sécurité de précision
SERENICITY

Glossaire Cyber

Adresse IP La communication sur l'internet est fondée sur un protocole appelé IP pour Internet Protocol qui permet aux ordinateurs de communiquer entre eux. Ce protocole utilise des adresses numériques pour distinguer ces machines et tronçonne la communication en paquets comportant chacun une adresse de source et une adresse de destination.
La version la plus couramment employée du protocole est la version IPv4 dans laquelle les adresses sont composées de 4 nombres par exemple 213.56.176.2.
Une nouvelle version du protocole est en cours de déploiement : IPv6. Elle utilise des adresses plus longues composées de 8 nombres notés en hexadécimal par exemple 1 fff:0000:0a88:85a3:0000:0000:ac1f:8001.
Enfin IPsec désigne un protocole de chiffrement et de signature des paquets IP.

Backdoor (porte dérobée) Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive. Une porte dérobée peut également être la cause d'une mise en œuvre incorrecte d'un protocole.

Botnet (contraction de réseau de robots) : C'est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise.
Certains ensembles peuvent atteindre des nombres considérables de machines (plusieurs milliers). Celles-ci peuvent faire l'objet de commerce illicite ou d'actions malveillantes contre d'autres machines. Elles sont souvent pilotées par des commandes lancées à travers un canal de contrôle comme le service IRC (Internet Relay Chat).

Cheval de Troie (Trojan Horse) : Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante.
La fonction cachée exploite parfois les autorisations légitimes d'une entité du système qui invoque ce programme. Elle peut par exemple permettre la collecte frauduleuse, la falsification ou la destruction de données.

Cybercriminalité : Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberdéfense : Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Firewall (Pare-feu) : Un pare-feu (ou garde-barrière), est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

Hacker (pirate informatique) : Personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique.

Hameçonnage ciblé (spearphishing) : Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée. Généralement, le courriel usurpe l'identité d'une personne morale (établissement financier, service public, concurrent…) ou d'une personne physique (collègue de travail, famille, ami…) dans le but de duper le destinataire qu'il invite à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette première machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation constituant la véritable cible (on parle ici « d'infiltration »).Une fois sa première victime compromise, l'attaquant cherchera à obtenir des droits « d'administrateur » (on parle alors « d'escalade de privilèges ») pour pouvoir rebondir et s'implanter sur les postes de travail et les serveurs de l'organisation où sont stockées les informations convoitées. Cette manœuvre est également appelée « propagation latérale ». Une fois ses cibles atteintes, il recherchera les informations qu'il s'efforcera de capter le plus discrètement possible (on parle alors ici « d'exfiltration ») soit en une seule fois, en profitant d'une période de moindre surveillance du système (la nuit, durant les vacances scolaires, lors d'un pont…), soit de manière progressive plus insidieuse. Il prend généralement soin de toujours effacer derrière lui toute trace de son activité malveillante.

Hameçonnage, filoutage (Phishing) Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.
Les sites sont reproduits, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.

Homme-au-milieu, entre-deux (Man-in-the-Middle, MITM) : Catégorie d'attaque où une personne malveillante s'interpose dans un échange de manière transparente pour les utilisateurs ou les systèmes. Remarques : La connexion est maintenue, soit en substituant les éléments transférés, soit en les réinjectant. Une attaque connue dans cette catégorie repose sur une compromission des tables ARP (ARP Poisoning). Contrer les attaques par le milieu est aussi l'un des objectifs des infrastructures de gestion de clés

Intrusion : L'intrusion est le fait, pour une personne ou un objet, de pénétrer dans un espace (physique, logique, relationnel) défini où sa présence n'est pas souhaitée.

Poste-à-poste (Peer-to-Peer, P2P) Réseau d'échange et de partage de fichiers de particulier à particulier (exemples : e-mule, kasaa, limewire, eDonkey).

Rançongiciel (Ransomware) : Forme d'extorsion imposée par un code malveillant sur un utilisateur du système.
C'est est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon.
Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données (fichiers clients, comptabilité, factures, devis, plans, photographies, messages, etc.), par exemple en les chiffrant, puis lui indiquer les instructions utiles au paiement de la rançon.
Lorsqu'un rançongiciel infecte un poste de travail, le plus souvent (mais pas nécessairement) par l'envoi d'un courrier électronique piégé, l'infection est dès lors susceptible de s'étendre au reste du système d'information (serveurs, ordinateurs, téléphonie, systèmes industriels, etc.).

Test d'intrusion (Penetration Test) : Action qui consiste à essayer plusieurs codes d'exploitation sur un système d'information, afin de déterminer ceux qui donnent des résultats positifs. Il s'agit à la fois d'une intention défensive (mieux se protéger) et d'une action offensive (agresser son propre système d'information).

Ver (Worm) : Logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis à l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. Les deux termes ver et virus sont relativement proches. Un ver est un virus qui se propage de manière quasi autonome (sans intervention humaine directe) via le réseau. Les vers sont donc une sous-catégorie de virus, dont le vecteur primaire de propagation reste le réseau.

Virus : Un virus est un programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes : réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc. Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB…

Voix sur réseau IP (VoIP Voice over Internet Protocol) : Technologie qui permet de véhiculer la voix sur l'Internet ou tout autre réseau acceptant le protocole TCP/IP. Cette technologie est notamment utilisée par le service de téléphonie IP (ToIP – telephony over internet protocol) à travers des logiciels tels que Skype, Asterisk…

Vulnérabilité (Vulnerability) : Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

Spyware Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.

IDS (Système de détection des intrusion) / IPS (Système de prévention des intrusions) : Les IDS analysent le trafic réseau pour détecter des signatures correspondant à des cyberattaques connues. Les IPS analysent également les paquets, mais ils peuvent aussi les bloquer en fonction du type d'attaques qu'ils détectent, ce qui contribue à stopper ces attaques. Les IDS/IPS comparent les paquets de réseau à une base de données de cybermenaces contenant des signatures connues de cyberattaques et repèrent tous les paquets qui concordent avec ces signatures.

La principale différence entre les deux tient au fait que l'IDS est un système de surveillance, alors que l'IPS est un système de contrôle.

SIEM (Security Information and Event Management) : Gestion des informations et des événements de sécurité. On peut définir le SIEM comme la collecte d'événements en temps réel, la surveillance, la corrélation et l'analyse des événements à travers des sources disparates.

Source : ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information

https://www.ssi.gouv.fr/entreprise/glossaire/c/