OBVIOUS CHOICE

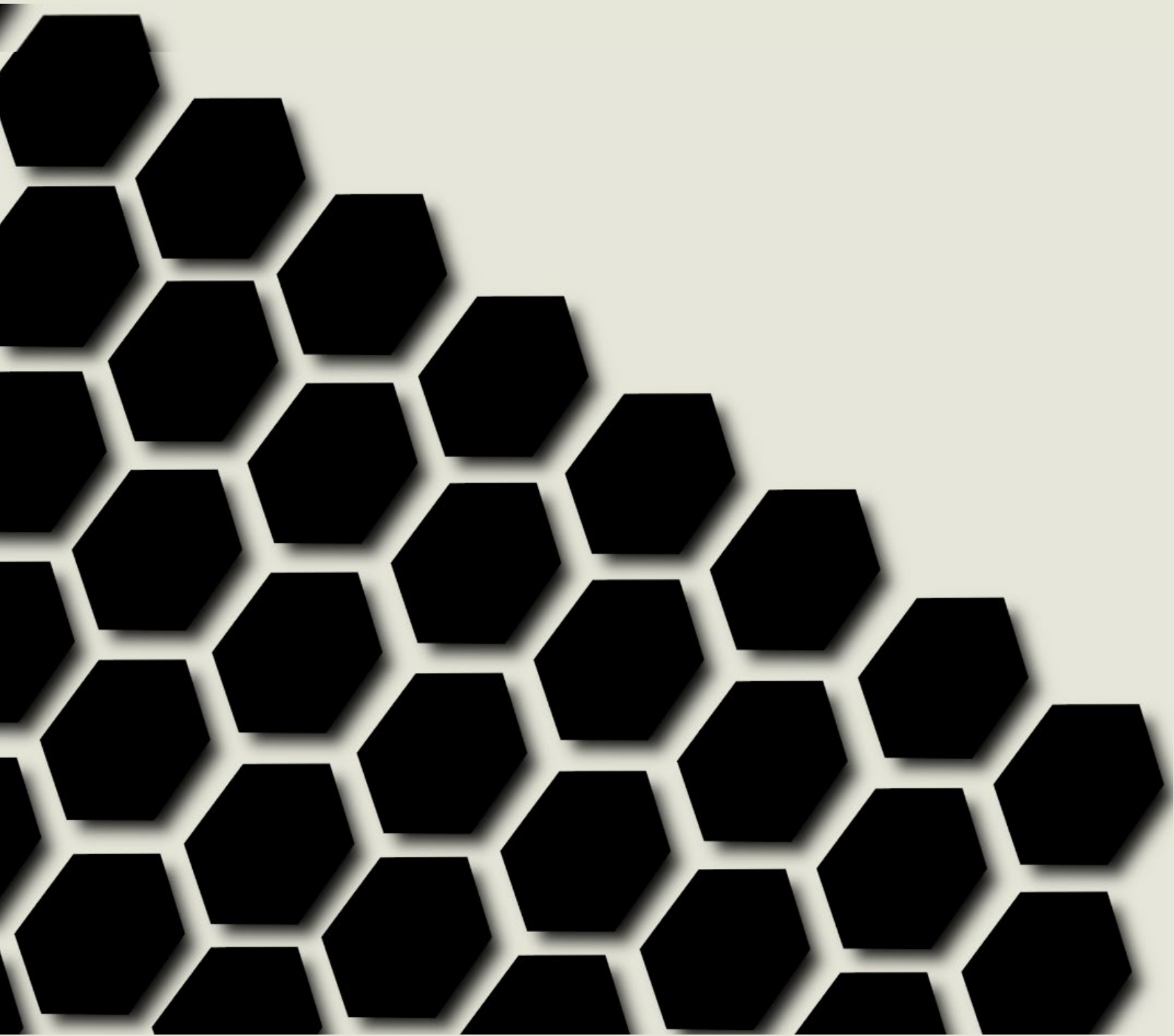

TABLE DES MATIERES

THREATS & DEFENSES

https://www.youtube.com/watch?v=11M6wXZvTa0

THREATS

Définition

Cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

Source : Norme ISO 27 000)

MALWARES

Définition

Logiciel malveillant conçu spécifiquement pour endommager ou interrompre un système, attaquer la confidentialité, l'intégrité et/ou la disponibilité.

Source : Norme ISO 27 033

Un malware, ou « logiciel malveillant » est un terme générique qui décrit tous les programmes ou codes malveillants qui peuvent être nocifs pour les systèmes.

Hostiles, intrusifs et intentionnellement méchants, les malwares cherchent à envahir, endommager ou mettre hors service les ordinateurs, les systèmes informatiques, les tablettes ou les appareils mobiles, généralement en prenant le contrôle partiel de leurs opérations. Comme la grippe, ils interfèrent avec le fonctionnement normal.

L'objectif des malwares est de vous soutirer de l'argent illégalement. Bien que les malwares ne puissent pas endommager physiquement vos systèmes ou vos réseaux (à une exception près : voir la section Google Android ci-dessous), ils peuvent voler, crypter ou supprimer vos données, modifier ou pirater les fonctions informatiques principales, et espionner les activités de votre ordinateur sans que vous le sachiez ou l'autorisiez.

Source : Malwarebytes

Les types de malware

Trojan / Cheval de Troie

Programme apparemment inoffensif contenant un logiciel malveillant qui permet la collecte, la falsification ou la destruction non autorisées de données.

Source : Norme ISO 2382

https://www.youtube.com/watch?v=LSgk7ctw1HY

Ransomware / Rançongiciel

Les rançongiciels (ransomwares en anglais) sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore à la suite d'une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

Source : Cybermalveillance.gouv.fr

https://www.youtube.com/watch?v=P3hH7ryVZdg

Worms / Vers

Programme autonome qui peut se propager au travers des systèmes de traitement de données ou des réseaux informatiques.

Source : Norme ISO 2382

Virus

Logiciel malveillant qui se propage en modifiant des programmes pour inclure une copie éventuellement modifiée de lui-même et qui est exécuté lorsque le programme infecté est exécuté.

L'objectif d'un virus est de nuire en causant des dommages sur le SI.

Source : Norme ISO 2382

Adware / Logiciel publicitaire

Application qui envoie de la publicité aux utilisateurs et/ou recueille le comportement en ligne des utilisateurs.
L'application peut ou non être installée avec la connaissance ou le consentement de l'utilisateur ou imposée à l'utilisateur via des conditions de licence pour d'autres logiciel. Source : Norme ISO 27 032

Spyware / Logiciel espion

Logiciel espion qui collecte des informations privées ou confidentielles auprès d'un utilisateur.

Les informations peuvent inclure des sujets tels que les sites Web les plus fréquemment visités ou des informations plus sensibles telles que les mots de passe.

Source : Norme ISO 27 032

Spyware. Ce mot évoque un gadget tout droit sorti d'un James Bond, mais il s'agit en fait d'un terme générique désignant un logiciel malveillant qui infecte votre PC ou appareil mobile et qui collecte des informations vous concernant, vos habitudes de navigation et d'utilisation d'Internet ainsi que d'autres données.

Pas de surprise : les spywares sont sournois. Généralement, ils accèdent à votre ordinateur sans que vous vous en rendiez compte et sans votre autorisation, puis ils s'installent sur votre système d'exploitation pour maintenir une présence sur votre PC. Vous avez peut-être même, involontairement, autorisé l'installation d'un spyware en acceptant les conditions générales d'un programme en apparence légitime que vous avez téléchargé, sans prendre la peine de lire les petits caractères.

Mais peu importe la technique d'invasion des spywares, ils s'exécutent discrètement en arrière-plan, collectent des informations ou surveillent vos activités afin de déclencher des activités malveillantes liées à votre ordinateur et la façon dont vous l'utilisez. Ces activités incluent notamment l'enregistrement de vos saisies, de vos identifiants, de vos adresses e-mail personnelles, de données de formulaires Web, d'informations concernant l'utilisation d'Internet et d'autres informations personnelles telles que des numéros de cartes de crédit, ainsi que des captures d'écran.

Source : Malwarebytes

Macro-malware / Macrovirus

Les virus macro ajoutent leur code aux macros associées à des documents, feuilles de calcul et autres fichiers de données.

Source : Kaspersky

Keylogger / Enregistreur de frappe

L'enregistrement de frappe consiste à surveiller toutes les frappes effectuées sur un clavier d'ordinateur, souvent sans la permission de l'utilisateur ou à son insu. Un enregistreur de frappe peut être un composant matériel ou logiciel. S'il constitue un outil légitime de surveillance informatique personnelle ou professionnelle, il peut toutefois également être utilisé à des fins criminelles. Le plus souvent, l'enregistreur de frappe prend la forme d'un logiciel espion malveillant utilisé pour enregistrer des informations sensibles, telles que mots de passe ou données financières, qui sont ensuite transmises à des tiers pour être exploitées à des fins criminelles.

Source : Kaspersky

DEMO

Rootkit

Un rootkit est un terme anglais qui désigne un type de malware conçu pour infecter un PC et qui permet au pirate d'installer une série d'outils qui lui permettent d'accéder à distance à un ordinateur. Le malware sera habituellement bien caché dans le système d'exploitation et ne sera pas détecté par les logiciels anti-virus et autres outils de sécurité. Le rootkit peut contenir de nombreux outils malicieux tels qu'un enregistreur de frappe, un programme de capture de mots de passe, un module pour voler les informations de cartes et de comptes bancaires en ligne, un robot afin de mener des attaques DDoS ou possédant des fonctionnalités capables de désactiver les logiciels de sécurité. Les rootkits agissent typiquement comme une porte dérobée qui permet au pirate de se connecter à distance à l'ordinateur infecté quand il le souhaite ainsi que d'installer ou de supprimer des components spécifiques.

Source : Kaspersky

Scareware

Un scareware est un logiciel malveillant qui trompe les utilisateurs pour les amener à visiter des sites Web infestés de programmes malveillants. Également connus sous les noms de rogues ou logiciels de sécurité non autorisés, les scarewares peuvent prendre la forme de fenêtres contextuelles. Ces fenêtres qui ressemblent à des avertissements légitimes d'éditeurs de logiciels antivirus prétendent que les fichiers de votre ordinateur ont été infectés. Leur présentation est si convaincante que les utilisateurs inquiets se laissent persuader d'acheter un logiciel payant pour résoudre un problème fictif. En réalité, ils téléchargent un faux logiciel antivirus qui n'est autre qu'un programme malveillant destiné à voler les données personnelles de la victime.

Pour distribuer leurs scarewares, les cyber-criminels recourent également à d'autres techniques telles que l'envoi de courriers indésirables. Une fois le message ouvert, la victime est incitée à acheter des services totalement inutiles. Selon Kaspersky Lab, tomber dans le piège de ces escroqueries et transmettre ses informations de carte de crédit ouvre la porte à d'autres méfaits relevant de l'usurpation d'identité.

Source : Kaspersky

Others

Backdoor / Portes dérobées

Le principe de la mise en œuvre d'une « Backdoor » ou porte dérobée correspond à prévoir un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel. Le principe de la mise en œuvre d'une « Master Key » ou « clé maître » correspond à prévoir ouvertement un tel accès, mis en œuvre via cette clé, aux données chiffrées contenues dans un logiciel ou sur un matériel.

Source : CNIL

Exploit

Méthode définie d'outrepasser la sécurité des systèmes d'information par la vulnérabilité.

Sources : Norme ISO 27 039

DDoS

Les attaques contre les réseaux distribués sont également appelées attaques DDoS (Distributed Denial of Service, déni de service distribué). Ce type d'attaque tire profit des limites de capacité spécifiques qui s'appliquent aux ressources d'un réseau, comme l'infrastructure qui prend en charge le site Internet d'une entreprise. Une attaque DDoS consiste à envoyer de multiples requêtes à la ressource Web attaquée dans le but d'entraver la capacité du site Internet à gérer les requêtes et bloquer son fonctionnement.

Source : Kaspersky

Phishing / Hameçonnage

Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations à la suite d'un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).

Source : CNIL

SPAM

Le spam, également appelé courrier électronique commercial non sollicité (UCE, Unsolicited Commercial Email) ou courrier indésirable, correspond à des annonces publicitaires douteuses, non sollicitées et envoyées en masse.

À son apogée, le spam composait 92 % de l'ensemble du trafic de messagerie électronique et malgré tout sa plus grande partie n'avait rien de malveillant. Les spammeurs peuvent acheter des listes de destinataires en toute légalité, mais récupèrent en général les adresses de messagerie accessibles au public via la technique dite du « Web scraping » (technique d'extraction du contenu de sites Web). Ils peuvent aussi générer des listes de contacts en permutant certains noms et domaines, par exemple prenoma@gmail.com ou prenomb@gmail.com.

Comme le succès d'une opération de spam dépend de son volume, les auteurs génèrent et envoient le même message (via le système) à toute la liste de contacts qu'ils ont dressée dans l'espoir qu'une personne cliquera. Les spammeurs ajoutent parfois aux messages des phrases ou des mots générés aléatoirement afin de modifier l'aspect de chacun d'eux et de leurrer les filtres de messagerie automatiques.

Le contenu du message lui-même fait généralement la promotion d'un produit ou d'un service, et fournit au destinataire les coordonnées de contact qui lui permettent de commander.

Source : Proofpoint

SQL INJECTION

Une injection SQL est une forme de cyberattaque lors de laquelle un pirate utilise un morceau de code SQL (« Structured Query Language », langage de requête structurée) pour manipuler une base de données et accéder à des informations potentiellement importantes.

C'est l'un des types d'attaques les plus répandus et menaçants, car il peut potentiellement être utilisé pour nuire à n'importe quelle application Web ou n'importe quel site Web qui utilise une base de données SQL.

Les attaques majeures contre Sony Pictures et Microsoft sont des exemples frappants parmi d'autres.

Source : Kaspersky

Payload

Dans le cadre d'une cyber-attaque, le payload malveillant est le composant de l'attaque qui cause un préjudice à la victime. À la manière des soldats grecs dissimulés à l'intérieur du cheval de Troie, un payload malveillant peut demeurer inoffensif pendant un certain temps jusqu'à ce qu'il soit déclenché.

Source : Cloudflare

Botnet

« Botnet » est une contraction des termes « robot » et « network » (réseau). Les cyber-criminels utilisent des chevaux de Troie spéciaux pour violer la sécurité des ordinateurs de différents utilisateurs, prendre le contrôle de chacun de ces ordinateurs infectés et les regrouper au sein d'un réseau de « bots » gérables à distance.

Source : Kaspersky