Grand-duché de Luxembourg: une douzaine de sites Internet "*défigurés*"

*par Charles Delbrassine**

Dans le courant des mois de Juillet et Août 2001, une douzaine de sites Internet luxembourgeois ont vu leur page d'accueil transformée sous l'action de divers pirates informatiques répondant aux doux noms de tty0, Silver Lords ou RB Team. Les sujets traités sur les sites endommagés sont divers et vont de la banque à l'association religieuse. Hormis le nom de domaine "*.lu*", le seul point commun entre ces sites est l'utilisation de Ms Windows en tant que système d'exploitation et donc la capacité d'utiliser un seul et même outil pour perpétrer ces attaques.

Qui sont les "Hackers" ?

On reprend sous le nom de "*Hacker*" une catégorie de pirates informatiques agissant dans les réseaux informatiques. Tout l'art du "*Hacker*" est de perpétrer ses actes sans laisser de traces au niveau des barrières de détection implémentées et de ne signaler sa présence qu'en fin d'attaque au travers de marques bien visibles telles que le blocage d'accès ou la défiguration de sites Internet.

Une connaissance pointue des éléments constitutifs de l'Internet : routeur, firewall, protocole de communications, systèmes d'exploitations ainsi que des applications est indispensable pour mener à bien des attaques. Toutefois la mise à disposition "*libre*" des outils développés par ces mêmes spécialistes permet à des non-initiés, appelés "*script kiddies*" de perpétrer des actes répréhensibles. L'attaque de vrais réseaux de communication protégés est la plupart du temps inaccessible pour ces "*jeunes*" bricoleurs dont la capacité se limite à lancer un programme via la touche "*Enter*".

La communauté des "*Hackers*" a établi sa propre structure et quelques groupes mythiques y jouent un rôle important (Cult of the Dead Cow , Chaos Computer Club, L0pht...). D'autres figures emblématiques tels que Kevin Mittnick ou Vladimir Levin participent à la publicité faite autour des pirates informatiques. Chaque été se tient à Las Vegas, le séminaire des pirates appelé DEFCON. Cette conférence rassemble les acteurs de la sécurité et du piratage informatique, en présence du FBI.

Dans quels buts perpétrer de telles attaques ?

Il y a lieu de faire une claire différenciation entre les "*Black Hat Hackers*" aux agissements frauduleux et les "*White Hat Hackers*" agissant sous couverture d'un engagement signé avec le propriétaire du site Internet, dans un but d'évaluation du niveau de sécurité de l'infrastructure.

Les motivations des pirates peuvent être de plusieurs types :

- Pur esprit de jeu et plaisir de défier des solutions ou organismes réputés infaillibles.
- But lucratif.
- Vengeance ou attaque personnelle.
- Avantage compétitif économique.
- Propagande politique ou religieuse.

En ce qui concerne l'aspect politique de ce type d'agissements plusieurs types d'actions sont possibles allant de la mise hors service d'un site jusqu'à l'affichage d'un message à portée politique.

Certains groupes de pirates informatiques se fixent pour but de nettoyer la toile de sites jugés inopportuns tels que ceux relatifs à la pédophilie ou la pornographie. Sous cet aspect le piratage peut être considéré comme positif.

Quels sont les dommages liés à la défiguration de sites?

Les attaques étant perpétrées au travers d'un vecteur de communication, il n'y a que très peu de risques de dommages matériels.

Dans le cas de sites Internet à vocation transactionnelle, le dommage commercial direct s'évaluera sur base du nombre moyen de transactions journalières. Il est sans doute plus compliqué d'estimer l'impact indirect lié à la perte de confiance d'un utilisateur face à un site défiguré et à son éventuel recours à des sites concurrents.

Ce type de risque est à prendre sérieusement en compte par les entreprises dont le site Internet est abrité (Hosting) par une société tierce. Lors de la mise en place de solution abritée, il est très rare que cet aspect soit suffisamment pris en compte. Lors de la défiguration d'un site Internet l'impact contre-publicitaire est subit directement par le propriétaire du site et non par l'hébergeur. La vraie plus-value entre ces derniers pourrait bien devenir à court terme la promesse d'un environnement hautement protégé.

Il est donc conseillé d'exiger la production d'un rapport de mises à l'épreuve réalisées récemment par une société indépendante spécialisée en ce domaine.

D'ou proviennent ces attaques ?

La structure même de la toile élimine les notions de temps et de distance et permet de perpétrer ce type d'attaques au départ de n'importe quel point du globe.

Sur base des dernières statistiques disponibles (www.dshield.org) il apparaît que les actes perpétrés au départ de l'Asie est en constante progression.

Provenance des attaques	**%**
Amérique du Nord	44%
Asie	29%
Europe	21%
Amérique du Sud	3%
Australie	2%
Afrique	1%

Ces statistiques ne couvrent que les attaques dites "*externes*", c'est à dire celles réalisées au départ d'une station non officiellement rattachée au réseau informatique cible. Il est intéressant de noter que l'on estime à 65 % le nombre de piratages réalisé en interne.

Les seuls éléments indispensables demeurent la possession d'un ordinateur personnel et d'une connexion téléphonique à haut débit. Un ordinateur personnel n'est pas assez puissant à lui seul pour mettre en difficulté des grands sites Internet. Toutefois la disponibilité d'outils de piratage permettant de transformer d'autres ordinateurs ou réseaux en esclaves rend possible la paralysie des géants de la nouvelle économie au départ d'un simple ordinateur personnel. L'effet de ce type d'attaque distribuée est le même que si des milliers de clients décidaient en même temps d'entrer par la porte d'entrée d'un magasin.

Quelle est la méthode utilisée pour "défigurer" un site Internet ?

L'ensemble des éléments constituant la toile utilise un langage de communication commun appelé "*Internet Protocol*" ou IP.

Derrière l'adresse alphabétique d'un site Internet ou tout autre élément connecté, se cache une adresse IP unique qui sera utilisée de manière à déterminer l'émetteur, le récepteur d'un paquet de données, ainsi que le chemin à suivre pour atteindre sa destination.

La démarche suivie par les "hackers" peut être synthétisée comme suit :

1) Cartographie du réseau cible :

Cette étape consiste à utiliser différents outils de manière à établir un plan de l'infrastructure cible. Ce plan sera dans un premier temps établi sur base des adresses IP. Ensuite l'utilisation du repérage des routes utilisées par les paquets de données pour atteindre une adresse destinataire permettra une découverte de la topologie.

Certains sites (www.netcraft.com) permettront déjà d'obtenir des informations relatives au système d'exploitation ou aux applications utilisées sur les sites.

Les outils basiques nécessaires sont installés à l'origine sur les ordinateurs personnels, d'autres sont disponibles en large diffusion gratuitement via Internet.

Le "*Social Engineering*", c'est à dire l'obtention d'informations en conversant directement avec les utilisateurs du réseau cible demeure une méthode facile et très souvent fructueuse.

2) La découverte des vulnérabilités :

Le but de cette étape est d'utiliser la carte établie lors de la première phase de manière à découvrir les vulnérabilités de la structure.

Les outils utilisés pour la découverte sont des Scanners, Sniffers...

L'existence sur la toile d'une multitude de sites de recensement et de documentation des vulnérabilités sera d'une grande utilité aux pirates.

3) L'exploitation :

Sur base des vulnérabilités découvertes, le pirate sera capable de déterminer les outils appropriés à l'exploitation des failles.

Le but fixé pour cette étape peut être de transformer l'apparence d'un site Internet.

4) Le camouflage :

Selon le but recherché par le pirate, il prendra soin d'afficher ou non sa présence sur le site. Dans tous les cas il aura à coeur d'effacer toutes les traces pouvant mener à son identification physique.

Quelle est la méthode utilisée pour rendre inaccessible un site Internet ?

Seule l'exploitation des vulnérabilités sera différente par rapport à une défiguration. En effet les attaques de type "*Refus de Service*" ont pour but de rendre inactif l'un des éléments constitutifs de l'architecture attaquée (routeur, switch, firewall, serveur ou application) de manière à rendre inopérant le site visé.

Les attaques distribuées sont très souvent utilisées de manière à obtenir un impact maximum sur la machine cible ainsi que sur tous les éléments constitutifs de la chaîne de transit des informations, en mettant à profit les ressources informatiques parasitées.

La manipulation de la partie relative aux adresses "*émetteur*" et "*destinataire*" des paquets

Que faire pour limiter les risques ?

La stratégie de sécurité doit demeurer un bon compromis entre les dangers encourus et la nécessité de conserver un outil offrant les services nécessaires au "*Core-business*".

Les aspects à prendre à compte sont :

1) Une équipe sécurité formée et dédiée à cette tâche ;

2) Une infrastructure sécurité appropriée ;

3) Un état des lieux complet et "vivant" de la sécurité.

4) Des missions de test d'intrusion réalisées à intervalles réguliers par une société indépendante spécialisée.

5) Une veille technologique.

En ce qui concerne les attaques de type "*refus de Service*", il est évident que le blocage du premier élément suffit à bloquer l'ensemble de la chaîne de communication. Ce premier élément est le point d'attache au réseau Internet, donc le routeur du fournisseur d'accès. Même s'il n'existe actuellement aucune arme absolue contre ce type d'attaque, une configuration appropriée de cet élément permet de limiter le risque de mise hors d'état mais également de filtrer le trafic indésirable de manière à protéger les éléments suivants. Il est donc vivement conseillé de se pencher sur la configuration de ce routeur souvent géré par le fournisseur d'accès sans aucune implication du locataire de services.

**Charles Delbrassine (e-mail: cdelbrassine@deloitte.lu) est Senior Manager - Deloitte Consulting Luxembourg (Tél: (352) 451 452 716)*