous son nom **NSA** d'origine : **ETERNALBLUE**.) Si le système est patché contre **WannaCry** - Microsoft a publié des correctifs qui ont empêché l'attaque bien avant la sortie de **WannaCry** - alors le système est patché contre cette partie de **PetyaWrap**.
- Deuxièmement, il essaie de se propager à l'aide d'un outil d'exécution à distance Windows populaire appelé **PsExec** - **PetyaWrap** a une copie du logiciel **PsExec** intégrée à l'intérieur, il n'a donc pas besoin de le télécharger en premier. **PsExec** fait partie de la propre suite **Sysinternals** de Microsoft, couramment utilisée à mauvais escient par les cybercriminels comme un moyen pratique de se déplacer à l'intérieur d'un réseau après qu'ils soient entrés de l'extérieur.
- Troisièmement, **PetyaWrap** cherche dans la mémoire des mots de passe qui renforceront ses privilèges d'accès et lui donneront un accès administratif à d'autres ordinateurs du réseau. Cette recherche de mot de passe est effectuée à l'aide d'une copie modifiée d'un outil de saisie de mot de passe appelé **LSADUMP** de la boîte à outils **Mimikatz** - comme avec **PsExec**, cet outil de piratage est intégré au programme **PetyaWrap**, il n'a donc pas besoin d'être téléchargé en premier.

PARTIE 1

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

L'impact de l'attaque **PetyaWrap**

- Certaines des plus grandes multinationales du monde ont été durement touchées par **Petya** ou **PetyaWrap**.
- Le total des dommages causés par la famille **Petya** est estimé à plus de 10 milliards de dollars.
- Lors de l'attaque lancée le 27 juin 2017, le système de surveillance des rayonnements de la centrale nucléaire ukrainienne de Tchernobyl s'est déconnecté. Plusieurs ministères, banques et systèmes de métro ukrainiens ont également été touchés. On dit qu'il s'agit de la cyberattaque la plus destructrice de tous les temps.

- Parmi les sociétés victimes de cette attaque, nous pouvons retrouver la société pharmaceutique américaine **Merck & Co**., la compagnie pétrolière russe **Rosneft** (sa production de pétrole n'a pas été affectée), le cabinet d'avocats multinational **DLA Piper**, l'entreprise de construction française **Saint-Gobain** et ses points de vente au détail et ses filiales en Estonie, etc.
- L'interruption des activités de **Maersk**, le plus grand opérateur mondial de porte-conteneurs et de navires de ravitaillement, aurait généré entre 200 et 300 millions de dollars de perte de revenus. L'impact commercial sur **FedEx** est estimé à 400 millions de dollars en 2018, selon le rapport annuel 2019 de la société.

PARTIE 1

Activité 1

Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

LockBit (source https://www.kaspersky.fr/resource-center/threats/lockbit-ransomware)

- Le rançongiciel LockBit est un logiciel malveillant conçu pour bloquer l'accès des utilisateurs aux systèmes informatiques en échange du paiement d'une rançon. **LockBit** recherchera automatiquement des cibles précieuses, propagera l'infection et chiffrera tous les systèmes informatiques accessibles sur un réseau. Ce rançongiciel est utilisé pour des attaques très ciblées contre des entreprises et d'autres organisations. En tant que cyberattaque autopilotée, les attaquants de **LockBit** ont fait leur marque en menaçant les organisations du monde entier avec certaines des menaces suivantes :
  - ✓ Interruption des opérations avec des fonctions essentielles s'arrêtant soudainement.
  - ✓ Extorsion pour le gain financier du pirate.
  - ✓ Vol de données et publication illégale comme chantage si la victime ne se conforme pas.

PARTIE 1

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

Le fonctionnement **LockBit**

- Le rançongiciel **LockBit** est considéré par de nombreuses autorités comme faisant partie de la famille des logiciels malveillants « **LockerGoga & MegaCortex** ». Cela signifie simplement qu'il partage des comportements avec ces formes établies de rançongiciels ciblés. Les caractéristiques de ces attaques sont :
  - ✓ Auto-diffusion au sein d'une organisation plutôt que d'exiger une direction manuelle.
  - ✓ Ciblage plutôt que propagation de manière éparse comme les logiciels malveillants de spam.
  - ✓ Utilisation d'outils similaires pour se propager, comme **Windows Powershell** et **Server Message Block** (**SMB**).

- Le plus important est sa capacité à s'auto-propager, ce qui signifie qu'il se propage tout seul. Dans sa programmation, **LockBit** est dirigé par des processus automatisés préconçus. Cela le rend unique par rapport à de nombreuses autres attaques de rançongiciels qui sont motivées par la vie manuelle dans le réseau - parfois pendant des semaines - pour compléter la reconnaissance et la surveillance.
- Une fois que l'attaquant a infecté manuellement un seul hôte, il peut trouver d'autres hôtes accessibles, les connecter aux hôtes infectés et partager l'infection à l'aide d'un script. Ceci est complété et répété entièrement sans intervention humaine.
- De plus, il utilise des outils dans des modèles natifs de presque tous les systèmes informatiques Windows. Les systèmes de sécurité des terminaux ont du mal à signaler les activités malveillantes. Il cache également le fichier de cryptage exécutable en le déguisant en format de fichier image .PNG commun, trompant davantage les défenses du système.

PARTIE 1

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

- Étapes des attaques LockBit. Les attaques LockBit peuvent être appréhendées en trois étapes environ :

  - ✓ **Exploiter** des faiblesses d'un réseau. La violation initiale ressemble beaucoup à d'autres attaques malveillantes. Une organisation peut être exploitée par des tactiques d'ingénierie sociale telles que le phishing, dans lesquelles les attaquants se font passer pour un personnel ou des autorités de confiance pour demander des informations d'identification d'accès. L'utilisation d'attaques par force brute sur les serveurs intranet et les systèmes réseau d'une organisation est tout aussi viable. Sans une configuration réseau appropriée, les sondes d'attaque peuvent ne prendre que quelques jours.
  - ✓ **Infiltrer** plus profond pour terminer la configuration de l'attaque si nécessaire. À partir de ce moment, le programme LockBit dirige toutes les activités de manière indépendante. Il est programmé pour utiliser ce que l'on appelle des outils de « post-exploitation » pour obtenir des privilèges d'escalade afin d'atteindre un niveau d'accès prêt pour les attaques. Il s'enracine également dans l'accès déjà disponible via le mouvement latéral pour vérifier la viabilité de la cible.
  - ✓ **Déployer** la charge utile de chiffrement. Une fois que le réseau a été préparé pour que LockBit soit entièrement mobilisé, le ransomware commencera sa propagation sur toute machine qu'il peut toucher. Comme indiqué précédemment, LockBit n'a pas besoin de beaucoup pour terminer cette étape. Une seule unité système avec un accès élevé peut envoyer des commandes à d'autres unités du réseau pour télécharger LockBit et l'exécuter.

PARTIE 1

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

4. Présenter un scénario plausible d'attaque par rançongiciel détaillant au maximum, pour chaque étape, les pratiques et les outils mis en œuvre.

Dans cette question, nous allons donner les étapes pour une attaque ayant pour objectif le déploiement d'un ransomware sur l'infrastructure AWS de Swile. Une étape clé de notre mouvement latéral passe par la compromission du service d'identité d'entreprise (Azure Active Directory).

- Confirmer l'utilisation de Azure AD : https://login.microsoftonline.com/getuserrealm.srf?login=username@swile.onmicrosoft.com&xml=1
- Préparer une liste d'e-mails Microsoft de l'entreprise (Hunter.io, Spiderfoot …)
- Valider les e-mails (o365creeper)
- Préparer une liste de mots de passe communs et lancer un password spraying (MailSniper)
- Hypothèse : un mot de passe trouvé
- Se connecter et commencer une reconnaissance authentifiée (O365recon)
- Hypothèse : confirmer l'existence de la synchro avec l'AD on premise
- Hypothèse : l'utilisateur Alice trouvée a un rôle d'administrateur d'application

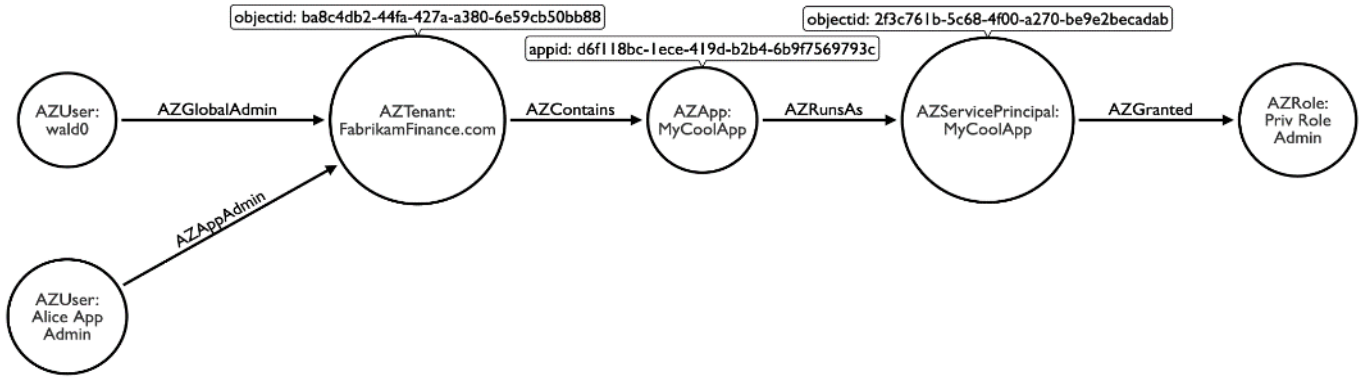
PARTIE 1

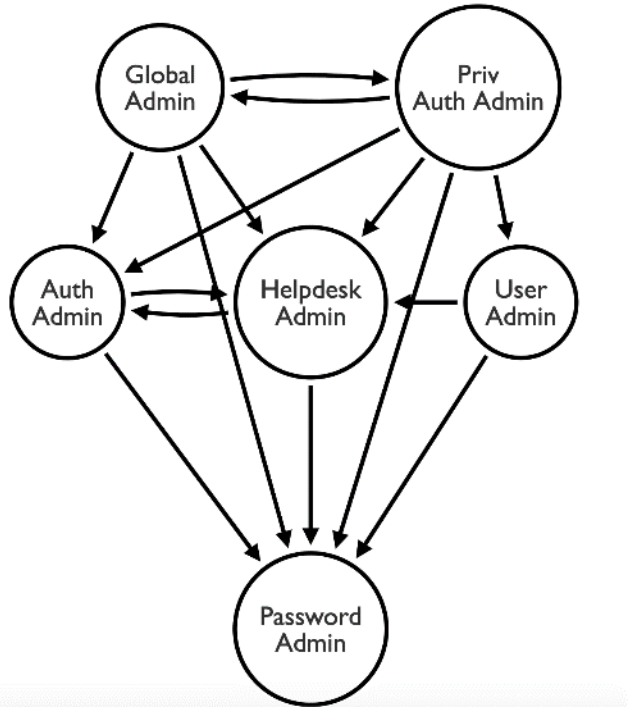
Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

- Elévation des droits à travers l'abus du service principal (Hypothèse) : au moins un service principal a un rôle de privilege authentication admin





- Alice App Admin a le rôle d'administrateur d'application, limité au tenant.
- Le tenant contient l'application MyCoolApp, accordant à Alice App Admin le contrôle de l'application.
- Alice App Admin peut ajouter un nouveau secret pour le service principal service de cette application.
- MyCoolApp s'authentifie auprès du tenant en tant que service principal MyCoolApp.
- Le service principal MyCoolApp a le rôle PRA.
- Alice App Admin peut s'authentifier auprès du tenant en tant que principal de service MyCoolApp et utiliser les droits de ce service principal en tant que PRA pour se promouvoir elle-même ou un autre utilisateur en tant qu'administrateur global.

PARTIE 1

Activité 1
Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

- Déterminer les machines à jointure hybride (hybrid-joined)
  - ✓ Se connecter sur Azure, cliquez sur « Azure Active Directory »
  - ✓ Cela nous amène à la page overview. Dans la navigation de gauche, cliquez sur « devices »
  - ✓ Nous aurons toutes les machines jointes au tenant, ce qui nous intéresse, sont les machines avec la jointure « Hybrid Azure AD joined »
- Utiliser **Microsoft Endpoint Manager** pour exécuter un script powershell sur une machine à jointure hybride.
  - ✓ Ne pas oublier les techniques de AMSI-bypass et AV-bypass
  - ✓ Se connecter sur Azure avec les rôles “Global Admin” or “Intune Administrator” actifs
  - ✓ Accéder au Microsoft Endpoint Manager : https://endpoint.microsoft.com
  - ✓ Dans la navigation de gauche, cliquez sur « devices » > Policy > Scripts
  - ✓ Cliquer sur « Add » et choisir Windows 10 et suivant
  - ✓ Nommer le script et remplir une description
  - ✓ Importer le script que l’on va utiliser, dans notre un powershell reverse shell
  - ✓ Garder toutes les options à « non » permettra d’exécuter le script en tant que SYSTEM
  - ✓ Option : choisir comme cible “All devices” et “All users” > next > next > Add
  - ✓ Lancer un nc en écoute sur le port 4444 (voir le scipt)
  - ✓ Intune Agent Check et exécute les scripts chaque heure …. Attendre de recevoir le shell

PARTIE 1

Activité 1

Réaliser une veille sur les dernières attaques par rançongiciel

Les attaques par rançongiciel

Corrigé

- Hypothèse : shell reçu de la part de la machine de Thiebaud avec un accès SYSTEM
- Hypothèse : Thiebaud utilise un access key id et un secret access key AWS
- Créer une clé KMS avec son propre compte AWS « personnel » (ou un autre compte compromis) et l'expose en public pour utiliser cette clé KMS pour le chiffrement. Cela signifie qu'il peut être utilisé par n'importe quel utilisateur/rôle/compte AWS pour chiffrer, mais pas pour déchiffrer des objets dans S3.
- Identifier les buckets S3 cibles accessibles par Thiebaud en écriture.
- Vérifier la configuration des buckets S3 pour déterminer s'il peut être ciblé par un ransomware. 2 conditions :
  - ✓S3 Object Versioning désactivé → Ransomware OK
  - ✓S3 Object Versioning activé & MFA delete désactivé → Ransomware OK
  - ✓S3 Object Versioning activé & MFA delete activé → Ransomware KO (difficile)
- Utiliser l'API AWS pour remplacer les objets des buckets S3 par leurs copies chiffrées avec la clé KMS de l'attaquant

PARTIE 1

Les attaques par rançongiciel

Corrigé

5. Préparer 2 possibles contre-mesures de sécurité pouvant complexifier une attaque par rançongiciel

   - ✓ Activer l'authentification multifacteur : l'authentification multifacteur (MFA) rend plus difficile pour les cybercriminels l'accès initial à votre appareil, votre compte et vos informations en les obligeant à franchir davantage d'obstacles de sécurité et des couches d'authentification supplémentaires. Cela signifie que le cybercriminel devra consacrer plus de temps, d'efforts et de ressources pour accéder à votre appareil avant que toute attaque de ransomware ne puisse commencer. MFA nécessite généralement une combinaison de deux ou plusieurs des types d'authentification avant d'accorder l'accès à un compte. Donner la priorité à l'activation de MFA sur les services critiques tels que la messagerie électronique ou l'accès à distance.
   - ✓ Mettre à jour régulièrement les systèmes, configurer et effectuer des sauvegardes régulières : les cybercriminels utilisent des faiblesses connues pour pirater vos appareils. Les mises à jour ont des mises à niveau de sécurité afin que les faiblesses connues ne puissent pas être utilisées pour vous pirater. Vous devez toujours mettre à jour votre système et vos applications lorsque vous y êtes invité. Vous pouvez également activer les mises à jour automatiques sur certains appareils et applications afin que les mises à jour se produisent sans votre intervention.

     Une sauvegarde est une copie numérique de vos informations les plus importantes qui est enregistrée sur un périphérique de stockage externe ou sur le cloud. La meilleure méthode de récupération après une attaque de ransomware consiste à restaurer à partir d'une sauvegarde non affectée. Sauvegardez régulièrement vos fichiers sur un périphérique de stockage externe ou sur le cloud.

Activité 2

Préparer une analyse à communiquer concernant une attaque

Compétences visées :

- Analyser une grande quantité d'informations techniques et les résumer
- Communiquer sur un sujet nouveau, technique et urgent

Recommandations clés :

- Avoir une compréhension pointue des éléments communiqués

7 heures

CONSIGNES

Pour le formateur :

- Il n’y pas qu’une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices
- Le corrigé est pour orienter l’apprenant à chercher plus et challenger les propositions
- Il est recommandé de consacrer un temps pour une présentation orale des résultats

Pour l’apprenant :

- L’intérêt de chaque activité est le processus de recherche et d’analyse des résultats
- Le support de réponse
- Utiliser des sites fiables et sécurisés

Conditions de réalisation :

- Une connexion internet
- Le guide théorique
- Un minimum de compréhension de l’anglais facilitera la recherche et donnera plus d’options

Critères de réussite :

- Définition claire de la cybersécurité
- Compréhension correcte des objectifs de la cybersécurité

Activité 2

Préparer une analyse à communiquer concernant une attaque

Communiquer sur Lockbit 3.0

Exercice

- Vous êtes un analyste SOC niveau 2 dans une entreprise avec plusieurs filiales et partenaires. Vous avez reçu de la part de votre manager la demande suivante à laquelle vous allez répondre dans cette activité :

« Bonjour,

Nous venons d'être informés qu'une attaque par rançongiciel est en cours chez l'un de notre partenaire.

Le rançongiciel utilisé est Lockbit 3.0

Merci de préparer une communication à envoyer à tous les collaborateurs de l'entreprise qui inclut :

- ✓ *Présentation de Lockbit, ses versions, son historique et ses spécificités*
- ✓ *La méthode d'attaque par rançongiciel et par Lockbit en particulier*
- ✓ *L'impact de ce type d'attaque (financier, image, technique, etc.)*
- ✓ *Les méthodes de propagation*
- ✓ *Les gestes et les recommandations à appliquer en urgence*

Cordialement,

Manager SOC »

PARTIE 1

Communiquer sur Lockbit 3.0

Corrigé

Notre partenaire XX victime du ransomeware Lockbit

- Contexte et résumé de la vulnérabilité ou de la menace

Le SOC a un rôle de veille et d'alerteur sur les nouvelles vulnérabilités publiées et qui sont susceptibles d'affecter les systèmes du Groupe et ses filiales.

Le présent document est une alerte de sécurité faisant état d'une cyberattaque dont XX a été victime lundi dernier (05/09/2022), et dresse les mesures à mettre en œuvre et donne les moyens à notre entreprise de s'en prémunir.

Découvert pour la première fois en 2019, LockBit est une famille relativement nouvelle de ransomwares qui exploite rapidement les protocoles et outils couramment disponibles tels que SMB et PowerShell. Il était à l'origine connu sous le nom de « ABCD » en raison de l'extension de nom de fichier des fichiers cryptés, avant de commencer à utiliser l'extension .lockbit actuelle.

Depuis ses débuts, il est devenu l'une des souches de logiciels malveillants les plus calamiteuses à ce jour, demandant une rançon moyenne d'environ 40 000 $ par organisation. LockBit, cependant, ne nécessite la présence d'un humain que pendant un certain nombre d'heures, après quoi il se propage à travers un système et infecte d'autres hôtes par lui-même, sans avoir besoin de surveillance humaine. De manière cruciale, le malware effectue une reconnaissance et continue de se propager pendant la phase de cryptage. Cela lui permet de causer un maximum de dommages plus rapidement que les autres approches manuelles. Lockbit est à ce jour très difficile à détecter par l'antivirus classique car contrairement à d'autres familles de rançongiciels, il ne chiffre pas d'un coup l'ensemble d'un fichier mais juste l'entête. Ceci lui permet d'avoir un comportement humain habituel et classique vu d'un antivirus ou un EDR.

A ce jour, les détails de l'attaque dont XX fait l'objet sont en cours d'évaluation mais l'impact semble important.

Communiquer sur Lockbit 3.0

Corrigé

Cette attaque concerne le système de gestion administrative qui gère notamment la partie business (vente et souscription de forfaits téléphoniques) et la facturation.

Elle n'empêche pas les clients d'utiliser normalement leur téléphone et leur abonnement.

L'Active Directory de 1000 utilisateurs a été compromis, ainsi que de nombreux serveurs. Cette attaque ne concerne pas le Groupe ni d'autres filiales du Groupe.

- Actions

Des mesures de coupure et d'isolation des systèmes informatiques ont été prises au sein de l'entreprise, avec ses partenaires et le reste du Groupe. Une mission d'expertise de réponse à l'incident est en cours pour assainir le système informatique infecté et restaurer les services de XX. Une prestation a été signée en ce sens avec la société Intrinsec qui se coordonne avec les équipes de cyberdéfense internes au Groupe.

- Risque(s)
  - ✓ Usurpation de comptes
  - ✓ Chiffrement des répertoires sur l'ensemble du parc
- Service(s) / Système(s) / Application(s) impacté(es)

Tous les systèmes

Communiquer sur Lockbit 3.0

Corrigé

- Solutions / Mesure(s) de Contournement

Le SOC dresse des mesures à mettre en œuvre rapidement afin de prévenir la propagation de ce rançongiciel chez le Groupe à travers les interconnexions réseaux existantes :

✓ Identifier toute interaction réseau (VPN, express routes, exchange, etc.) entre le Groupe et XX

✓ Suspendre l'ensemble des interactions réseaux initiées depuis XX vers le Groupe

✓ Bloquer l'ensemble des iOC qui seront transmis par XX dans les prochaines heures

✓ Maintenir une vigilance accrue dans l'ouverture des emails en cette période

✓ Remonter au csirt@leGroupe.fr toute activité suspecte identifiée

✓ En cas de réception d'email douteux, continuer à suivre la fiche réflexe ; mettez l'email en pièce jointe et envoyez-le à phishing@leGroupe.fr pour analyse.

Communiquer sur Lockbit 3.0

Corrigé

- XX vient de nous communiquer les IOCs découverts lors des investigations numériques

Nom	Chemin Complet	Taille (Bytes)	SHA1	Commentaire
LockBit.exe	C:\Windows\LockBit.exe	982528	B7CA6F047A461DB06E1E020A1C5178633B006A2F	Binaire de chiffrement
Lock-Bit_AC94A81B89A9962C.exe	C:\Windows\Lock-Bit_AC94A81B89A9962C.exe	982528	B7CA6F047A461DB06E1E020A1C5178633B006A2F	Binaire de chiffrement
LockBit_Ransomware.hta	C:\Users\USER\Desktop\Lock-Bit_Ransomware.hta	47369	BFE6533F4AFE3255046F7178F289A4C75AD89E76	Note de rançon
go.bat	C:\Users\USER\Desktop\go.bat	27051	9883f1c37a0f74acadbbfd411851defb4995f239	Script de déploiement du ransomware
Restore-My-Files.txt	Dans les dossiers chiffrés	512	fb5759fc9d5559482d1f1e2f7dd300e49aa8d179	Note de rançon

Protocole	URI	Commentaire
HTTP	http[://]193.201.9[.]107/aster	URL Cobalt Strike

PARTIE 1

Communiquer sur Lockbit 3.0

Corrigé

Nom	Commentaire	AS	Localisation
193.201.9[.]107	C2 Cobalt Strike	AS 49505 (OOO Network of data-centers Selectel)	RU

Ci-dessous la liste des services Windows créés par les adversaires découverts pendant les investigations :

Nom	Commande	Contexte (Compte)
PSEXESVC	PSEXESVC	USER

Ci-dessous la liste des clés registres modifiées par les adversaires découvertes pendant les investigations :

Clé	Valeur	Data	Commentaire
\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	N/A	c:\users\[USER]\desktop\lockbit_ransomware.hta	Persistance permettant d'afficher la note de rançon au démarrage de l'équipement.

Activité 2

Préparer une analyse à communiquer concernant une attaque

Communiquer sur Lockbit 3.0

Corrigé

- Documentation et informations techniques :

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-moves-quietly-on-the-network-strikes-fast/

https://www.kaspersky.com/resource-center/threats/lockbit-ransomware.

https://www.ic3.gov/Media/News/2022/220204.pdf

https://www.ic3.gov/Media/News/2022/220204.pdf

PARTIE 1

PARTIE 2

DÉCOUVRIR LES DIFFÉRENTES NORMES ET STANDARDS DE LA CYBERSÉCURITÉ

Dans ce module, vous allez :

- Étudier l’analyse des risques à travers le cas du cloud
- S’initier au domaine du cloud et de ses solutions et challenges

10 heures

ACTIVITÉ 1

Réaliser un benchmark des solutions de sécurité chez 2 fournisseurs Cloud

Compétences visées :

- Identifier les avantages et les inconvénients d'une solution ou d'une technologie
- Proposer des solutions à des nouvelles problématiques sécurité

Recommandations clés :

- Se référer au cours
- Se mettre dans le contexte de la problématique posée dans l'activité

5 heures

CONSIGNES

1. Pour le formateur :

- Il n'y pas qu'une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices
- L'apprenant n'est pas censé maitriser les éléments du corrigé, mais l'objectif est de susciter sa curiosité pour approfondir ses connaissances dans ce domaine

2. Pour l'apprenant :

- Cette activité est l'occasion d'introduire de nouvelles technologies et d'affronter des nouvelles problématiques

3. Conditions de réalisation :

- Une connexion internet
- Le guide théorique
- Il est possible d'avoir un accès gratuit de test sur des plateformes cloud

4. Critères de réussite :

- Connaissance basique des normes ISO
- Connaissance aisée des standards de gestion des vulnérabilités

Activité 1

Réaliser un benchmark des solutions de sécurité chez 2 fournisseurs Cloud

La sécurité dans le cloud

Exercices

En utilisant internet, réaliser un benchmark des solutions de sécurité chez 2 fournisseurs Cloud :

1. Choisir 2 fournisseurs de cloud bien implémentés dans le marché.
2. Étudier la tendance de migration vers le cloud en analysant les points suivants :
   - ✓ Les avantages du cloud par rapport à une infrastructure physique sur site (on premise)
   - ✓ Les types de cloud
   - ✓ Les types de déploiements possibles
3. Pour chacun des 2 fournisseurs Cloud, donner le nom des solutions proposées qui permettent de :
   - ✓ Gérer les accès et les droits des utilisateurs
   - ✓ Chiffrer les données et les stockages
   - ✓ Tracer l'activité des utilisateurs et des API
   - ✓ Isoler des ressources dans un réseau privé
4. Pour chacun des 2 fournisseurs Cloud :
   - ✓ Comment les utilisateurs peuvent se connecter aux ressources dans le cloud (serveurs, base de données, etc.)

PARTIE 2

Activité 1

Réaliser un benchmark des solutions de sécurité chez 2 fournisseurs Cloud

La sécurité dans le cloud

Corrigé

1. Choisir 2 fournisseurs de cloud bien implémentés dans le marché.

AWS : Amazon Web Services

Azure : La plateforme de cloud Microsoft

2. Étudier la tendance de migration vers le cloud en analysant les points suivants :

- ✓ Les avantages du cloud par rapport à une infrastructure physique sur site (on premise)
  - Changement des coûts de capital en coûts opérationnels, donc des coûts variables
  - Possibilité de faire des économies quand l'infrastructure grandit et évolue
  - Pas de besoin de faire de prévision de capacités infra
  - Augmenter l'agilité et réduire les délais de déploiement
  - Zéro coûts de maintenance et de run des datacenters
- ✓ Les types de cloud
  - Infrastructure as a service (IAAS)
  - Plateforme as a service (PASS)
  - Software as a service (SAAS)

PARTIE 2

Activité 1

Réaliser un benchmark des solutions de sécurité chez 2 fournisseurs Cloud

La sécurité dans le cloud

Corrigé

✓ Les types de déploiements possibles :

- Cloud public : AWS, Azure, GCP
- Cloud hybride : Un mélange de cloud publique et de cloud privé
- Cloud privé : l'entreprise est responsable de ses datacenters et utilise des solutions de virtualisation comme Openstack ou Vmware

3. Pour chacun des 2 fournisseurs Cloud, donner le nom des solutions proposées qui permettent de :

	AWS	Azure
Gérer les accès et les droits des utilisateurs	IAM	IAM
Chiffrer les données et les stockages	KMS	PMK
Tracer l'activité des utilisateurs et des API	CloudTrails	Log analytics
Isoler des ressources dans un réseau privé	VPC	VNet

PARTIE 2

Activité 1

Réaliser un benchmark des solutions de sécurité chez 2 fournisseurs Cloud

La sécurité dans le cloud

Corrigé

4. Pour chacun des 2 fournisseurs Cloud :

   ✓ Comment les utilisateurs peuvent se connecter aux ressources dans le cloud (serveurs, base de données, etc.) ?

AWS	AZURE
SSH	SSH
EC2 Instance connect	Remote desktop
Session manager	Azure bastion

PARTIE 2

ACTIVITÉ 2

Étude de cas des risques sur le cloud

Compétences visées :

- Découvrir les services cloud qui répondent à des problématiques de la cybersécurité
- Comparer les services et choisir par rapport à la situation présentée

Recommandations clés :

- Se référer au cours
- Se mettre dans le contexte de la problématique posée dans l'activité

4 heures

CONSIGNES

1. Pour le formateur :

- Il n'y pas qu'une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices
- L'apprenant n'est pas censé maitriser les éléments du corrigé, mais l'objectif est de susciter sa curiosité pour approfondir ses connaissances dans ce domaine

2. Pour l'apprenant :

- Cette activité est l'occasion d'introduire de nouvelles technologies et d'affronter des nouvelles problématiques.

3. Conditions de réalisation :

- Une connexion internet
- Le guide théorique
- Il est possible d'avoir un accès gratuit de test sur des plateformes cloud

4. Critères de réussite :

- Connaissance basique des normes ISO
- Connaissance aisée des standards de gestion des vulnérabilités

Activité 2
Étude de cas des risques sur le cloud

Les risques sur le cloud

Exercices

Maintenant que nous avons étudié les avantages et les solutions de sécurité Cloud. Analysons les risques et les inconvénients du cloud.

1. Donner 2 inconvénients du cloud par rapport à une infrastructure physique sur site (on premise)
2. Quels sont les risques cybersécurité d'une infrastructure physique sur site et qui sont accentués dans le cloud ?
3. Quels sont les nouveaux risques cybersécurité introduits par le mouvement vers le cloud ?
4. Quels sont les risques cybersécurité évités/diminués par le mouvement vers le cloud ?
5. Pour ces 3 types de risques (ce sont des types de risques et non pas des risques), proposer des solutions chez les 2 fournisseurs choisis dans l'activité précédente.
    - ✓ Risques sur les données
    - ✓ Risques d'attaque par rançongiciel
    - ✓ Risques d'attaques DOS (attaque par déni de service)

PARTIE 2

Activité 2
Étude de cas des risques sur le cloud

Les risques sur le cloud

Corrigé

Maintenant que nous avons étudié les avantages et les solutions de sécurité Cloud. Analysons les risques et les inconvénients du cloud

1. Donner 2 inconvénients du cloud par rapport à une infrastructure physique sur site (on premise) :

- L'entreprise n'a plus la maitrise totale des données stockées dans un cloud public.
- Les possibilités et les fonctionnalités sont limitées par les services proposés par le fournisseur et il n'est pas toujours possible de les personnaliser.

2. Quels sont les risques cybersécurité d'une infrastructure physique sur site et qui sont accentués dans le cloud ?

- Le risque d'accès aux données et la divulgation des données est plus important et l'impact est plus grave dans un déploiement cloud.
- Le risque des mauvaises configurations est plus important dans le cloud avec des services non maitrisés ou des fonctionnalités non comprises.

PARTIE 2

Les risques sur le cloud

Corrigé

3. Quels sont les nouveaux risques cybersécurité introduits par le mouvement vers le cloud ?

- Les utilisateurs et les clients ont une visibilité et un contrôle réduits. Lors de la transition des actifs/opérations vers le cloud, les organisations perdent une certaine visibilité et un certain contrôle sur ces actifs/opérations. Lors de l'utilisation de services cloud externes, la responsabilité de certaines politiques et infrastructures est transférée au fournisseur.
- Le service à la demande simplifie l'utilisation non autorisée. Les fournisseurs facilitent la fourniture de nouveaux services. Les fonctionnalités de provisionnement en service à la demande du cloud permettent au personnel d'une organisation de fournir des services supplémentaires à partir du fournisseur cloud sans le consentement du service informatique. La pratique consistant à utiliser un logiciel dans une organisation qui n'est pas prise en charge par le service informatique de l'organisation est communément appelée shadow IT.
- Les API de gestion accessibles sur Internet peuvent être compromises. Les fournisseurs Cloud exposent un ensemble d'interfaces de programmation d'applications (API) que les clients utilisent pour gérer et interagir avec les services cloud (également appelés plan de gestion). Les organisations utilisent ces API pour provisionner, gérer, orchestrer et surveiller leurs actifs et leurs utilisateurs. Ces API peuvent contenir les mêmes vulnérabilités logicielles qu'une API pour un système d'exploitation, une bibliothèque, etc. Contrairement aux API de gestion pour l'informatique sur site, les API fournisseurs sont accessibles via Internet, ce qui les expose plus largement à une exploitation potentielle.

  Les pirates recherchent des vulnérabilités dans les API de gestion. Si elles sont découvertes, ces vulnérabilités peuvent être transformées en attaques réussies et les ressources cloud de l'organisation peuvent être compromises. À partir de là, les attaquants peuvent utiliser les actifs de l'organisation pour perpétrer d'autres attaques contre d'autres clients du fournisseur.

Les risques sur le cloud

Corrigé

4. Quels sont les risques cybersécurité évités/diminués par le mouvement vers le cloud ?

- La disponibilité est plus assurée sur le cloud. Lorsque vous passez au cloud, les données sont stockées dans plusieurs data centers géo-indépendants, avec une redondance mise en œuvre dans tout le système. Vos données ne sont pas simplement copiées dans un centre de données ; elles sont distribuées à plusieurs centres de données. Ainsi, si l'un tombe en panne, vos données basculeront automatiquement vers un autre.
  Les grands fournisseurs de cloud protègent également la disponibilité grâce à la virtualisation. Lorsque les serveurs sont virtualisés dans le cloud, les fournisseurs peuvent facilement migrer les serveurs d'un data center à un autre en cas de panne. La plupart des systèmes sur site peuvent n'avoir que deux serveurs physiques qui basculent l'un vers l'autre. Cela n'est pas utile en cas d'incendie ou de panne de réseau importante.
- La sécurité physique est prohibitive. Il faut beaucoup de temps et d'argent pour prévenir le vol physique. Pour protéger complètement vos serveurs sur site, vous devez mettre en place une sécurité renforcée, avec des gardes, des mantraps et des cages verrouillées pour les serveurs.
  Dans le cloud, vos efforts et dépenses pour tout cela disparaissent. Les fournisseurs de cloud dépensent de l'argent pour des gardes 24 heures sur 24 et des contrôles de sécurité physique à la pointe de la technologie. La taille et la sécurité de ces centres de données rendent le vol physique ciblé presque impossible.
- Améliorer la sécurité technique. L'application de correctifs est l'un des plus gros problèmes de sécurité auxquels les entreprises de toutes tailles sont confrontées jusqu'à ce qu'elles passent au cloud. En fait, certaines des violations les plus importantes - pensez à Equifax et à l'épidémie de WannaCry - résultaient d'un mauvais correctif.
  Contrairement à la plupart des entreprises, les grands fournisseurs de services cloud tels que Microsoft, Amazon et Google disposent des ressources nécessaires pour embaucher des équipes à temps plein dédiées à la correction de leurs produits. Le processus de correction dans le cloud est en grande partie automatisé, ce qui élimine les temps d'arrêt requis par la correction sur site.

Activité 2
Étude de cas des risques sur le cloud

Les risques sur le cloud

Corrigé

2. Pour ces 3 types de risques (ce sont des types de risques et non pas des risques), proposer des solutions chez les 2 fournisseurs choisis dans l'activité précédente.
   - ✓ Risques sur les données
   - ✓ Risques d'attaque par rançongiciel
   - ✓ Risques d'attaques DOS (attaque par déni de service)

	AWS	Azure
Risques sur les données	KMS	PMK
Risques d'attaque par rançongiciel	MFA, La gestion des versions Simple Storage Service (Amazon S3)	Azure backup
Risques d'attaques DOS (attaque par déni de service)	AWS shield	DDOS Protection Standard DDOS Protection Basic

PARTIE 2

PARTIE 3

DÉFINIR DES CRITÈRES DE LA CYBERSÉCURITÉ

Dans ce module, vous allez :

- Appliquer les critères de la sécurité à des cas pratiques
- Analyser les dysfonctionnements et l'impact de chaque critère
- Proposer des scénarios de réponse ou de prévention

12 heures

ACTIVITÉ 1

Cas pratique 1

Compétences visées :

- Identifier les critères de la cybersécurité
- Analyser des incidents cybersécurité à travers le prisme des critères de la cybersécurité

Recommandations clés :

- L'énoncé de chaque situation est succinct, laissant à l'apprenant la liberté d'analyser la situation et de poser toutes les hypothèses allant dans le sens de l'objectif du cas

11 heures

CONSIGNES

1. Pour le formateur :

- Il n’y pas qu’une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices
- Le corrigé est fait pour orienter l’apprenant à chercher plus et challenger les propositions
- Il est recommandé de réaliser cette partie en groupe

2. Pour l’apprenant :

- L’intérêt de chaque activité est le processus d’analyse et d’imagination
- La formulation de la réponse est aussi importante que la réponse
- Si c’est possible, proposer plusieurs scénarios de réponse pour chaque cas

3. Conditions de réalisation :

- Les cas pratiques peuvent être réalisés en seul ou en groupe
- Le support du guide théorique de la compétence

4. Critères de réussite :

- Différenciation exacte des trois critères de la cybersécurité
- Identification claire des niveaux de chaque critère de cybersécurité

Activité 1
Cas pratique 1

Cadre général

Exercices

Dans tout scénario de cyberattaque, il y a un élément de guerre de tranchées. **Groupomo** (une société fictive) avait identifié la cybersécurité et la confidentialité comme des objectifs clés au début de la dernière décennie, mais n'a en grande partie pas investi dans des processus et des outils de sécurité pour rendre la protection des données efficace.

Ce manque de préparation signifiait qu'en cas d'attaque, l'entreprise devait se démener et s'adapter pour contrer les avancées de l'adversaire.

En l'espace de neuf mois, l'entreprise a survécu à trois cyberattaques qui se trouvaient directement dans les trois catégories (disponibilité, confidentialité, intégrité).

Dans cette étude de cas, l'entreprise a subi des attaques qui ont eu un impact sur les trois objectifs de sécurité de l'information :

- ✓ Confidentialité : des informations sensibles ont été exposées en permanence
- ✓ Intégrité : les informations au repos ont été menacées par des logiciels malveillants
- ✓ Disponibilité : pendant la pandémie, les systèmes ont été inutilisables pendant une longue période

Activité 1
Cas pratique 1

COVID-19

Exercices

Que s'est-il vraiment passé?

Au début de la pandémie de COVID-19, Groupomo a pris la décision de fermer ses serveurs pour réduire son exposition aux menaces.

Malheureusement, cette décision a également eu pour effet d'empêcher les utilisateurs légitimes d'accéder à leurs ressources de travail. En conséquence, l'entreprise a dû se démener pour fournir des ordinateurs portables et des jetons VPN non testés aux employés.

Le travail qui avait lieu à l'intérieur du périmètre du réseau sécurisé devait désormais être effectué à domicile, faisant essentiellement de chaque employé son propre administrateur système.

La difficulté de fournir une assistance informatique à divers bureaux à domicile distants, aggravée par l'impact sur la productivité de l'interruption d'activité, a illustré à quel point de tels événements malveillants peuvent être perturbateurs.

La transition cahoteuse vers ce modèle de « pandémie » inefficace a illustré le besoin urgent de planifier, de répéter, de s'entraîner et d'avoir accès à des ressources fiables en un clin d'œil.

1. Quel type critère de la cybersécurité a été impacté par cet incident ?
2. Proposer un scénario d'action pour répondre à cet incident

COVID-19

Corrigé

1. Quel type critère de la cybersécurité a été impacté par cet incident ?

Le critère impacté est la disponibilité.

2. Proposer un scénario d'action pour répondre à cet incident

Au premier trimestre de 2020, la pandémie mondiale de COVID-19 a forcé Groupomo à interrompre ses opérations normales et à fermer ses portes au public.

Dès le début de cette situation perturbatrice, Groupomo IT a pris des mesures clés pour donner la priorité à l'assistance aux utilisateurs, en veillant à ce que le personnel dispose d'un accès sécurisé aux ressources de travail, d'une connectivité sécurisée et de conseils pour les scénarios nécessitant des exceptions, des recherches supplémentaires et une exécution rapide. Au sein de n'importe quelle PME, ce travail serait un travail à temps plein. Les capacités de l'équipe informatique de Groupomo ont été mises à rude épreuve.

ACTIVITÉ 2

Cas pratique 2

Compétences visées :

- Identifier les critères de la cybersécurité
- Analyser des incidents cybersécurité à travers le prisme des critères de la cybersécurité

Recommandations clés :

- L'énoncé de chaque situation est succinct, laissant à l'apprenant la liberté d'analyser la situation et de poser toutes les hypothèses allant dans le sens de l'objectif du cas

11 heures

CONSIGNES

1. Pour le formateur :

- Il n’y pas qu’une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices.
- Le corrigé est fait pour orienter l’apprenant à chercher plus et challenger les propositions
- Il est recommandé de réaliser cette partie en groupe

2. Pour l’apprenant :

- L’intérêt de chaque activité est le processus d’analyse et d’imagination
- La formulation de la réponse est aussi importante que la réponse
- Si c’est possible, proposer plusieurs scénarios de réponse pour chaque cas

3. Conditions de réalisation :

- Les cas pratiques peuvent être réalisés en seul ou en groupe.
- Le support du guide théorique de la compétence

4. Critères de réussite :

- Différenciation exacte des trois critères de la cybersécurité
- Identification claire des niveaux de chaque critère de cybersécurité

Activité 2
Cas pratique 2

Fuite de données

Exercices

Que s'est-il vraiment passé ?

À l'insu de Groupomo, son fournisseur de services, **EnterTrust**, a subi une cyber-brèche qui a exposé tous les dossiers clients appartenant à Groupomo.

Un employé interne a accédé aux données des clients et en a fait des copies dans l'espoir de tirer profit des ventes d'informations sur les clients.

L'incident n'a été signalé à Groupomo que sept semaines plus tard, par l'intermédiaire de l'avocat d'EnterTrust.

Ce retard dans le signalement a donné un ton inquiétant à la relation avec ce fournisseur, obligeant l'entreprise à informer immédiatement les personnes concernées et à s'adapter pour gérer l'afflux de requêtes des clients concernés.

1. Quel type critère de la cybersécurité a été impacté par cet incident ?
2. Proposer un scénario d'action pour répondre à cet incident

Fuite de données

Corrigé

1. Quel type critère de la cybersécurité a été impacté par cet incident ?

Le critère impacté est la confidentialité.

2. Proposer un scénario d'action pour répondre à cet incident :

Dès que Groupomo a eu connaissance de la violation des données, le responsable de la protection de la vie privée et conseiller en cybersécurité de l'entreprise a signalé l'incident au Commissariat à la protection de la vie privée du Canada (OPC), l'agence responsable du respect de la vie privée, qui a émis les recommandations suivantes :

- ✓ Établissez une ligne téléphonique pour permettre aux clients de Groupomo d'appeler et de poser des questions sur la violation et d'être référés à la propre ligne d'assistance d'EnterTrust.
- ✓ Souscrivez une assurance cyber-responsabilité pour éviter que l'exploitation future potentielle des enregistrements compromis ne devienne un grave problème de responsabilité pour Groupomo.
- ✓ Avertissez les clients et informez-les de la gravité de l'impact et offrez une assistance, des ressources et des conseils supplémentaires si nécessaire.

ACTIVITÉ 3

Cas pratique 3

Compétences visées :

- Identifier les critères de la cybersécurité
- Analyser des incidents cybersécurité à travers le prisme des critères de la cybersécurité

Recommandations clés :

- L'énoncé de chaque situation est succinct, laissant à l'apprenant la liberté d'analyser la situation et de poser toutes les hypothèses allant dans le sens de l'objectif du cas

11 heures

CONSIGNES

1. Pour le formateur :

- Il n’y pas qu’une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices
- Le corrigé est fait pour orienter l’apprenant à chercher plus et challenger les propositions
- Il est recommandé de réaliser cette partie en groupe

2. Pour l’apprenant :

- L’intérêt de chaque activité est le processus d’analyse et d’imagination
- La formulation de la réponse est aussi importante que la réponse
- Si c’est possible proposer plusieurs scénarios de réponse pour chaque cas

3. Conditions de réalisation :

- Les cas pratiques peuvent être réalisés en seul ou en groupe
- Le support du guide théorique de la compétence

4. Critères de réussite :

- Différenciation exacte des trois critères de la cybersécurité
- Identification claire des niveaux de chaque critère de cybersécurité

Activité 3
Cas pratique 3

Disponibilité

Exercices

Que s'est-il vraiment passé ?

Deux mois plus tard, Groupomo a subi une cyberattaque directe par e-mail qui a installé un logiciel malveillant et menacé de crypter et de supprimer les données sur les serveurs de Groupomo.

Comme le font de nombreux types de logiciels malveillants modernes, l'approche de cette cyberattaque consistait à envoyer des e-mails personnalisés à une douzaine d'employés Groupomo à partir de ce qui ressemblait à leurs propres collègues, leur demandant d'ouvrir de toute urgence une pièce jointe.

Une fois ouverte, la pièce jointe a procédé à l'analyse de l'ordinateur local et du réseau environnant, à la recherche de vulnérabilités et d'un moyen d'"appeler à la maison" pour plus de logiciels malveillants.

Groupomo IT s'est empressé d'évoluer rapidement pour tenter de devancer la menace invisible.

1. Quel type critère de la cybersécurité a été impacté par cet incident ?
2. Proposer un scénario d’action pour répondre à cet incident

PARTIE 3

Activité 3
Cas pratique 3

Disponibilité

Corrigé

1. Quel type critère de la cybersécurité a été impacté par cet incident ?

Le critère impacté est l'intégrité.

2. Proposer un scénario d'action pour répondre à cet incident

L'objectif du logiciel malveillant était de localiser et de voler les données sensibles de Groupomo et d'interrompre les opérations suffisamment longtemps pour extraire le paiement d'une rançon.

Cet incident a été désamorcé avec succès par une série d'activités rapides et appropriées menées par l'équipe informatique de Groupomo.

Cela a été possible grâce au travail de l'équipe informatique qui a répondu à la violation de données initiale.

La prévention réussie d'une violation potentielle avant qu'elle n'atteigne la phase d'extorsion a été un effort conjoint entre l'équipe informatique de Groupomo et son CPA, qui a été formé à la réponse aux incidents de cybersécurité.

Relevant du CIO et du CFO, la fonction de conseil du CPA a été en mesure de surmonter les obstacles et de traduire rapidement le langage des menaces techniques en impact commercial réel.

Ces approches décisives ont permis à l'entreprise d'analyser et d'isoler rapidement les ordinateurs du réseau, d'arrêter les périphériques inutiles et d'enquêter individuellement sur tous les actifs qui étaient entrés en contact avec les systèmes infectés d'origine.

Cette approche de la « recherche numérique des contacts » est différente dans chaque scénario, mais le résultat est le même : contenir efficacement une violation de données dès que possible avec des ressources informatiques limitées.

PARTIE 4

DÉCOUVRIR LES MÉTIERS DE LA CYBERSÉCURITÉ

Dans ce module, vous allez :

- Analyser les métiers des équipes IT et sécurité
- Répartir les rôles des équipes IT et sécurité dans le cadre d'un incident sécurité

11 heures

ACTIVITÉ 1

Mise en situation d’un incident cybersécurité lié à la blockchain à travers différents rôles/métiers

Compétences visées :

- Etudier une nouvelle attaque et rassembler le maximum d’informations sur l’attaque
- Identifier les acteurs pour faire face à des attaques sécurité

Recommandations clés :

- Beaucoup de modèles d’organisation existent. Il recommandé d’être familiarisé avec 2 ou 3 modèles en plus du modèle proposé dans l’activité.

11 heures

CONSIGNES

1. Pour le formateur :

- Il n’y pas qu’une seule solution possible à chaque question
- Il faut orienter les apprenants en cas de blocage et donner des indices
- Le corrigé est fait pour orienter l’apprenant à chercher plus et challenger les propositions

2. Pour l’apprenant :

- L’intérêt de chaque activité est le processus d’analyse et d’imagination
- Se mettre dans la position de chaque rôle et identifier les compétences nécessaires
- Si c’est possible proposer plusieurs scénarios de réponse

3. Conditions de réalisation :

- Une connexion internet
- Le guide théorique

4. Critères de réussite :

- Connaissance générale des métiers de la cybersécurité et leurs parcours
- Connaissance générale des tendances de la cybersécurité

Activité 1

Mise en situation d'un incident cybersécurité lié à la blockchain à travers différents rôles/métiers

Étape 1 : Préparer un tableau de bord des vulnérabilités identifiées

Exercices

Bien qu'elle ne soit pas incassable, la blockchain a évolué pour devenir l'une des formes de transaction les plus infaillibles dans le domaine des réseaux numériques. Telle qu'elle a été conçue et prévue, la technologie a été créditée pour son assurance de l'intégrité de l'information. Si elle st bien utilisée, de nombreux secteurs peuvent en bénéficier. Cependant, les nouvelles technologies s'accompagnent de nouveaux outils et méthodes d'exploitation, et la blockchain ne fait pas exception. Une nouvelle classe de cybermenaces est en train d'émerger, impliquant des tactiques propres aux réseaux blockchain.

Votre entreprise a été victime d'une attaque de **cryptojacking** :

1. Définir ce type d'attaque.
2. Quelle vulnérabilité ou caractéristique de la blockchain rend cette d'attaque possible ?
3. En suivant le modèle prévenir/détecter/bloquer/restaurer, donner les noms d'équipes et les rôles/métiers cybersécurité responsables de chaque partie.
4. Détailler comment chaque équipe/métier aurait pu intervenir/intervient/interviendra dans le cadre de cette attaque.

PARTIE 4

Activité 1

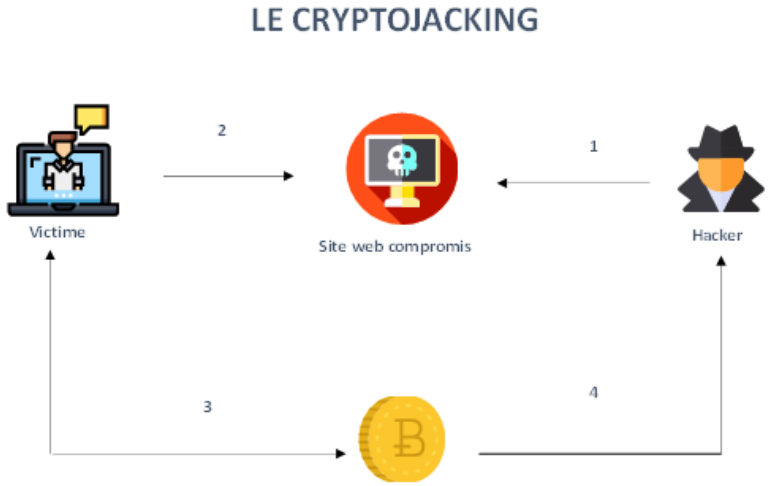
Mise en situation d'un incident cybersécurité lié à la blockchain à travers différents rôles/métiers

Étape 1 : Préparer un tableau de bord des vulnérabilités identifiées

Corrigé

1. Définir ce type d'attaque.

- L'attaque cryptojacking se produit lorsque des ordinateurs sont détournés pour leur puissance de calcul afin d'extraire des crypto-monnaies. Il s'agit d'un exemple d'exploits de porte dérobée et sur la rampe, qui sont similaires aux attaques de la chaîne d'approvisionnement. Cette attaque est aussi une pratique de plus en plus courante qui consiste pour certains sites Web à mettre la connexion Internet d'un utilisateur à disposition pour du minage, au détriment de cet utilisateur dont les ordinateurs sont ainsi mis au service de tierces personnes. Votre navigateur, votre ordinateur et votre bande passante sont ainsi utilisés pour générer de nouvelles cryptomonnaies.
- Le cryptojacking a gagné en popularité au cours de la dernière année, principalement en raison de sa facilité d'utilisation. De nombreux pirates considèrent cette technique de piratage comme une version moins chère et plus rentable du rançongiciel. Il est également plus facile de s'en tirer avec le cryptojacking car le code minier peut fonctionner sans être détecté pendant longtemps.



PARTIE 4

Étape 1 : Préparer un tableau de bord des vulnérabilités identifiées

Corrigé

2. Quelle vulnérabilité ou caractéristique de la blockchain rend cette d'attaque possible ?

- La nature distribuée de la blockchain permet ce type d'attaque. La blockchain est basée sur les registres distribués. Les registres distribués utilisent des ordinateurs indépendants (appelés nœuds) pour enregistrer, partager et synchroniser les transactions dans leurs registres électroniques respectifs (au lieu de centraliser les données comme dans un registre traditionnel). La blockchain organise les données en blocs, qui sont enchaînés dans un mode d'ajout uniquement.
- La blockchain est la pierre angulaire de « l'Internet de la valeur » et permet d'enregistrer les interactions et de transférer la « valeur » de pair à pair, sans avoir besoin d'une entité de coordination centrale. La « valeur » fait référence à tout enregistrement de la propriété d'un actif - par exemple, de l'argent, des titres, des titres fonciers - ainsi qu'à la propriété d'informations spécifiques telles que l'identité, les informations sur la santé et d'autres données personnelles.
- Cette nature de distribution rend la traçabilité et donc la détection de cette attaque difficile. D'autant plus que les attaques de cryptojacking sont souvent masquées comme un comportement standard et normal, ce qui rend cette activité malveillante encore plus difficile à détecter.

Activité 1

Mise en situation d'un incident cybersécurité lié à la blockchain à travers différents postes/métiers

Étape 1 : Préparer un tableau de bord des vulnérabilités identifiées

Corrigé

3. En suivant le modèle prévenir/détecter/bloquer/restaurer, donner les noms d'équipes et les rôles/métiers cybersécurité responsables de chaque partie.

- Nous pouvons proposer une organisation de réponse aux incidents de la manière suivante :

Pôle	Équipes	Rôles
Prévenir	Gestion des risques liés aux informations Gestion des risques techniques Renseignements sur les menaces	- Analyse des risques - Mise en place de la posture et les process de défense - Veille sur les nouvelles menaces et d'actualité
Détécter	Security operations centre (SOC)	- Surveillance des attaque et des incidents
Bloquer	CSIRT Réseau & Sécurité Systèmes & infrastructure	- Investigation des incidents - Traitement des incidents
Restaurer	Réseau & Sécurité Systèmes & infrastructure Gestion des risques liés aux informations Gestion des risques techniques	- Restauration des services - Amélioration de la posture de défense

PARTIE 4

Étape 1 : Préparer un tableau de bord des vulnérabilités identifiées

Corrigé

4. Détailler comment chaque équipe/métier aurait pu intervenir/intervient/interviendra dans le cadre de cette attaque.

Pôle	Équipes	Actions
Prévenir	Gestion des risques liés aux informations	- Réaliser un inventaire et une analyse de risques des actifs les plus exposés
	Gestion des risques techniques	- Réaliser un état des lieux et une analyse de risques des applications utilisées et des flux réseaux des actifs exposés
	Renseignements sur les menaces	- Documenter les attaques de cryptojacking et les méthodes d'infection
Détécter	Security operations centre (SOC)	- Mise en place d'une surveillance des actifs exposés - Alerter sur des connexions vers des IPs malveillantes ou non standards
Bloquer	CSIRT	- Analyse numérique des process/connexions/applications qui tournent sur les actifs infectés et comparaison avec l'inventaire des équipes gestions des risques
	Réseau & Sécurité	- Analyse des connexions non standards et blocage des flux malveillants sur les firewalls
	Systèmes & infrastructure	- Isolation et application des recommandations de l'équipe CSIRT sur les actifs infectés
Restaurer	Réseau & Sécurité	- Mise à jour des IPS/IDS/Firewalls avec les signatures récuprées de l'attaque
	Systèmes & infrastructure	- Restaurer les actifs infectés à partir d'un backup non infecté
	Gestion des risques liés aux informations	- Analyse de l'attaque et des vulnérabilités qui ont été exploitées
	Gestion des risques techniques	- Etudier la décision de la mise en place d'un EDR sur les actifs exposés