

Les dessous de l'économie souterraine des codes malicieux : Chevaux de Troie, virus et malwares

Yury Mashevsky, l'un des plus éminents experts de Kaspersky Lab à Moscou, consacre un rapport aux événements marquants de l'année 2005. Il y aborde les tendances du développement de l'économie souterraine des logiciels et analyse la situation actuelle. Il énonce certaines recommandations destinées à prévenir les utilisateurs contre les attaques d'individus mal intentionnés. Il s'adresse avant tout aux professionnels de la sécurité informatique que l'étude des programmes malveillants intéresse, mais il peut être utile également à tous les utilisateurs sensibles à la problématique de la virologie informatique.

Analyse de la situation actuelle et tendances : trois grandes catégories de codes malicieux en 2005

L'année 2005 est marquée par les changements perceptibles qui ont touché le milieu des programmes malveillants. A la fin de l'année, le nombre de programmes malveillants détectés en moyenne chaque mois par Kaspersky Lab s'élevait à 6 368. L'année se solde par une croissance de 117 %, soit 24% de plus que le bilan de l'année passée. Ces chiffres témoignent de l'augmentation du taux de croissance de l'économie souterraine des applications malicieuses.

Selon le classement de Kaspersky Lab accessible sur <http://www.viruslist.com/fr/virusdescribed>, il existe trois catégories de programmes malveillants :

1. Chevaux de Troie : différents types de chevaux de Troie incapables de se multiplier de manière autonome (portes dérobées, rootkits et tous les chevaux de Troie possibles) ;
2. Virus : programmes malicieux autoreproducteurs (virus et vers) ;
3. Malwares : programmes très populaires auprès des individus mal intentionnés qui les utilisent pour créer des programmes malicieux et/ou pour organiser des attaques.

La popularité des programmes malicieux identifiés par les experts de Kaspersky Lab se répartit de la manière suivante :

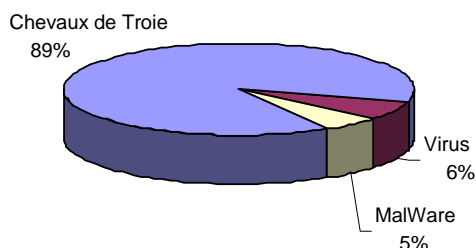


Illustration 1 : Répartition des programmes malicieux par catégorie (fin 2005)

Le tableau suivant indique la progression de chacune de ces classes par rapport à 2004 :

| Classe | Progression |
|------------------|-------------|
| Chevaux de Troie | +8.76% |
| Virus | -6.53% |
| Malware | -2.23% |

Tableau 1. Progression de chaque catégorie entre 2004 et 2005

L'intérêt croissant porté à la famille des chevaux de Troie ressort clairement de l'analyse des données du tableau. Cette tendance s'inscrit dans la continuité de 2004. Elle se produit au détriment des représentants des deux autres groupes : les virus et les malwares. Ici aussi, la tendance de 2004 se confirme.

Cette situation s'explique en grande partie par des facteurs économiques : le développement d'un cheval de Troie est plus rapide et coûte moins cher que le développement de programmes malicieux autoreproducteurs. De plus, la diffusion par courrier électronique (courrier indésirable) permet de toucher plus vite de nouveaux utilisateurs en comparaison à la diffusion via des vers de messagerie.

Chevaux de Troie

Si l'on transpose le nombre de chevaux de Troie découverts chaque mois par les analystes de Kaspersky Lab dans un graphique, on obtient le résultat suivant :

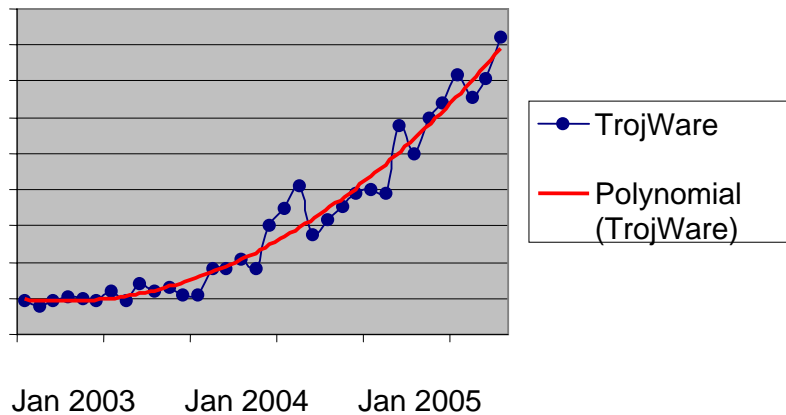


Illustration 2 : Développement des chevaux de Troie

Ce graphique indique clairement la croissance soutenue du nombre de chevaux de Troie interceptés chaque mois, croissance qui a commencé à se manifester au début de l'année 2004 et qui s'est poursuivie tout au long de l'année 2005. De plus, le rythme de cette croissance n'a cessé d'augmenter et correspond, fin 2005, à un taux de 124% par rapport à 2004. Ainsi, le nombre de programmes appartenant à la famille des chevaux de Troie a plus que doublé en 2005.

Le schéma n°3 illustre le développement des différents types de chevaux de Troie :

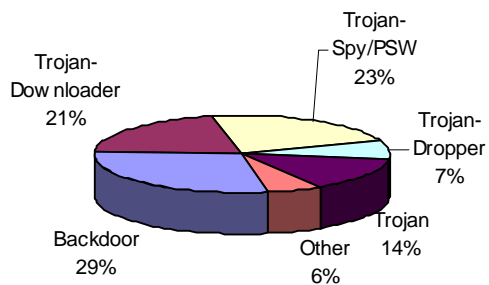


Illustration 3 : Répartition des chevaux de Troie par type à la fin 2005

Les chiffres cités dans le tableau 2 indiquent que le nombre de chevaux de Troie découverts en 2005 a changé par rapport à 2004. Le caractère « - » signale des comportements uniques dont les modifications ne sortent pas des limites statistiques.

| Manifestation | Progression du nombre de programmes malveillants entre 2004 et 2005 |
|-------------------|---|
| Backdoor | +95% |
| Trojan | +90% |
| Trojan-AOL | - |
| Trojan-ArcBomb | - |
| Trojan-Clicker | +86% |
| Trojan-DDoS | - |
| Trojan-Downloader | +272% |
| Trojan-Dropper | +212% |
| Trojan-IM | - |
| Trojan-Notifier | - |
| Trojan-Proxy | +68% |
| Trojan-PSW | +122% |
| Trojan-Spy | +104% |
| Rootkit | +413% |
| TrojWare | +124% |

Tableau 2 : Taux de croissance de chaque type de cheval de Troie en 2005

La majorité de ces chevaux de Troie se caractérise par une forte croissance.

Les représentants des classes Trojan-AOL, Trojan-ArcBomb, Trojan-DdoS, Trojan-IM et Trojan-Notifier sont assez rares et leur nombre n'a pas dépassé quelques exemplaires par mois tout au long de l'année 2005.

Les éléments les plus populaires sont les représentants des catégories Backdoor, Trojan-Downloader, Trojan-Dropper et Trojan-Proxy utilisés par les individus mal intentionnés pour le développement de Botnets.

Botnets : des réseaux utilisés par des cyber-criminels

Ces réseaux de bots sont constitués d'un grand nombre d'ordinateurs infectés et sont soumis à une administration centralisée. Le comportement du réseau de bots dans son ensemble est défini par l'individu mal intentionné, propriétaire du réseau. Dans la majorité des cas, ces réseaux d'ordinateurs zombies servent à diffuser du courrier indésirable ou à mener des attaques par déni de service sur des cibles définies par l'individu mal intentionné. Ces derniers temps, ces réseaux de bots ont été largement plébiscités par les cyber-criminels, ce qui explique le renforcement de la croissance des trois catégories indiquées : ils interviennent plus souvent dans la construction et l'entretien de réseaux de machines infectées. Le courrier indésirable est le mode de diffusion de plus en plus souvent utilisé pour ces types de chevaux de Troie.

Les experts de Kaspersky Lab observent également un intérêt croissant pour Trojan-PSW et Trojan-Spy, ce qui illustre le développement du marché des applications criminelles : les actions des cyber-criminels sont clairement motivées par l'appât du gain. Bien souvent, ce sont des informations à caractère financier qui sont volées. Ceci étant, les autres biens virtuels ne laissent pas indifférents les hackers qui peuvent tenter de les revendre à la victime ou sur le marché noir des biens virtuels.

Les experts de Kaspersky Lab ont constaté l'émergence d'un Trojan-Spy capable de récolter directement des informations sur plusieurs centaines de systèmes bancaires et de paiement en ligne, ce qui témoigne une fois de plus de l'appétit croissant du milieu criminel.

Dans la majorité des cas, les Trojan-Clicker servent à faire augmenter les compteurs de visites de sites définis par l'auteur. Ils connaissent le taux de croissance le plus faible ce qui explique qu'ils soient délaissés au profit de programmes malicieux « plus rentables ».

Les chevaux de Troie représentent les plus anciens codes malicieux. Cette famille regroupe tous les programmes qui, pour une raison quelconque, ne correspondaient à aucun des comportements cités ci-dessus. Leur progression est inférieure à la progression du groupe dans son ensemble mais reste tout de même significative.

Les rootkits sont peut-être les membres les plus récents de cette classe (ils sont apparus il y a 2 ou 3 ans). A la fin de l'année 2005, leur nombre avait augmenté de 413% selon les données de Kaspersky Lab. Il faut néanmoins relativiser cette véritable explosion en rappelant que l'année dernière, on recensait en moyenne 6 rootkits par mois. En 2005 par contre, ce chiffre est passé à 32 nouveaux rootkits par mois, ce qui témoigne clairement de l'intérêt marqué par le milieu cyber-criminel pour ce comportement. Il faut préciser que les rootkits en tant que tels n'exécutent aucune action malveillante. Ils sont utilisés par les individus mal intentionnés principalement pour dissimuler la présence dans le système d'autres programmes malicieux.

Il convient de remarquer que le taux de croissance de la majorité des comportements de cette catégorie est en augmentation par rapport à 2004. Il s'agit de la seule classe qui suscite un tel intérêt croissant.

Virus

Le graphique n°4 illustre le nombre de nouveaux virus découverts chaque mois par les analystes de Kaspersky Lab. Il prend la forme suivante :

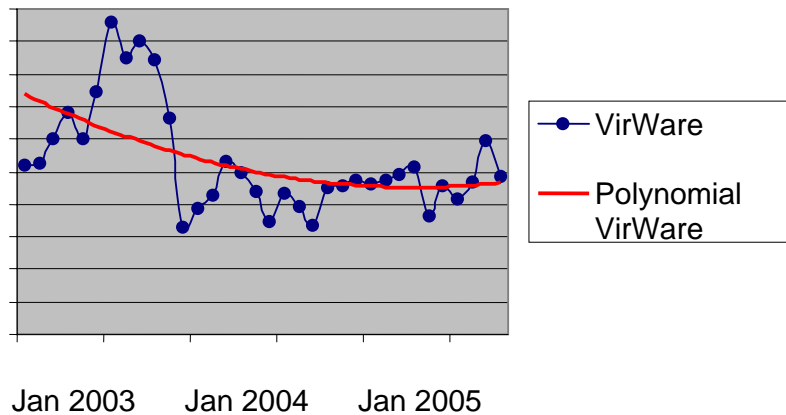


Illustration 4 : Développement des virus

Le schéma n°5 illustre le développement des différentes familles de virus (manque la fin de l'année 2005) :

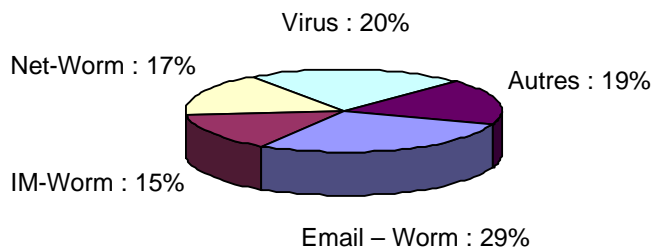


Illustration 5 : Répartition des virus par type à la fin 2005

Le graphique n°4 indique clairement que la stagnation qui s'était amorcée en 2004 s'est confirmée en 2005. La croissance globale de cette catégorie est insignifiante par rapport à la croissance totale du nombre de programmes malicieux. De plus, la stagnation se maintient uniquement grâce à l'augmentation de certains vers. Pour le reste, le déclin est évident. Le tableau 3 illustre en détail cette tendance (la perte d'intérêt vis-à-vis des représentants de la famille des virus se produit au profit des chevaux de Troie).

| Type de virus | Progression du nombre de programmes malveillants entre 2004 et 2005 |
|---------------|---|
| Email-Worm | +2% |
| IM-Worm | 35 nouvelles modifications/mois |
| IRC-Worm | -31% |
| Net-Worm | +43% |
| P2P-Worm | -43% |
| Worm | -3% |
| Virus | -45% |
| VirWare | -2% |

Tableau 3 : Rythmes de croissance de chaque type de virus en 2005

Les vers de messagerie affichent une certaine croissance qui est à mettre au compte des auteurs du ver Bagle et de l'activité des programmes malveillants détectés, principalement par habitude, comme vers de messagerie alors qu'il s'agit principalement de chevaux de Troie qui servent à maintenir les réseaux de bots à un niveau actuel. Sans l'activité de quelques groupes criminels, ces chiffres auraient reculé en 2005. De plus, même si l'on tient compte de l'augmentation de 2%, il faut se dire qu'elle est inférieure à la croissance de tous les programmes malveillants dans leur ensemble, ce qui confirme la tendance évoquée antérieurement sur l'abandon des vers de messagerie au bénéfice des chevaux de Troie qui coûtent moins chers à élaborer et qui, de plus, peuvent être envoyés efficacement sous forme de courrier indésirable.

Vers de messagerie : toujours en croissance

Bien que les vers de messagerie instantanée aient fait leur apparition en 2001, ce n'est que vers le milieu de l'année dernière qu'ils ont commencé à faire l'objet d'une certaine attention.

A la fin 2005, le nombre de nouveaux vers de messagerie instantanée atteignait déjà les 32 unités par mois, ce qui démontre l'intérêt qui leur est porté.

Les vers IRC (Internet Relay Chat) ont disparu un peu plus encore de la scène des programmes malicieux au cours de l'année 2005 et sont réapparus sous la forme de portes dérobées. L'apparition de nouveaux représentants de cette famille reste un phénomène isolé.

Les vers Internet ont doublé leur taux de croissance au cours de l'année écoulée : 43% en 2005 contre 21% en 2004. Cela s'explique tant par l'apparition de nouveaux exploits (par exemple, MS05-39 qui a servi à l'écriture d'un ver à l'origine d'une épidémie globale) que par les caractéristiques propres de ce comportement qui contourne l'utilisateur en tant que chaînon de la propagation (il n'est pas nécessaire d'attendre que l'utilisateur double-clique sur le ver pour le lancer), ce qui accélère sensiblement la vitesse de propagation des vers de réseau.

Les vers P2P (Peer-to-Peer) continuent à perdre du terrain, une tendance qui s'était amorcée en 2004. Ceci s'explique en partie par les campagnes menées contre les réseaux d'échange de fichiers.

Les vers maintiennent également la tendance entamée l'année dernière. Et il s'agit du seul comportement parmi tous les virus dont le taux de croissance n'a absolument pas changé (il est toujours de -2%, ce qui s'inscrit dans les limites statistiques et qui confirme la stagnation).

Les virus classiques chutent de manière moins brutale : -45% en 2005 contre -54% en 2004. Cette situation s'explique dans la mesure où les virus, du point de vue du développement, demeurent les programmes malveillants les plus compliqués. De plus, la vitesse de propagation des virus classiques ne peut être comparée à la vitesse de propagation d'une infection basée sur la diffusion de messages non sollicités.

Ainsi, le recul d'un comportement au sein de cette classe est compensé par la progression d'autres comportements, ce qui entraîne une chute légère de 2% de la classe dans son ensemble.

Malware

Cette catégorie est la moins représentée en termes de programmes malveillants découverts, mais la plus importante en termes de comportements. L'année se solde par une croissance mais le taux de croissance pour la catégorie est inférieur au taux de croissance de tous les programmes malveillants découverts par Kaspersky Lab, comme l'illustre le graphique suivant :

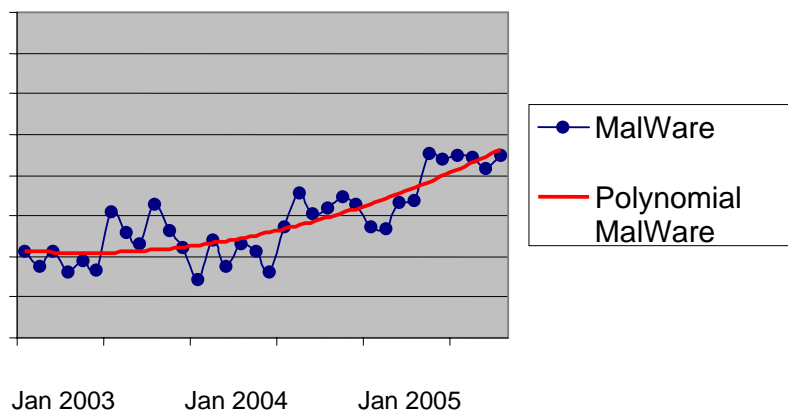


Illustration 6 : Développement des malwares

Le schéma n°7 illustre la popularité des différentes familles de malware :

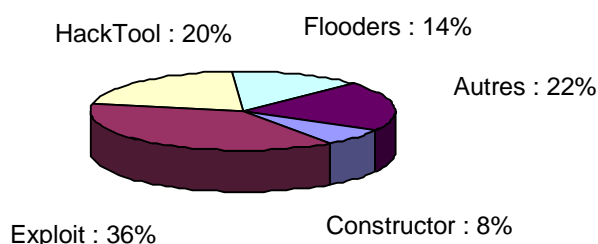


Illustration 7 : Répartition des malwares par type à la fin 2005

Seuls cinq représentants de cette classe méritent l'attention. Les programmes malveillants qui appartiennent aux autres comportements sont assez rares et on ne peut pas vraiment parler d'un développement sérieux.

| TYPE : Comportement | Progression du nombre de programmes malveillants entre 2004 et 2005 |
|---------------------|---|
| Exploit | +68% |
| HackTool | +33% |
| Constructor | +1% |
| Flooders | +20% |
| SpamTool | 6 nouvelles modifications/mois |
| MalWare | +43% |

Tableau 4 : Taux de croissance de chaque type de malware en 2005

Les exploits constituent le taux de croissance le plus élevé parmi les malwares. Les nouvelles vulnérabilités sans cesse identifiées ont renforcé la position de leader des exploits dans cette classe. Et rien ne laisse supposer que la situation changera dans un avenir proche : ce comportement occupe sans aucun doute la première place en terme de nouveaux représentants.

Les outils d'attaque (hacktool) sont utilisés pour mener toutes les attaques possibles et imaginables. La croissance de 33% est inférieure à la croissance de la classe dans son ensemble mais elle souligne néanmoins l'intérêt grandissant que les individus mal intentionnés portent à ces outils.

Les flooders (IM-Flooders, Email-Flooder, SMS-Flooder, etc.) sont utilisés par les individus mal intentionnés pour diffuser massivement des informations aléatoires via une usurpation de la source. Le nombre de représentants de cette catégorie est caractérisé par la même croissance que pour l'ensemble de la classe : +20%.

Les représentants SpamTool servent à recueillir des adresses électroniques sur les objets infectés afin de les transmettre à l'individu mal intentionné qui les utilisera dans l'envoi de messages non sollicités. Les analystes de Kaspersky Lab ont remarqué un intérêt minime mais stable pour cette manifestation.

Dans l'ensemble, on ne peut pas dire que l'année 2005 fut une année remplie de grande croissance pour les malwares car la croissance mensuelle de cette catégorie de malware reste légèrement inférieure à la croissance de l'ensemble des programmes malveillants.

Tout au long de l'année, les différentes catégories de malwares ont perdu en popularité face aux chevaux de Troie.

Opérations bancaires via Internet : 402% de croissance en 2005

Kaspersky Lab constate une augmentation du taux de croissance des chevaux de Troie utilisés pour le vol d'informations bancaires. Ces informations sont nécessaires pour accéder aux services bancaires en ligne afin de voler l'argent du compte de la victime.

Le taux de croissance de cette catégorie est le plus élevé parmi les programmes malicieux et représente 402% à la fin de l'année 2005. On observe également des tentatives de création de réseaux de bots particuliers : tout débute par la diffusion d'un programme permettant l'installation de tous les Trojan-Spy.Win32.Banker. Puis, l'individu mal intentionné configure son réseau de bots afin de voler les informations de n'importe quel système bancaire.

Attaques sur de nouvelles plates-formes et création de programmes malicieux multi plates-formes notamment sur les consoles de jeux

L'intérêt croissant que portent les cyber-criminels à de nouvelles plates-formes est un fait marquant, tout comme les tentatives continues de créer des programmes malicieux multi plates-formes.

En 2005, les analystes de Kaspersky Lab ont décelé l'apparition de programmes malicieux pour quelques nouvelles plates-formes dont PSP (Trojan.PSP.Brick.a) et Nintendo (Trojan.NDS.Taihen.a). La simple création de concepts pour ces plates-formes indique une fois de plus que le milieu cyber-criminel est en « veille » permanente afin de « développer » de nouvelles méthodes d'enrichissement illégal.

Kaspersky Lab observe l'apparition de programmes malicieux intéressants. Ainsi, Worm.SymbOS.Comwar.a est le premier ver pour les appareils nomades qui tournent sous Symbian à avoir assimilé un nouveau mode de diffusion, les MMS, pour se défaire des limitations du protocole Bluetooth (ce protocole permettait la diffusion dans un rayon de 10 mètres uniquement).

L'apparition de Trojan.SymbOS.Cardtrap.a est un autre phénomène intéressant de l'année 2005. Il s'agit d'un fichier SIS normal qui, une fois lancé, conserve les programmes malveillants pour la plate-forme Win32 sur la carte Flash. Et même si les programmes Win32 enregistrés au départ du corps de Trojan.SymbOS.Cardtrap.a ne peuvent pas être exécutés automatiquement sur les ordinateurs personnels en raison de particularité du système d'exploitation, les tentatives pour créer des virus multi plates-formes doivent être considérées avec la plus grande prudence.

Unix / Linux : 45% de croissance de codes malicieux

Il faut parler également de l'environnement Unix / Linux qui connaît un développement constant. Le monde des systèmes ouverts devient la cible de programme malicieux. Alors qu'en 2004, nous ne recensons en moyenne que 22 nouveaux programmes malicieux par mois pour cette plateforme, le nombre est passé à 31 en 2005. A la fin 2005, la croissance par rapport à 2004 était de 45%.

Concernant la famille des Adwares dont la croissance s'élève à 63% par rapport à 2004, 2005 apparaît comme une année de transition. Comme déjà signalé par les experts de Kaspersky Lab, les représentants de cette classe transgressent de plus en plus souvent la ligne qui sépare les programmes malicieux des autres. Ceci est confirmé par l'identification de plus en plus fréquente de logiciels publicitaires qui exploitent des technologies propres aux virus.

Les éditeurs de logiciels antivirus ont de plus en plus souvent tendance à classer les représentants de cette classe dans la catégorie des applications à caractère criminel. De plus, le nombre de procès impliquant des compagnies éditrices de logiciels publicitaires est également en augmentation.

Conclusion

Dans le monde de la virologie informatique, 2005 a été une année riche en changements. Les attaques sont désormais industrielles. L'informatique souterraine s'est fortement criminalisée et se concentre sur le profit via l'exploitation de données confidentielles qu'il s'agisse de ressources systèmes, de comptes en banque, de secrets professionnels, ou de jeux en ligne. Les chevaux de Troie, qui peuvent être utilisés pour accéder à ce type de données, ont été largement utilisés.

L'augmentation du nombre de chevaux de Troie combinée à la relative stabilité des vers démontre que les auteurs de codes malicieux lancent des attaques de plus en plus ciblées pour un maximum de profit.

Enfin, en 2005, les malwares ont étendu leur influence à de nouvelles plates-formes épargnées jusqu'alors (les consoles de jeux), et ont adopté de nouvelles tactiques d'approche pour les anciennes plates-formes (Symbian OS).

Les changements observés en 2005 continueront certainement à se développer en 2006 avec l'arrivée de nouvelles technologies et appareils influençant dans une certaine mesure l'évolution des codes malicieux.

A propos de Kaspersky Lab

Kaspersky Lab est un éditeur de logiciels privé, spécialisé dans la protection des données informatiques. La société dispose de bureaux à Moscou (Russie), en Allemagne, au Benelux, en Chine, en Corée du Sud, aux Etats-Unis, en France, au Japon, aux Pays-Bas, en Pologne et au Royaume-Uni. Fondée en 1997, Kaspersky Lab concentre ses efforts sur le développement de solutions de pointe permettant de protéger les informations. Kaspersky Lab développe des logiciels de sécurité destinés à un large spectre d'applications et de clients, de l'utilisateur familial aux grands comptes ; des pare-feux à usage individuel ou professionnel ; et des solutions de filtrage d'informations pour les entreprises. 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 : www.kaspersky.fr

Pour plus d'informations sur l'actualité virale : www.viruslist.com/fr

Toute l'actualité de Kaspersky Lab est accessible aux journalistes directement depuis <http://presse.kaspersky.fr/>.

Contacts presse :

MEDIASOFT COMMUNICATIONS
Emmanuelle Bureau du Colombier
Ebdc@mediasoft-rp.com
Carole Scheppler
Carole.scheppler@mediasoft-rp.com
Tél : 01 55 34 30 00

KASPERSKY LAB FRANCE
Stéphane Le Hir / PDG
Jean-Philippe Bichard / Directeur Marketing
Jean.philippe.bichard@fr.kaspersky.com
Tél : 0 825 888 612