Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 21 avril 2006
N° CERTA-2006-INF-002

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Terminologie d'usage au CERTA

Gestion du document

Référence	CERTA-2006-INF-002
Titre	Terminologie d'usage au CERTA
Date de la première version	20 février 2006
Date de la dernière version	21 avril 2006
Source(s)	Voir Documentation
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Table des matières

1 Introduction

Plusieurs phénomènes malveillants sont découverts, analysés, listés ou simplement repertoriés chaque jour. Dans la majorité des cas, il s'agit de la manifestation d'un *code malveillant*, traduction choisie du terme anglais *malware* (pour *malicious software*), ou de *virus*, *vers* et autres *bombes logiques*.

De manière générale, de nombreux termes sont utilisés par les professionnels de la sécurité informatique, et relayés par les médias pour qualifier les malveillances observables sur l'Internet. Leurs usages se banalisent alors,

mais contribuent parfois à obscurcir davantage leur définition originelle. Ce document n'a nullement la prétention de remplacer leurs diverses définitions, mais bien de signaler au lecteur celles qui sont employées au sein du CERTA. Elles servent de références à l'ensemble des notes et documents rédigés par l'équipe de réponse aux incidents.

Nous énumérons ci-dessous et dans l'ordre lexicographique un ensemble de termes. Il s'agit pour la majorité d'entre eux d'activités malveillantes, nommées en fonction des principes de leur *modus operandi*. Cette liste n'est pas exhaustive et sera régulièrement mise à jour. Nous mentionnons également leurs équivalents en anglais, dans la mesure où les expressions anglophones apparaissent dans de nombreuses publications.

2 Définitions existantes

Comme il est précisé ci-dessus, cette note n'a pas pour objectif de redéfinir les termes. Elle s'appuie sur l'existant (documents officiels, articles spécialisés), auquel il est fait référence autant qu'il est possible. Ce glossaire reprend ainsi quelques termes publiés au Journal Officiel par la commission générale de terminologie et de néologie, en application du décret 96602 du 3 juillet 1996 relatif à l'enrichissement de la langue française [GOUV96, JO00, JO05]. Il s'inspire également de rapports de recherche publiés ces dernières années ([KIEN03, WEA03, CLUS06, RFC]), et de discussions tenues dans le cadre de certaines listes de sécurité [FRCO06].

3 Définitions

Accaparement de noms de domaine / *Cybersquatting*, *Domain Name Grabbing*

- *Définition :* Action malveillante qui consiste à faire enregistrer un nom de domaine dans le seul but de bloquer toute attribution ultérieure de ce nom au profit de titulaires plus *naturels* ou légitimes.
- *Remarques :* L'objectif est souvent d'obtenir un avantage financier en échange de la rétrocession du nom ainsi détourné. Cette pratique est particulièrement fréquente pour certains noms de domaine comme .net, .com, ou .org.
- *Voir aussi :* Chantage, Typosquatting.
- *Références :* Pour régler les litiges du *.fr* et du *.re*, se reporter à [PARL05].

Balayage de ports / *Port Scanning*

- *Définition :* Technique qui consiste à envoyer des paquets sur les différents ports d'une machine, puis à en déduire les états de ces ports en fonction de la réponse retournée, si elle existe.
- *Remarques :* Cette technique peut être utilisée pour découvrir les services fonctionnant sur la machine, en faisant une extrapolation entre les ports vus en l'état *ouvert*, et les services fonctionnant traditionnellement avec ce port. Les paquets peuvent être envoyés sur les ports linéairement, ou bien de manière plus discrète, en modifiant les temps d'envoi des paquets, en les envoyant dans un ordre aléatoire ou à partir de plusieurs adresses IPs.
- *Voir aussi :* Test d'intrusion,Porte dérobée
- *Références :* Note d'information du CERTA [CERTA16].

Bombardement de courriels / *Mail Bombing*

- *Définition :* Envoi d'une grande quantité de courriels à un destinataire unique dans une intention malveillante.
- *Remarques :* Forme particulière de déni de service contre les systèmes de courriers électroniques.
- *Voir aussi :* Déni de service, Spam.
- *Références :* Parution au Journal Officiel le 1er septembre 2000 [JO00]. Note d'information du CERTA [CERTA14].

Bombe programmée, Bombe logique / *Logic Bomb*

- *Définition :* Logiciel malveillant conçu pour causer des dommages à un système informatique et qui est déclenché lorsque certaines conditions sont réunies.

– *Remarques :* Certains virus contiennent une fonction de bombe logique : déclenchement à date fixe, déclenchement quand une adresse réticulaire (URL) particulière est renseignée dans le navigateur, etc.
– *Voir aussi :* Virus.
– *Références :* Parution au Journal Officiel le 20 mai 2005 [JO05].

Canal caché / *Covert Channel*

– *Définition :* Canal de communication qui permet à un processus malveillant de transférer des informations d'une manière dissimulée. Le canal caché assure une communication par l'exploitation d'un mécanisme qui n'est pas censé servir à la communication.
– *Remarques :* Les canaux cachés sont l'objet de nombreux travaux de recherche, tant pour les créer que pour les détecter [LAMP73, HAIG87, BERK05].
– *Voir aussi :* Réseau de Zombies.
– *Références :* Travaux de recherche [LAMP73, HAIG87, BERK05]. Notes d'information du CERTA [CERTA15, CERTA16].

Canular / *Hoax*

– *Définition :* Information vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables.
– *Remarques :* Il peut s'agir d'une fausse alerte aux virus, de propagande, chaîne de solidarité, pétitions, promesse de cadeaux, etc. Quelques canulars fréquents sont répertoriés sur des sites dédiés comme [HOAX06].
– *Voir aussi :* Pourriel, Polluriel.
– *Références :* Site [HOAX06]. Projet français Signal Spam [SPAM]. Reflexions sur la notion de rumeur proposées par P. Froissart dans [FROI02]. Note d'information du CERTA [CERTA03].

Capteur clavier, Enregistreur de frappes / *Keylogger*, *Keystroke Logger*

– *Définition :* Logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne frappe au clavier.
– *Remarques :* Cette technique permet de voler efficacement les mots de passe, les données bancaires, les messages électroniques, etc.
– *Voir aussi :* Logiciel espion, Cheval de Troie.
– *Références :* Recommandation du CERTA [CERTA17].

Chantage / *Ransomware*

– *Définition :* Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Si ce dernier refuse de payer ou d'effectuer une tâche imposée, le service auquel il veut accéder lui est refusé par le code malveillant.
– *Remarques :* On peut citer par exemple un code qui a chiffré des fichiers, et qui empêche alors l'utilisateur d'y accéder. Ce dernier reçoit également une note fournissant des indications de paiement (ou autre forme de chantage) afin de pouvoir récupérer les fichiers inutilisables en l'état.
– *Voir aussi :* code malveillant, Ingénierie sociale.
– *Références :* Article scientifique [YY96].

Cheval de Troie / *Trojan Horse*

– *Définition :* Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante.

– *Remarques :* 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. Une note théorique et une recommandation ont été publiées à ce sujet par le CERTA en 2001 et 2005 [CERTA01, CERTA02].
– *Voir aussi :* Porte dérobée.
– *Références :* Documents du CERTA [CERTA01, CERTA02]. Parution au Journal Officiel le 20 mai 2005 [THOM95].

Clonage de serveurs DNS / *DNS Pharming*

– *Définition :* Activité malveillante visant à modifier un serveur DNS, dans le but de rediriger un nom de domaine vers une adresse IP différente de l'adresse légitime.
– *Remarques :* Par conséquent, le trafic envoyé au domaine souhaité (organisme bancaire, messagerie électronique, etc) peut être capturé par un utilisateur malveillant, qui, par exemple, a déjà copié des pages du domaine visé à l'adresse nouvellement indiquée par le DNS. La personne qui se connecte au domaine risque alors d'entrer des informations confidentielles sur le site factice, même si elle a pris la précaution de renseigner l'adresse correcte.
– *Voir aussi :* Phishing.

Code d'exploitation / *Exploit*

– *Définition :* Tout ou partie d'un code permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes.
– *Remarques :* Les objectifs malveillants consistent souvent en une intrusion, une élévation de privilèges ou un déni de service. L'exploitation peut se faire directement à partir du système ciblé si l'utilisateur malveillant possède un accès physique (*local exploit*), ou à distance s'il s'y connecte (*remote exploit*).
– *Voir aussi :* Vulnérabilité.
– *Références :* Projet IST [MAFTIA].

Code malveillant,Logiciel malveillant / *Malicious Software*, *Malware*

– *Définition :* Tout code développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau.
– *Remarques :* Les virus ou les vers sont deux types de codes malveillants connus.
– *Voir aussi :* Virus, Ver.
– *Références :* Parution au Journal Officiel le 20 mai 2005 [JO05].

Homme-au-Milieu, Entredeux / *Man-in-the-Middle, MITM*

– *Définition :* Catégorie d'attaque où une personne malveillante s'interpose dans un échange, et 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*).
– *Voir aussi :* Situation de compétition.
– *Références :* Examples liés aux protocoles SSL/TLS dans la recommandation du CERTA [CERTA17].

Injection de code indirecte / *Cross Site Scripting*, CSS, XSS

– *Définition :* Activité malveillante qui consiste à injecter des données arbitraires dans le code de pages HTML. Un utilisateur malveillant peut faire afficher à un site web vulnérable un contenu aggressif ; ce contenu peut rediriger l'utilisateur vers d'autres sites, ou transmettre des informations (jetons de sessions, aussi appelés `cookies`, etc) ou des droits.

– *Remarques :* Les données arbitraires sont souvent écrites en `javascript`, en `html` ou en `vbscript`. La personne malveillante introduit ainsi du code dans le serveur vulnérable qui héberge le site. Ce serveur est rarement affecté par ce code (porteur sain). Les visiteurs du site, potentiellement victimes, consultent la page contenant le code injecté. L'exécution du code ne se fait pas au niveau du serveur, mais par le client de navigation de l'utilisateur. Une note a été rédigée à ce sujet par le CERTA [CERTA13]. La notation XSS a été introduite pour remplacer CSS, acronyme déjà utilisé pour signifier *Cascading Style Sheet*.
– *Voir aussi :* Code malveillant.
– *Références :* Note d'information du CERTA [CERTA13].

Injection de requêtes illégitimes par rebond / *Cross-Site Request Forgery*, CSRF, CSRF

– *Définition :* Attaque provoquant l'envoi de requêtes, par la victime, vers un site vulnérable, à son insu et en son nom.
– *Remarques :* L'envoi des requêtes est provoqué par la visite d'un site malveillant (ou compromis) ou en cliquant un lien. L'attaque est souvent appelée détournement de session car l'attaquant peut profiter de l'authentification préalable de la victime sur le site vulnérable. Cette attaque peut également être utilisée pour accéder frauduleusement à des interfaces de configuration Web internes au réseau.
– *Voir aussi :* Code malveillant.
– *Références :* Note d'information du CERTA [CERTA20].

Défiguration, Barbouillage / *Defacement*

– *Définition :* Résultat d'une activité malveillante qui a modifié l'apparence ou le contenu d'un serveur Internet, et a donc violé l'intégrité des pages en les altérant.
– *Remarques :* Cette action malveillante est souvent accompagnée de revendications. Le CERTA mentionne des facteurs susceptibles d'augmenter le risque d'apparation de tels problèmes dans la note d'information [CERTA11]. Il est important de distinguer les deux points suivants :

  1° l'injection illégitime de code dans une page Web ;

  2° les finalités de cette injection.

  Une défiguration est une de ces finalités, qui modifie l'aspect visuel de la page Web. Elle indique également un défaut de garantie de l'intégrité de la page.
– *Voir aussi :* Déni de service.
– *Références :* Note d'information du CERTA [CERTA11].

Démonstration de faisabilité / *Proof of Concept*, PoC

– *Définition :* Code écrit pour démontrer la faisabilité d'une attaque utilisant une vulnérabilité donnée.
– *Remarques :* Ce code de démonstration n'est généralement pas malveillant. Il est souvent écrit pour inciter l'éditeur à produire un correctif pour la vulnérabilité. Toutefois, il est évident qu'un code malveillant peut être développé par la suite, à partir de ce code rendu public.
– *Voir aussi :* Code d'exploitation.

Déni de Service / *Denial of Service*, DoS

– *Définition :* Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.
– *Remarques :* Cette action n'est pas nécessairement malveillante. Elle peut aussi traduire un mauvais dimensionnement du service, incapable de fournir la réponse à une forte demande. Si l'action est lancée depuis plusieurs sources, il est fréquent de parler de Déni de Service Distribué (DDoS).

  Les attaques en déni de service existent et représentent un risque à prendre en compte, mais il faut bien faire attention à ne pas conclure trop vite. La qualification d'une activité comme attaque en déni de service exige *a priori* une analyse approfondie des journaux et des traces.

– *Voir aussi :* Bombardement de courriels.
– *Références :* Notes d'information du CERTA [CERTA07, CERTA10].

Dépassement ou débordement de mémoire / *Buffer Overflow*

– *Définition :* Technique d'exploitation d'une vulnérabilité dans le code d'un programme qui ne vérifie pas correctement la taille de certaines données qu'il manipule.
– *Remarques :* A titre d'illustration, le principe peut être utilisé pour profiter de l'accès à certaines variables du programme, par le biais de fonctions particulières. Il faut considérer celles qui ne contrôlent pas la taille de la variable à enregistrer dans le tampon, afin de pouvoir écraser la mémoire jusqu'à l'adresse de retour de la fonction en cours d'exécution. L'utilisateur malveillant peut alors choisir les prochaines instructions qui seront exécutées par le système. Le code introduit est généralement lancé avec les droits du programme détourné. Les exemples les plus communs sont les fonctions `scanf()` ou `strcpy()` dans la bibliothèque du langage C.
– *Voir aussi :* Vulnérabilité.

Faute de frappe opportuniste,Coquille / *Typosquatting*

– *Définition :* Action malveillante qui consiste à déposer un nom de domaine très proche d'un autre nom de domaine, dont seuls un ou deux caractères diffèrent.
– *Remarques :* Les objectifs de cette action sont de capter une partie du trafic adressé au site officiel. Plusieurs exemples concrets sont mentionnés dans [HARV06]. Par exemple, nous pouvons imaginer un nom de domaine correspondant à *certa.ssi.gouve.fr*, ou encore *certa.ssi.gouv_.fr*.
– *Voir aussi :* Cybersquatting.
– *Références :* Site de l'AFNIC [PARL05].

Hameçonnage, Filoutage / *Phishing*

– *Définition :* 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 dun système légitime.
– *Remarques :* Les sites sont reproduits, après avoir été *aspirés*. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.
– *Voir aussi :* Clonage DNS.
– *Références :* Quelques documents [APWG06]. Site de la Fédération Bancaire Française [FBF06].

Ingénierie Sociale / *Social Engineering*

– *Définition :* Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.
– *Remarques :* Il s'agit, pour les personnes malveillantes usant de ces méthodes, d'exploiter le facteur humain, qui peut être considéré dans certains cas comme un maillon faible de la sécurité du système d'information. Une étude de certaines techniques de manipulation est présentée dans [JOUL02].
– *Références :* Livre [JOUL02].

Injection SQL / *SQL Injection*

– *Définition :* Terme qui désigne l'interprétation imprévue d'un code SQL dans une application. Ce code a été introduit par une voie détournée.
– *Remarques :* Cette technique permet, pour une application vulnérable à cette attaque, à un utilisateur malveillant de modifier la base de données, ou accéder à des informations qui ne lui sont pas destinées.
– *Voir aussi :* Code malveillant.

– *Références :* Note d'information du CERTA [CERTA18].

Logiciel espion, Espiogiciel / *Spyware*

– *Définition :* Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations qui concernent l'environnement sur lequel il est installé, ou sur les usages habituels du système, à l'insu de son propriétaire ou utilisateur.
– *Voir aussi :* Cheval de Troie.

Logiciel Publicitaire / *Adware*

– *Définition :* Code ayant pour finalité d'afficher des bandeaux publicitaires par le biais du navigateur Internet de l'utilisateur.
– *Remarques :* Ce code est très souvent perçu comme une méthode envahissante. Il engendre dans de nombreux cas d'autres effets sur le système, comme l'apparition de fenêtres surgissantes (`popups`), la dégradation de la connectivité ou de la performance de la machine de l'utilisateur.

Moisson de courriels / *Mail Harvesting*

– *Définition :* Action qui consiste à parcourir un grand nombre de resources publiques (pages Internet, groupes de discussion, etc), afin d'y collecter les adresses électroniques pour des intentions malveillantes.
– *Remarques :* Les adresses récupérées sont utilisées, par exemple, pour envoyer des courriels contenant des virus, des canulars, ou des pourriels. Une méthode pour s'en prémunir est de présenter sur ces ressources publiques une adresse électronique qui trompe les outils de recherche (comme prenom.nom_AT_domain.fr pour les outils cherchant '@', caractéristique d'une adresse) ; ceci est appelé *address munging*.
– *Voir aussi :* Canular, Pourriel.
– *Références :* Règles d'or de la prospection par courrier électronique énoncées par la CNIL [CNI05].

Mouchard Internet / *Web Bug*

– *Définition :* Support graphique implanté dans une page Internet ou un courriel, qui a pour objectif de surveiller la consultation de cette page ou de ce courriel, à l'insu des lecteurs.
– *Remarques :* Ces supports sont souvent invisibles, car beaucoup sont paramétrés avec une taille très petite (1x1 pixel). Ils sont aussi fréquemment représentés par des balises `HTML IMG`.
– *Voir aussi :* Logiciel espion.

Numéroteur / *Dialer*

– *Définition :* Logiciel qui compose automatiquement des numéros de téléphone.
– *Remarques :* Les numéroteurs sont souvent proposés pour accéder à des sites à caractère pornographique (appels surtaxés). Par extension, un `war dialer` est une application composant une liste de numéros, et qui enregistre ceux retournant une tonalité spéciale, comme un modem ou un fax.

Outils de dissimulation d'activité / *Rootkit*

– *Définition :* Tout programme ou ensemble de programmes permettant à une personne malveillante de maintenir un contrôle illégitime du système d'information en y dissimulant ses activités.
– *Remarques :* L'installation de ces programmes nécessite que le système soit préalablement compromis (Cheval de Troie, intrusion). Ces programmes modifient souvent les commandes usuelles de l'administrateur, afin de dissimuler toute trace de leur présence. Ils effectuent aussi fréquemment plusieurs opérations au niveau du noyau du système d'exploitation, comme l'installation de portes dérobées, la capture des frappes clavier, etc. La note [CERTA12] du CERTA présente l'exemple concret d'un tel programme.

– *Voir aussi :* Capteur Clavier, Portes dérobées, Cheval de Troie.
– *Références :* Note d'information du CERTA [CERTA12].

Polymorphe / *Polymorphic*

– *Définition :* Se dit d'un ver ou d'un virus dont le code est chiffré, changeant le code de déchiffrement d'une infection à l'autre, et donc l'apparence et/ou la signature.
– *Remarques :* Se reporter à [SZOR05] pour de plus amples détails.
– *Voir aussi :* Ver.
– *Références :* Livres [FIL05, SZOR05].

Porte dérobée / *Backdoor*

– *Définition :* Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine distante, de manière furtive.
– *Remarques :* Une porte dérobée peut également être la cause d'une mise en œuvre incorrecte d'un protocole. Une liste de portes dérobées et une méthode de détection peut se trouver dans [PAX00].
– *Voir aussi :* Canal caché, Cheval de Troie.
– *Références :* Document [THOM95].

Pourriel, Polluriel / *Spam*

– *Définition :* Tout courrier électronique non sollicité par le destinataire.
– *Remarques :* Le courrier est souvent envoyé massivement à un large nombre d'adresses électroniques. Les produits les plus vantés sont les services pornographiques, les médicaments (hormones pour la lutte contre le vieillissement, dopage des activités sexuelles, etc), le crédit financier, etc.
– *Voir aussi :* Phishing, Bombardement de courriel, Canular, Moisson de courriels.
– *Références :* Note d'information du CERTA [CERTA14].

Renifleur / *Sniffer*

– *Définition :* Outil matériel ou logiciel dont l'objet est de capturer les trames transitant sur le réseau.
– *Remarques :* Si les trames contiennent des données non chiffrées, un utilisateur malveillant peut aisément récupérer des données confidentielles, comme des mots de passe, des courriers électroniques, des contenus de pages Internet, etc. L'utilisateur malveillant peut aussi, à partir des trames, récupérer des informations sur les systèmes échangeant les trames, comme le système d'exploitation ou les services employés.
– *Références :* Note d'information du CERTA [CERTA19].

Situation de compétition / *Race Condition*

– *Définition :* Situation révèlant la vulnérabilité d'un système dont la réponse varie fortement en fonction de l'ordonnancement des évènements qu'il reçoit.
– *Remarques :* Cette situation est par exemple possible lorsque deux systèmes essaient d'accéder simultanément à une même ressource, mais qu'un seul accès est autorisé. Un utilisateur malveillant peut demander accès à cette ressource en envoyant un grand nombre de requêtes dans un intervalle de temps donné, et ainsi prendre de vitesse un système normal.
– *Voir aussi :* Homme-au-Milieu, Entredeux.

Test d'intrusion / *Penetration Test*

– *Définition :* Action qui consiste à essayer plusieurs codes d'exploitation sur un système d'information, afin de déterminer ceux qui donnent des résultats positifs.

– *Remarques :* Il s'agit à la fois d'une intention défensive (mieux se protéger) et d'une action offensive (aggresser son *propre* système d'information).
– *Voir aussi :* Code d'exploitation.

Usurpation d'adresse / *Address Spoofing*

– *Définition :* Action malveillante qui consiste à utiliser délibéremment l'adresse d'un autre système en lieu et place de la sienne.
– *Remarques :* Il faut rapprocher cette action de l'usurpation d'identité, considérée comme un délit par le droit pénal français. L'idée est de faire passer son système d'information pour un autre. L'adresse usurpée peut être une adresse MAC (pour `Medium Access Control`), une adresse IP, une adresse de messagerie, etc.
– *Voir aussi :* Canular, Polluriel.
– *Références :* Note d'information du CERTA [CERTA14].

Ver / *Worm*

– *Définition :* Code malveillant qui se propage de façon plus ou moins autonome sur le réseau une fois la machine infectée. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.
– *Remarques :* 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. Le CERTA a publié de nombreux avis concernant des vers, ainsi que plusieurs notes d'information [CERTA08, CERTA09].
– *Voir aussi :* Polymorphe, Virus.
– *Références :* Notes d'information du CERTA [CERTA08, CERTA09]. Document RFC 2828 [RFC]. Parution au Journal Officiel le 20 mai 2005 [JO05].

Virus / *Virus*

– *Définition :* Programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, ...) et, bien souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Il s'implante au sein de programmes, se duplique à l'insu des utilisateurs, et peut nécessiter l'intervention explicite de ces derniers pour se propager (ouverture d'un courrier électronique, lancement d'un programme exécutable, etc).
– *Remarques :* Plusieurs ouvrages décrivent les différentes familles de virus, leurs systèmes de prédilection et leurs stratégies d'installation ([SZOR05, FIL05]). La définition présentée ci-dessus diffère de celle qui a été proposée par F. Cohen, le premier scientifique ayant proposé un modèle mathématique formel des vers informatiques, en 1984 : "A virus is a program that is able to infect other programs by modifying them to include a possibly evolved copy of itself" [COH87]. Le CERTA a publié de nombreux documents concernant les virus, notamment [CERTA04, CERTA05, CERTA06], ainsi que de nombreux avis.
– *Voir aussi :* Code Malveillant.
– *Références :* Documents du CERTA [CERTA04, CERTA05, CERTA06]. Parution au Journal Officiel le 20 mai 2005 [JO05].

Vulnérabilité / *Vulnerability*

– *Définition :* 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.
– *Remarques :* Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.
– *Voir aussi :* Code d'exploitation.
– *Références :* Projet IST Maftia [MAFTIA].

Zombies, Réseau de Zombies / *Botnet*

- *Définition :* Ensemble de machines compromises, contrôlées par un même utilisateur malveillant.
- *Remarques :* 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).
- *Voir aussi :* Déni de service distribué.

0jour / *Zero-Day*

- *Définition :* Catégorie particulière de codes d'exploitation qui cible des vulnérabilités qui ne sont pas encore publiquement annoncées par l'éditeur, le constructeur ou un chercheur en sécurité.
- *Remarques :* Ces codes d'exploitation sont particulièrement dangereux sur le plan SSI, car ils ne sont pas connus, et il n'y a pas de correctif pour s'en protéger. Seule une défense en profondeur permet de limiter les risques.
- *Voir aussi :* Code d'exploitation.

4 Documentation

Références

[APWG06] Anti-Phishing Working Group, page d'accueil
http://www.antiphishing.org

[BERK05] V. Berk, A. Giani, G. Cybenko. "Detection of Covert Channel Encoding in Network Packet Delays". Rapport technique TR536, de l'Université de Dartmouth. Novembre 2005.
http://www.ists.dartmouth.edu/library/149.pdf

[CERTA01] Note D'information du CERTA : « Les chevaux de Troie ». Octobre 2001.
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-002

[CERTA02] Recommandation du CERTA : « Attaque ciblée par cheval de Troie ». Juin 2005.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-REC-002

[CERTA03] Note d'information du CERTA : « Les canulars par messagerie ». Mai 2000.
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-005

[CERTA04] Avis du CERTA : « Rappel sur les virus de messagerie ». Mai 2003.
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-084

[CERTA05] Bulletin d'alerte du CERTA : « Rappels concernant les virus ». Janvier 2002.
http://www.certa.ssi.gouv.fr/site/CERTA-2001-ALE-012

[CERTA06] Note d'information du CERTA : « Rappel sur les virus et chevaux de Troie ». Novembre 2000.
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-007

[CERTA07] Note d'information du CERTA : « Le déni de service distribué ». Juin 2000.
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-001

[CERTA08] Bulletin d'alerte du CERTA : « Propagation du ver `Code Blue` ». Septembre 2001.
http://www.certa.ssi.gouv.fr/site/CERTA-2001-ALE-010

[CERTA09] Bulletin d'alerte du CERTA : « Apparition de vers exploitant des vulnérabilités de MS-SQL Server ». Novembre 2001.
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-005

[CERTA10] Note d'information du CERTA : « Evolution des outils de déni de service distribué ». Mai 2000.
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-003

[CERTA11] Note d'information du CERTA : « Bonnes pratiques concernant l'hébergement mutualisé ».
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005

[CERTA12] Note d'information du CERTA : « Chronique d'un incident ordinaire ». Novembre 2002.
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-003

[CERTA13] Note d'information du CERTA : « Vulnérabilité de type *Cross Site Scripting* ». Mars 2002.
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001

[CERTA14] Note d'information du CERTA : « Limiter l'impact du SPAM ». Octobre 2005.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004

[CERTA15] Note d'information du CERTA : « Tunnels et pare-feux : une cohabitation difficile ». Octobre 2005.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003

[CERTA16] Note d'information du CERTA : « Filtrage et pare-feux ». Janvier 2006.
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001

[CERTA17] Recommandation du CERTA : « La bonne utilisation des protocoles SSL/TLS ». Mars 2005.
http://www.certa.ssi.gouv.fr/site/CERTA-2005-REC-001

[CERTA18] Note d'information du CERTA : « Sécurité des applications Web et vulnérabilité de type *injection de données* ». Janvier 2005.
http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001

[CERTA19] Note d'information du CERTA : « Les mots de passe ».
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001

[CERTA20] Note d'information du CERTA : Les attaques de type « cross-site request forgery ».
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-003

[CLUS06] CLUSIF : Glossaire du cédérom des Critères Communs
https://www.clusif.asso.fr/cd/BasesPar/Glossair/

[COH87] F. Cohen. "Computer viruses: Theory and experiments". Computer & Security, 6:22-35, 1987.

[CNI05] Commission Nationale de l'Informatique et des Libertés CNIL. « Les règles d'or de la prospection par courrier électronique ». Septembre 2005.
http://www.cnil.fr/index.php?id=1277

[FBF06] Fédération Bancaire Française, organisme professionnel rassemblant des entreprises bancaires en France.
http://www.fbf.fr

[FIL05] E. Filiol. « Les virus informatiques : théorie, pratique et applications ». Editions Springer, Collection IRIS, 384 p., 2004, ISBN 2-287-20297-8.

[FROI02] P. Froissart. « La rumeur, Histoire et fantasmes ». Collection Belin *"Débats"*, 280 pages, 2002.
http://pascalfroissart.online.fr

[FRCO06] FAQ du forum de discussion Usenet fr.comp.securite.virus
http://www.lacave.net/ jokeuse/usenet/

[GOUV96] Le Portail Société de l'Information
http://www.internet.gouv.fr/informations/ressources/glossaire/

[HAIG87] J.T. Haigh, R.A. Kemmerer, J. McHugh, W.D. Young. "An experience using two covert channel analysis techniques on a real system design". Publié dans la revue *IEEE Transactions on Software Engineering*, Volume 13, pp.157-168, 1987, ISSN:0098-5589.

[HARV06] B. Edelman. "Large-Scale Registration of Domains with Typographical Errors". Faculté de Droit de Harvard, 2006.

[HOAX06] Hoaxbuster.com
http://www.hoaxbuster.com

[JO00] Commission Générale de Terminologie et de Néologie - JO du 1er septembre 2000. « Liste des termes, expressions et définitions adoptés et publiés au Journal Officiel de la République Française : Vocabulaire de l'Internet ».
http://www.culture.gouv.fr/culture/dglf/cogeter/publications-jo.htm

[JO05] Commission Générale de Terminologie et de Néologie - NOR : CTNX0508288K - JO du 20 mai 2005, p. 8803, texte 98.
http://www.culture.gouv.fr/culture/dglf/cogeter/publications-jo.htm

[JOUL02] R.V. Joule, J.L. Beauvois. « Petit traité de manipulation à l'usage des honnêtes gens ». Publié aux éditions Presses Universitaires de Grenoble, Collection Vies Sociales, 286p., 2002.

[KIEN03] D.M. Kienzle, M.C. Elder. "Recent Worms: A Survey and Trends". Publié dans le groupe de travail ACM Workshop 2003, Washington DC, USA, 2003.

[LAMP73] B.W. Lampson. "A Note on the Confinement Problem". Publié dans la revue Communications d'ACM, 16(10):613-615. Octobre 1973.

[MAFTIA] Projet IST MAFTIA (Malicious and Accidental Fault Tolerance for Internet Applications). "DeliverableD3 : Taxonomy of Intrusion Detection Systems and Vulnerabilities".
http://www.maftia.org/deliverables/full.htm

[PARL05] Association Française pour le nommage Internet en Coopération, AFNIC. « Les Procédures Alternatives de Résolution de Litiges (PARL) du *.fr* et du *.re* ».
http://www.afnic.fr/doc/ref/juridique/parl

[PAX00] Y. Zhang, V. Paxson. "Detecting Backdoors". Publié au 9ième Symposium USENIX, Colorado, USA, août 2000.

[RFC] *Request for Comments* RFC 2828. "Internet Security Glossary". Mai 2000.
http://rfc.net/rfc2828.html

[SPAM] Direction du Développement des Médias (DDM). « Groupe de contact des acteurs de la lutte contre le *spam* ».
http://www.ddm.gouv.fr

[SZOR05] P. Szor. "Virus Research and Defense". Editions Addison-Wesley Professional, 2005, ISBN 0-321-30454-3.

[THOM95] Ken Thomson. "Reflexions on Trusting Trust". Publié dans le journal *Communications of the ACM*, vol. 27, numéro 8, pp. 761-763, août 1984.
http://www.acm.org/classics/sep95/

[WEA03] N. Weaver, V. Paxson, S. Staniford, R. Cunningham. "A Taxonomy of Computer Worms". Publié dans le groupe de travail ACM Workshop 2003, Washington DC, USA, 2003.

[YY96] A. Young, M. Yung. "Cryptovirology: Extorsion-Based Security Threats and Countermeasures". Publié dans la conférence IEEE *Security & Privacy*, pp.129-141, mai 1996.

Index des termes français

Index des termes anglais

Gestion détaillée du document

20 février 2006 version initiale.
07 avril 2006 mise à jour des références et liens croisés.
21 avril 2006 ajout de références.