

Présentation

Pourquoi le thème de la sécurité ?

J'ai créé ce thème parce que ce sujet m'intéressait particulièrement, mais aussi parce que, chemin faisant, j'ai constaté qu'il y avait beaucoup de choses à partager pour l'intérêt de tous.

Objectif

Ce dossier doit faire simple tout en vous donnant les clés dont vous avez besoin. De plus en plus de services sont disponibles en ligne. De plus en plus de personnes tentent de tirer profit de cela au détriment des utilisateurs.

L'auteur

L'informatique est chez moi une passion autant qu'un outil. Au fil du temps, je me suis décidé à ouvrir un serveur. Ce thème vous permettra d'avoir une idée générale sur la sécurité des données, les précautions à prendre.

Le web aujourd'hui

Dans les grandes lignes

Depuis quelques années internet a pris un d'accélérateur. Cette croissance est liée à plusieurs faits :

- l'accès au haut débit est de plus en plus généralisé*
- le développement de multiples services en ligne*

Le débit actuel se situe souvent entre 250 et 1500 Kio/s (kibiocets) ce qui permet un grand nombre de choses.

Normalisation

Différents organismes travaillent à normer les systèmes de l'information, de plus en plus de possibilités sont désormais offertes et l'interopérabilité tend à s'accroître entre les différents navigateurs et le standard des pages web.

SECURITÉ DES SYSTÈMES DE L'INFORMATION

Services en ligne

Il y a aujourd'hui une volonté grandissante de proposer des services en ligne pratiques et modernes permettant un gain de temps tout en étant ludiques.

Les services en ligne les plus performants nous permettent d'effectuer de plus en plus d'opérations comme achat, vente, consultation de comptes bancaires etc ...

Exploits

Dans le même temps, les pirates effectuent les exploits les plus complexes et décortiquent les vulnérabilités de tout logiciel pouvant être exploité à distance.

Le niveau de sécurité même si il tend vers le haut a des failles potentielles à plusieurs niveaux.

Un exemple, les exploits :

Dans le monde de l'informatique, les exploits sont des codes utilisés pour pirater des systèmes.

Quelques faits

Vecteurs d'infection

Les virus et exploits en tout genre se multiplient et ont permis l'émergence d'une économie d'organisations pirates.

Nombre d'entre nous a connu de multiples réinstallations du système d'exploitation.

Voici quelques vecteurs d'infection binaires :

- *Les virus*
- *Les maliciels*
- *Les failles de sécurité du système d'exploitation*
- *Les failles de sécurité des logiciels tiers*
- *Les spams*

Quelle est notre responsabilité ?

Si le haut débit a multiplié les possibilités offertes par les services en ligne, il a aussi donné la possibilité de détourner des informations privées importantes. Un nombre d'individus important apprennent à exploiter les failles informatiques à des fins nuisibles telles que le blocage de sites commerciaux ou le détournement d'informations

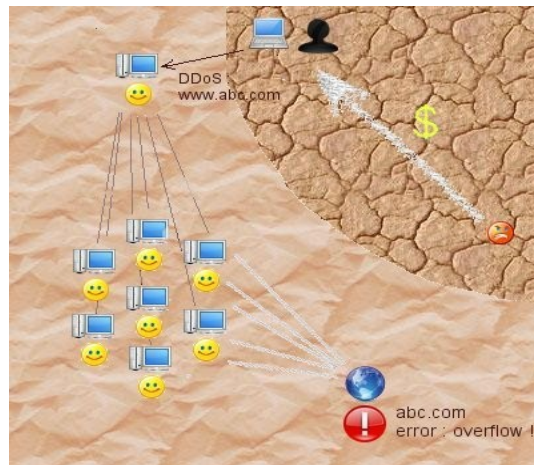
SECURITÉ DES SYSTÈMES DE L'INFORMATION

privées.

Pourquoi est-ce que je vous parle de cela ? La réalité des faits est que sans nous, les internautes, tout cela ne serait possible, et nous sommes les victimes d'un trafic alors que de simples mesures permettent de se protéger avec une certaine efficacité.

Un exemple, le DDoS

Le détournement d'une partie assez importante des ordinateurs a permis au plus petit nombre de mener des attaques DDoS c'est à dire. Distributed Denial of Service.



Voici une expérience que j'ai menée

Je récupère par mail un fichier que je suspectais d'être un virus et l'exécuter alors le moniteur d'activité voit alors transiter des paquets entre ma machine et d'autres sur internet. Je scrute quelques paquets pour y découvrir des messages publicitaires type spam à destination de dizaine, de centaine d'adresses mail que l'on me transférait. Heureusement j'avais pris soin d'exécuter ce virus dans un environnement virtualisé, ne compromettant en rien le reste du système.

Quelques failles de sécurité

Comment fonctionnent les exploits de failles

Une faille est une fonctionnalité d'un logiciel ou du système d'exploitation qui peut être manipulée de façon à obtenir un résultat qui franchit les limites de celle pour laquelle elle a été programmée.

SECURITÉ DES SYSTÈMES DE L'INFORMATION

Il existe un grand nombre de variété d'exploits parmi lesquels :

- *les exploits en local : on exploiter une faille si on a accès directement à la machine*
- *les exploits en à distance : pourvu que l'on ait accès à distance on peut exploiter la faille (internet)*
- *exploits permettant une élévation de privilèges : on peut avoir les droits plus élevés que ceux qui nous ont été donné (ex obtenir les droits administrateurs sur une machine)*
- *exploits permettant l'exécution de code : diverses manipulations permettent de faire exécuter le code de son choix sur une machine où cela est prohibé (ex. sur un serveur web)*

Les systèmes de piratage automatisés ciblent des failles relativement anciennes et pour lesquelles maintenir votre système à jour peut être suffisant, c'est du moins mon constat jusqu'à ce jour (voir dossier suivant : une étude sur la sécurité des systèmes informatiques).

Les logiciels comme les systèmes d'exploitation ont souvent des failles de sécurité. Les codes d'infection utilisent des techniques élaborées notamment :

- *débordement de tampon : on utilise le fait qu'un message trop long va générer des données écrites en dehors de la zone mémoire prévue à cet effet*
- *entrée de données inattendues dans un champ de valeur produisant un effet très différent de celui prévu*
- *certaines techniques ou méthodes permettent d'exploiter certains services si la sécurité n'a pas été ajoutée comme une couche supplémentaire*

Comment fonctionnent les virus

Les virus sont en quelque sorte des programmes invisibles pour l'utilisateur, programmés pour se charger en mémoire, se répandre par tout les moyens et, de nos jours, créer un réseau de machines infectées dont le contrôle est donné à un serveur commun

La plupart des logiciels pirates modernes ne se contentent pas d'exploiter les failles de sécurité et les maladresses des utilisateurs dans le but de s'introduire dans le système, ils enregistrent les données confidentielles, loguent la victime sur un serveur, avertissent les pirates etc ...

Dans le monde d'internet d'aujourd'hui, il n'est plus possible de se connecter à internet sans être la ciblé par les requêtes automatisées de piratage.

Les virus de troie par exemple semblent chercher de nouvelles victimes à travers l'exploitation de certaines failles de sécurité pour l'exploit desquelles ils été écrit. Ainsi les virus de troie tentent de se rprogaper par eux même créant les botnet.

Malice et organisation

A l'heure où j'écris ces lignes, mes expériences ont montré que les recherches de failles sont menées de façon organisée, par exemple une certaine vulnérabilité potentielle est découverte (ex le port 22 est ouvert) vous recevez de plus en plus de connexions venant de toute part sur cette faille potentielle.

Cela traduit le fait que le réseau pirate s'est organisé et est inter-connecté. Les informations intéressantes s'échangent de façon à exploiter le plus possible le réseau.

D'autre part, chacun à son rôle dans cette organisation. Le réseau est organisé de façon à exploiter les données récoltées.

Il est important dans le monde d'aujourd'hui de savoir protéger ses données et ce particulièrement lorsque l'on est amené à effectuer des opérations sensibles en ligne.

Sécuriser ses données et son environnement de travail n'est pas chose aisée.

Cas des navigateurs

On découvre généralement de nombreuses failles de sécurité sur les navigateurs. Ces failles permettent des exploits à travers des pages spécifiquement conçues. La simple navigation sur les sites vous met face à cette probabilité d'infection. Les pirates cherchent généralement à infecter en piratant des sites ordinaires et suffisamment fréquentés. Si votre navigateur n'est pas suffisamment à jour ou si la faille est trop récente, vous pouvez être infecté de cette façon.

Quelques systèmes d'exploitation

Parts de marché (hors serveurs)

Dans le marché des systèmes d'exploitation, nous avons dans l'ordre approximativement décroissant de part de marché :

- *Windows XP, Vista, part de marché ~85%*
- *Mac, part de marché ~10%*
- *Linux, part de marché ~1%*
- *BSD, part de marché semble < 1%*
- *Bien d'autres*

En matière de sécurité

En matière de sécurité, chacun est assez différent. L'approche de certains systèmes est orientée accessibilité, pour d'autres l'approche est d'abord celle de la sécurité.

De part leur conception, certains systèmes ne peuvent offrir une grande sécurité alors qu'ils peuvent offrir une utilisation à la portée de chacun, alors que d'autres systèmes sont à l'inverse capables d'offrir une plus grande sécurité alors que leur utilisation peut sembler plus restrictive.

Windows offre de multiples possibilités tant au niveau des jeux que applications de bureautique ou professionnelles. La plupart des pilotes pour matériels sont disponibles pour Windows. L'ergonomie de Windows s'est faite au détriment de la sécurité du système d'exploitation qui pourtant tend à s'améliorer à mesure des évolutions, cependant c'est le système d'exploitation le plus ciblé en tant que tel, mais aussi au niveau des applications, Internet Explorer, Office, etc ...

Macintosh, de la lignée des BSD, offre une certaine sécurité, d'autant que très peu de virus ont été développés pour cet environnement. Les application tierces semblent aussi bénéficier d'une sécurité correcte

Linux est aussi un environnement très peu touché par les virus et assez robuste au niveau de la sécurité

Certains environnements permettent une sécurité accrue comme OpenBSD ou FreeBSD

Mac est issu de BSD et Linux d'UNIX. Dans les deux cas le principe de fonctionnement du système d'exploitation nous met protège notamment en instaurant un politique de droit administrateur par défaut. Il semble que la façon dont le noyau du système fonctionne soit plus saine au niveau de la sécurité dans des environnements comme Linux ou MAC bien que ce dernier soit plus sain encore.

Parmi les BSD, OpenBSD est un des plus sécurisés. C'est aussi le système d'exploitation qui bénéficie probablement de la meilleure sécurité parmi tout les systèmes publics existant. Seulement deux failles de sécurité aient été détectées dans l'installation par défaut en plus de dix ans. Les ténors publient régulièrement des mises à jour de sécurité critiques.

Les problèmes de sécurité communs pour Windows

Windows est un système qu'il faut sécuriser pendant ou après installation, puisque par défaut il présente plusieurs faiblesses.

- *Une seule partition pour le système et pour les données*
- *L'utilisateur à les droits suffisant pour installer des logiciels et accéder au système*

SECURITÉ DES SYSTÈMES DE L'INFORMATION

Sous BSD Mac Linux

L'utilisateur n'a pas les droits administrateurs, il doit les rentrer à chaque fois que le système a besoin de faire des modifications dans des zones système. L'espace des données et l'espace du système sont séparés.

- *Séparation des partitions*
- *Séparation des privilèges*

Différents navigateurs

Ergonomie et sécurité

Outre l'ergonomie et l'apparence, les navigateurs se différencient par :

- *le respect des normes*
- *le respect des règles de sécurité*

Firefox est un navigateur à jour et respectant les normes et possibilités offertes par XHTML / CSS.

Internet Explorer dans sa version 7 ne respecte pas encore toutes les règles des normes modernes. IE 7 a amélioré sa compatibilité par rapport à IE 6.

Internet Explorer est pour l'heure un navigateur en retard de développement face à ses concurrents.

Du point de vue de la sécurité, son bilan est aujourd'hui assez mitigé. Les mises à jour de sécurité critiques arrivent tard, laissant les utilisateurs à la merci des sites infectés pendant de longues périodes.

Pendant l'année 2006, IE7 a connu 284 jours pendant lesquels une ou plusieurs failles exploitables étaient présentes.

Firefox n'en a connu que 9 la même année.

Les ActiveX de IE sont un vecteur d'infection virale exploité de diverses manières.

Les parts de marché donnent approximativement IE6 et IE7 à 25% chacun et Firefox entre 20 et 25% selon les pays.

Pour les utilisateurs de Windows, je recommande une utilisation de Firefox qui permet à l'heure actuelle de naviguer en bénéficiant d'une sécurité accrue.>

Reste pour compléter cette rubrique à étudier les autres navigateurs (à venir) ...

Tenants aboutissants

Si votre système est infecté par un virus de troie ou une autre technique permettant d'obtenir le contrôle à distance, vous devenez l'instrument des pirates à votre insu. A ce moment là vous pouvez sans vous en apercevoir devenir un relai de spam, un 'proxy' ou une plate-forme de DDoS.

Que recherchent les pirates ?

Les motivations des pirates sont essentiellement :

- *Le gain*
- *La notoriété*

Il existe un marché pirate où les compétences s'échangent, se monnaient. Les organisations qui agissent semblent à la fois en mouvement permanent et compartimentées de sorte qu'y remédier n'est réellement efficace que si chacun prend en charge la sécurité de ses propres données.

Distrubuted Denial of Service :

Les BotHerder (propriétaires de botnet) ayant réussi à intégrer un nombre élevé de machines (plusieurs centaines voir plusieurs milliers) revendent leurs services. Il existe de nombreux réseaux botnet.

Le botnet est un réseau de machines piratées aux ordres d'un ou plusieurs serveurs.

Le DDoS consiste à donner l'ordre à un grand nombre d'ordinateur de lancer des requêtes sans cesse à une ou plusieurs adresses destinataires qui se retrouvent submergées. Lors de toute la durée de l'attaque, le serveur ne peut plus répondre aux clients légitimes. Cette attaque est menée dans le but de nuire ou d'obtenir une rançon.

La distribution de spams

Les machines infectées relaient des spams (mails publicitaires) par milliers. Cela crée un flux permanent de mails sur les réseaux, cependant les techniques permettant de classer les spams à leur réception sont efficaces, notamment si l'émetteur n'est pas un serveur reconnu par une liste ou au contraire s'il se trouve dans une liste de spammeur connus.

SECURITÉ DES SYSTÈMES DE L'INFORMATION

La fraude aux clics

Il s'agit de simuler des clients qui ouvrent les liens publicitaires, rémunérant le site qui les héberge aux nombre de clients ayant cliqué sur le lien.

Le proxy

Un pirate se connectant à votre machine et agissant depuis celle-ci, effaçant les éventuelles traces avant de se déconnecter, se masque derrière vous lorsqu'il agit.

La capture des données sensibles

Les données qui intéressent les pirates et qu'ils peuvent collecter si vous êtes par exemple infecté par son virus comprennent :

- *Des numéros de carte bleue*
- *Votre adresse mail et celles de vos contacts*
- *Toute information sensible*

A partir du moment où votre machine est compromise, il existe des techniques comme l'installation de logiciels permettant la capture de vos mots de passe.

Plus d'informations

Garantir la sécurité de votre système

Votre sécurité ne peut être garantie simplement par l'utilisation de logiciels de protection.

Si vous utilisez Windows, il peut être très utile d'installer pare-feu, anti-virus.

D'autres systèmes comme Mac, Linux, BSD peuvent se passer d'anti-virus, généralement le pare-feu est employé.

Qu'est-ce qu'un pare-feu, comment ça fonctionne ?

La communication TCP/IP utilise des ports (65535) qui sont en quelque sorte l'adresse de destination sur votre machine, et une adresse IP qui représente votre ordinateur vis à vis du réseau internet tout entier.

Un ordinateur une fois installé contient souvent des applications qui écoutent sur

SECURITÉ DES SYSTÈMES DE L'INFORMATION

différents ports. Windows en particulier écoute sur les ports qui permettent l'échange de fichiers sur le réseau ou d'autres services.

En manipulant les données transmises et en exploitant des failles, un attaquant peut parvenir à ses fins.

Les deux solutions principales consistent à

- Maintenir son système à jour
- Utiliser un pare-feu

Lorsque une requête parviens de l'extérieur et si elle n'est pas la réponse à une demande faite au préalable, elle est refusée.

Ce principe demande au pare-feu de mémorises chaque message sortant puis d'attendre la réponse.

Les principes de la communications TCP/IP permettent cela, chaque message porte naturellement un numéro d'identification.

Il est assez difficile de savoir si l'on est piraté ou non. Une des méthodes pour cela est de regarder les flux d'entrée / sortie. Si votre ordinateur semble échanger en permanence des données et que les flux sont assez importants (par exemple quelques ko / s) cela peut être un indicateur. Il faut vérifier si le système ne télécharge pas automatiquement des mises à jour, ce qui est le cas de beaucoup de systèmes d'exploitation et de logiciels.

Protégez vos données

Si vous le pouvez, sauvegardez régulièrement vos données importantes. Gravez sur CD, DVD ou sur disque externe.

Si votre machine est infectée, vous risquez de sauvegarder le virus sur votre support.

Les cibles préférées

Les ordinateurs vulnérables et rapidement infectés sont certainement les systèmes anciens (comme Windows 98 ou 2000) dont les failles de sécurité sont semble-t-il multiples et massivement exploitées par les robots.

Les requêtes automatisées sont l'œuvre de pirates ratissant tout le réseau pour trouver de nouveaux systèmes vulnérables.

Mon constat est qu'à chaque écho en face d'une tentative d'accès donnée, les 'butineurs' arrivent, ces robots pirates qui scrutent internet. Votre adresse devient l'objet d'attaques de plus en plus nombreuses et si certaines ouvertures sont détectées, elles deviennent la proie de nombreux systèmes automatisés qui essaient nombre de failles connues pour une ouverture en particulier.

Par exemple, si vous n'avez pas de pare-feu et si vous utilisez Windows, à certaines requêtes sur les ports système, votre ordinateur répondra RST ACK ce qui correspond à "J'ai bien reçu la requête. Celle-ci est rejetée, fin de la communication.". Viennent ensuite nombre de requêtes tentant d'exploiter des failles de sécurité.

SECURITÉ DES SYSTÈMES DE L'INFORMATION

Les serveurs web sont l'objet de tentatives d'intrusion par diverses manipulations du port 80, le port TCP 80 étant voué à la communication des pages web.

Différentes solutions et leur niveau de sécurité

Une sélection de systèmes d'exploitation

- *Winwows, Microsoft*
- *Macintosh, Apple*
- *BSD : FreeBSD, NetBSD, OpenBSD*
- *Linux : RedHat, Fedore, OpenSUSE, Mandriva, Ubuntu, bien d'autres*

qu'est-ce qui les distingue ?

- *La qualité du code du système d'exploitation*
- *La variété des logiciels développés pour chaque plate-forme*
- *Le support des matériel, des périphériques*
- *Les objectifs*

Windows

Profil d'utilisateur : non expérimenté

Support matériel : très bon

Variété de logiciels disponibles : très bonne

Qualité du code : code fermé non disponible

Objectifs : grand public, facilité d'utilisation

Sécurité : pas de politique de sécurité par défaut, c'est une couche à ajouter.

Mac

Profil d'utilisateur : non expérimenté

Support matériel : bon

Variété de logiciels disponibles : bonne

Qualité du code : noyau BSD aux qualités reconnues par les spécialistes

Sécurité : sécurité élevée par défaut

BSD (OpenBSD FreeBSD NetBSD)

Profil d'utilisateur : expérimenté (en particulier pour OpenBSD)

SECURITÉ DES SYSTÈMES DE L'INFORMATION

Support matériel : suffisante pour les applications de bureautique

Variété de logiciels disponibles : suffisante pour les applications professionnelles et bureautique

Qualité du code : bonne qualité de code

Objectifs : sécurité d'utilisation, liberté d'utilisation

Sécurité : sécurité par défaut

Linux (en général)

Profil d'utilisateur : selon les distributions de non expérimenté à très expérimenté

Support matériel : suffisante pour les applications de bureautique

Variété de logiciels disponibles : assez bonne

Qualité du code : code de qualité correcte

Objectifs : stabilité, rapidité

Sécurité : varie selon les distributions

Optimiser votre sécurité

Dans le cas où vous auriez besoin d'une sécurité importante, vous pouvez considérer plusieurs solutions :

- Utiliser une machine hors réseau sur laquelle seulement des application sûres sont installées*
- Virtualisation de l'environnement servant aux applications à risques*
- Emploi d'un système d'exploitation ayant une sécurité reconnue*