



Malwares, quels enjeux ?

SOMMAIRE DU DOSSIER :

Remerciements

Introduction du dossier

I Introduction aux malwares

Introduction

1- Comment se fait-on infecter ?

A Les attaques informatiques

1-Par simple connexion

2-Par canaux IRC

3-Par failles de sécurités

4-Par sites piégés

5-Par les cracks

6-Par le P2P

7-Par faux codecs

8-Par Disques Amovibles

B-Les attaques psychologiques

1-Par E-mails

2-Le Phishing

2--La cyber-criminalité et les pirates de nos jours

A L'évolution de la cyber-criminalité et des pirates, de la gloire au profit.

B Les différents types d'infections.

1-Les infections de masses.

2-Les infections ou attaques ciblées.

C L'organisation des pirates.

3--- Pourquoi tout le monde est concerné

Conclusion

II Les Botnets

1- Introduction au botnets

A Définition/Fonctionnement des botnets

1-Définition

2-Taille

3-Les différents modes de fonctionnements

- A Les 2 architectures possibles
- B Les différents modes de contrôles

- 1-Via IRC
- 2-Via HTTP
- 3-Via P2P
- 4-Via les messageries instantanées

B L'évolution des botnets

2-- Les différents angles lucratifs des botnets

- A Le spam/phishing
- B Vente/Location de botnets
- C Les attaques par dénis de services distribués/chantage
- D Vol de données sensibles
- E Manipulation des sondages/Fraudes «au clic»
- F Diffusions de malwares
- G La vengeance

3 Les enjeux politiques des botnets

- A Le hacktivisme

4 Conclusion sur les botnets

III Les autres malwares

- 1- Le virus une espèce en déclin
 - 2-- Les vers d'aujourd'hui
 - 3--- Les trojans les malwares de l'ombre.
 - 4---- Les rootkits un réel danger peu connu du public.
 - 5----- Les Rogues un business très lucratif.
 - 6----- Le phénomène ransomware
- Conclusion sur les malwares

IV Comment s'en prémunir

- 1- Comment se protéger face aux menaces du net.
 - 2-- Comment se protéger face aux botnets.
 - 3---Une dernière mise au point
- Conclusion générale du dossier

Glossaire

==REMERCIEMENTS==

Ce dossier, à été commencé en Aout 2009 et terminé en Février 2010, par moi même (sayce) et réalisé dans son ensemble par moi même. Mais je ne l'ai bien sur pas fait totalement seul. Je me suis aidé de nombreux sites internet, ainsi que de nombreuses revues notamment les revus «MISC»; à chaque partie/article, les sources utilisées sont citées.

Mais je me suis aussi fait aider par des helpeurs plus expérimentés, qui m'ont donné des conseils, ont relu mon article pour me permettre de l'améliorer, etc..

C'est pourquoi je tiens à les remercier non pas d'un seul bloc sous le nom de «helpeurs», mais un par un.

Je tiens à remercier chaleureusement, ceux sans qui ce dossier n'aurait pas vu le jour,

Ric025, **Regis59** et **Cyrrus** pour leur relecture attentive, et leurs conseils.

A, **M@thew** pour la correction des fautes d'orthographes.

A, **Shimik_Root** pour sa magnifique illustration.

Et, hommage à **Toptibal** qui nous a quitté le jeudi 4 mars 2010

Je remercie aussi **Michael Forest** pour sa coordination des correction orthographiques, alliée à **Anthony5151**, **Nathandre**, **Ric025**, **ddbush91** et **supergeronimo44**.

==INTRODUCTION DU DOSSIER==

Ce dossier à été réalisé dans le but de faire découvrir, et de faire comprendre tous les risques qui résultent d'internet. La majorité des personnes utilisant internet ne connaissent absolument pas les risques liés à internet; soit par naïveté, soit par méconnaissance dans le domaine informatique.

Ceux qui utilisent les sites d'achats en ligne sans faire attention si leur PC est sain ou pas, s'étonnent de se faire voler leur numéro de carte bancaire .. alors qu'ils avaient un antivirus ...

Ceux qui téléchargent à tout va, des logiciels sur le net sans vérifier leur légitimité, et surfent sur des sites à risques, s'étonnent que leur PC plante ou ralentisse.

Ceux qui utilisent des cracks, les réseaux P2P etc, s'étonneront de voir germer sur leurs PC toutes sortes des publicités ou de faux logiciels antivirus.

Je pourrais continuer encore longtemps à vous énumérer les erreurs commises par la majorité des internautes, mais je préfère que vous lisiez ce dossier qui, je l'espère, vous évitera dans l'absolu, des infections.

Rappelez vous que la majorité des infections (environ 80%) sont dues aux utilisateurs, et non à la défaillance du système ou des logiciels de sécurités ..

Bonne lecture a tous, en cas de question n'hésiter pas à me contacter par message privé via mon compte de Comment Ça Marche : <http://www.commentcamarche.net/communaute/>

=I. INTRODUCTION AUX MALWARES=

==INTRODUCTION==

Nous voici partis dans la première partie de ce dossier, ici nous parlerons de, comment nos PC se font infecter par les malwares, de l'évolution des pirates, et nous tenterons de mobiliser tous les esprits, dans la dernière partie, je démontrerai que TOUS les systèmes sont vulnérables face aux malwares.

Inutile de «blablater» encore longtemps pour vous présenter la partie qui suit.

==1. COMMENT SE FAIT-ON INFECTER==

Voici la question principale :

«Comment un PC est t-il infecté par un malware ?»

Voici une énumération (non exhaustive) de la majorité des techniques utilisées par les pirates pour infecter les PC

Premièrement, il existe deux grandes sortes d'attaques/infections des machines. Les attaques dites «informatiques», elles regroupent donc toutes les attaques qui utilisent les failles purement informatiques, et non humaines. Les deuxièmes sortes d'attaques, sont les attaques psychologiques, c'est à dire les attaques qui reposent quasiment entièrement sur les failles humaines.

A-Les attaques informatiques

Comme dit plus haut, les attaques informatiques sont des attaques qui utilisent exclusivement des failles informatiques, ou toutes autres méthodes informatiques qui permettent l'infection d'un système par un malware.

1-Par simple connexion

Dés qu'un PC se connecte à internet, il est en danger, c'est à dire, que même sans rien faire, il peut se faire infecter, le plus souvent par des vers.

Une fois que le ver est sur le net, il scanne le réseau à la recherche d'un PC qui n'est pas à jour et qui a une faille de sécurité qu'il pourrait exploiter, il infecte le PC et une fois le PC infecté il scanne le réseaux à la recherche d'un second PC non à jour et ainsi de suite.

2-Par canaux IRC

Les infections par canaux IRC (infection MSN) se répandent de plus en plus. Voici comment elles fonctionnent :

Votre correspondant vous envoie une pièce jointe, le plus souvent avec un titre qui attire, vous acceptez l'envoi et votre PC est infecté. Ce genre d'infection sera traité plus loin dans ce dossier. Il ne faut jamais accepter une pièce jointe soit d'une personne inconnue soit d'une personne avec qui

vous n'êtes pas en discussion, demandez toujours la confirmation de la personne.

3-Par failles de sécurités

Les failles de sécurité, sont très souvent utilisées par les malwares pour infecter les PC. Les exploits, les vers, utilisent les failles de sécurité.

Les sites contenant des exploits (Sites de cracks) utilisent les failles de sécurité pour infecter automatiquement les PC qui se connectent à ce site.

4-Par sites piégés

Les sites piégés, sont des sites sur lequel des exploits, des balises i-frame, ou autres dispositifs sont installés, permettant l'infection automatique des PC se connectant à ces derniers.

Lorsque vous vous rendez sur un site piégé, l'exploit recherche si des failles de sécurité exploitables sont présentes, si oui il télécharge et exécute le fichier infecté à votre insu sur votre PC si votre PC est totalement à jour vous ne serez pas infecté. La balise i-frame agit de façon similaire.

Les Pirates ont tout intérêt à mettre des exploits sur des sites "populaires" ce qui leur permettra l'infection d'un plus grand nombre de machines, et donc un gain plus élevé. Les sites qui contiennent des exploits sont le plus souvent, les sites de cracks, les sites pornographiques ...

5-Par les cracks

Les cracks sont un des plus gros vecteurs d'infection sur le net, la majorité des cracks, une fois exécutés sur la machine, l'infecte. La famille Smitfraud, est un exemple d'infection s'attrapant par les cracks. Les sites de cracks, sont eux aussi porteurs d'infection du fait que la majorité d'entre eux contiennent des exploits. Il existe aussi de faux sites de cracks, ces sites ne servent qu'à infecter les PC des utilisateurs.

L'utilisation des cracks et donc très largement déconseillée si l'on veut garder un PC sain.

6-Par le P2P

Le P2P tout comme les cracks, est un gros vecteur d'infection, mais cela est énormément utilisé.

Un bon nombre de fichiers circulant sur les réseaux P2P sont des fichiers infectés, l'infection Lop s'attrape par certains logiciels de P2P, les rogues peuvent aussi s'attraper par le P2P.

Il faut donc éviter au maximum les réseaux P2P, au même titre que les cracks.

7-Par faux codecs

Les faux codecs sont téléchargeables le plus souvent pour les vidéos pornographiques.

L'internaute souhaite visionner la vidéo, et on lui demande de télécharger un ou plusieurs codecs pour la lire. En réalité, ces codecs, sont des fichiers infectieux qui installeront une infection sur le PC.

8-Par Disques Amovibles

Les infections par disques amovibles se sont énormément développées et aujourd'hui un grand nombre d'infections utilisent cette technique pour infecter les machines. Il suffit de brancher une clé USB ou tout autre disque amovible sur un PC infecté, pour infecter la clé USB. Une fois la clé infectée, en la rebranchant sur un PC sain, le PC sain devient infectieux.

B-Les attaques psychologiques

Les techniques psychologiques, utilisent pour la plupart les techniques de social engineering

1-Par E-mails

Les infections par pièces jointes ou par liens piégés via un e-mails fonctionnent encore mais sont de moins en moins utilisées. Cette technique repose sur le social engineering ou ingénierie sociale, et certains internautes naïfs croient encore à la légitimité de ces messages. La technique étant d'envoyer à quelqu'un soit une pièce jointe infectée avec un message demandant de l'ouvrir, soit un message contenant un lien vers un site piégé.

Dès que l'utilisateur ouvrira la pièce jointe, le PC sera infecté (Les pirates utilisent de plus en plus les faits d'actualités pour bernier et infecter les utilisateurs, par exemple la photo de machine ou encore de fausses informations à scandale: mort d'un tel ...)

Si le message contient un lien piégé le message demandera de l'ouvrir, et l'internaute sera envoyé vers un site piégé
Soyez donc très vigilants en regardant vos e-mails.

2-Le phishing

Le Phishing ou Phising est une technique d'ingénierie sociale. Il est utilisé la plupart du temps par e-mails. Les pirates reproduisent par exemple la page d'accueil d'un e-mail envoyé par une Banque ils y insèrent un message ou ils demandent le numéro de code de la carte bleue pour une raison quelconque, ou d'autres informations confidentielles L'utilisateur lambda pensera tout bonnement que c'est sa véritable banque et tombera dans le panneau.

Maintenant que j'ai énuméré les principales sources d'infection nous allons analyser plus en détail comment se déroule une infection.

Premièrement il faut que le malware réussisse à pénétrer dans le PC et comme vu ci dessus il existe des dizaines de techniques. Une fois que le malware à réussi a pénétrer dans le système du PC il s'y installe.

Une fois l'infection sur le PC elle crée plusieurs fichiers infectieux, plus des clés de registre et dans certains cas des rootkits

Voilà, l'infection a pénétré le système, elle s'est installée, il ne lui reste plus qu'à effectuer la tâche pour laquelle elle a été conçue, et c'est à partir de là que l'utilisateur peut se rendre compte de quelque chose, je dis bien «peut» car comme je l'ai dit certaines infections se prémunissent d'un rootkit, ce qui rend quasi impossible la découverte du malware sur le PC.

Ce que l'utilisateur voit sur son PC, les ralentissements, les messages d'erreur, les pubs, etc... est ce que l'on nomme les symptômes d'une infections. La plupart des infections sont caractérisées par certains symptômes (apparitions intempestives de pages à caractère pornographique est une des caractéristiques de l'infection navipromo) et c'est a partir de là que lors d'une désinfection le Helpeur saura quel outil utiliser.

Voici une image qui schématise ce que je viens d'expliquer :



Ensuite :

Exécution des malwares sur le PC

Ensuite :

Les malwares commencent
leurs taches sur le PC

Sources de la partie I.1 : Différents articles de Malekal : <http://forum.malekal.com/pourquoi-et-comment-je-me-fais-infecter-t3259.html>

http://www.malekal.com/securiser_ordinateur.php

http://www.malekal.com/securiser_ordinateur.php

Sites de Malekal :

http://www.malekal.com/menu_windows_securite.php

==2. LA CYBER-CRIMINALITE ET LES PIRATES DE NOS JOURS==

Dans cette partie nous analyserons comment les pirates et la cyber-criminalité ont évolué depuis la création de l'Internet. Nous verrons comment; s'organisent les pirates pour infecter les ordinateurs, quels sont leurs enjeux, les différents types d'infections.

A L'évolution de la cyber-criminalité et des pirates, de la gloire au profit.

Lors de l'apparition des premières infections, ceux qui les créaient, ne recherchaient aucun profit, mais seulement à montrer à autrui leur capacités informatiques. C'étaient principalement les Hackers qui se livraient à une «guerre sans merci», à celui qui infectera le plus de PC, ou qui créera le ver le plus spectaculaire. Vint ensuite ce que l'on appelle le Hacktivisme, ces Hackers qui déjouent les systèmes pour leurs idéaux, font tomber les serveurs d'organisations qu'ils rejettent, ce n'était que pour défendre leurs idées.

Aujourd'hui les pirates à la recherche de gloire sont de plus en plus rares, les Hacktivistes sont encore présents, mais de nouveaux pirates sont apparus, des pirates d'un nouveau genre qui n'existaient pas dans le passé et qui aujourd'hui se sont imposés. Ces pirates n'ont qu'un seul et même but, et font tout pour l'obtenir, un but qui n'existait pas avant: le profit.

En effet, le profit est ce qui motive la grande majorité des pirates de nos jours.

Pour gagner de l'argent, via internet, les pirates ont le choix :

- Utilisations de malwares en tous genres qui récupèrent les numéros de cartes bancaires, les mots de passe, ou autres informations personnelles qui pourront être revendus à des tiers.
- Ventes de malwares // failles // botnets // d'informations personnelles (NB, MDP)
- Racket par attaques DDOS // ransomwares
- Diffusions de malwares via le P2P
- Diffusion de malwares via les Cracks
- Diffusions de disques amovibles infectieux
- Par ingénierie sociale (Phishing ..)
- Infections par adwares
- Infections par rogues
- Exploitation de failles de sécurité via un exploit // balise i-frame.

...

Il en existe d'autres mais je ne vais pas tout lister.

Le fait que les pirates ne recherchent plus que le profit les rend bien plus dangereux que lorsqu'ils cherchaient simplement à se faire connaître/reconnaître.

Depuis que les pirates sont en quête du profit, de nouveaux dangers sont apparus, ou se sont développés; je parle notamment des botnets (dont nous parlerons plus loin), des rogues et adwares en tous genres, mais surtout des Rootkits et des chevaux de Troie; on peut aussi citer les exploits, qui permettent d'automatiser les infections par sites piégés. L'ingénierie sociale s'est aussi beaucoup développée depuis l'apparition des «nouveaux pirates».

Le recherche du profit, a obligé les pirates à s'organiser autrement qu'avant. C'est à dire: répartition des tâches entre les pirates, professionnalisation de chaque pirates dans un domaine précis, professionnalisation des pirates eux même; les pirates sont aussi devenus de plus en plus discrets, en effet comment mener des attaques, sur une vulnérabilité si tous le monde en parle ? Les pirates préférerons aux projecteurs des attaques par DDOS à l'encontre de grandes entreprises, la discrétion du vol de mots de passe par un cheval de Troie allié à un rootkit. Ce ne sont plus des petits rigolos qui créent les malwares (ceux qui permettent de générer de l'argent) mais des professionnels du crime informatique.

Les pirates pour gagner de l'argent peuvent vendre leurs outils sur des forums, et n'importe qui peut les acheter. Mais si leurs outils étaient compliqués à utiliser, rares seraient les acheteurs, c'est pour cela que les pirates les simplifient au maximum, pour permettre à n'importe qui de les acheter et de les utiliser sans avoir aucune connaissance en programmation, réseau sécurité ... Ce phénomène, rend donc possible à un pirate de ne plus maîtriser l'ensemble de la chaîne d'une attaque (recherche sur la/les cible(s), développement...) mais seulement, de monnayer son malware sur un site de pirates, et ensuite de laisser les acheteurs l'utiliser . Les pirates sont de véritable businessmen, ils permettent à leur clients, de rajouter des modules en plus, de mettre à jour leurs outils, ou encore d'avoir accès à des tutoriels.

Cette profusion d'outils faciles à prendre en main, risque d'entraîner une augmentation de la cybercriminalité, du fait que n'importe quel utilisateur lambda va pouvoir réaliser des attaques DDoS, récupérer des numéros de cartes bancaires via son cheval de Troie, il ne faudra plus être un «génie de l'informatique» ou un «informaticien chevronné» pour pirater des milliers de machines, il suffira d'acheter un outil de piratage quelconque, pour réussir à pirater des machines, sans savoir, ni programmer dans aucun langage, ni connaître le fonctionnement des réseaux/systèmes.

Il existe deux grands types d'infections, nous allons les analyser ici même :

1-Les infections de masse.

Les infections de masse correspondent aux infections les plus répandues, ce sont celles dont on parle le plus souvent et qui arrivent constamment sur le net. Ces attaques sont préparées par des personnes qui souhaitent toucher le plus de monde possible, pour augmenter leur gain.

Prenons pour exemple une infection par adware, ou autre logiciel publicitaire : plus les pirates arriveront à infecter un grand nombre de machines, plus ils gagneront d'argent.

Il y a 3 principales étapes aux infections de masse :

L'utilisation d'outils performants, qui permettent l'infection du plus grand nombre de PC possible. Soit les personnes à la tête de cette attaque codent eux même le malware soit ils font appel à un autre pirate qui codera pour eux.

Pour une infection de masse, le problème de l'hébergement se pose à un moment ou à un autre. Le choix de l'hébergement va jouer sur la réussite d'une opération de phishing ou autre opération de masse. Il existe de nombreux moyens d'hébergement pour les pirates, comme les sites web piratés, mais de plus en plus, les pirates les mieux organisés utilisent les hébergements «pare-balles», ou à l'aide de botnets. Le choix de l'hébergement repose aussi sur l'efficacité de «protection» des données frauduleuses du pirate.

Si l'hébergeur est un pays où il n'existe pas (ou quasiment pas) de lois anti-cybercriminalité, si de plus il a un décalage horaire élevé, tous ces atouts permettent une meilleure protection des contenus illicites.

De plus en plus, apparaît sur internet des hébergements pare-balle ou «bulletproof». Ces hébergements sont créés spécialement pour les pirates. Ils sont situés dans des pays sans

législation sur la cyber-criminalité, les administrateurs de ces hébergeurs garantissant un laxisme total envers les contenus qu'ils hébergent. Nous pouvons citer comme exemple d'hébergeur bulletproof l'hébergeur «Russian Business Network» (RBN).

Vient ensuite l'étape de la diffusion du malware. Le pirate, même dans le cas d'une infection de masse, doit cibler un minimum ses cibles. En effet envoyer des spams en français à des adresses e-mails japonaises n'a aucun sens. Le pirate doit donc trier les adresses e-mails qu'il se procure sur les forums dédiés au spam, pour que son attaque ait un minimum de sens.

Les infections de masse utilisent aujourd'hui de plus en plus des infections par le web. C'est à dire des infections par pages web infectées. Ce genre de pages web infectées utilisent un exploit, qui permet l'infection d'une machine par l'exploitation d'une faille de sécurité, du navigateur, de l'OS, ou encore des add-ons (= extensions). Les bannières de publicités infectées sont aussi beaucoup utilisées. Elles sont soumises à des régies publicitaires, qui ensuite les rediffusent auprès de sites totalement légitimes.

L'utilisation de balises «i-frame» sur des sites largement visités permettent l'exploitation automatique de failles.

Les infections de masse s'appuient aussi sur l'ingénierie sociale. En effet, les campagnes de phishing, d'envois de spam ou d'e-mails avec une pièce jointe piégée utilisent toutes des techniques d'ingénierie sociale. Malgré la sensibilisation des internautes, l'ingénierie sociale permet encore aux pirates d'infecter des machines par milliers, et de fonder leurs infections sur l'ingénierie sociale.

Faisons pour finir, un petit tour par les communautés de pirates. Les plus actives sont bien entendu les Russes et les Anglaises. Pour communiquer, les pirates utilisent des forums spéciaux dans la majorité des cas. La méfiance règne sur ces réseaux, en effet les pirates ne se connaissent pas et préfèrent s'organiser sous forme de réseaux.

Ce genre d'infection s'est maintenant banalisée sur internet, et risque de ne jamais s'arrêter. Aujourd'hui, et dans le futur, ces infections sont/seront à la portée de n'importe qui.

2-Les infections ou attaques ciblées.

Ces attaques sont les attaques les plus rares, ou du moins celles dont on parle le moins mais qui, le plus souvent, sont bien plus spectaculaires que les attaques de masse. Alors pourquoi n'en parle-t-on pas autant que des attaques de masse ? Du fait que ce sont justement des attaques ciblées, et comme leur nom l'indique, elles ciblent un groupe de personnes bien distinctes, ou une organisation, et non une «masse» quelconque de personnes.

De plus les personnes visées par ce genre d'attaques, sont le plus souvent de grandes entreprises, et elle n'iront pas se vanter d'avoir été espionnées par un pirate, qui a réussi à voler des centaines de giga-octets d'informations.

Les attaques ciblées peuvent de nos jours être mises en place par «n'importe qui», en effet comme vu ci-dessus les attaques de masse pouvaient, elles, être réalisées de plus en plus par des utilisateurs lambda. Les attaques ciblées, demandent elles une longue préparation, et de nombreuses connaissances avant de pouvoir être réalisées.

En effet, le pirate doit enquêter sur sa cible (une entreprise par exemple), récupérer des informations; quand à son système de protection informatique, quelle politique de sécurité impose t-il? etc ... En effet un pirate ne peut pas se permettre de lancer une attaque contre une entreprise sans avoir réalisé la moindre «enquête» à son égard, infecter des milliers d'internautes ne représente aujourd'hui pas un grand danger pour le pirate si son attaque a un minimum de sérieux, par contre attaquer une entreprise, pour voler des données, ou lui extorquer de l'argent est bien plus risqué.

Les entreprises ont des moyens bien plus importants que M. tout le monde en terme «d'enquête» pour retrouver la source de l'attaque. Les entreprises, peuvent faire appel à des entreprises spécialisées dans la sécurité informatique, ont des informaticiens à disposition, peuvent plus facilement faire intervenir la police .. Alors que M. tous le monde ne va déjà, la plupart du temps, pas se rendre compte d'une infection, sauf si il y a présence de symptômes comme des ralentissements, apparitions d'adwares (mais je ne dis pas que les entreprises découvrent systématiquement qu'elles ont été la cibles d'attaques), mais si nous n'avons pas conscience de l'infection, comment irait-on porter plainte, ou demander de l'aide ? Et même si on découvre l'infection, irait-on porter plainte ? Rarement, très rarement. Il est très difficile de remonter à la source de l'infection, et parfois impossible, si le pirate a bien effacé ses traces.

De plus, l'utilisateur lambda tentera en premier de supprimer le malware seul (via son antivirus, et en téléchargeant une ribambelle de logiciels de sécurité en tout genre), puis si cela ne fonctionne pas il ira soit sur des forums de désinfection, soit il enverra son PC chez un «réparateur» qui le lui formatera tout simplement, en sauvegardant *peut-être* les données de l'utilisateur.

De toutes façons, il est extrêmement rare, que des pirates tentent d'attaquer le PC d'une seule personne, à moins que ce soit une personnes connue, et que cela ait un effet médiatique ou autre. Les attaques ciblées visent ainsi dans la quasi-totalité des cas, des entreprises et des organisations (ONG, Politiques ..).

Ces attaques, sont très complexes, demandent des connaissances pointues en programmation, en système etc, et ne sont pas encore à la portée de n'importe qui, mais ça ne saurait tarder ...

C L'organisation des pirates.

Après l'apparition de ce nouveau «but», les pirates ont dû s'organiser en véritables réseaux, pour pouvoir continuer à «travailler» en toute discrétion.

En effet, fut un temps où les pirates travaillaient le plus souvent en solo.

De nos jours, certains pirates travaillent encore en solo, mais ils s'organisent de plus en plus en petits réseaux, où chaque pirate a une fonction bien définie (développement des malwares par exemple), et ne se concentre que sur celle-ci. Ces communautés de fraudeurs sont organisées comme de petites «entreprises», chacun des membres occupe un poste bien défini, développement, vente, infection...

Les pirates solos, n'exploitent que rarement leur «création», un pirate qui crée des chevaux de troie, va préférer les vendre plutôt que de les utiliser car ceci, est d'une part moins dangereux, et en plus cela rapporte plus d'argent; il arrive souvent, que les troyens soient conçus sur mesure, pour une personne bien distincte.

De plus en plus, les réseaux mafieux ou de crimes organisés se penchent sur l'argent généré par le marché du malware. Et de plus en plus, des informaticiens, ou des pirates sont recrutés par des réseaux mafieux pour réaliser telles ou telles opérations.

Le marché du malware et un marché florissant encore jeune mais en pleine expansion. Les réseaux mafieux qui se cachent derrière déjà bien des crimes (prostitutions, drogues..), se penchent de plus en plus sur le marché du malware pour une bonne raison : Il n'est que très peu surveillé.

Alors que celui de la drogue subit de fortes répressions, celui du malware est quasi immunisé face à la taille gigantesque du problème.

Il est très difficile de retrouver les créateurs de botnet, de trojan ou encore de chantage informatique. De plus la police est mal organisée face à ce nouveau visage du crime organisé.

Pour conclure, nous retiendrons que la cybercriminalité a encore de très beaux jours devant elle, que le seul but des pirates est principalement le profit, et que l'on assiste à une véritable professionnalisation des pirates avec répartition des tâches.

Les pirates n'étant plus simplement poussés par le désir de renommée ou de défi, mais de profit, ils risquent de trouver de plus en plus d'idées pour infecter les systèmes, en utilisant des techniques de plus en plus poussées et compliquées à contrer. Face à cette menace, seule une «bonne hygiène informatique» et une sensibilisations des internautes permettra d'éviter les infections, en plus des logiciels de sécurité installés, qui eux, malheureusement, ont plus d'une longueur de retard face aux pirates.

Sources de la partie I.2 : Revus MISC numéro 41.

==3. POURQUOI TOUT LE MONDE EST CONCERNE==

Je vais dans cette partie démontrer que personne n'est sûr à 100% de son système, que personne n'est à l'abri d'une infection.

Même si certains dispositifs permettent de minimiser les infections, on n'est jamais sûr à 100% de son efficacité.

Bien souvent sur les forums on entend parler de «Windaube» par des personnes n'ayant , le plus souvent, absolument pas étudié le problème des malwares et de Windows.

Du fait est que Windows est le système d'exploitation le plus répandu au monde, il est logique alors que ce soit celui qui soit le plus atteint par les malwares puisque les pirates souhaitent atteindre le plus d'ordinateurs possible.

Au moment de leur apparition, les systèmes d'exploitations alternatifs (Linux, Mac) ont été quasi-immunisés contre les malwares car ces derniers visaient seulement Windows.

Au fur et à mesure que les gens se sont intéressé à ces systèmes d'exploitation quasi-immunisés, les créateurs de malwares s'y sont eux aussi intéressé.

Commençons par «le concurrent» de Windows, Macintosh ou Mac, le système d'exploitation à la pomme. Il est apparu en 1984, créé par Jef Raskin et depuis connaît un certains succès auprès des fatigués du virus.

Le 1er malware découvert sur le système d'exploitation Mac OS X est Renepo (ou Opener) qui est apparu en octobre 2004, bien qu'il y ait eu controverse à ce sujet, certains affirmant que ça n'était pas un virus (=>Apple) alors que d'autres (=>Sophos) si.

C'est en Février 2006 qu'apparaîtra le premier «vrai virus» sur Mac OS X bien que Apple une fois de plus campe sur ses positions pour garder son image de «système d'exploitation immunisé», mais cette fois un grand nombre de sociétés antivirus le considéraient bien comme un virus, ce qui nous permet de douter sur la fiabilité des dires d'Apple.

Plusieurs failles jugées «critiques» ont été repérées sur Mac OS X dans les années 2003-2004; elles furent corrigées avec retard (plusieurs mois) par la firme à la pomme qui une fois de plus avait minimisé les risques liés à ces failles ...

De plus, l'utilisation de la suite bureautique Microsoft Office sous Macintosh peut engendrer une infection par virus macro. En effet de simples fichiers texte/tableur peuvent être la cible d'infections macro.

Ceux-ci sont des virus présents dans les scripts des fichiers du genre Excel, Word etc, ils permettent d'automatiser certaines tâches (remplir des tableaux par exemple).

Les macro-virus permettent de faire différentes actions, contrôler des données, de détruire des données et même d'effectuer des formatages de disque dur. Pour exemple, le vers Melissa qui se répandait via les macros, à ainsi pu infecter quelques milliers d'utilisateurs de Mac. La suite OpenOffice est aussi concernée par ce genre de virus.

Pour conclure rapidement, nous pourrions simplement dire que les utilisateurs de la pomme ne sont pas immunisés contre les infections.

Passons maintenant au système d'exploitation GNU/Linux, premier système d'exploitation libre créée en 1991 par Richard Stallman ainsi que par des milliers d'informaticiens qui ont contribué au projet.

Pour rappel, un logiciel libre est un logiciel qui doit remplir au minimum les 4 critères suivants :

Liberté 0 : La liberté d'exécuter le programme — pour tous les usages

Liberté 1 : La liberté d'étudier le fonctionnement du programme — ce qui suppose l'accès au code source

Liberté 2 : La liberté de redistribuer des copies — ce qui comprend la liberté de vendre des copies

Liberté 3 : La liberté d'améliorer le programme et de publier ses améliorations — ce qui suppose, là encore, l'accès au code source

Voilà, pour en revenir aux malwares, ceux existants sous linux sont de moins de 1000 (870). Le plus connu de tous est Bliss, virus qui fit très peu de dégâts (ce virus à surtout été crée pour démontrer l'immunité de Linux).

Linux est un système d'exploitation sur le quel la sécurité est plus au point que sur Windows. Pour résumer, les droits d'administrateur ne sont pas donnés par défauts ce qui évite beaucoup d'infections (impossibilité de modifier les fichiers systèmes..), les failles sont souvent rapidement réparées ou encore le fait que GNU/Linux soit totalement Open Source permet à des experts en sécurité d'analyser le code source et donc d'apporter leurs connaissances contrairement à celui de Windows.

Donc Linux est moins vulnérable aux virus que Windows, mais ce n'est pas pour cela qu'il est immunisé. Le plus grand danger pour les systèmes d'exploitation comme Linux/Mac... sont les virus que l'on appelle «multi-plateforme», ce sont des virus capable d'infecter autant les systèmes Windows que Linux ou encore Mac.

Je dirais donc simplement pour finir cette partie, que, qui que vous soyez, ne vous croyez JAMAIS immunisés contre les malwares, car quelque soit votre OS, votre Antivirus, ou autres systèmes, votre protection ne pourra jamais être fiable à 100%.

==CONCLUSION==

Pour conclure cette 1ère partie «Introduction aux malwares», je rappellerai simplement que les pirates de nos jours se fichent de la renommée, ils ne cherchent que les gains; et c'est cela qui les rend plus dangereux que jamais. Ils trouvent chaque jour de nouveaux moyens pour infecter les internautes, chaque jour plusieurs centaines de malwares sont créés, et enfin que, face à cette menace, il faut être vigilant sur le net, et surtout ne pas faire l'erreur de se croire intouchable.

Sources de la partie I.3 : Article de CCM : <http://www.commentcamarche.net/faq/5865-mythe-linux-est-invulnerable-face-aux-virus>

Sujet du forum CCM :

<http://www.commentcamarche.net/forum/affich-15806462-gnu-linux-et-les-virus>

Autres liens : <http://pjarillon.free.fr/redac/virus.html>

=II LES BOTNETS=

==1.INTRODUCTION AUX BOTNETS==

A Définition / Fonctionnement des botnets

1-Définition

Les botnets sont des réseaux de taille variable d'ordinateurs «zombies» dirigés par un pirate informatique. Ils ont été infectés par un logiciel de type backdoor nommé bot qui permettra au pirate de diriger à distance les ordinateurs. Ces réseaux de PC zombies sont utilisés la plupart du temps à des fins lucratives ou encore politiques.

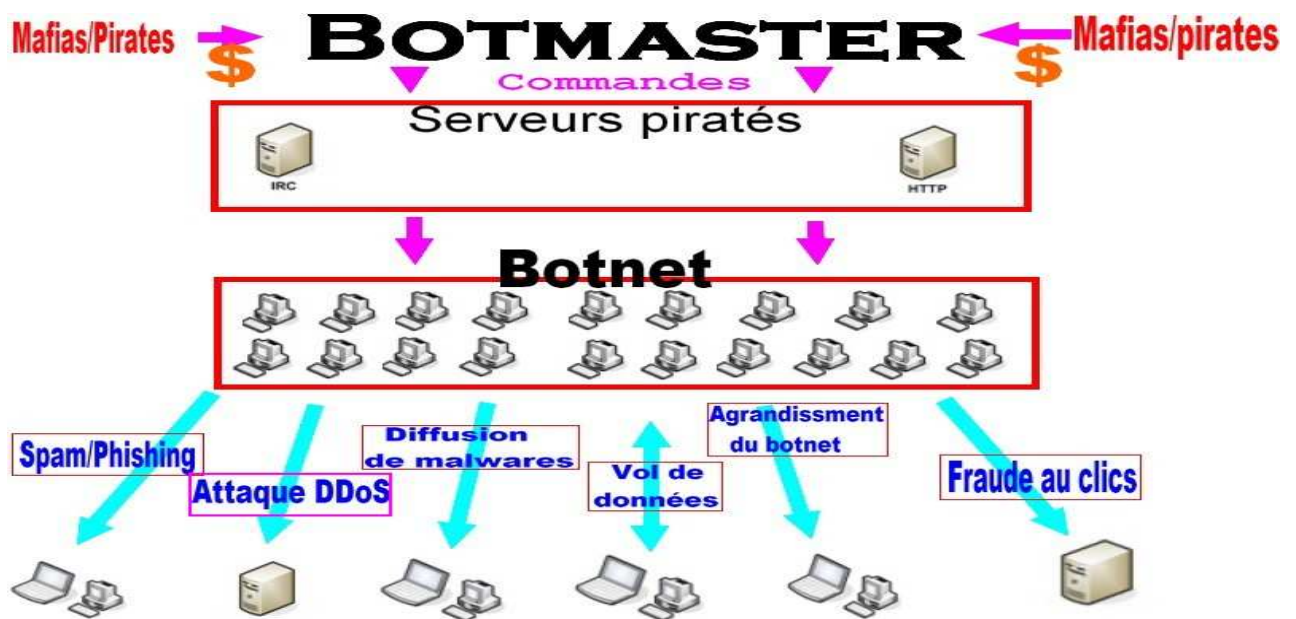
Nous verrons dans cette partie quelle utilisation en font les botmaster (pirate dirigeant un botnet), quels en sont les dangers et nous verrons qu'il existe plusieurs architectures et différents mode de fonctionnement de botnets.

Les botnets constituent un réel danger pour l'internet, qui n'a pas encore été pris très au sérieux par les utilisateurs, bien que les experts en sécurité ne fassent qu'interpeller *les gens*. Les botnets sont un problème dont très peu de personnes sont au courant et encore moins de personnes comprennent l'envergure du problème.

C'est pour cela en partie que je rédige ce dossier pour avertir les utilisateurs d'internet et leur annoncer qu'un danger encore plus grand que les vers comme «Melissa» et «I Love You» qui faisaient la une des journaux il y a 9/10 ans, un danger encore plus grand que les premiers chevaux de Troie qui permettaient la prise de contrôle à distance de PCs. Aujourd'hui, grâce à leurs botnets, les botmaster peuvent de leur sous-sol contrôler des milliers d'ordinateurs de façon totalement anonyme à des fins totalement illégale et lucrative.

En 2007 Vinton Cerf cofondateur de internet, estime que un quart des PC reliés à internet serait des PC zombies.

Voici pour finir un schéma qui montre le fonctionnement des botnets :



2-Taille

16

La taille des botnets est variable, elle peut être minime mais peut être immense comme par exemple ce cas de trois pirates informatique néerlandais accusés d'avoir corrompu 1,5 million d'ordinateurs. Ce genre de cas reste encore rare la plupart des botnets sont formés d'une dizaine de milliers de machines ou plus. Voici quelques exemples évoqués par Joe Stewart, directeur de la recherche sur les malwares chez SecureWorks en avril 2008 :

- Srizbi - 315 000 machines
- Bobax - 185 000 machines
- Rustock - 150 000 machines
- Grum - 50 000 machines
- Ozdok - 35 000 machines
- Wopla - 20 000 machines

3-Les différents modes de fonctionnement (Architecture Centralisée / Décentralisée) (mode de contrôle : IRC HTTP P2P Ajax)

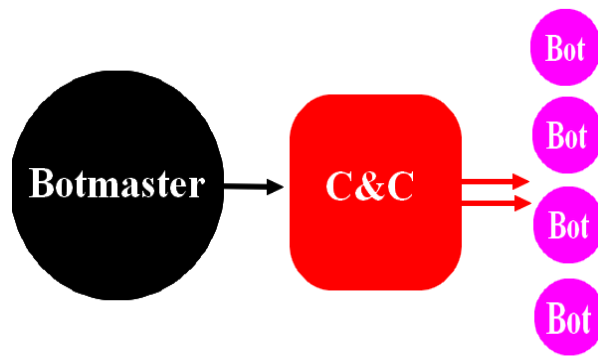
C'est une partie que je veux abordable à tous niveau de connaissance informatique, c'est pour cela que je ne m'attarderai pas trop sur certaines choses, cette partie est surtout destinée aux personnes qui veulent comprendre en gros comment fonctionne un botnet.

A Les 2 architectures possibles

Il existe 2 architectures possibles dans les réseaux botnets. L'architecture centralisée et l'architecture décentralisée.

Commençons par les botnets à architecture centralisée, appelés aussi «réseaux zombies à centre unique».

Voici un schéma d'un botnet à centre unique :



Le créateur de ce genre de botnet ne contrôle pas directement les PC zombies, il les dirige via l'intermédiaire d'un **Centre de Contrôle et de Commande** (Control & Command Center en anglais)

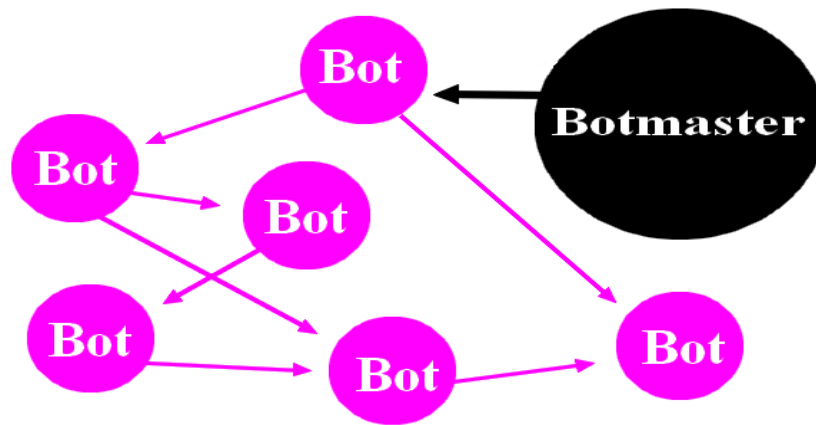
Le centre attend la connexion des nouveaux bots les enregistre dans sa base et leur envoie des instructions sélectionnées par le propriétaire du réseau de zombies. Le propriétaire doit obligatoirement pouvoir accéder au C&C sinon il ne peut **PLUS gérer son Botnet**. C'est une administration dite "centralisée". Grâce à cette technique les instructions du propriétaire circulent très rapidement dans le réseau, en contre partie la lutte contre ce genre de réseaux est facilitée par le fait qu'il suffit de stopper le C&C pour «tuer» le botnet.

La 2ème architecture possible est une architecture dite décentralisée ou P2P

Dans ce genre de réseau les PC zombies ne se connectent pas à un Centre de Contrôle et de Commande. Ils se connectent entre eux pour recevoir les instructions du propriétaire. Ainsi chaque PC possède l'adresse de quelques uns des autres PC du réseaux, il suffit donc à l'administrateur du réseau de pouvoir se connecter à un seul des PC pour pouvoir l'administrer en entier, c'est une administration dite "décentralisée". La circulation des instructions est bien plus longue dans ce genre de réseau.

Ce genre d'administration est plus rare car plus difficile à créer. La lutte contre ces réseaux est aussi bien plus difficile car ils sont décentralisés, et non centralisés comme les précédents, il faut donc repérer les uns après les autres les machines zombies du botnet pour le stopper définitivement.

Voici un schéma d'un botnet décentralisé :



Parfois pour se simplifier la tâche les botmasters créent un botnet centralisé puis le décentralisent au fur et à mesure du temps.

B Les différents modes de contrôles

Après avoir différencié les différentes architectures des botnets, nous allons voir qu'il existe aussi plusieurs modes de contrôles pour administrer un botnet.

1-Via IRC

C'est une des architectures les plus répandues, les PC zombies se connectent à un canal IRC privé, et attendent leur mise à jour, les instructions... C'est une approche très simple pour le botmaster du fait qu'il lui suffit de se connecter au réseau IRC pour donner ces instructions à toutes les machines zombies. Mais en contre partie c'est assez simple à repérer, il suffit de surveiller le trafic IRC, une fois le canal repéré il est neutralisé et le botnet est tué. Mais parfois certains botnets déploient des mesures de protection contre la police anti-cybercriminalité. Mais ce mode de contrôle tend à disparaître du fait que lors de la contamination et de l'entrée dans le botnet de PC appartenant à une entreprise le port correspondant au protocole IRC (compris entre 6664 et 6667) sera dans la plupart des cas stoppé par le proxy.

2-Via HTTP

Bien plus difficile à repérer que les trafics IRC, cette architecture tend à se développer de plus en plus. Il suffit que le bot émette une requête, il reçoit une réponse et après exécution il reviendra chercher des instructions du botmaster. Cela permet une meilleure furtivité des botnets HTTP contrairement aux botnets IRC / P2P car ces derniers demandent une connexion permanente et sont donc plus simple à repérer.

3-Via P2P

Grâce à ce système là, les bots ne dépendent pas d'une tête centrale (C&C) mais s'appuient sur une architecture similaire à celle utilisée par les réseaux peer-to-peer (P2P).

Il est assez difficile de stopper ce genre de botnet, car chaque bot fait office de C&C pour les autres bots. Le botnet Storm Worm utilise ce mode de contrôle.

4-Via messagerie instantanée

Cette architecture utilise des canaux de messagerie instantanée comme MSN, ICQ... Ce genre de botnets n'est que peu répandu car cette technique s'avère peu populaire. Les instructions du botmaster circule assez lentement entre tous les bots.

B L'évolution des botnets

Les réseaux zombies sont apparus dans les années 1998-1999, avec l'apparition des premiers logiciels de type backdoor.

En mai 1999, un ver fit son apparition visant les environnement Windows. Il permettait d'envoyer des données du PC infecté aux pirates, en attendant les ordres de ce dernier sur un canal IRC. C'est aux alentours des années 2000 (plus précisément 2002) que le terme «robot» est apparu dans les médias.

Les experts en sécurité informatique ont toujours tenté d'alerter les internautes de ce que représentaient les botnets, et représentent toujours aujourd'hui ; mais rares sont les internautes connaissant seulement les mots «botnet» et encore moins en connaissent les réels dangers. Encore aujourd'hui les botnets évoluent, et les réseaux zombies de la tempête effraie réellement les experts.

Ces réseaux de PC zombies démontrent bien l'évolution des malwares et de la cybercriminalité, qui hier ne correspondait qu'à quelques individus isolés qui se défiaient, et qui aujourd'hui correspond à des groupes d'individus organisés dont le but est seulement lucratif. Je peux simplement dire que l'évolution des botnets n'est sûrement pas finie, et qu'ils demeureront un grand danger pour le monde.

==2 LES DIFFERENTS ANGLES LUCRATIFS DES BOTNETS==

A Le spam / phishing

L'angle le plus lucratif des botnets est bien entendu le spam et le phishing. Certains botnets envoient plusieurs milliard de spams par jour ! Il est estimé que environ 80% à 90% du spam émis provient des botnets.

Le spammeur paye le botmaster pour envoyer un certain nombres de spams, les tarifs seraient d'environ 300€ à 800€ pour 1 million de spams à des adresses spécifiques, ou encore environ 500€ pour 20 millions de spams en 15 jours. Grâce à ce trafic les botmaster s'enrichissent rapidement. Cisco dans son rapport trimestriel interview un botmaster et annonce , qu'il peut gagner grâce à son botnet entre 5 000 à 10 000 \$ par semaine.

Des botnets comme Srizbi composé d'environ 300 000 machines permet d'envoyer 60 milliards de spam par jours, d'autre comme Spamthru composé «seulement» de 12 000 machines permet tout de même d'envoyer 350 millions de spams par jour. L'envoi de spams est l'angle le plus lucratif dans les «affaires» d'un botmaster

B Vente/Location de botnets

Les botmasters peuvent, comme n'importe qui qui louerait / vendrait sa maison, louer ou vendre son botnet. Cette tendance se nomme le «Malware as a Service» (MaaS). Du fait que l'argent à envahi le net, et que la plupart des pirates créent des malwares pour l'argent, et bien aujourd'hui le malware se gère comme une offre, en fonction de ses fonctions, qualités etc et par ses caractéristiques, il correspondra à tel ou tel tarif.

Cette tendance intéresse particulièrement les escrocs incapables de développer des botnets, et qui préféreront louer ou acheter directement le botnet tout fait au propriétaire.

C Les attaques par déni de service distribué / chantage

Les attaques par déni de service distribués (DDoS) sont des attaques qui consistent à rendre indisponible pendant un laps de temps plus ou moins long les services d'une organisation, le plus

souvent les serveurs d'une entreprise. Ce genre d'attaques est très souvent mené par des botnets, du fait qu'il sont constitués d'un grand nombre d'ordinateurs. Ce genre d'attaques coûte environ entre 25 et 100\$ pour leur mise en place et ensuite environ 20\$ l'heure et 100\$ la journée. Elles sont le plus souvent lancées sur les serveur d'une entreprise pour lui soutirer une certaine somme d'argent. De nombreuses entreprises en ont subi les conséquences et souvent payent la rançon pour éviter de devoir subir une attaque plus grande, qui leur ferait perdre des grosses sommes d'argent. Pour exemple, récemment, en novembre 2009, les sites d'Amazon et de Wal-Mart ont été touchés par des attaques DDoS, en août 2009 c'est Twitter le géant du micro-blogging qui a été victime d'une attaque DDoS. Même si des rançons ne sont pas toujours demandées ce genre d'attaques entraîne de lourdes pertes d'argent pour les sociétés touchées ; et c'est parfois cela qui est recherché si l'attaque DDoS à été lancée par vengeance, ou encore par un concurrent de l'entreprise.

D Vol de données sensibles

La possession du botnet permet aussi de dérober des informations sensibles aux ordinateurs infectés par le bot. Ces vols d'informations peuvent êtres réalisés à des fins politiques, terroristes etc, mais le plus souvent sont réalisés au hasard pas les botmaster, qui ensuite revendent ces informations sur des forums underground. En 2008, un botnet spécialisé dans le vol de données confidentielles (mot de passe, identifiant, numéro de carte bancaire, ...) nommé Clampi agissant depuis 2007 a été repéré. En 2008, Joe Stewart, directeur de recherche chez SecureWorks Inc a présenté à la conférence Black Hat de Las Vegas un botnet russe lui aussi spécialisé dans le vol de données, les pirates avaient réussis à accumulé 500 Go de données en 6 mois dont 8 485 comptes bancaires, 3 233 numéros de cartes de crédit...

Je vous conseille donc de vous assurer de l'intégrité de votre machine et de ne pas vous connecter à votre e-mail, ou de faire des transaction bancaire d'un PC qui n'est pas le votre (cyber-café ...).

E Manipulation des sondages / Fraude «au clic»

Certains webmasters, pour gagner de l'argent, passent des contrats avec des agences publicitaires, ils affichent des bannières publicitaires sur leur site et en fonction du nombre de «clics» payent une certaine somme d'argent au webmaster. Les botmasters grâce à leur botnet peuvent simuler des clics publicitaires, ce qui entraîne une explosion des sommes versées par les sociétés publicitaires.

Selon Click Forensics, fin 2008 les botnets représentaient 27% des clics frauduleux. Récemment c'est le botnet Bahama qui faisait parler de lui en créant une gigantesque fraude aux clics. Ce type «d'attaques» représente un grand danger pour les sociétés publicitaires en ligne.

F Diffusion de malwares

Comme dit précédemment, les botmasters louent leurs botnets aux spammeurs et autres escrocs du net, mais ils louent aussi leurs services, en proposant par exemple la diffusion d'adwares ou autres malwares à travers le net. Plus il réussit à installer le logiciel demandé sur un nombre important de machines plus il sera rémunéré. Officiellement il faut que l'utilisateur soit d'accord pour installer ce genres de logiciels sur son PC, mais grâce au botnets il est tout à fait possible de s'en passer.

G La vengeance

Certaines fois les actions menées par les botnets ont pour mission d'assouvir la vengeance de certaines personnes envers une autre. Et ce notamment via les attaques DDoS qui permettent de déstabiliser un site et de lui faire perdre de colossales sommes d'argent.

=3.LES ENJEUX POLITIQUE DES BOTNETS=

A Le hacktivisme

Les botnets de par leurs puissance d'action intéressent non plus les pirates ou autres mais intéressent de plus en plus les états. Tout comme la bombe nucléaire à son époque, les botnets d'aujourd'hui qui eux ne tuent pas mais qui permettent pour les plus gros d'empêcher un état entier de se connecter à internet. Ou encore pour les dictatures en place, de lancer des attaques botnets contre un site de l'opposition lui permettra d'asseoir sa légitimité. Nous avons déjà été les témoins de la première cyber-guerre en été 2007 entre l'Estonie et la Russie. Le déplacement d'une statue en hommage aux soldats russes de la capitale à un cimetière militaire a été l'origine d'attaques massives envers des sites estoniens.

=4.CONCLUSION SUR LES BOTNETS=

Que dire, vous l'aurez compris tout seul je pense, les botnets représentent une menace gigantesque, ils ne sont pas prêt de disparaître.

Ils ont révolutionné la cyber-criminalité, ont accru le désir de gains qui nourrissent déjà les pirates avant leur explosion. Ils permettent à un individu, de racketter en tout anonymat, ils permettent à un individu de faire tomber des serveurs entiers, de faire pression sur un pays entier, de lui faire gagner de grosses sommes... Alors pourquoi s'arrêteraient-ils ? Comment les détruire ? Comment lutter contre cette menace ?

C'est très difficile, il n'existe aucune solution satisfaisante, mais seulement des «solutions» qui permettent de limiter leurs dégâts.

Encore une fois, soyez vigilant en surfant, ou alors vous risquez de participer à votre insu à un cyber-racket, ou autres actions illégales.

Sources de la partie II : Botnet Business :

<http://www.viruslist.com/fr/analysis?pubid=200676152> ,

Bots et Botnets :

<http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2009-Bots-et-Botnets.pdf>

==III LES AUTRES MALWARES==

==INTRODUCTION==

Dans cette partie nous allons simplement analyser l'évolution des différentes sortes de malwares. Les virus en premier lieu, nous verrons qu'il ont perdu de leur «splendeur» natale ; puis nous analyserons les vers d'aujourd'hui pour faire remarquer, que eux n'ont pas pris une ride. Ensuite nous passerons au troyens, pour montrer qu'ils demeurent encore une menace pour les internautes, ensuite viendront les rootkits, qui eux représentent une très forte menace, inconnue du public.

Puis nous passerons aux rogues et pour finir nous parlerons ransomware.

=1.LE VIRUS, UNE ESPECE EN DECLIN=

Fut un temps ou l'on ne parlait que de virus voir de vers (qui sont en fait des *virus réseau*) en ce temps là, les chevaux de Troie, les rogues, les rootkits et tous les autres malwares n'existaient pas, ce temps là correspondait comme vous l'aurez peut être deviné aux temps des années 1980-1990, le temps de la naissance de l'internet. Comme dit plus haut dans ce dossier, le terme «virus» désigne (pour ceux qui l'utilisent de façon courante et souvent ignorante) l'ensemble des menaces du net, alors qu'il n'en est rien ; si les virus étaient aujourd'hui la seule menace du net alors ce dossier n'aurait pas vraiment lieu d'être car les menaces présentes de nos jours n'ont rien

à voir avec de simples virus. Je ne dis pas que les virus ne représentent pas de danger, mais face à des menaces telles que les rootkits ou les botnets, les virus ne sont «pas dangereux». De nos jours, les virus sont de plus en plus rares, ils ne sont plus de «simples» virus, ils comportent des fonctionnalités en plus comme keyloggers (enregistrement des mots de passe) ou chevaux de Troie (prise de contrôle à distance).

Pour faire un peu d'histoire, je prendrai l'exemple du virus Tchernobyl qui sévit des années 1998 à 2002. C'est l'exemple type du virus dont certaines personnes ont encore idée, il permettait tout simplement de détruire l'ensemble des informations du système infecté, et parfois rendait la machine inutilisable. Ce genre de virus est aujourd'hui très rare (voir inexistant). Pour vous donner d'autres exemples que les pirates des années 1980-2000 n'avaient pas tellement d'imagination hormis la destruction entière ou partielle du système, je peux vous citer des noms de virus comme, Datacrime qui agit en 1989 et qui formatait le système du 13 octobre au 31 décembre, ou encore Jerusalem (un vicieux !) qui lui, tous les vendredi 13, supprimait tous les programmes exécutés par l'utilisateur.

Voilà je pense que la partie virus peut s'arrêter là, il faut simplement retenir que maintenant les virus «destructeurs» n'existent quasiment plus et que contrairement aux premiers virus qui souhaitaient faire le plus de dégâts possible, les malwares d'aujourd'hui eux se font le plus discret possible, car comme dit dans la partie «qui sont les pirates d'aujourd'hui» le but principal des pirates d'aujourd'hui est le profit, qu'y a-t-il comme profit de détruire un ordinateur ? Aucun ! Alors que de le contrôler à distance, d'y voler par l'intermédiaire de quelque malware (cheval de Troie le plus souvent) les mots de passe ou autres informations personnelles est largement plus rentable.

Sources partie III.1 : Wikipedia : http://fr.wikipedia.org/wiki/Virus_informatique
Autres sites divers.

==2.LES VERS D'AUJOURD'HUI==

Contrairement aux virus les vers continuent à se développer et, de temps en temps, des vers comme le célèbre « I Love You », apparu en mai 2000, ou bien Sasser en 2004 et plus récemment Conficker (2008), font la une des médias de par leur vitesse de propagation extrêmement rapide cf. Vidéo. Ce genre de vers exploite des failles de sécurité informatique, ou utilise l'ingénierie sociale pour infecter les PC. Il faut souligner que parfois ce genre de vers utilise l'actualité pour se diffuser, par exemple la saint Valentin, ou encore très récemment lors de la mort de Michael Jackson certains pirates ont utilisés cette information pour diffuser des malwares ; soyez donc vigilants aux messages du genre «*le président giflé*»... . Les vers sont encore assez présents de nos jours, et constituent une menace pour les internautes.

Le développement de ce que l'on appelle des «réseaux sociaux» dont le plus connu est bien entendu le célèbre «facebook» à entraîné le développement d'une nouvelle sorte de vers. Le ver le plus célèbre exploitant les réseaux sociaux est bien entendu le ver Koobface découvert en 2008. Les machines infectées par ce ver envoient automatiquement des messages attrayant à tous les «amis» de facebook de l'utilisateur. Si la personne recevant le message a la malheureuse idée de l'ouvrir, alors il lui sera demandé de télécharger une nouvelle version de Adobe, qui n'est en fait qu'un fichier infectieux, ce fichier permet de rediriger l'utilisateur sur des sites néfastes et parfois de récupérer des données sensibles sur la machine de l'utilisateur.

En plus des réseaux sociaux, est apparu il y a maintenant une dizaine d'années environ les messageries instantanées ; et depuis leur apparition elles n'ont cessé de se développer et de regrouper toujours plus de fans. C'est notamment les adolescents qui utilisent la messagerie instantanée dont la plus connue est bien sûr MSN. Et bien sûr, tout ce qui attire du monde, facebook, MSN ou autre attire aussi les pirates...

Eh oui ! Il est apparu des vers «de messagerie instantanée» qui se propagent via MSN ou tout autre canal de messagerie instantanée. Ce genre de vers se propage de la façon suivante : vous êtes sur MSN et un de vos contact vous envoie un fichier à télécharger avec un message du genre : «Regarde la photo là...» ou un autres titre qui pourrait éveiller votre curiosité. Si vous acceptez, une fois le fichier téléchargé sur votre PC, vous serez à votre tour infecté, et à votre tour vous enverrez à vos contacts des fichiers infectieux. Ce genre de vers fonctionne comme des trojans (chevaux de Troie), c'est à dire que, une fois sur la machine, il peuvent récupérer des informations et les transmettre à un tiers et, dans certains cas, ils peuvent même transformer le PC en zombie. La famille des trojans IRCBot se propage via MSN, en envoyant un fichier accompagné d'un message à tous les contacts de l'utilisateur, une fois le fichier téléchargé, il se copie dans le répertoire Windows et dans system32 puis modifie la Base De Registre (BDR) pour se lancer au démarrage du PC. Une fois cela fait, il patiente en attendant les instructions du pirate.

Voici une image, prise sur mon PC d'une personne atteinte d'une infection MSN, et m'envoyant un lien :
Cela vous donne un aperçu du genre de message envoyé.



En début de cette partie, j'ai énuméré quelques uns des vers les plus connus au monde, nous allons parler maintenant de l'un d'eux, Storm.

Le ver Storm qui a permis la création du plus grand botnet connu à ce jour tient son nom d'une tempête ayant ravagé l'Europe en 2007, comme je l'ai dit plus haut, les pirates utilisent souvent les faits divers pour attirer les utilisateurs dans leurs pièges; dans ce cas-ci, les créateurs de Storm ont incité les utilisateurs à exécuter un fichier .exe attaché à un e-mail. Storm incarne bien le fait que les malwares évoluent aux cours du temps. En effet il a été l'un des 1^{er} à utiliser une architecture décentralisée pour diriger son botnet, de plus il utilise des techniques d'ingénierie sociale faisant référence à l'actualité, dans leurs e-mails, les créateurs de Storm utilisent des illustrations riches en design, ce qui accroît leur crédibilité pour les internautes.

Citons quelques uns des thèmes utilisés par Storm dans ce mini tableau :

Actualités	Décembre 2006/Mai 2007
Halloween	Octobre/Novembre 2007
Souhaits du nouvel an	Janvier 2007
Carte pour la St Valentin	Février 2008

Voilà, ceci vous montre bien que l'ingénierie sociale est un gros vecteur d'infections (tout comme le P2P/cracks) et qu'il faut être très vigilant sur le net.

La taille de ce botnet est difficile à estimer du fait qu'il est décentralisé. Microsoft a annoncé que son outil pour supprimer Storm des systèmes Windows en a désinfecté 274372. Il a été annoncé qu'il avait infecté plusieurs millions de PC, mais ce genre d'annonce est à prendre avec méfiance.

Comme la majorité des botnets, storm a été utilisé pour mener des attaques par déni de service (DoS). En 2007, Joe Stewart a publié un article pour montrer que Storm lançait des attaques DoS contre les sites d'organismes combattant le spam. De plus storm a été utilisé pour l'envoi massif de spams.

Les créateurs de storm utilisent aussi le pump and dump pour s'enrichir, la promotion des actions a ensuite été faite via des fichiers mp3 attachés aux e-mails pour contourner les filtres anti-spams.

Voilà pour la présentation de ce botnet, bien que ce botnet ait subi un très fort suivi médiatique, il existe des botnets comme Srizbi ou Kraken, qui peuvent chacun envoyer 50 milliards de messages par jour pour le premier, et 9 milliards pour le second

Je vous propose avant de conclure cette vidéo: <http://www.youtube.com/watch?v=kH8cS1AkqI> qui présente la vitesse de diffusion de Storm à travers le monde ... impressionnant ...

Pour conclure sur cette partie, je dirai que contrairement aux «véritables virus», les vers sont encore très présents sur le net, et représentent encore un grand danger pour les internautes; ils permettent comme vous l'avez vu, de créer de gigantesques botnets de plusieurs milliers de machines. Ils se répandent souvent par le biais de l'ingénierie sociale, ou alors par les failles de sécurité présentes sur les ordinateurs.

C'est pour cela qu'il faut être très «critique» vis-à-vis de ce que l'on vous propose sur le net, pour éviter d'être victime de l'ingénierie sociale, et tenir tous ses logiciels à jour.

Sources de la partie III.2 : Wikipedia http://fr.wikipedia.org/wiki/Ver_informatique

Connaissances personnelles

Revus MISC numéro 38

Autres liens :

<http://www.secureworks.com/research/threats/storm-worm/>

<http://www.computerworld.com.au/article/211890/rsa/>

==3.LES TROJANS, LES MALWARES DE L'OMBRE==

Les célèbres chevaux de Troie, eux qui firent si peur, à leur apparition, peu après les virus, et qui aujourd'hui sont quasiment banals. Rappelons qu'ils permettent de voler les données contenues dans un PC (mots de passe, numéros de cartes bancaires...) et de les envoyer aux pirates; Ils permettent aussi la prise de contrôle à distance du PC par le pirate. Le pirate peut donc manipuler à sa guise le PC à distance, et à grande échelle ceci crée comme vu plus haut des botnets de plusieurs milliers de machines. Je tiens à souligner, que même après la suppression du trojan de votre PC, il faut changer tous vos codes, au risque de vous faire voler votre e_mail, ou de l'argent (via le numéro de carte bancaire) ..

Rien de spécial à dire au sujet des trojans, seulement, qu'aujourd'hui la majorité des malwares ont des fonctionnalités propres aux trojans: prise de contrôle à distance, vol de mots de passe ...

==4.LES ROOTKITS, UN DANGER PEU CONNU DU GRAND PUBLIC==

Attention : Cette partie du dossier est un peu plus compliquée que les précédentes, du fait que les Rootkits sont des logiciels utilisant des fonctionnalités très pointues.

Les rootkits (littéralement «kit racine») correspondent à un ensemble de modifications dans le système permettant à un pirate de maintenir dans le temps(via une backdoor), un accès frauduleux à ce système. Pour cela ils cachent les activités de la backdoor et du pirate sur le PC. Les rootkits permettent de cacher les activités du pirate/backdoor en cachant les processus, fichiers, ou connexions aux réseaux, mais ils permettent aussi d'espionner l'utilisateur (vols de mots de passe ...).

Ils sont apparus il y a une dizaine d'années environ et depuis ont énormément évolué.

Nous n'allons pas faire un historique des rootkits, car ce n'est pas le but de l'article nous en citerons seulement quelques-uns.

Nous pouvons citer «Tornkit» qui fut l'un des 1er (il évoluait sur Linux), il permettait de cacher les connexions réseau, les fichiers, les processus, et implanter une backdoor.

Puis «Knack», qui était un rootkit noyau, ses activités étaient donc plus discrètes. S'en suivent les rootkits Andore (puis sa version 2), et KIS.

Arriva «enfin» «Suckit», qui fut le 1er rootkit grand public le plus efficace (à cette époque).

Dans l'année 2007, c'était le rootkit «Mood-NT» qui sortait du lot. [AJOUTER 2008 ET CEUX D'AUJOURD'HUI]

Les rootkits sont des programmes compliqués, c'est pour cela que je ne m'attarderai pas trop sur ce sujet (du moins pas dans ce dossier), nous verrons seulement les bases de l'architecture, rapidement quelques méthodes utilisées par les rootkits, comment détecter un rootkit, et enfin nous verrons que les antivirus sont totalement inadaptés à la lutte anti-rootkit.

Un rootkit est constitué de 3 choses primordiales qui le caractérisent :

Ce que l'on appelle «l'injecteur» c'est l'injecteur qui permet au pirate d'installer le rootkit sur la machine cible.

Puis le «module» de protection. C'est ce qui permet de protéger les activités du rootkit et celles du pirates.

La backdoor, c'est ce qui permet au pirate de gérer le rootkit depuis sa propre machine.

Passons maintenant aux techniques utilisées par les rootkits pour «s'infiltrer» dans un PC. Je vais faire bref: pour passer inaperçus sur une machine ils utilisent des techniques très pointues.

Il existe deux grands types de techniques, les méthodes d'injection et les méthodes de détournements de flux.

Dans les méthodes d'injection, les exploits «noyau» (c'est à dire l'exploitation des failles présentes dans les noyaux du système), et les compromissions du BIOS (modifications du BIOS, pour qu'il charge le noyau corrompu au lieu du noyau d'origine) sont les techniques les plus simples à évoquer, mais attention ce ne sont pas les seules, il en existe beaucoup d'autres.

Enfin dans les techniques de détournement de flux nous ne citerons aucune attaque (car elles sont trop compliquées à expliquer).

Lorsqu'un rootkit infecte une machine, il va dans la plupart des cas modifier le noyau du système pour être le plus discret possible; Il existe donc des programmes qui permettent de détecter dès une éventuelle modification du noyau. D'autres permettent de détecter les processus cachés (comme Ice Sword). Les processus sont ceux qui sont exécutés en mémoire lorsqu'un logiciel est lancé sur le PC. Lorsque l'antivirus scanne le PC à la recherche de processus ou de fichiers infectieux, il ne peut pas repérer les fichiers/processus du rootkit du fait qu'ils sont cachés, et c'est à cela que les programmes décrits précédemment servent, à montrer quels processus sont cachés.

Comme il existe des antivirus ou des antispywares, il existe des antirootkits. Nous pouvons citer Rootkit-Scan RootkitHunter ou encore Gmer

De nos jours, rares (voire très rares) sont les logiciels antivirus qui arrivent à détecter et à supprimer les rootkits du système. Les antivirus ne détectent les rootkits, que lorsque leur module de protection (Cf définition plus haut) n'est plus actif, cela entraîne donc la visibilité des fichiers/processus anciennement cachés, pour l'antivirus. Ici il est clairement montré que lorsqu'il y a suppression du module de protection, l'antivirus peut entrer en action.

Comme il a été répété plus haut dans le dossier, de nos jours, c'est sur la discrétion que veulent jouer les pirates. Ils ne veulent plus (ou alors rarement) se démarquer des autres; Ils veulent gagner le plus d'argent possible et pour cela restent très discrets.

C'est pour cela que lorsqu'ils infectent une machine via un malware, les pirates tentent de plus en plus d'ajouter des techniques de furtivité pour permettre à leurs malwares d'éviter leur détection par les logiciels antivirus. Une fois ces techniques ajoutées aux malwares, ils vont pouvoir en toute impunité effectuer leurs méfaits sur le système, c'est à dire :

Ouvrir un accès aux pirates (via une backdoor), transformer le PC en zombie, espionner l'utilisateur désinstaller les logiciels de sécurité (Comme Bagle par exemple).

Les techniques de rootkit sont amenées à évoluer très rapidement, et vont être bientôt utilisées par tous les malwares, ce qui rendra les logiciels de sécurité (antivirus, firewall ...) encore plus inefficaces qu'ils le sont de nos jours.

Et c'est pour cela, que seuls le bon sens et une bonne attitude sur le net permettront aux gens de se prémunir des infections.

Sources de la partie III.4 : Revus MISC numéro : 34.

Article sur Malekal : <http://forum.malekal.com/ftopic3500.php>

==5.LES ROGUES: UN BUSINESS TRES LUCRATIF==

Ah, les rogues (nommés plus rarement scarewares)... Ces faux antivirus, qui se font passer pour de réels logiciels de protection, et qui une fois installés détectent les malwares par dizaines sur votre ordinateur, et qui, lorsqu'on leur demande de supprimer les 60 malwares en tous genres détectés, demandent une petite contribution de plusieurs dizaines de dollars. Nombreux sont encore les internautes qui se font piéger par ces faux antivirus, et pourtant ils sont assez voyants. Ils affichent des messages d'alerte toutes les 5 minutes, scannent le PC en permanence et y trouvent toujours des malwares. Ce genre de logiciels peut s'attraper via des infections comme SmitFraud, Vundo, ou encore Navipromo qui affichent des publicités pour inciter à l'achat de rogues. Vous l'aurez compris les rogues utilisent le social engineering pour faire peur à l'utilisateur en lui faisant croire à une infection, et pour l'inciter à acheter le produit, les créateurs de rogues créent ces logiciels pour gagner de l'argent bien entendu. Ces logiciels s'attrapent aussi via les P2P, les faux sites de cracks, les exploits, via les faux codecs aussi (famille des rogues Renos); c'est pour cela aussi que le P2P, les cracks et autres pièges, sont à éviter. Les principaux symptômes des infections par rogues sont, affichage de fenêtre d'alerte en bas à droite de l'écran, modification de votre fond d'écran avec des messages du genre «Your privacy is in danger» (votre vie privée est en danger) ou encore «Your Pc is infected» (votre PC est infecté), affichage de pop-ups . De plus les rogues sont traduits en différentes langues pour viser un maximum de pays et donc de personnes, mais les messages et les rogues eux même sont traduits informatiquement ce qui entraîne des incohérences ou des fautes d'orthographe dans les messages d'alerte... autant dire qu'ils sont assez voyants . Si un de vos logiciels de sécurité agit ainsi, désinstallez le vite fait. Certaines infections comme Magic.Control, affichent des pubs casino, pornographiques et bien sûr, des pubs incitant à l'affichage de rogues. Il faut aussi se méfier des bannières publicitaires de certains sites qui proposent, lorsque l'on clique dessus, l'installation de rogues. Ne téléchargez jamais les logiciels proposés par des bannières de sécurité.

Il existe aussi de fausses pages de scan qui vous proposent sans rien installer sur votre ordinateur (ce qui est impossible) de scanner votre machine pour voir si elle est infectée... Bien entendu, le scan n'est qu'une animation flash destinée à faire peur à l'internaute pour l'inciter à télécharger le rogue.

De plus en plus, se développe une technique nommée le Search Engine Optimisation (Optimisation pour les moteurs de recherche) qui consiste à créer de «faux» sites référencés sur Google et qui apparaîtront dans vos recherches lors de la frappe de mots clés; l'internaute sera redirigé vers ces sites, et une fois qu'il cliquera dessus, il sera redirigé vers une des fausses pages de scan dont j'ai parlé précédemment. Tout comme les virus, cette technique le SEO (Search Engine Optimisation) utilise tout comme les vers, l'actualité pour infecter les utilisateurs lors de leurs recherches. Pour finir maintenant que vous savez reconnaître un rogue, et que vous en connaissez les dangers, il serait bien de savoir le supprimer... Je vous conseille d'utiliser Malwarebytes anti malware et de demander de l'aide sur un forum spécialisé
Voilà pour la partie rogues, il faut simplement éviter de télécharger des logiciels proposés par des pubs ou autres, le choix d'un antivirus est un choix personnel et important pour la «survie» du PC sur le net. Lorsque qu'un rogue est présent sur un PC, il est très facile à remarquer, ils sont tout sauf discrets, donc à vous de faire attention.

Sources de la partie III.5 : Différents articles de Malekal : <http://forum.malekal.com/quel-est-ce-que-les-rogues-scareware-t589.html>

[s-et-alertes-de-securite-t7139.html](http://forum.malekal.com/rogues-et-alertes-de-securite-t7139.html)

<http://forum.malekal.com/rogues>

<http://forum.malekal.com/les-bannières-popups-de-publicités-dangereuses-sur-la-toile-t3412.html>

[http://forum.malekal.com/les-](http://forum.malekal.com/les-bannières-popups-de-publicités-dangereuses-sur-la-toile-t3412.html)

Voici les images de plusieurs rogues :

Antivirus 2009 Protection

HOME OVERVIEW FEATURES DOWNLOAD REGISTER NOW AFFILIATES SUPPORT

Designed for Microsoft Windows 98/NT/2000/XP/Vista

What is Antivirus 2009 Protection

Total Antivirus Protection is one of the most hi-tech, visible achievements in the development of protection software all over the world. Its main aim is to relieve you of dangerous programs, which destroy your system.

know more scan for free purchase now

FREE SCAN
Click here to perform free scan

REGISTER
Click here to register

Latest threats

July 05 2008

Trojan.Win32.VB.azv
not-a-virus:
Trojan.Win32.WinFixer.y
Trojan.Win32.Agent.bor
Virus.Win32.Delf.bq
Backdoor.Win32.Bifrose.afg

So, what is Spyware?

The latest researches prove that 92% of all home PCs are under the threat of infection, the main source of which is still the Internet. The vast majority of Internet users fall for the bait of various trading companies and commercial websites which make large-scale distribution of viruses. Usually, these viruses get to inexperienced users through "free-of-charge" software products.

Internet Antivirus

Status: scan finished

Name	File	Type	Threat level
Trojan-IM.Win32.Faker.a	C:\WINDOWS\	Trojan	Low
Virus.Win32.Faker.a	C:\WINDOWS\assembly\GAC\Acce...	Virus	Critical
Trojan-PSW.BAT.Counter	C:\WINDOWS\assembly\GAC\IEEx...	Virus	Critical
Trojan-PSW.VBS.Half	C:\WINDOWS\assembly\GAC\ISym...	Spyware	Critical
Trojan-PSW.Win32.Ant...	C:\WINDOWS\assembly\GAC\Micr...	Virus	Medium
Trojan-PSW.Win32.Delf.d	C:\WINDOWS\assembly\GAC\misc...	Virus	Critical
Trojan-PSW.Win32.Dri...	C:\WINDOWS\assembly\GAC\Syst...	Virus	Medium
Trojan-PSW.Win32.Fan...	C:\WINDOWS\assembly\GAC\Syst...	Virus	Critical

100%

Scanned files: 1253
Infected files: 32

Recommended: Click "Cleanup" to protect Windows and delete malicious files

Get immediately protection for your PC

Action: Scanning Database: 2.0.4.37.8/11/2008 Update

Listes des rogues : <http://assiste.com.free.fr/p/craptheque/craptheque.html>

==6.LES RANSOMWARES ==

Les ransomwares (mot construit par le rassemblement des mots "ransom" et "malwares"), sont des logiciels malveillants qui permettent la modification de certains fichiers du PC infecté, et qui demandent à la victime une rançon pour permettre de retrouver les fichiers dans leur état initial. Les modifications apportées sont souvent le chiffrement des fichiers. Le phénomène de "racket informatique" est apparu dans le courant de l'année 2005.

Les "attaques" des ransomwares peuvent être découpées en 3 parties :

1ère phase, le chiffrement : Les ransomwares chiffrent généralement les fichiers aux formats suivants : .doc .odt .jpg .jpeg .mp3, en effet les maîtres chanteurs pourront faire une plus grande pression sur leur victime en chiffrant ses documents de travail, ses photos, ou encore sa musique qu'en chiffrant un fichier au hasard.

2ème phase, l'interdiction d'accès : Les maîtres chanteurs, pour obliger leurs victimes à payer la rançon doivent leur interdire l'accès à certains fichiers.

3ème phase, la demande de rançon : Le but du ransomware est de faire gagner de l'argent à celui qui l'a créé. De ce fait, une fois qu'il a chiffré les fichiers de la victime, le ransomware va se faire remarquer le plus possible, en affichant à l'écran des messages (via un fichier texte) affirmant qu'il a empêché l'accès à certains fichiers, et qu'il faut payer pour les récupérer.

Lors de leur 1ère apparition, les ransomwares ont suscité une sorte de «buzz» chez les médias comme chez les éditeurs d'antivirus qui n'avait pas lieu d'être. Ils affirmaient que les ransomwares marquaient «une nouvelle ère dans le monde du cyber-crime» ce qui est totalement faux. Aucun des ransomwares parus pour le moment ne méritent une telle phrase, nous verrons que la majorité des ransomwares ne présente qu'un faible danger et utilisent pour la plupart l'effet de peur que suscite ce genre de pratique chez un utilisateur lambda et que les médias contribuent à renforcer.

Il est important d'insister sur le fait que la majorité des ransomwares utilisent de faibles algorithmes, voir des algorithmes totalement ridicules.

La force principale des ransomwares, est la peur qu'ils peuvent générer chez les victimes. Un utilisateur lambda n'aura pas les compétences informatiques pour déjouer le chiffrement d'un ransomware même le plus simple.

La majorité des ransomwares sont destinés à une influence de masse, et les victimes potentielles sont les internautes lambda.

Prenons l'exemple du ransomware Gpcode.aj ; son auteur affirme que son ransomware utilise l'algorithme RSA-4096, alors qu'il a été démontré qu'il utilise le RC4 modifié, beaucoup plus facile à décoder.

Nous voyons donc que les ransomwares ne présentent pas toutes les «qualités» (voir aucune) pour ouvrir une «nouvelle ère» dans le cyber-crime, et que finalement la majorité des ransomwares puisent leur pouvoir plus dans l'intimidation des victimes que dans leurs prouesses techniques.

Malgré cette réalité, les médias ont contribué à un l'effet de peur injustifié auprès des internautes.

Notons deux points importants, les rançons demandées par les pirates sont rarement très élevées, ce qui leur fait prendre peu de risques face aux systèmes de lutte contre le blanchiment d'argent, alors que si les rançons étaient plus élevées, ils seraient obligés de mieux s'organiser et de se professionnaliser ce qui n'est pas le cas aujourd'hui, vu le niveau technique des ransomwares; ceci porte d'ailleurs à penser que leurs auteurs ont peu de connaissances en cryptographie. Enfin, les dernières vagues d'infections de masse de ransomwares datent des années 2007-2008 ce qui peut nous laisser penser que les auteurs de ransomwares se sont tournés vers des activités plus lucratives, et surtout moins visibles.

Sources de la partie III.6 : Revus MSIC numéros 38, 46.

Autres liens :

http://news.bbc.co.uk/2/hi/uk_news/england/manchester/5034384.stm

=IV COMMENT SE PREMUNIR=

==1.COMMENT SE PROTEGER FACE AUX MENACES DU NET==

A moins d'être totalement coupé de la réalité, tout le monde, même ceux qui ne possèdent pas de PC, a déjà entendu parler de " virus informatiques ".

Comme dit plus haut, nous utiliserons le terme Malware et non le terme Virus, défaut de langage utilisé pour désigner l'ensemble des menaces informatiques mais qui en réalité ne désigne seulement les menaces classées comme virus (Voir définitions). Il est vrai qu'au début de «l'ère internet» il n'existait que des virus (voire des vers qui sont en fait des virus réseau) et c'est petit à petit que sont apparues les nouvelles menaces : les chevaux de troies, les keyloggers, les spywares, les rogues etc... Les gens pour qui l'informatique n'est pas une passion ou pour ceux qui n'y comprennent rien, le terme virus est resté, et est encore utilisé. Même les grandes sociétés de lutte contre les malwares comme Kaspersky ont utilisé pendant longtemps le terme «antivirus» pour désigner des logiciels capables de détecter toutes sortes de malwares. Aujourd'hui encore, ce terme est utilisé à tort même si l'on rencontre de plus en plus couramment le terme malware..

Nous allons voir ici comment nous prémunir d'une infection.

Voici, en trois points, les informations générales pour éviter les infections :

A-Adopter une bonne attitude de surf

Il faut faire attention où l'on clique et sur quoi l'on clique.

Éviter les sites de Cracks/Pornos/warez car ce sont des gros vecteurs d'infections, le P2P aussi est à bannir car tout comme les sites de Cracks/Pornos/warez c'est un gros vecteur d'infections.

Ne téléchargez pas de logiciels n'importe où, téléchargez-les soit sur le site de l'éditeur ou sur des sites dits « sûrs ». (*IDN CCM 01.net*)

Faites attention aux réseaux IRC (MSN) où l'on peut vous envoyer des fichiers infectieux, aux clés USB aussi elles peuvent être infectées

(évittez de brancher vos clés dans des cyber-cafés etc)

Et surtout surfez Seulement en session Utilisateur car cela vous évitera d'installer tout et n'importe quoi.

De plus les Malwares doivent eux aussi avoir des droits pour s'installer. Ils ne les auront donc

que si vous êtes en session Administrateur.

B-Maintenir son Système A Jour

Comme je vous l'ai dit plus haut, gardez votre OS, votre navigateur et les add-on à jour cela vous évitera un bon nombre d'infection, car les failles de sécurité seront alors comblées.

C-Maintenir ses Logiciels de sécurités A Jour

Il faut bien entendu utiliser un Anti-Virus et un Firewall pour protéger votre PC
Il faut (tout comme l'OS, le navigateur ..) les maintenir à jour sinon ils sont inefficaces.
Mais ces programmes ont des limites et c'est pour cela que les gestes simples exposés plus haut permettront de vous prémunir plus efficacement que ces logiciels des infections du web.

Voilà pour la «morale», si vous avez bien lu vous aurez remarqué que ce n'est pas le fait de multiplier ces logiciels de protection sur son PC qui évitera l'infection. C'est surtout des gestes

32

simples et réfléchis qui vous permettront d'éviter l'infection. Il faut savoir qu'il existe des failles sur

les OS, navigateurs, add-on etc... Elles sont régulièrement comblées via les mises à jour, mais la faille la plus dure à combler et la faille humaine! Cette faille est celle qui est responsable de la majorité des infections. Vous avez beau avoir un antivirus, un firewall, tous vos systèmes à jour, si vous téléchargez en P2P, utilisez des cracks, ouvrez n'importe quoi, vous serez infecté !!

Ce qu'il faut bien comprendre c'est qu'il faut adopter un «clic responsable», c'est à dire comme dit maintes et maintes fois ci-dessus, ne pas cliquer n'importe où ne pas faire n'importe quoi sur le net. Malgré les apparences, le net est un lieu dangereux, pour tous.

Faisons maintenant un point sur quelques idées reçues :

Les antivirus gratuits sont nuls !

Absolument FAUX ! Certains antivirus gratuits sont meilleurs que des payants, il est vrai qu'il est plus «rassurant» de payer pour sa sécurité. On a l'impression d'être mieux protégé, mais ça n'est pas nécessairement vrai. Ce qu'il faut bien comprendre, c'est que bien souvent les créateurs d'antivirus utilisent la naïveté des gens pour vendre leurs produits en annonçant des comparatifs dans lesquels ils sont les meilleurs, avoir découvert de nouvelles technologies infaillibles etc

Je conseille fortement de tester soit-même son antivirus et de voir si il convient, et de ne pas agir sur le seul conseil d'une personne qui «s'y connaît».

Plus je mets de logiciels de sécurité mieux ça va !

FAUX ! La surmultiplication de logiciels de sécurité n'altère en rien les risques d'infections. Et au contraire même ! Ils se gênent, ralentissent le système, voire le font planter. Il est aussi dangereux d'avoir deux Antivirus actifs sur une même machine que pas du tout ! De plus, le plus souvent les logiciels utilisés sont du genre «Ad-Aware Personal, Spybot Search and Destroy ... » ces logiciels étaient bon il y a 5 ans environ, aujourd'hui les menaces ont changé, les menaces ont évolué. Certains logiciel non ! Ce qui les relègue très loin dans le «classement» des logiciels performants.

Mettre à jour ? Pour quoi faire ?

Pour éviter les infections! Ici nous allons rapidement analyser le fonctionnement de logiciels nommés «exploits». Ces logiciels sont relativement peu connus du grand public, et pourtant ils sont responsables de beaucoup d'infections notamment l'infection par sites piégés.

Exemple :

Je me connecte sur internet et je me balade normalement, soudain je tombe sur un forum où un gars dit : «Si tu veux utiliser Photoshop gratis, va sur ce site il y a la version crackée» alors moi, fan de graphisme mais n'ayant pas les moyens d'acheter Photoshop, je clique sur le lien donné. J'arrive sur un site où partout l'on peut télécharger des logiciels crackés, je m'esclaffe en me disant «Aaaah, dire qu'il y a des imbéciles qui payent alors que l'on peut les avoir gratuitement». Et bien ceux qui payent sont plus malins que toi, oui peut être qu'ils déboursent de l'argent pour se payer leurs logiciels mais cela leur évite des infections.

Alors à quel moment me suis-je fait infecter ? Et bien dès ma connexion sur le site de crack, dès que je me suis connecté, l'exploit se lance et recherche sur mon PC s'il y a des failles, et comme je suis un partisan du «*Mettre a jour ? Pour quoi faire ?*» il en trouve plusieurs belles qu'il se dépêche d'exploiter. Une fois les failles exploitées le PC est infecté par l'exploit, ensuite on télécharge le crack et rebelote on se fait ré-infecter car la majorité des cracks sont néfastes. Voilà pour une petite démonstration de comment on se fait infecter par un exploit/crack .

«Moi je suis sur Mac, alors les virus»

Nous voilà arrivé à cette légende de l'immunité de certains OS face aux malwares. Il est vrai que Linux/Mac sont largement moins exposés que Windows aux malwares. Cela est dû à de nombreuses choses expliquées dans la partie « 3--- Pourquoi tout le monde est concerné ». Je dirais simplement que les utilisateurs de Mac se croyant immunisés, risquent, le jour où un malware débarque sur Mac, de se laisser avoir, et de déclencher une «cyber-pandémie». Pour simple rappel, il vaut mieux être un peu paranoïaque, que de se croire invulnérable.

«Ouais, mais l'antivirus ça ralentit le PC»

Pas nécessairement, certains, oui, ralentissent le système. Mais la plupart passe quasi inaperçu. Comme dit plus haut, testez les version d'évaluations pour les payants pour vous forger une idée et testez à votre guise les gratuits. Le plus souvent, les personnes qui disent ça ont sur leur PC,

3-4 toolbars, une dizaine de BHOs etc... Il vaut mieux avoir un PC ralenti par un antivirus mais un PC sain; que pas d'antivirus et un PC infesté de malwares en tout genre qui finiront par le ralentir 10 fois plus que l'antivirus.

Voilà, je pense que pour les idées reçues c'est bon. Il en reste sûrement encore, mais sans les énoncer, vous aurez compris qu'il faut vous faire un avis seul, et ne pas écouter les ragots.

Pour conclure cette partie, je dirais seulement que c'est l'attitude sur le net qui vous évitera la grande majorité des infections.

==2.COMMENT SE PROTÉGER FACE AUX BOTNETS==

Contre les botnets, dans l'état actuel des choses, est impossible. C'est à dire qu'il n'existe pas encore de solution satisfaisante contre les botnets. Mais plusieurs méthodes permettent de réfréner leurs dégâts.

Premièrement, il est important de souligner que les botherders vivent dans un sentiment d'impunité totale. Les condamnations envers les dirigeants de botnets sont encore très rares, pour qu'ils s'inquiètent et stoppent leurs activités. De plus, la majorité des botherders sont des «newbies», c'est à dire des débutants. En effet, ils n'ont pas besoin de compétences spéciales pour diriger les botnets.

Ces botherders sont motivés par un seul et unique but, comme tous les pirates : le gain.

Pour que les botherders n'aient plus ce sentiment d'impunité, il faudrait une harmonisation des lois contre la cyber-criminalité dans le monde pour que les actions juridiques se réalisent contre les botherders.

Les botnets dirigés par un centre de contrôle peuvent être «facilement» stoppés ! En effet, il «suffit» de couper le cordon reliant les botnets au centre de commande pour amputer le botnet d'une partie de ses zombies. Mais, de plus en plus, l'architecture P2P est utilisée, cette architecture ne comportant pas de centre de commandes, sa suppression est bien plus difficile.

Les botnets reposent sur des PC zombies qui eux-même reposent sur les bots. Si le PC n'est pas infecté par un bots, il ne devient pas un PC zombie, donc ne participe pas à la création d'un botnet.

Il faudrait donc que les internautes du monde soit éduqués en matière de sécurité et d'infections pour éviter la création de botnets.

Le profilage réseau est aussi nécessaire pour lutter contre les botnets, c'est à dire «d'espionner» grâce à certains logiciels ce qui se passe sur les réseaux .

La chasse aux botherders, la suppression des centres de commandes, l'éducation des internautes, et la détection des activités réseaux pourra permettre, peut-être un jour .. la fin des botnets ?

Sources de la partie IV : Connaissances personnelles (Différents sites sur la sécurité informatique.) Revus MISC numéro 30

==UNE DERNIERE MISE AU POINT==

Ce dossier ne serait pas complet sans une ultime mise en garde:

Combien d'entre nous ne se sont pas un jour esclaffés devant la dernière histoire drôle, ou extasiés devant le dernier diaporama, transmis en pièce jointe à un courriel, par un ami ?

Outre le fait, que personne ne pense jamais à vérifier ladite pièce jointe, et que d'ailleurs il n'est pas certain que l'antivirus pourra repérer le ver qui s'y cache, faisons un rapide calcul estimatif:

Chaque « ami » transmet le fichier à tout son carnet d'adresses, disons 30 personnes, au 2ème tour nous sommes déjà à 900; sachant que la transmission se fait, au bas mot, une centaine de fois, je vous laisse admirer le paysage du haut de ce nombre vertigineux.

Alors, quand sur les forums, on voit arriver des demandes d'aide parce que certains soirs, vers certaines heures, le débit des connexions s'effondre, à votre avis, que faut il répondre ?

Faites comme moi, soyez le dernier maillon, et dites vous que vous n'êtes pas le plus faible.

==CONCLUSION GÉNÉRALE DU DOSSIER==

Voilà, ce dossier est terminé, il aura fait un tour d'horizon des différentes menaces, connues ou méconnues de l'Internet. Entre les botnets, les rootkits, et autres nouveautés des pirates, l'utilisateur lambda n'osera plus toucher à Internet. Comme je l'ai dit plusieurs fois, une bonne attitude, une bonne mentalité sur le net, cela évite la majeure partie des infections. Utiliser des logiciels à jour et respecter les «règles» de sécurité, et vos risques d'infections seront largement réduites.

Ce dossier aura au moins permis de faire connaître à tous les menaces inconnues, et pourtant extrêmement dangereuses comme les botnets.

J'espère que ce dossier vous aura plu, et vous aura apporté des connaissances.

Comme dit plus haut, en cas de question n'hésitez pas à me contacter par message privé via mon compte de Comment Ça Marche : <http://www.commentcamarche.net/communaute/>

=GLOSSAIRE=

Ces définitions sont toutes tirées de l'encyclopédie libre Wikipédia, du site communautaire Comment ça marche (CCM), et sont parfois légèrement modifiées. Celles provenant d'autres sites, comportent un lien qui renvoie vers le site source.

Malware

Un logiciel malveillant (*malware* en anglais) est un logiciel développé dans le but de nuire à un système informatique.

Virus

Un virus est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé.

Cheval de troie

Un cheval de Troie (ou trojan) est un logiciel d'apparence légitime, mais conçu pour exécuter subrepticement (de façon cachée) des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permettra à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

Rootkit

Un rootkit est un type de programmes dont le but est d'obtenir un accès frauduleux aux ressources d'une machine, de la manière la plus furtive et indétectable possible. Un rootkit peut s'installer à différents niveaux du système d'exploitation, il peut cacher, des processus, des clés registres, des fichiers.

Ver

Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

Spyware

Un logiciel espion (aussi appelé mouchard ou espioniciel ; en anglais spyware) est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations

sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

Backdoor

Dans un système, une porte dérobée (de l'anglais backdoor, littéralement porte de derrière) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret, et à distance au système.

Ransomware

Un rançongiciel, ou ransomware est un logiciel malveillant qui prends en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Exploit

Un exploit est un programme permettant à un individu d'exploiter une faille de sécurité informatique dans un système d'exploitation ou un logiciel, ceci afin de prendre le contrôle d'un ordinateur, de permettre une augmentation de privilège d'un logiciel ou d'un utilisateur.

Bot

Un bot informatique, ou robogiciel, est un logiciel automatique qui interagit avec des serveurs informatiques. C'est ce logiciel qui permettra au pirate de donner des ordres à son botnet.

PC Zombie

Une machine zombie est un ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique. Ce dernier l'utilise alors le plus souvent à des fins malveillantes, par exemple afin d'attaquer d'autres machines (attaques DDOS par exemple) en dissimulant sa véritable identité.

Botnet

Un botnet est un ensemble de bots informatiques qui sont reliés entre eux.

Rogue

Un rogue est un logiciel malveillant qui se fait passer pour un logiciel anti-malware\virus\spyware

Celui-ci vous harcèle en vous ouvrant d'innombrables pop-ups, et en vous demandant de payer une licence pour soi-disant "nettoyer les infections".

Ce type de programme malveillant est généralement téléchargé par un cheval de Troie à votre insu.

Codec

Un codec est un procédé capable de compresser et/ou de décompresser un signal numérique.

Ingénierie sociale

L'ingénierie sociale (social engineering en anglais) est une forme d'escroquerie utilisée en informatique pour obtenir une information personnelle. Cette pratique exploite les failles humaines pour soutirer des informations confidentielles à un utilisateur. Utilisant ses connaissances, son charisme, l'imposture ou le culot, le pirate abuse de la confiance, l'ignorance ou la crédulité de personnes possédant ce qu'il tente d'obtenir.

Phising

L'hameçonnage (ou phishing, et parfois filoutage), est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale (sécurité de l'information).

OS

Le système d'exploitation, abrégé SE (en anglais operating system, abrégé OS), est l'ensemble de programmes qui se place entre le matériel et les logiciels applicatifs. Voir :

http://upload.wikimedia.org/wikipedia/commons/e/ed/Operating_system_placement-fr.svg

BHO

Un BHO est une petite application tierce partie (de type "plug-in") qui, une fois installée, ajoute des fonctionnalités (désirées ou non) à Internet Explorer

<http://www.dicodunet.com/definitions/internet/bho.htm>

Toolbar

En informatique, une barre d'outils (en anglais : toolbar) est un élément de base des interfaces graphiques (un widget) qui regroupe en une barre plusieurs boutons. Certaines barres d'outils tierces sont malveillantes. Une fois installées, ces barres malveillantes introduisent des malwares sur le PC.

Crack

Un crack est un programme qui s'applique sur un logiciel pour :

Soit pouvoir utiliser le logiciel sans avoir besoin que le CD du logiciel soit inséré dans le lecteur CD (on nomme souvent ces crack des « No CD »).

Soit pour enlever une protection ou une limitation du jeu. Souvent, ces modifications sont destinées à utiliser des programmes payants comme si le cracker en avait payé la licence.

P2P

Le pair-à-pair (traduction de l'anglais peer-to-peer, souvent abrégé « P2P »), est un modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur. En gros, ce genre de réseaux permet le libre partage de fichiers en tous genres.

Warez

Le terme warez désigne des contenus numériques protégés par les lois du copyright mais diffusés illégalement sans reverser de droits. Ils sont souvent diffusés via Internet (par exemple en utilisant les protocoles p2p), ou par cédéroms

IRC

IRC, abréviation de Internet Relay Chat (en français, « discussion relayée par Internet »), est un protocole de communication textuelle sur Internet. Il sert à la communication instantanée principalement sous la forme de discussions en groupe par l'intermédiaire des canaux de discussion, mais peut aussi être utilisé pour de la communication individuelle. Il peut par ailleurs être utilisé pour faire du transfert de fichier.

Algorithme

On désigne par algorithmique l'ensemble des activités logiques qui relèvent des algorithmes; en particulier, en informatique, cette discipline désigne l'ensemble des règles et des techniques qui sont impliquées dans la définition et la conception des algorithmes (Tire son appellation du nom du mathématicien arabe Al-Khwarizmi, le père de l'algèbre, né au 8ème siècle)

RSA

Rivest Shamir Adleman ou RSA est un algorithme asymétrique de cryptographie à clé publique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

RC4

RC4 est un algorithme de chiffrement à flot conçu en 1987 par Ronald Rivest, l'un des inventeurs du RSA, pour les Laboratoires RSA.

DDOS / DOS

Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web, empêcher la distribution de courrier dans une entreprise ou rendre indisponible un site internet.

Firewall

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau

Pump and dump

Egalement appelé "stock dump", le Pump and dump est une fraude financière. Elle consiste à présenter une action ordinaire comme une affaire dans laquelle investir, et créer de cette manière une demande artificielle surélevée. Les fraudeurs revendent ensuite leurs actions au prix le plus fort, avant qu'elles ne reviennent à un cours normal.

http://www.journaldunet.com/encyclopedie/definition/1107/43/20/pump_and_dump.shtml

Faible de sécurité

Dans le domaine de la sécurité informatique, une vulnérabilité est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient.

Disque Amovible

Les disques amovibles désignent toutes les structures pouvant contenir des données: clés USB, disques durs externes, CD, DVD ..

I-frame

La balise IFRAME signifie inline frame et s'écrit en HTML <iframe>. Elle est utilisée pour inclure à l'intérieur d'une page HTML un autre document HTML. Elle est souvent utilisée de façon malveillante pour infecter les machines. La balise IFRAME inclut un contenu malveillant au cœur d'une page d'un site normale, ce qui entraînera, lors de la connexion des internautes au site, l'infection de leur machine.

http://www.cases.public.lu/fr/publications/dossiers/iframe/iframe_1/index.html

Spam

Le spam ou pourriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

Hacktivisme

Le hacktivisme est une contraction de hacker et activisme. Le "hacktiviste" est un hacker mettant son talent au service de ses convictions politiques, et organisant des opérations coup de poing technologiques : piratages, détournements de serveurs, remplacement de pages d'accueil par des tracts, etc.

HTTP

Le HyperText Transfer Protocol, plus connu sous l'abréviation HTTP, littéralement le « protocole de transfert hypertexte », est un protocole de communication client-serveur développé pour le World Wide Web.

Adware

Un publiciel (adware en anglais) est un [logiciel](#) qui affiche de la [publicité](#) lors de son utilisation.

Quelques liens sur la sécurité informatique :

Malekal : <http://www.malekal.com/>

Assiste : <http://assiste.com.free.fr/>

Zebulon : <http://www.zebulon.fr/>

Secuser.com : <http://www.secuser.com/index.htm>

Articles :

<http://forum.zebulon.fr/prevention-le-crack-dans-toute-sa-splendeur-t93281.html>

<http://forum.zebulon.fr/prevention-le-p2p-et-ses-consequences-t85544.html>

<http://forum.malekal.com/index-des-menaces-et-programmes-malveillants-malwares-t17042.html>

<http://forum.malekal.com/les-exploits-sur-les-sites-web-pieges-t3563.html>

<http://forum.malekal.com/le-social-engineering-t4043.html>

<http://forum.malekal.com/explications-infections-disques-amovibles-clefs-usb-etc-t5544.html>

<http://forum.malekal.com/virus-msn-explications-fonctionnement-et-parade-t9130.html>

<http://forum.malekal.com/le-danger-et-fonctionnement-des-rootkits-t3500.html>

<http://forum.malekal.com/le-danger-des-failles-de-securite-t3452.html>

<http://forum.malekal.com/prevention-logiciels-et-sources-de-telechargements-t5546.html>

<http://forum.malekal.com/pourquoi-ne-pas-surfer-avec-les-droits-administrateur-t6662.html>

...

Forums :

<http://forum-aide-contre-virus.be/entraide/>

<http://www.commentcamarche.net/forum/forum-7-virus-securite>

<http://www.infos-du-net.com/forum/forum-11.html>

<http://forum.pcastuces.com/securite-f25>

<http://forum.generation-nt.com/securite-and-virus/>

<http://forum.malekal.com/virus-trojans-spywares.html>

<http://forum.malekal.com/securite-prevention-virus.html>

...