|  |  |  |
| --- | --- | --- |
| F:\BTS cours\portfolio\logoIMC.jpg | **BTS SIO****Services Informatiques aux Organisations** | F:\BTS cours\portfolio\logolaposte.jpg |
| **Option** | **SISR** |
| **Session** | **2015** |

|  |  |  |
| --- | --- | --- |
| **Costes Antoine** | **Activité professionnelle N°** |  |

|  |  |
| --- | --- |
| **NATURE DE L'ACTIVITE** | Procédure de décontamination d’une machine |
| **Contexte**  | En cas de pollution du système informatique, d’une machine infesté par des virus |
| **Objectifs**  | Retirer les virus d’un ordinateur |
| **Lieu de réalisation** | DSEM – ATM Vaugirard, Paris |

|  |
| --- |
| **SOLUTIONS ENVISAGEABLES** |
| Formater le disque dur et réinstaller Windows |

|  |
| --- |
| **DESCRIPTION DE LA SOLUTION RETENUE** |
| **Conditions initiales** | Anti-virus non à jour et machine infecté |
| **Conditions finales** | Mis à jour de l’antivirus et machine nettoyer  |
| **Outils utilisés**  | Anti-virus, Anti-malware |

|  |
| --- |
| **CONDITIONS DE REALISATION** |
| **Matériels**  | Clef USB, machine |
| **Logiciels**  | Windows defenderMcaffeeMicrosoft Safety ScannerAnti malwarebit |
| **Durée** | 5 heures |
| **Contraintes**  | Le pc ne doit pas etre mis en réseaux afin d’éviter toute propagation des virus. |

|  |
| --- |
| **COMPETENCES MISES EN OEUVRE POUR CETTE ACTIVITE PROFESSIONNELLE**  |
| A1.1.1 A2.2.1 A2.2.2 A2.2.3 A2.3.1 A3.2.2  | Prise en charge d’incidents et de demandes d’assistance liés au domaine de spécialité du candidat Elaboration de documents relatifs à la production et à la fourniture de servicesAnalyse du cahier des charges d'un service à produireSuivi et résolution d'incidents Suivi et réponse à des demandes d'assistance Réponse à une interruption de service Identification, qualification et évaluation d'un problème Remplacement ou mise à jour d'éléments défectueux ou obsolètes |
| **DEROULEMENT DE L'ACTIVITE** |
| **Les différents types de virus :****Virus Classique**(Synonymes: Virus informatique, Programme malicieux, Virus classique) :Un virus est un programme ou un code capable d'infiltrer des systèmes, disques ou fichiersindividuels sans que l'utilisateur soit au courant ou consentant. Une fois que le virus a atteintsa cible, la suite des évènements dépend du type de virus mais peut comporter :· Une réplication uniquement sur le système infecté donné· Infection d'autres fichiers lors de leur ouverture ou de leur création· Suppression ou corruption des données dans les fichiers/systèmes hôtes· La consommation de ressources sans causer de dommages directsAujourd'hui le terme de virus désigne les virus classiques et, est un terme génériquepour les programmes malicieux comprenant les virus, les trojans etc.**Chevaux de Troie** (Trojans, Troyens) :Les chevaux de Troie ou trojans sont des programmes malicieux qui endommagent le systèmehôte lors de leur installation. La différence principale entre les virus, les vers et les chevaux deTroie est que ces derniers ne se dupliquent pas.Ils ont été dénommés ainsi car de la même façon que les grecs ont utilisé un chevalapparemment innocent pour conquérir Troie, le premier cheval de Troie électroniqueprétendait être un jeu ou une application innocente, alors qu'il endommageait l'ordinateur hôteaprès son installation.Aujourd'hui les Trojans sont programmés pour être installer de manière invisible et mener desactions destructrices y compris la corruption de l'ordinateur hôte, de manière invisible làaussi.Les chevaux de Troie sont divisés en plusieurs sous-classes englobant les backdoors, leslogiciels espions, les droppers, downloaders et bien d'autres encore.**Phishing :**Forme de cyber crime et/ou fraude reposant sur des techniques de social engineering. Le nomest la fusion de 'fishing' qui veut dire pêche, et 'phreaking' qui désigne le piratage de lignestéléphoniques.Le criminel crée de toutes pièces une réplique parfaite d'une institution financière ou d'un siteweb commercial. Le criminel va ensuite à la ' pêche ' : une lettre est envoyée sous forme despam dont l'adresse est faussée afin d'imiter une vraie correspondance en provenance del'institution commerciale ciblée. Les phishers utilisent de vrais logos, un style correct decorrespondance d'affaires et des noms appartenant pour de vrai aux cadres exécutifs.Dans tous les cas, toutes ces lettres poursuivent le même objectif : duper le client et le fairecliquer sur le lien contenu dans la lettre. Les liens fournis par les phishers conduisentdirectement les utilisateurs à une imitation du site web ou le ' poisson ' malchanceux procède àla confirmation de ses données personnelles et bancaires.**Keylogger**(Keystroke logger) :Utilisé par un cyber-criminel pour obtenir des données confidentielles (compte d'utilisateurs,numéros de cartes bancaires, mots de passe etc.) en interceptant les frappes au clavier. LesBackdoor Trojans (Trojans de porte dérobée) sont généralement dotés d'un keylogger intégré;les données personnelles interceptées sont transmises au malfaiteur à distance et peuvent êtreexploitées pour obtenir de l'argent illégalement, ou un accès non autorisé à un réseau.**Virus furtif :**Les virus furtifs tentent de duper les scanners antivirus en présentant des données saines lorsde l'analyse antivirus. Certains de ces virus exposent une version saine du fichier infecté lorsdu scanning. D'autres virus furtifs cachent la nouvelle taille du fichier infecté et expose lataille du fichier avant infection.**Blacklists** (Listes noires) :En référence au spam, les listes noires sont des listes de sources connues de spams :· spammeurs· adresses connues expéditrices de spams· ISP spammeurs· relais ouvertsLes blacklists sont une des méthodes employées par les filtres anti-spams pour bloquer lesspams. Plusieurs blacklists open source (au code source libre) sont accessibles au public et lesinternautes peuvent ajouter des informations sur la blacklist locale.L'aide apportée par les blacklists oblige les ISP (Internet Service Provider) à contrôler leurcourrier sortant : si un ISP est mis sur blacklist, alors tous les emails en sa provenance serontretournés, ce qui peut entraîner de sérieuses pertes financières.**Vulnérabilité** (Faille, Brèche) :Une vulnérabilité (universelle) est un état dans un système informatique (ou ensemble desystèmes) qui peut soit :· Autoriser un attaquant à exécuter des commandes au même titre qu'un utilisateur· Autoriser un attaquant à accéder à des données contrairement aux règles restrictivesd'accès à ces données· Autoriser un attaquant à masquer son identité· Autoriser un attaquant à mener une attaque par déni de serviceLes hackers et auteurs de virus exploitent régulièrement les vulnérabilités pour collecter desdonnées confidentielles afin de prendre le contrôle des machines victimes pour un usageillicite ultérieur.**Relais ouvert** (Open relay) :Un relais ouvert désigne les serveurs de messagerie qui autorisent le passage de mails venantd'utilisateurs non admis. Ce que ne font pas la plupart des serveurs de messagerie et dessociétés qui sont au fait des risques de sécurité encourus.Malheureusement il y a toujours suffisamment de serveurs relais ouverts sur l'Internet pourque les spammeurs et hackers les utilisent pour envoyer du malware et du spam.**Rootkits :** Chargés d'écraser la plupart des outils du système et de les remplacer par des commandes équivalentes masquant la présence du pirate. il est rare que le pirate parvienne à compromettre un système du premier coup. Il agit la plupart du temps par tâtonnement, en essayant différentes requêtes.Ainsi la surveillance des journaux permet de détecter une activité suspecte. Il est en particulier important de surveiller les journaux d'activité des dispositifs de protection car tout aussi bien configuré qu’il soi, il se peut qu'ils soient un jour la cible d'une attaque.**Le SPAM :**Le spam est un email anonyme, indésirable et envoyé en masse. C'est la description basique utilisée à l'heure actuelle aux Etats-Unis et en Europe pour instaurer une législation anti-spam. Examinons de plus près les termes de cette définition :· Anonyme: le vrai spam est envoyé sous des adresses volées à l'insu d'utilisateurs tierspour masquer le véritable expéditeur.· Mailing de Masse: le vrai spam est envoyé en très grand quantité. Les spammeurs fontde l'argent grâce au petit pourcentage de réponses. Pour que le spam soit rentable, lemail initial doit être envoyé en masse.· Indésirable: les listes de mailing, newsletters et autres matériels publicitaires auxquelsles internautes ont souscrits, peuvent ressembler à des spams mais sont en fait desemails légitimes. En d'autres termes, un mail peut être considéré comme spam oucomme mail légitime selon que l'utilisateur ait choisi de le recevoir ou non.Remarquez bien que le mot publicité n'est pas employé pour définir le spam. De nombreuxspams ne sont pas de la publicité. En plus de vanter des produits et des services, le spam peutappartenir aux catégories suivantes :· Messages politiques· Appels à la charité· Arnaques financières· Chaînes de courriels· Faux spam destiné à distribuer des logiciels malveillants**Plusieurs façons afin d’éviter les Spams :**1. Avoir aux moins 2 adresses emails. Une adresse privée uniquement pour votre correspondance personnelle. L'autre adresse pour vous inscrire aux forums, salles de discussion (chat rooms), listes de mailing etc. N'indiquez jamais votre adresse privée sur des ressources accessibles par le grand public.
2. L’adresse privée doit être difficile à usurper. Les spammeurs utilisent des combinaisons de noms évidents, mots et numéros pour reconstituer des adresses existantes. Votre adresse privée ne doit pas se composer uniquement de votre nom et prénom.
3. Si vous devez publier votre adresse privée sur le Net, masquez-la pour éviter que les spammeurs ne se jettent dessus. Exemple : Paul.Durand@yahoo.com : Paul point Durand arobase yahoo point com. Si vous avez besoin de publier votre adresse privée sur un site web, faites le sous forme de fichier graphique plutôt que sous forme de lien.
4. Considérez votre adresse publique comme temporaire. Il y a de grandes chances que les spammeurs s'en emparent à un moment ou à un autre. N'hésitez pas à en changer souvent.
5. Utilisez toujours votre adresse publique pour vous enregistrer sur les forums, les salles de discussion (chat rooms) et pour vous inscrire aux listes de mailings et promotions. Il est aussi judicieux d'utiliser plusieurs adresses publiques afin de déterminer quels sont les services qui vendent vos adresses aux spammeurs.
6. Ne répondez jamais à un spam. La plupart des spammeurs vérifient les accusés de réception et les réponses loggées. Plus vous répondez, plus vous recevrez de spams.
7. Ne cliquez jamais sur des liens pour annuler l'inscription. Les spammeurs envoient de faux messages pour soi-disant annuler l'inscription afin d'obtenir la liste des adresses active. Il ne faut surtout pas que les spammeurs détectent votre adresse comme active car cela ne fera qu'augmenter le nombre de spams.
8. Si votre adresse privée est découverte par des spammeurs – changez-la, modifier son adresse email est un bon moyen pour éviter les spams.
9. Assurez-vous que votre courriel est filtré par une solution antispam. Pensez à installer une solution antispam personnelle. Ouvrez des comptes de messagerie uniquement par le biais de fournisseurs offrant un filtrage antispam du courriel entrant.

**Méthodes courantes infections :*** Surf sur un site internet infecté par des scripts malveillants qui tentent d’exploiter une vulnérabilité du poste de travail le WE ou le soir à la maison avec le portable connecté en WIFI, les évènements seront remontés dès que le poste sera branché sur le réseau de La Poste.
* Clé USB personnelle infectée et ayant pas mal circulé insérée sur un poste de travail : bien souvent le virus va tenter par le principe d’Autorun de s’installer sur la machine, l’antivirus va détecter et bloquer les écritures mais remonter de nombreux évènements au serveur EPO, ce qui va alerter sur cette machine en particulier.
* Téléchargements et Utilisation de programmes freeware et autres non validés par La Poste : même les outils qui semblent anodins font désormais l’objet de détections et d’analyse de produits illicites (accès distant, scans réseau, mots de passe, etc…)

**Procédure Anti-pollution :**L’administrateur des réseaux est prévenu de la préséance d’un virus sur un ordinateur par mail (paramétrable dans l’antivirus.Pour toutes les interventions, il faut être administrateur du poste. L’utilisation de périphérique de stockage tel que la clé USB nécessite de la rigueur. Il faut toujours s’assurer que ce matériel utilisé est sain d’où l’intérêt de le scanner à partir d’un poste isolé et à jour de son antivirus.Ce matériel possède un mécanisme appelé Autorun permettant d’automatiser le lancement de certains programmes lors de son insertion. Cet Autorun est potentiellement dangereux, en effet, il peut être utilisé pour exécuter des programmes malveillants lors de la connexion du périphérique.Il existe une façon simple d’empêcher son activation : Maintenir la touche « Shift » (Majuscule) enfoncée avant la connexion du périphérique et jusqu’à son apparition dans l’explorateur. Ensuite, il est conseillé de faire une « Recherche des menaces, … » par un click droit sur le dossier de la clé USB avant toute utilisation.L’utilisation de clé USB avec protection en écriture est fortement recommandée pour copier des fichiers (mise à jour par exemple) vers la station infectée, cela évitera tout risque d’infection de votre support amovible.Si toutefois la station infectée ne démarre pas, il faut utiliser soit un CD soit une clé USB de boot avec l’Antivirus. Avant chaque intervention, il est conseillé de se munir d’un support dédié Antipollution à jour (clé USB,…) sur lequel il y aura tous les produits et outils d’aide à la désinfection (anti-malware, anti-virus)L’opération de vérification est faite à partir d’un scan complet de la machine qui doit être déconnectée du réseau.**Microsoft Safety Scanner :**L'application "Microsoft Safety Scanner" est un outil de sécurité gratuit téléchargeable qui offre des scans sur demande et d’aide à éliminer les virus, logiciels espions et autres logiciels malveillants. Il fonctionne avec votre logiciel antivirus existant et est mis à jour par Microsoft 3 fois par jour.Exécution en mode commande : Ouvrir un invite de commande, puis lancer la commande « msert.exe /N /F » L’utilisation de l’outil en ligne de commande permet d’optimiser le scan, en effet, il est préconisé d’utiliser les options « /N /F » pour que le scan puisse détecter et localiser la souche virale afin que cette dernière soit soumise à l’éditeur d’antivirus.(pour être plus facilement identifiable à l'avenir)Autres commandes:/Q ou /quiet : Utiliser le mode silencieux. Cette option supprime l'interface utilisateur de l'outil./? Ou help : Afficher une boîte de dialogue qui répertorie les commutateurs de ligne de commande./N : Exécuter en mode détection seule. Dans ce mode, les logiciels malveillants seront signalés àl'utilisateur mais ne seront pas supprimés./F : Forcer une analyse complète de l'ordinateur./F:Y : Forcer une analyse complète de l'ordinateur et nettoie automatiquement d'éventuellesinfections./H: Détecte uniquement les menaces élevées et graves**Identifier et récupérer une souche virale :**La récupération du fichier souche est nécessaire uniquement dans les cas suivants :- Le fichier ou la clé de registre ont été supprimés mais réapparaissent- Dans le journal, la suppression aura lieu au prochain redémarrageQuelques soit l’analyse (McAfee ou Microsoft), la souche virale doit être envoyée uniquement dans les cas où celle-ci n’est pas nettoyée et n’est pas supprimée. Pour cela bien vérifier les résultats de chaque analyse dans chaque journal de logs.Journal de logs: gestionnaire de mis en quarantaine pour voir le ou les virus qui ont été mis en quarantaine avant d’être supprimé(s) ou nettoyé(s) à la date du scan ou Afficher le fichier journal commun a beaucoup d’antivirus. |

|  |
| --- |
| **CONCLUSION** |
| TOP 3 Antivirus gratuit : Antivir Free Edition, Avast home et AVG |

|  |
| --- |
| **EVOLUTION POSSIBLE** |
| / |