Cnam Ile-de-France – Formation Ouverte à Distance

Année 2022/2023 – 1er semestre

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Examen SEC101 – FOAD IDF

Session 2
Mars 2023

Durée	3 heures
Document (s) autorisé(s) :	tout document papier
Calculatrice :	x
Téléphone portable :	**Interdit**

Le sujet comporte 3 pages (dont celle-ci).
Barème d'évaluation : voir ci-dessous

Les 8 questions à développement court représentent respectivement 2 pts chacune, sauf la dernière à 3 pts.

1pt pour la présentation et l'orthographe si et seulement si toutes les questions sont traitées

Votre note sur 20.

Courage, la première fois ne fut pas la bonne

« Les opportunités ne sont pas offertes. Elles doivent être arrachées. Et cela demande de la persévérance... et du courage.»

Indira GANDHI

NE SERONT NOTEES SEULEMENT CELLES DONT LES REPONSES SERONT ARGUMENTEES.
Attention à répondre à la question, à la relecture prenez le temps de lire la question

Questions à développement court

1/ Menace virale du programme malveillant Darkhotel (APT)
Source : site web Kaspersky

DÉFINITION DU VIRUS

Type de virus : programme malveillant, menace persistante avancée (APT)

Qu'est-ce que la menace Darkhotel ?

La dernière menace virale appelée « Darkhotel », a été analysée par l'équipe Global Research and Analysis de Kaspersky Lab. Elle semble correspondre à une combinaison de phishing ciblé et de programme malveillant dangereux conçus pour capturer des données confidentielles.

Les cybercriminels à l'origine de Darkhotel opèrent depuis près d'une décennie en ciblant des milliers de victimes à travers le monde. 90 % des infections Darkhotel que nous avons observées ont été recensées au Japon, à Taïwan, en Chine, en Russie et en Corée mais également en Allemagne, aux États-Unis, en Indonésie, en Inde et en Irlande.

Informations détaillées sur la menace virale

Comment fonctionne la menace Darkhotel ?

Ces campagnes sont inhabituelles dans la mesure où elles utilisent des degrés différents de ciblage malveillant.

(1) Phishing ciblé

D'un côté, elles utilisent des e-mails de phishing ciblé pour infiltrer des bases industrielles de défense (BID), des gouvernements, des organisations non gouvernementales, des grands fabricants d'électronique et d'appareils, des entreprises pharmaceutiques, des prestataires de la santé, des organisations militaires et des responsables dans le secteur de l'énergie. Les attaques suivent un processus type de phishing ciblé avec des implantations Darkhotel bien dissimulées. Les e-mails utilisés comme leurres portent bien souvent sur les thèmes de l'énergie nucléaire et les capacités en matière d'armes. Ces dernières années, les e-mails de phishing ciblé contiennent une faille d'exploitation de type « zero-day » en pièce jointe ou des liens qui redirigent les navigateurs des cibles vers des failles d'exploitation zero-day d'Internet Explorer, leur but étant de dérober des données à ces organisations.

(2) Diffusion de programmes malveillants

De l'autre côté, elles propagent le programme malveillant à l'aveugle via des sites japonais de partage de fichiers P2P. Le programme malveillant est diffusé en tant qu'élément d'une archive RAR de taille importante qui prétend proposer du contenu à caractère sexuel mais qui, en réalité, installe un cheval de Troie qui recueille des données confidentielles appartenant à la victime.

(3) Infection

Dans une approche qui se situe entre ces deux extrémités, elles ciblent des cadres dirigeants peu méfiants qui voyagent à l'étranger et séjournent dans un hôtel. Dans ce type de campagne, les victimes sont infectées par un cheval de Troie rare, se faisant passer pour une mise à jour importante d'un logiciel connu, notamment Google Toolbar, Adobe Flash et Windows Messenger. La première phase de l'infection permet aux pirates de cerner leurs victimes et de télécharger d'autres programmes malveillants sur les ordinateurs de victimes plus importantes en vue de leur dérober des données confidentielles.

D’après une chaîne figurant au sein du code malveillant, il semble que les menaces proviennent d'un coréen.

Quelle est l'importance de Darkhotel ?

Hormis la sophistication technique de nombreuses attaques ciblées, elles commencent généralement par inciter des employés individuels à commettre une erreur qui met directement en péril la sécurité de l'entreprise. Le personnel en relation directe avec le public (ex. dirigeants, commerciaux et personnel marketing) peut être particulièrement vulnérable, notamment du fait qu'il est souvent en déplacement et susceptible d'utiliser des réseaux non fiables (ex. dans des hôtels) pour se connecter à un réseau d'entreprise.

Caractéristiques de la campagne Darkhotel

- Attaques ciblées visant des cadres supérieurs : PDG, vice-présidents, directeurs des ventes et du marketing, et personnel de haut niveau travaillant dans le service de recherche et de développement
- Le gang utilise des attaques ciblées et des opérations de style botnet. Il compromet les réseaux hôteliers, puis prépare des attaques à partir de ces réseaux contre des victimes haut placées. Dans le même temps, il utilise des opérations de style botnet pour une surveillance à grande échelle, exécute d'autres actions telles que des attaques DDoS (déni de service distribué) ou installe des outils d'espionnage plus sophistiqués sur les ordinateurs de victimes particulièrement intéressantes.
- Utilisation de failles d'exploitation de type « zero-day » ciblant Internet Explorer et des produits Adobe.
- Utilisation d'un enregistreur de frappe de faible niveau avancé pour dérober des données confidentielles.
- Code malveillant signé utilisant des certificats numériques volés.

- Campagne persistante : Darkhotel opère depuis près d'une décennie.

En tant que RSSI, quel serait vos propositions organisationnelles et techniques afin de se prémunir de ce risque ?

Si vous envisagez d'accéder à un réseau wifi public ou semi-public, utilisez exclusivement des tunnels VPN fiables.

Découvrez comment les attaques de phishing ciblé fonctionnent afin de mieux les comprendre.

Assurez la maintenance et la mise à jour de l'ensemble des logiciels système.

Vérifiez systématiquement les fichiers exécutables et gérez les fichiers partagés sur des réseaux P2P avec prudence et méfiance.

Pendant vos déplacements, essayez de limiter les mises à jour des programmes.

Installez un logiciel de sécurité Internet : assurez-vous qu'il inclut une protection proactive contre les nouvelles menaces plutôt qu'une simple protection antivirus de base

Questions à développement court

2/ Le cyber threat intel (CTI) (renseignement sur la menace cyber) est un processus complet.
En expliquant son fonctionnement, vous expliquerez comment il est intégré à un SOC et pourquoi les RSSI doivent aussi suivre les alertes

Correction : le CTI est la production d'indicateur permettant de se prémunir et détecter les attaques informatiques. Pour cela, on va analyser les assets (biens de l'organisme) et les sources de menaces via les modes d'attaques des groupes pouvant cibler le ou les SI.
En produisant des IOC (indicator of compromission) le CTI est integré à la recherche de traces ou éléments pouvant poindre sur une attaque informatique. La forme évoluée de ceci est le hunting. C'est-à-dire de rechercher des signaux faibles dans les alertes déjà générées pour détecter des attaques complexes type APT

3/l'analyse de risque est une activité importante dans de nombreux domaines dont la cybersécurité. En vous basant sur un exemple d'attaque de ransomware, vous expliquerez les étapes de traitement du risque propre à ce type d'incident de sécurité.

Le traitement du risque est composé de 3 phases :

- **Identifier les mesures potentielles relevant de la prévention, de la préparation, de l'intervention et du rétablissement :**
  - **Sensibiliser à ce risque (prévention)**
  - **Desactiver les modules inutiles sur le système d'exploitation (prévention)**
  - **Mettre en place une solution anti-virale (préparation)**
  - **Solution de sauvergarde (prévention)**
  - **Mettre en place un edr (intervention et rétablissement)**
- **L'évaluation et la sélection des mesures.**
  - **Vérifier l'impact des mesures sur le SI**
    - **Disponbilité**
    - **Cout licences**
    - **Cout formation**
    - **Complexite de mise en œuvre**
    - **Décrire les test de non régression**
- **Planification et de la mise en œuvre des mesures retenues.**
  - **Planifications des Mises en prod**
  - **Dérouler les test de non régression**
  - **Communiquer sur les indisponibilites ou les objectifs**

4/la mise en place d'une certification IS0 22301 est en cours. Que pouvez-vous utilisez afin de faciliter ou nourrir la mise en place d'un SMSI au sein de la même entité.
Vous penserez à synthétiser votre réponse pour argumenter votre projet au près d'une gestion.

La norme ISO 22301 explique la mise en place d'un système de management de la continuité d'activité. A ce titre, elle rejoint

- **les analyses de risques, `**
- **le listing des biens,**
- **la responsabilité des parties internes et externes**

- **la mise en place des communités de pilotage et de contrôle**

à ce titre les certifications croisées sont plus rentables mais nécessite une séléction rigoureuses des organismes de certifications.

5/l'intelligence économique est plus qu'une activité de la sphère géopolitique. Comment l'intégrer dans la cybersécurité sans la réduire à une activité de CTI ?

Correction : l'IE permet de lister les biens immatérielles de l'organisme plus finement que ne serait le faire une analyse des fichiers et dossier vu par une équipe d'exploitation. De plus, l'approche géopolitique assure une plus grande connaissance des sources de menaces exogènes à l'organisme. Enfin l'approche et les techniques propres à l'OSINT permettent de se placer dans la position d'un groupe de hacker réalisant la première étape de la killchain (le repérage)

6/ Proposer 4 indicateurs de performance permettant de prouver que l'investissement dans un SOC est pertinent. On parle de retour sur investissement de sécurité (ROSI), peut-on le comparer à un ROI classique ?

Correction :

- **Nombre d'alertes par jours et son évolution**
- **Connaissance du périmètre et des postes à jour (évolution mensuel)**
- **Délai de traitement moyen constaté par ticket d'incident**
- **Détection apportée par le CTI par rapport aux règles de base proposées par les éditeurs des éditeurs de sécurités.**

Le ROI permet de connaitre la rentabilité d'un investissement. Dans le ROSI on va calculer par exemple le cout qu'aurez créer une attaque informatique pour l'organisme. Donc il ne faut pas voir la rentabilité mais les économies potentielles aux ressources consacrées.

7/ une SMSI ne se copie pas, il doit être créé dans un cadre précis et sur un périmètre maitrisé. Qui peut réaliser ce projet ? doit-il être forcément certifié pour mener à bien celui-ci ?

Le RSSI peut réaliser ce type de projet mais un responsable de projet SMSI peut etre désigné. La certification d'une personne ne permet de s'assurer que ses compétences quant à un cadre normatif nullement que ces compétences ne sont pas suffisantes à la mise en place. On pourra néanmoins préférer une personne ayant une certification 27001 Lead Implementor.
Finalement, c'est le SMSI qui doit être certifié.

8/La gestion des vulnérabilités est de la responsabilité du RSSI. Mais en amont et en aval des actions sont réalisées afin de pouvoir valider ce processus de sécurité opérationnelle. En paraphrasant, quelles sont les informations et actions requises ?

Actions et informations

- **En amont :**
  - **La tenue de la liste des biens supports portant les vulnérabilités (informations)**
    - **Technique : reseau système web**
    - **Personnel :: suivi formation, sensibilisation, charte, engagement de responsabilité**
    - **Financement :: budget nécessaire et consenti**
  - **Abonnement à un CERT et flux de mise à jour de sécutité**
- **En aval :**

- **Suivi indicateur incident**
- **ROSI**
- **Pourcentage des biens supports techniques patchés**
- **Réagir aux diffusions de vulnérabilités des éditeurs et CERT**

9/

Dans cette question : Octo leebe c'est le leader français de la conservation de données de santé et des rdv médicaux

En tant que chef de la section infrastructure du groupe, vous avez une deuxième casquette de DPO.

Pierre votre nouvel admin système se plaint des lenteurs et temps d'accès aux bases de données. Il ne jure que par Amazon et ses services cloud. Lors de la réunion de début de semaine, il annonce lors de son tour de parole avoir transférer sur le week-end l'ensemble des services de stockage ainsi que les données utilisateurs de votre groupe « Octo leebe ». D'après son analyse, les technologies et capacités de stockage en France par l'entreprise ne correspondaient plus aux standards de l'industrie.

Indicateurs à l'appui, il annonce avoir solutionné les problèmes de performances de l'infra et du site web…

Quelle est votre réaction ? quelles sont les actions à mener sans délais ?

(Question sans intérêt) Pierre va-t-il être promu au poste de team leader system le mois prochain ?

Correction :

En tant que DPO vous devez sans délai déclaré un transfert des données de santé à la CNIL ainsi que communiquer auprès des utilisateurs. Ceci en préparant un message avec les responsables de octo leebe.

En effet, votre structure quoique lente est certifiée HDS (hebergeur de données de santé) donc son périmètre et contexte sont fixés. Amazon est aussi HDS mais les données sont stockées dans le cloud dont le *cloud act* et le *patriot act* s'appliquent. Les répercussions sont importantes en terme juridique.

Techniquement :

- **Le compte de pierre est suspendu, mais il reste à disposition pour expliquer les actions qu'il a mené.**
- **Il faut connaitre les impacts techniques sur les solutions de stockage et réaliser une série de test à prioriser afin de ne pas se perdre en action stériles.**
- **Evaluer un rollback**
- **Vérifier la disponibilité des données et prendre contact avec le service d'hebergement d'AMAZON**
- **Vérifier qui était d'astreinte ce WE (surement Pierre)**
- **Communiquer aux équipes internes**
- **Préparer beaucoup de café**

Une cellule de crise doit se constituer afin de gérer la situation dans le temps et la complexité en laissant les équipes techniques répondent aux questions.

Il n'y a pas bonnes ou de mauvaises réponses quant à la situation, le pragmatisme doit prédominer sur l'instinct et les actions portées par des émotions trop fortes comme la rage ou l'inscription à cours de MMA.

Vous doutez de la reconversion de Pierre chez amazon et vous envisagez plutôt quelque chose dans la culture du chanvre sur l'altiplano : Ceci ne fait aucun doute dans votre esprit au moment de la réunion de lundi à 23h00 avec la cellule de crise mais le café est bon.