Communiqué de Presse
Rueil Malmaison, lundi 24 avril 2006

« Le malware en 2005 – Unix, Linux et autres plates-formes »

Konstantin Sapronov, analyste spécialisé en virologie chez Kaspersky Lab, consacre un rapport sur les dangers visant les plates-formes alternatives à Microsoft Windows. A partir de statistiques collectées en 2004 et 2005, il expose les tendances et les voies de développement des cyber-menaces dans les environnements Unix, Linux, Mac OS X, etc. L'étude est disponible sur les sites www.viruslist.com/fr et http://presse.kaspersky.fr.

Si le premier virus pour ordinateur est apparu en 1988 sur la plate-forme Unix, les codes malicieux ont commencé à se propager quand des millions de particuliers se sont équipés en micro-ordinateurs fonctionnant sous DOS puis sous Microsoft Windows.

En effet, les virus se développent et se renouvellent sur le même rythme que l'informatique en général. La popularité d'une plate-forme s'évalue ainsi au nombre de virus créés pour l'attaquer.

La plate-forme de prédilection des hackers est incontestablement Intel + Win 32. La plate-forme Intel 32 bits est la plus répandue actuellement. Toutefois, d'ici peu, c'est la plate-forme 64 bits qui devrait prendre la première place. Plusieurs programmes malicieux conceptuels (POC) pour Win 64 ont d'ores et déjà été identifiés.

Après OS/2, il s'agit plutôt aujourd'hui de Linux, FreeBSD ou autres Unix.

Linux gagne incontestablement des parts de marché sur Microsoft Windows, non seulement sur les serveurs mais aussi sur les PCs. Avec l'adoption par Apple des processeurs Intel, il est fort probable que Mac OS X devienne une plate-forme plébiscitée par les utilisateurs.

Les PCs des internautes représentent aujourd'hui la cible favorite des cyber-criminels. Le flux principal de programmes malicieux pour Win 32 se compose de différents Trojans : Trojan-Spy, Trojan-Downloader ou Trojan-Dropper. Linux doit faire face aux portes dérobées (backdoors) qui donnent un accès distant à une machine compromise qui sera ensuite utilisée comme plate-forme d'attaques.

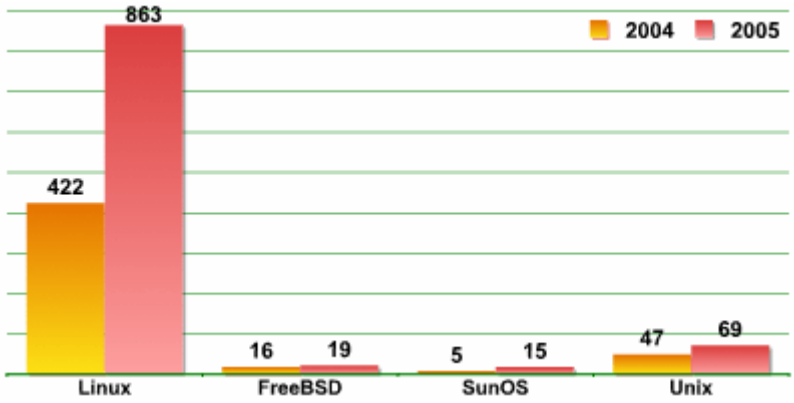
Dès que le taux de pénétration d'une plate-forme croît, le nombre de virus et de programmes malveillants augmente. Les malwares sont conceptuels (PoC - Proof of Concept) : ils ne sont pas porteurs d'un code aux fonctions destructrices. Ils démontrent simplement l'existence de vulnérabilités. Puis, ils s'activent via la création d'un exploit ou d'une porte dérobée qui utilise les vulnérabilités identifiées sur la machine. Les éditeurs mettent à la disposition des utilisateurs des solutions antivirales et obligent les cyber-criminels à imaginer de nouvelles méthodes d'attaques. La création de malwares fait très souvent effet « boule de neige ». C'est précisément le cas actuellement sur Win 32. Les autres plates-formes ne souffrent pas encore de ce type de phénomène.

Kaspersky Lab France
Immeuble l'Européen Bât C
2 Rue Joseph Monier
92500 RUEIL MALMAISON

☎ 0825.888.612
RCS 478 315 872
www.kaspersky.fr

Si les utilisateurs de plates-formes alternatives restent partiellement à l'abri de ces cyber-menaces, ils sont également victimes d'attaques.

Evolution des malwares sur les différents systèmes Unix :



Les chiffres indiquent le nombre de malwares identifiés.

On remarque une grande concentration de malwares sur Linux avec une augmentation de plus de 100%.

Rien d'étonnant puisque cette plate-forme est la plus populaire parmi les systèmes Unix. Bien que Linux fonctionne sur différentes plates-formes RISC, les fichiers binaires, autres que x86, se font beaucoup plus rares. Sur les autres plates-formes RISC, par exemple sur SPARC, il est plus facile de trouver des fichiers binaires pour SunOS. En règle générale, ces échantillons sont une série de petits utilitaires écrits et compactés pour une version bien particulière d'un système d'exploitation et conçu pour un serveur précis.

C'est le cas des sniffers, backdoors, logcleaners, modules de noyau dont l'objectif est de masquer les actions de l'attaquant (une telle série s'appelle « rootkit »). Ces derniers sont conçus pour frapper une machine en particulier. L'attaque est donc planifiée et beaucoup plus difficile à contrer que lorsqu'un trojan est lancé par un script-kiddies.

Le malware développé pour Unix se caractérise par l'absence de différents compresseurs de fichiers exécutables, qui compliquent généralement le procédé d'analyse et de détection des programmes malicieux. Excepté upx, le format de compression des données et l'une de ses variantes, nous n'avons rien enregistré d'autre.

En termes de codes malicieux, Unix se retrouve dans la même situation que Win 32. Les virus infectant les fichiers sur le disque local se font de plus en plus rares. Ces derniers sont plus créés pour s'amuser que pour détruire, à moins que l'auteur n'ait fait une erreur de programmation du code. Dans ce cas, ils ne font qu'altérer le fichier qui devient alors inactif.

Aucune épidémie n'a été identifiée à ce jour et les virus pour Unix restent exceptionnels. Toutefois, on trouve des exemples relativement intéressants. Par exemple, Virus.Linux.Grip utilise le traducteur brainfuck pour générer une clé de cryptage, qui à son tour est utilisée pour chiffrer par l'algorithme tea.

Pourtant ces virus ne présentent aucun intérêt si ce n'est pour la recherche. L'écriture de tels virus coïncide avec l'adage de Linus Torvalds : «Just for Fun».

En revanche, c'est différent en ce qui concerne les programmes conçus pour corrompre des serveurs afin de les utiliser ensuite comme plates-formes d'attaques. Les programmes de ce type sont nombreux. Il s'agit des backdoors, exploits, sniffers, flooders et autres outils de pirates. Leur nombre, tout comme la popularité de Linux, augmente régulièrement.

En 2005, les vers tels que Net-Worm.Linux. Lupper et Net-Worm.Linux.Mare ont été particulièrement remarqués. Ils utilisent la même vulnérabilité et les mêmes méthodes de diffusion. La backdoor Tsunami fait partie de leurs composants. Lorsque la version d'un ver est mise à jour, ce dernier se trouve automatiquement armé de nouvelles fonctions. La dernière version de Net-Worm.Linux.Mare par exemple, téléchargeait un ircbot, qui faisait office de porte dérobée.

En septembre 2005, un autre incident s'est produit dans le monde Linux. Ont été détectées sur un serveur public de nombreuses installations porteuses de fichiers binaires infectés du célèbre navigateur Mozilla dans sa version coréenne. Les fichiers étaient infectés par le virus Virus.Linux.Rst.

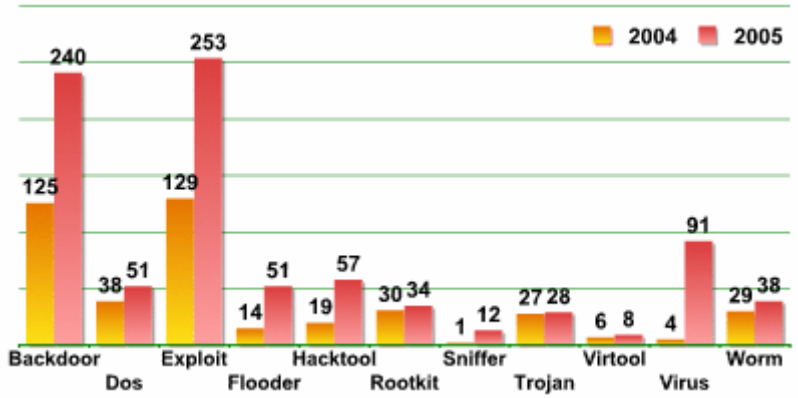
Voila donc les faits marquants de 2005 pour les systèmes ouverts. Dans le monde des systèmes ouverts, peu de codes malicieux existent mais les familles de virus identifiées progressent essentiellement sur les environnements Linux.

En ce qui concerne les rootkits, qui se multiplient sur la plate-forme Win 32, ils ne s'en sont pas encore pris à Linux.

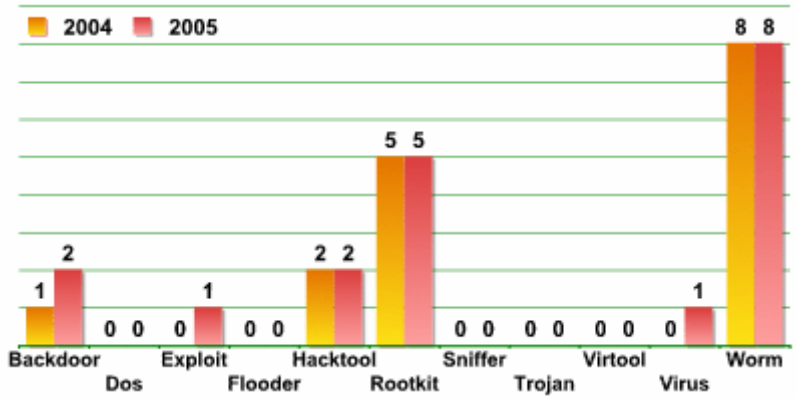
Sur les autres plateformes Unix, c'est encore plus calme. Ce qui est somme toute compréhensible puisque les autres systèmes Unix sont loin d'atteindre la popularité de Linux et de Microsoft Windows.

Les données statistiques ci-dessous sont basées sur l'analyse de données antivirus à différentes périodes. Les vides dans les diagrammes sont synonymes d'absence de représentants d'une famille sur une plateforme donnée.

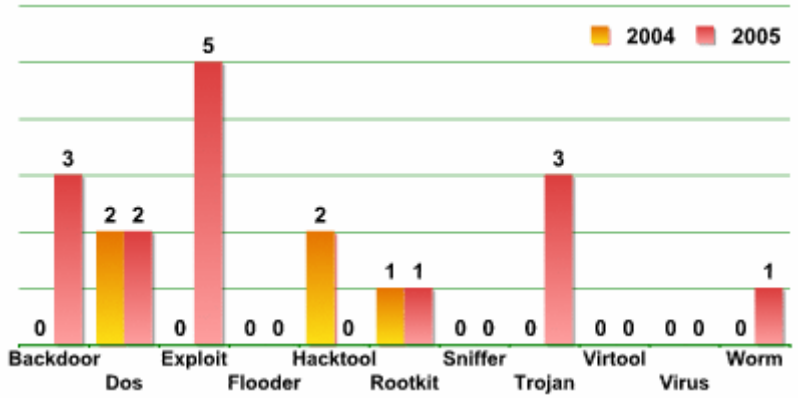
Linux Malware



FreeBSD Malware

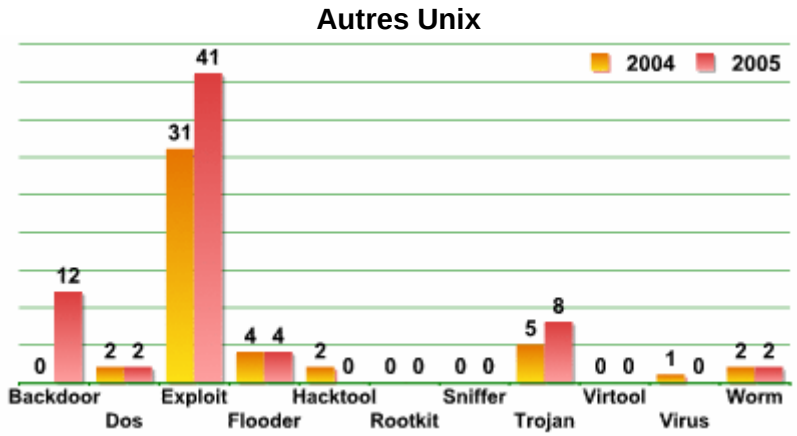


Sun OS



Kaspersky Lab France
Immeuble l'Européen Bât C
2 Rue Joseph Monier
92500 RUEIL MALMAISON

☎ 0825.888.612
RCS 478 315 872
www.kaspersky.fr



Prévisions

Les technologies 64-bits sont en cours de déploiement et dès qu'elles seront massivement installées sur les ordinateurs des internautes, les auteurs de virus vont réagir en conséquence.

Il faut ainsi s'attendre à des complications, le code binaire pour AMD 64 et pour IA 64 (Intel architecture) étant différent.

Ce qui signifie que des versions séparées doivent être compilées pour chaque plate-forme.

Apple n'est pas en reste. Le passage aux processeurs Intel peut s'avérer révolutionnaire. En plus de l'excellent design d'Apple, Mac OS X qu'on pourrait appeler « Unix avec une interface conviviale », peut obtenir un franc succès auprès des utilisateurs et devenir la proie des cyber-criminels.

Le noyau Mac OS X est basé sur FreeBSD. C'est pourquoi l'expérience et les idées déployées pour l'écriture de malwares pour FreeBSD peuvent être reprises pour Mac OS X. De plus, les développeurs du système ont inséré leurs propres erreurs. Au cours des semaines passées, 2 vers PoC pour Mac OS X ont été identifiés ce qui indique la présence d'erreurs dans l'architecture du système. Ces PoC ont été suivis de l'exploit pour le navigateur web Safari qui permet de lancer un script et d'exécuter des commandes sur la machine de l'internaute. Mac OS X peut être un terrain propice pour la recherche sur la sécurité.

Les appareils mobiles sont également un secteur de développement très dynamique du secteur IT. Et ici Linux se présente comme une alternative à Symbian et Microsoft Windows Mobile. De nombreux éditeurs développent ou annoncent la sortie d'appareils sous Linux. L'apparition de programmes malicieux ne devrait plus être très longue : il suffit d'attendre que le taux d'utilisation de ces appareils atteigne une masse critique.

Il est possible que la croissance explosive d'une nouvelle technologie stimule le développement de nouvelles technologies virales. Qui plus est, un nouvel environnement de diffusion (comme l'a été le bluetooth à une certaine période) peut se retrouver rapidement accaparé par les programmes malfaisants pour téléphones mobiles comme pour PCs.

A propos de Kaspersky Lab

Kaspersky Lab est un éditeur russe de solutions logicielles indispensables pour contrer toutes les formes de cyber-menaces en perpétuelle évolution. Depuis de nombreuses années, les meilleurs experts mondiaux travaillent dans les laboratoires de Kaspersky Lab afin d'offrir des services de hauts niveaux appréciés par les éditeurs et les utilisateurs. 24 h sur 24 h, 7 jours sur 7, les chercheurs analysent et traitent les codes malicieux. Des antidotes sont rapidement développés et validés puis proposés aux utilisateurs via les dizaines de mises à jour quotidiennes.

Kaspersky Lab dispose de bureaux à Moscou, en Allemagne, en Grande Bretagne, au Benelux, en Chine, en Corée du Sud, aux Etats-Unis, en France, au Japon, aux Pays-Bas, en Pologne.

Fondée en 1997, Kaspersky Lab concentre ses efforts sur le développement de solutions de pointe permettant de protéger les informations et les utilisateurs. Kaspersky Lab développe des logiciels de sécurité destinés à un large spectre d'applications et de clients, de l'utilisateur familial aux grands comptes. Kaspersky Lab distribue, supporte et assure la promotion de ses produits dans plus de 50 pays dans le monde.

Pour plus d'informations concernant Kaspersky Lab : http://www.kaspersky.fr
Pour plus d'informations sur l'actualité virale : http://www.viruslist.com/fr

Toute l'actualité de Kaspersky Lab est accessible aux journalistes sur :
http://presse.kaspersky.fr

Contacts presse :

MEDIASOFT COMMUNICATIONS
Emmanuelle Bureau du Colombier
Ebdc@mediasoft-rp.com
Peggy Lainé
Peggy.laine@mediasoft-rp.com
Tél : 01 55 34 30 00

KASPERSKY LAB France
Stéphane Le Hir / Directeur
Jean-Philippe Bichard / Directeur Marketing
Jean.philippe.bichard@fr.kaspersky.com
Tél : 01 41 39 04 89