Lexique des termes de sécurité informatique

Trojan, malware, spyware, ver, virus...

Connaissez-vous la signification de tous ces termes ?

Maintenant, grâce à ce lexique, ils n'auront plus aucun secret pour vous !

Retrouvez facilement le terme souhaité en cliquant sur la lettre correspondante à son classement alphabétique.

CLIQUEZ ICI POUR ACCEDER AU CLASSEMENT

CHOIX DE LA PREMIERE LETTRE DU TERME RECHERCHE

A	B	C	D
E	F	G	H
L	O	P	S
T	U	V	Z

FIN

LETTRE -A-

Accès frauduleux aux privilèges Root (Rootkit)

Les Rookit sont actuellement l'une des plus grandes menaces pour les utilisateurs d'ordinateurs. Ils s'installent eux-mêmes invisiblement sur une cible système et donne à l'attaquant le plein contrôle sur le système. Une fois installé, il se cache avec des mécanismes intelligents, et rend les Rootkits très difficiles, voire impossibles à détecter. Si vous détectez une installation de Rootkit, alors une nouvelle installation du système d'exploitation est généralement inévitable parce que vous ne pouvez plus faire confiance à l'ordinateur.

Agent logiciel (Botnet)

La traduction exacte de "Botnet" est la fusion de deux mots "bot => robot" et "network => réseau". Un Botnet désigne un très grand réseau dont les ordinateurs sont infectés avec un certain cheval de Troie. L'auteur du cheval de Troie contrôle l'ordinateur infecté, qui alors réagit à ses ordres quasi automatiquement comme le feraient des robots. De grands Botnet se composent d'un nombre de cinq à six-millions d'ordinateurs - à l'insu de leurs propriétaires.

LETTRE -B-

Badware

Décrit un logiciel présentant un comportement trompeur et qui est difficile à supprimer ou présente des comportements indésirables. Voir "Malware".

Balayeur, scanneur (Scanner)

À côté du matériel du même nom utilisé pour la numérisation de photos, le terme scanneur décrit également un programme utilisé pour la recherche sur l'ordinateur. Le scanneur de Malware utilise des définitions de signatures et d'analyse heuristique pour détecter les logiciels nuisibles.

Bloqueur de comportements (Behavior Blocker)

Traduit, signifie "Bloqueur de comportements", mais on peut l'appeler aussi "Protection de surveillance comportementale" ou "Protection proactive". Contrairement au scanneur basé sur les signatures, le bloqueur de comportements n'utilise pas les signatures et les analyses heuristiques pour reconnaître des logiciels nuisibles, mais plutôt le comportement du logiciel.

FIN

INDEX

LETTRE -C-

Cannular informatique (Hoax)

Décrit, intentionnellement l'envoi d'une fausse alerte au virus, qui est considéré et adopté par de nombreux utilisateurs, comme un fait réel. Un célèbre canular dit à ses utilisateurs de supprimer les supposés fichiers Malware tel que SULFNBK.EXE et JDBGMGR.EXE, malgré le fait que ces éléments sont d'importants fichiers de système.

Captcha

Captcha, est une forme de "test de Turing inversé", il est utilisé pour déterminer si un programme ou un service en ligne vient d'une nature humaine ou de l'utilisation d'une machine. La principale forme de Captcha est générée avec des images de manière aléatoire, qui contient des codes à tapper dans une boite de dialogue. Une machine ne peut pas décoder des lettres et des chiffres intentionnellement déformés. Cela permet de s'assurer que (par exemple) un programme ne peut pas être désactivé par un autre programme ou par Bot.

Cheval de Troie, Troyen (Trojan)

Le terme de cheval de Troie vient du célèbre cheval de Troie dans la mythologie grecque. En outre, l'utilisateur pense qu'il installe un programme utile, par exemple un petit jeu sur son ordinateur. Mais, avec ce soi-disant programme utile se dissimule derrière un Malware qui s'installera sur l'ordinateur et rendra possible à l'attaquant, de prendre le plein contrôle.

Composeur de numéros (Dialer)

Les Dialers sont certainement un type de Malware, plus précisément des programmes qui se connectent frauduleusement à des services payants à valeur ajoutée. À l'époque, où l'accès a Internet, se faisait principalement par l'intermédiaire de modems et de lignes ISDN (RNIS), les Dialers représentaient un grand danger sous la forme d'horribles factures de téléphone. Aujourd'hui avec la technologie de la RNA ou LNPA (ADSL) ils sont devenus moins fréquents parce que l'ADSL n'utilise pas une simple connexion téléphonique.

FIN

INDEX

LETTRE -D-

Définitions de signatures (Signatur)

Une signature représente l'unique empreinte d'un programme. Les signatures sont surtout utilisées par les scanneurs pour reconnaitre les logiciels nuisibles. Leur inconvénient majeur est la croissance exponentielle du nombre de versions différentes de logiciels nuisibles et le fait c'est d'avoir d'abord une empreinte du Malware qui doit être connue avant qu'une signature puisse être créée.

Dépassement de tampon (Buffer Overflow)

Les soi-disant "Dépassement de tampon" appelé parfois également "Débordement de tampon", ces soi-disant "buffer overflow" représentent la plus commune des failles de sécurité dans les programmes et les systèmes d'exploitation. Le dépassement de tampon, se provoque par un trop grand apporte de données dans une certaine Zone de la mémoire, ce qui pourrait entrainer des erreurs ou des plantages. Dans le pire des cas, un attaquant obtient ainsi le contrôle d'un autre ordinateur étranger. La mesure principale de protection, c'est de faire les mises à jour logicielles quotidiennes.

FIN

INDEX

LETTRE -E-

Enregistreur de frappe (Keylogger)

Les enregistreur de frappe sont de petits programmes, qui sont installés invisiblement sur un ordinateur et enregistrent toutes les frappes sur le clavier. Un attaquant peut par exemple connaitre vos mots de passe et se les approprier.

Espiogiciel, logiciel espion (Spyware)

Dans le cas de logiciels espions, il s'agit de logiciels que l'utilisateur de l'ordinateur sur lequel il est installé, espionne au sens propre du terme. Il moissonne toutes sortes de données personnelles, celles qui alors seront envoyées au créateur du logiciel espion.

.

LETTRE -F-

Failles de sécurité - Allemand (Sicherheitslücke)- anglais (Vulnerability)

Par une faille de sécurité, un attaquant peut pénétrer dans un autre ordinateur et y installer ses propres logiciels. Voir "Exploit". Très utiles contre les failles de sécurité sont des mises à jour logicielles régulières et l'utilisation d'une Bloqueur de comportement (Behavior Blockers).

Faux positif (False Positive)

Un faux positif décrit une erreur d'alerte dans le système - généralement dans les Anti-Malware ou IDS (Intrusion Detection Systemen - Fr : Détection d'Intrusions Système). Cela peut se produire quand le fichier ou la nature, des modèles de comportement, vient de programmes légitimes ou programmes malveillants qui sont parfois très similaires. En cas de fausse alerte, en règle générale, le fabricant, de logiciels, met à disposition assez rapidement une mise à jour (correctif).

.

FIN

INDEX

LETTRE -G-

Gardien ou Bouclier (Guard)

"Gardien" est la traduction correcte de l'expression anglaise "Guard". Les Gardiens sont en général des programmes ou des parties de programme, qui ont recours à une fonction protectrice, c'est-à-dire de préserver l'ordinateur ou certaines parties contre des attaques.

.

FIN

INDEX

LETTRE -H-

Hameçonnage ou Usurpation d'identité (d'entreprise) (Phishing)

Les attaquants utilisent de faux sites Web pour obtenir des mots de passe secret. Le terme dérive de "Password Fishing" (hameçonnage du mot de passe). Les adresses Internet sont déguisés de façon qu'elles sont presque identiques aux originaux. Ce phénomène concerne surtout les accès aux services bancaires en ligne.

Heuristique

On entend par là, une analyse algorithme (mathématique) de balayage de fichiers sur le disque dur. Le code du programme est utilisé pour effectuer un calcul de probabilité pour détecter d'éventuelles formes d'actions nuisibles.

.

LETTRE -L-

Logiciel à risque (Riskware) voir "Malware".

Riskware, vient de deux termes anglais "risk" et "ware", ce qui voudrait dire à peu près en français "Logiciel à risque". En termes simples, il s'agit d'un logiciel dont l'installation présente un possible risque pour l'ordinateur, mais pas nécessairement.

Logiciel malveillant (Malware)

Le terme Malware est composé de "malicieux" et "logiciel", ce qui se traduit et veut dire en gros "logiciel malveillant". Il s'agit du terme générique pour tous les types de logiciels malveillants, tels que les chevaux de Troie, logiciels espions ou de virus.

.

FIN

INDEX

LETTRE -O-

Ordinateur Zombie (Zombie Computer)

Un ordinateur infecté avec un cheval de Troie contenant une porte dérobée, qui est télécommandé à distance en prenant les ordres du pirate et qui réalisera des actions néfastes.

.

FIN

INDEX

LETTRE -P-

Porte dérobée (Backdoor)

Backdoor "Porte dérobée" quand on le traduit ne signifie littéralement rien d'autre que "porte de derrière" et c'est bien précisément de cela qu'il s'agit également. Les Backdoors sont soi-disant intentionnellement être des utilitaires utiles intégrés par le programmeur pour pénétrer dans les ordinateurs par la porte arrière sur lesquels ils seront installés. Un ordinateur infecté peut être entièrement télécommandé à distance, par exemple, pour l'envoi de pourriels.

Publiciel (Adware)

Adware est le terme pour les programmes, qui inclut par exemple de la publicité, des bannières publicitaires. C'est souvent, de cette façon que les couts de développement sont ainsi financés. Adware en général a une mauvaise réputation, car certains programmes ne suffisent pas à attirer l'attention sur la publicité ou sont trop intrusif. Les modules, Adware qui constamment télécharges de nouvelles données publicitaires, peuvent également créer des profils en surveillant l'activité des utilisateurs sur l'ordinateur et donc de mettre en danger la confidentialité de vos données.

.

FIN

INDEX

LETTRE -S-

Système de détection d'intrusion machine (HIPS) - Système de détection d'intrusion (IDS)

Les abréviations de "HIPS" pour Host (based) Intrusion Prevention System " et "IDS" "Intrusion Detection System " sont des programmes ou des éléments de programme permettant de détecter et d'empêcher l'exécution de code nuisibles. Leur principal avantage est sans la reconnaissance de la signature, qui permet de détecter de nouveaux exploits et d'attaques "0 jour" pour lesquelles il n'existe pas encore de signatures.

.

FIN

INDEX

LETTRE -T-

Témoin (Cookie)

Le Cookie représente une information très courte, qu'un serveur Web transmet au navigateur de l'utilisateur qui ensuite sera stocké. Lors d'une seconde visite sur le site, le même serveur peut de nouveau lire l'information et quasi "reconnaitre l'utilisateur". La technique est idéale pour enregistrer des profils d'utilisateurs (Qu'est-ce qui a été cliqué ?)

.

LETTRE -U-

Une preuve de concept (POC/Proof Of Concept)

Un preuve de concept (Proof of concept) est, pratiquement, le prototype d'une nouvelle attaque, mais, ne contient en règle générale pas de prolifération de routines. Quand un programmeur découvre un nouveau trou dans un programme (voir la vulnérabilité), alors il met à disposition des preuves de cela avec le POC. Les preuves de concept sont également créées par les hackers pour des raisons négatives, mais également par les employés d'entreprises de sécurité et de programmeurs indépendants pour créer des correctifs.

.

LETTRE -V-

Ver - Allemand (Wurm) - Anglais (Worm)

Un ver exploite des applications plus élevées, tel que les réseaux ou courriels pour se diffuser de manière incontrôlée. De plus, un ver n'a pas besoin d'une routine nuisible, mais le peut. Une diffusion typique se fait par exemple par le biais des courriels avec pièce jointe. Si l'utilisateur ouvre la pièce jointe, le ver sera automatiquement envoyé à tous les destinataires se trouvant dans le carnet d'adresses du client de messagerie.

virus informatique (Virus)

Les virus sont la plus ancienne forme de logiciels nuisibles et - malheureusement - toujours une menace très actuelle. Contrairement à tous les autres Malware, un virus infecte un programme légitime en infiltrant son propre code (comparable à un virus biologique, qui apporte ses informations génétiques dans une cellule du corps humain). Une fois lancé, le virus tente de se diffuser lui-même et peut provoquer toutes sortes de dégâts possibles. Un virus est, en règle générale, sans "hôte" il n'est pas autonome et ne peut s'exécuté de lui- même.

Vulnérabilité

Voir "Failles de sécurité" et "Exploit".

Vulnérabilité (Exploit)

Un exploit est le terme technique pour désigner un programme nuisible qui exploite les points faibles spécifiques dans un logiciel (par exemple débordements de tampon) Buffer Overflow. Ainsi, un attaquant peut prendre le contrôle d'un ordinateur attaqué par l'intermédiaire de points faibles dans le système d'exploitation ou des applications.

.

FIN

INDEX

LETTRE -Z-

0 jour (Zero-Day Attacke)

Les attaques, 0 jour, on cause d'un tout nouveau Malware, quasiment au premier jour de sa diffusion. C'est justement les premiers jours d'un nouveau Malware qui est très dangereux, car il faudra un peu de temps, jusqu'à ce qu'un laboratoire d'antivirus obtienne un exemplaire et puisse créer une signature. Le soi-disant Behavior Blocker propose ici une meilleure protection.

.

Retrouvez d'autres outils tout aussi sympathiques sur le site internet:

BOITEALAPIN.FR

Très bonne journée à vous et à bientôt…