

## La sécurité liée au protocole Bluetooth

*Kaspersky Lab, éditeur reconnu de solutions de sécurité informatique contre toutes les formes de cyber-menaces (cyber-escroquerie, botnet, spams, phishing...) publie le nouveau rapport dédié à la sécurité sur la technologie Bluetooth rédigé par Alex Gostev, analyste spécialisé en virologie chez Kaspersky Lab.*

*A l'occasion d'InfoSecurity 2006, les experts de Kaspersky Lab ont mis en évidence que les smartphones sont beaucoup plus utilisés pour fonctionner avec des appareils audio WiFi que pour la connexion avec d'autres appareils. Cette étude révèle qu'il est désormais indispensable d'informer les utilisateurs sur les menaces collatérales liées à l'utilisation du standard Bluetooth. Les sociétés éditrices de téléphones mobiles et smartphones doivent à leur tour accorder toute l'attention nécessaire aux problèmes de sécurité consécutifs au développement du protocole Bluetooth et lors de la mise en place de services utilisés via ce protocole.*

Le Bluetooth est actuellement le moyen de transfert de données sans fil le plus populaire. La grande majorité des téléphones mobiles disponibles aujourd'hui sur le marché bénéficient du standard Bluetooth. Cette technologie permet d'échanger des données entre appareils analogues. Cette norme offre également la possibilité de travailler de manière autonome à l'aide de kits « mains libres ». Le protocole Bluetooth est intégré dans les smartphones, les assistants personnels et à certains ordinateurs portables.

Comme n'importe quelle nouveauté prisée dans le domaine des hautes technologies, le standard Bluetooth a rapidement été pris d'assaut par les « cyber-terroristes ». Le problème est d'autant plus complexe qu'en plus de l'inexpérience des utilisateurs, qui ne comprennent pas toujours les spécificités de la fonction Bluetooth, les éditeurs d'appareils mobiles ont quant à eux bien souvent commis de regrettables erreurs dans l'intégration de cette technologie dans leurs appareils. En conclusion, en plus des attaques traditionnelles utilisant la méthode du social engineering, nos experts ont trouvé des failles dans le protocole même.

Début 2006, Kaspersky Lab a publié un article analytique sur l'architecture du protocole Bluetooth et ses faiblesses les plus connues. Les recherches se sont poursuivies à ce sujet. Les téléphones mobiles sont depuis longtemps les victimes de virus informatiques. Le plus diffusé d'entre eux reste le ver Cabir, qui s'appuie sur la norme Bluetooth pour se propager.

Dans ce cas précis, trois problèmes s'imposent à l'utilisateur :

1. **Le social engineering** (ou l'ingénierie sociale) : les cyber-terroristes accèdent aux données du téléphone mobile. Ils utilisent comme point d'entrée le standard Bluetooth pour établir des relations de confiance avec le possesseur du téléphone mobile ou pour le convaincre de baisser ou désactiver le système d'authentification lors d'une connexion Bluetooth.

2. **Les failles liées à l'installation du protocole Bluetooth** : Les cyber-terroristes peuvent dérober des données depuis le téléphone mobile de l'utilisateur, effectuer des appels, envoyer des messages, mener des attaques de DOS sur l'appareil, écouter des conversations...
3. **La menace virale** : le téléphone mobile peut être infecté par un ver qui va s'envoyer depuis le téléphone mobile (pas seulement par la technologie Bluetooth mais par exemple sous la forme de MMS). Les données peuvent être endommagées, volées ou chiffrées.

Il faut reconnaître que dans un grand nombre de cas pour que le téléphone soit attaqué, le protocole Bluetooth doit être en mode « visibilité ». Toutefois, il existe des méthodes de détection pour téléphone utilisant la technologie Bluetooth en mode « invisibilité ». Les méthodes citées précédemment ne seront pas étudiées dans ce rapport du fait de la complexité de réalisation. Le procédé de telles attaques est basé sur la détection du téléphone via la recherche de son adresse MAC. Cette tactique peut prendre énormément de temps sans pour autant garantir de résultat.

Le laboratoire de Kaspersky Lab a effectué, en fin d'année dernière et en début d'année 2006, quelques tests en fonction des statistiques collectées sur le nombre de téléphones mobiles connectés au standard Bluetooth sur Moscou. Les tests ont été réalisés à des endroits stratégiques disposant d'une grande concentration de personnes (supermarchés, métro...) Au cours de ces tests, 100 appareils par heure ont été détectés en moyenne. Il ne s'agit pas d'un indice très élevé cependant, une telle concentration peut s'avérer dangereuse et capable de provoquer des épidémies importantes si, par exemple, parmi ces appareils, l'un d'eux est infecté par le virus Cabir.

Lors de notre voyage au salon Infosecurity 2006 de Londres en avril dernier, nous avons pour projet de collecter des statistiques sur les réseaux sans fil WiFi mais également sur les appareils Bluetooth. Le salon s'est révélé un endroit idéal pour ce type d'étude dû à la masse importante de visiteurs. Par ailleurs, nous ne nous sommes pas limités au salon et nous avons étendu nos recherches à d'autres secteurs de Londres, afin de confronter les résultats obtenus avec les résultats moscovites.

Au cours des trois jours de tests, les experts de Kaspersky Lab ont identifié plus de 2000 appareils Bluetooth en mode « visibilité ». Plus de la moitié de ce chiffre concerne les visiteurs et les exposants présents à InfoSecurity. Nos partenaires Finnois F-Secure, ont effectué le même type de tests au CeBit 2006 (à Hanovre en mars dernier). Le nombre d'appareils détectés atteignait alors les 12 000. Si l'on tient compte du fait que le salon CeBit est environ 15 fois plus important en taille qu'InfoSecurity, alors nos résultats concordent avec ceux d'F-Secure.

En plus de la collecte de statistiques que nous utilisons pratiquement en temps réel lors de nos présentations sur le stand de Kaspersky Lab, nous avons pour mission de détecter les virus mobiles. Pour ce faire, nos ordinateurs portables et téléphones mobiles étaient paramétrés en mode « visibilité ». L'autorisation de réceptionner des fichiers et d'enregistrer automatiquement toutes les données entrantes était quant à elle désactivée. Le nom donné aux appareils qui servaient de leurre tenait compte du fait que la majorité des virus dédiés aux mobiles s'envoient sur le premier appareil détecté de la liste.

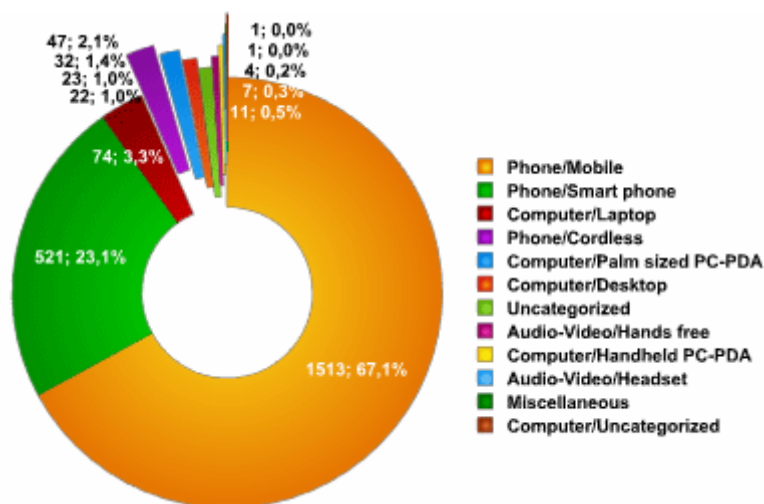
Les tests ont été réalisés à l'aide des programmes Blue Soleil, Blue Auditor et BTScanner.

La première partie des tests s'est déroulée dans les pavillons d'InfoSecurity. Les premiers jours du salon, la détection d'appareils était telle que nos scanners ralentissaient puisqu'ils tentaient de traiter toutes les données. Dans un rayon de 100 mètres, nos instruments ont détecté pas moins de 100 appareils, le dernier jour du salon lorsque la fréquentation des visiteurs a diminué. En une heure, nos outils ont réussi à détecter plus de 700 appareils. Il est évident que si un appareil infecté s'était trouvé sur le salon, en l'espace de quelques dizaines de minutes, tous les appareils vulnérables auraient subi une attaque.

La seconde partie des tests s'est déroulée en même temps que l'étude des réseaux sans fil dans le quartier de Canary Wharf, dans le métro londonien ainsi que dans plusieurs gares de Londres (Victoria, King Cross, Waterloo) aux heures de pointe.

Nous avons établi quelques comptes-rendus théoriques en cas d'épidémie par virus mobiles, en nous basant sur des épidémies biologiques par virus communs et quelques modèles d'épidémiologie mathématique. Ainsi, en présence d'une concentration normale d'appareils par mètre carré, le virus, pour mobile dans « l'idéal », peut infecter pratiquement tous les smartphones vulnérables de Moscou en l'espace de 15 jours. Dans la réalité, ce laps de temps sera bien supérieur, bien que le risque d'épidémies locales reste très grand. Gardons en mémoire l'année dernière à Helsinki, au stade où se déroulaient les championnats du monde d'athlétisme, une épidémie locale de cet acabit avait eu lieu. (données F-Secure - <http://www.f-secure.com/weblog/archives/archive-082005.html#00000621>).

## Les types d'appareils à technologie Bluetooth :



Les téléphones mobiles ordinaires représentent la grande majorité avec près de 70% du total. Il s'agit de téléphones sans réel système d'exploitation. Ils ne sont soumis théoriquement à la menace d'une infection que par codes malicieux réalisés sur Java pour téléphones mobiles. Toutefois, tous ces téléphones restent vulnérables à cause du standard Bluetooth. Au cours des tests effectués à Moscou, nous avons établi qu'environ 25% des appareils sont vulnérables à des attaques BlueSnarf.

BlueSnarf :

Il s'agit peut-être de l'attaque Bluetooth la plus célèbre. L'agresseur utilise l'OBEX Push Profile (OPP) exploité pour l'échange de cartes de visite et d'autres objets. Dans la majorité des cas, ce service ne requiert pas d'authentification. BlueSnarf exécute une requête OBEX GET vers un fichier connu, par exemple le carnet d'adresses « telecom/pb.vcf » ou bien le calendrier « telecom/cal.vcs ». Si la qualité du firmware est diminuée, l'agresseur peut accéder à tous les fichiers.

Nous n'avons pas récolté de données de ce type à InfoSecurity puisqu'en Grande Bretagne le balayage pour la recherche de failles est considéré comme criminel. Nous nous sommes limités aux données que l'on pouvait récolter conformément à la législation.

Les smartphones occupent la 2<sup>ème</sup> place en terme de popularité avec près de 25%. Force est de constater que la popularité des téléphones à système d'exploitation Windows Mobile et Symbian ne fait que croître. A ce rythme, le rapport téléphone/smartphone peut s'équilibrer dès l'année prochaine. Les smartphones utilisant l'OS Symbian sont la cible principale des virus mobiles. Cependant, la popularité de Windows Mobile (dans certains pays, il a déjà dépassé Symbian) va forcément s'accompagner d'une disponibilité de plus grande quantité de virus.

Les ordinateurs portables à adaptateur Bluetooth viennent en 3<sup>ème</sup> position. Leur part de marché est pourtant faible avec un peu plus de 3%. Néanmoins selon nos experts, le risque d'attaques de cyber-terroristes sur ce type d'appareils est bien plus élevé que sur les téléphones/smartphones. La raison est certainement due à l'importance des données conservées sur les ordinateurs, beaucoup plus variées et avantageuses pour un escroc que les données d'un téléphone.

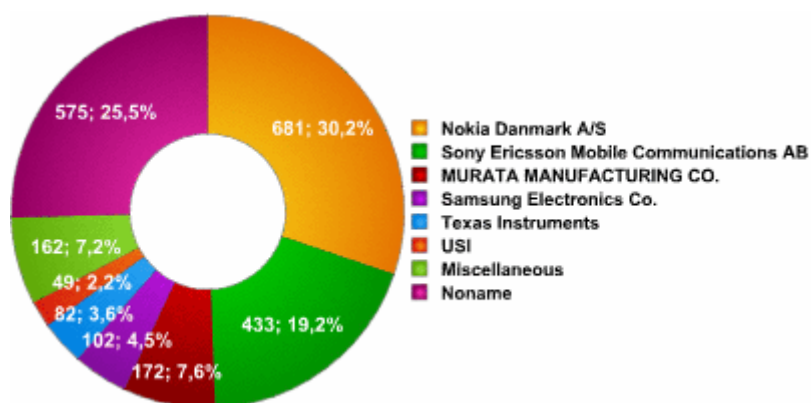
En ce qui concerne les autres appareils, nous noterons un petit pourcentage pour les ordinateurs de poche (Palm sized PC-PDA et Handheld PC-PDA) avec moins de 2%. Il s'agit d'un indice inattendu qui témoigne indirectement du fait que la plupart de ces utilisateurs sont bien informés des problèmes posés par Bluetooth. Ces utilisateurs avertis respectent les règles de sécurité.

Au total, 2000 appareils de 12 types différents ont été découverts. Parmi les différents types, nous avons trouvé également des « non classifiés » et « divers » mais leur part représente moins de 1%.

## Fabricants d'appareils

Cet indice est très intéressant car il permet d'observer de nombreux paramètres concernant la structure du marché. Par exemple, à partir d'informations sur le fabricant de l'appareil, nous pouvons en déduire le système d'exploitation utilisé (concernant uniquement les smartphones et les ordinateurs de poche) ou bien en déduire la popularité de certains éditeurs.

Au total 35 fabricants ont été identifiés dont 6 sont parmi les plus populaires avec 67% du total. Dans un grand nombre de cas, l'éditeur n'a pas pu être identifié soit 25.5%.



USI	2,17
Texas Instruments	3,63
Sony Ericsson Mobile Communications AB	19,19
Samsung Electronics Co.	4,52
Nokia Danmark A/S	30,19
MURATA MANUFACTURING CO.	7,62
Noname	25,49
Прочие	7,18

Au regard de ces chiffres, les téléphones Nokia sont sans conteste les leaders absolus. Sony Ericsson vient en 2<sup>ème</sup> position. La 6<sup>ème</sup> place revient à USI du fait de son utilisation dans les ordinateurs de bureau et portables y compris.

Répartition des produits développés par chaque fabricant :

#### Nokia

Phone/Smart phone	26,7%
Phone/Mobile	73,3%

#### Sony Ericsson

Phone/Smart phone	10,9%
Phone/Mobile	88,9%
Miscellaneous	0,2%

#### Murata

Phone/Mobile	99,4%
Computer/Desktop	0,6%

#### Samsung

Phone/Mobile	65,7%
Phone/Cordless	34,3%

#### Texas Instruments

Computer/Palm sized PC-PDA	1,2%
Phone/Smart phone	9,8%
Phone/Mobile	62,2%
Computer/Handheld PC-PDA	26,8%

#### USI

Computer/Laptop	81,6%
Computer/Desktop	18,4%

#### Statistiques concernant les éditeurs non identifiés :

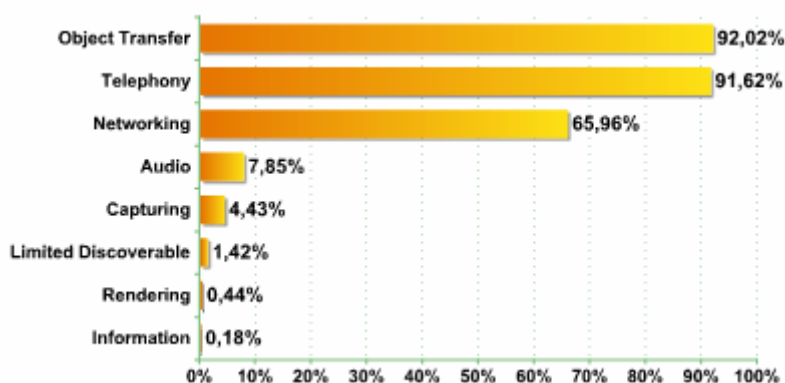
Phone/Smart phone	41,9%
Phone/Mobile	50,8%
Phone/Cordless	2,1%
Computer/Laptop	4,9%
Computer/Desktop	0,2%
Audio-Video/Hands free	0,2%

#### Services accessibles :

Ces données sont de grand intérêt d'autant plus que les attaques des cyber-terroristes et les infections virales dépendent d'eux. Lorsqu'un appareil se connecte à un autre appareil via la technologie Bluetooth, il met à la disposition de ce dernier des services. Par exemple, lorsque l'utilisateur se connecte aux périphériques de ses amis afin d'échanger des données, le téléphone mobile reste actif. Il permet en même temps de recevoir des appels, d'envoyer des SMS, de consulter le répertoire d'adresses etc. Cependant, il est possible qu'un cyber-terroriste se trouve à la place du destinataire. Pour arriver à ses fins, ce dernier a deux possibilités : réaliser une attaque de type social engineering ou exploiter une faille du protocole Bluetooth.

L'information que nous avons collectée sur les services nous permet de comprendre ce qui est accessible par l'escroc en ligne.

Voyons les données collectées pour chaque service. Sur plus de 2000 appareils détectés, nous avons identifié 6000 services répartis de la façon suivante :



Avec 6000 services pour 2000 appareils, nous obtenons une moyenne de 3 services par appareil. Toutefois, nous nous sommes également heurtés à des appareils dotés de 5 à 6 services.

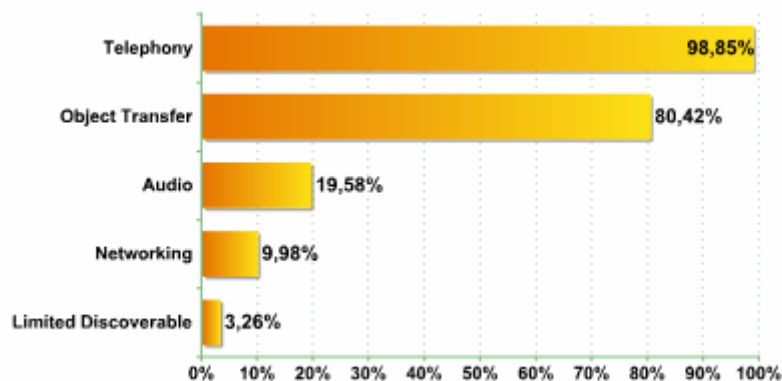
Trois services sont parmi les plus fréquents :

- La réception et le transfert de fichiers (Object Transfer) : Utilisé dans plus de 90% des appareils
- La téléphonie : Utilisée dans plus de 90% des cas
- Le Networking : Utilisé dans plus de 65% des cas

Etant donné que notre rapport vise en priorité les téléphones et les smartphones, nous allons voir les statistiques sur leurs services séparément.

Smartphones :

Pour les smartphones, le rapport "appareil/nombre de services" est de 1 pour 2.

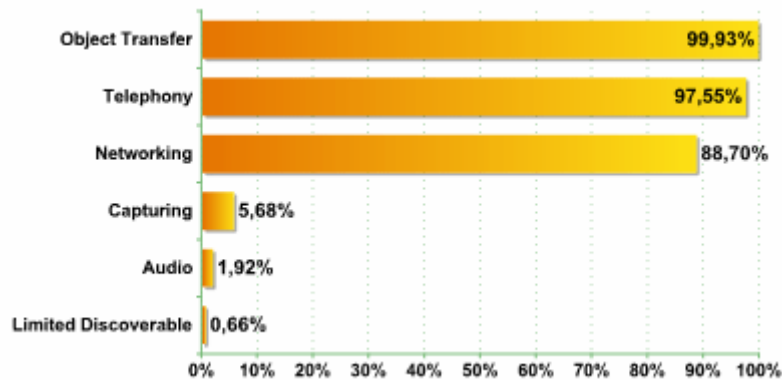


Nous assistons à de grandes variations par rapport aux statistiques générales. Dans les statistiques générales, le service le plus fréquent s'avérait être OBEX. Chez les smartphones, il occupe la 2<sup>ème</sup> place avec 90%. Le leader est la téléphonie traditionnelle avec près de 99%. La 3<sup>ème</sup> place est plutôt surprenante et est occupée par les services audio. En conclusion, les smartphones sont utilisés de manière beaucoup plus fréquente pour fonctionner avec des appareils audio sans fil que pour la connexion avec d'autres appareils dans le réseau.

Toutefois, notons que les smartphones représentent la plus grosse cible pour les virus mobiles et pour la diffusion de ces derniers. Le service permettant la réception et le transfert de fichier est indispensable. Sur le pourcentage total de smartphones détectés, environ 30% sont des Nokia. Cependant Nokia notifie l'utilisation du système d'exploitation Symbian qui est à l'heure actuelle la plate-forme principale pour le fonctionnement des virus mobiles y compris les virus comme Cabir et ComWar.

### Téléphones :

Pour les téléphones, le rapport « appareils/nombre de services » est de 1 pour 3. C'est un indice inattendu puisque la fonctionnalité des smartphones est bien supérieure aux téléphones. Toutefois, il s'agit sans doute du signe que la politique de sécurité pour les services et leur accessibilité sur les smartphones est mieux paramétrée.



Ici les 3 services leaders se distinguent à peine des statistiques générales. Nous ne nous attendions néanmoins pas à d'autres résultats puisque les téléphones mobiles représentent presque 70% du total des appareils détectés.

Par ailleurs, pour ce qui est du rapport « OBEX/téléphonie », la situation est contraire. Sur les téléphones mobiles, le transfert de fichiers est bien plus accessible avec plus de 97% contre 80% sur les Smartphones. Le service Networking est lui aussi répandu et atteint presque les 90%.

En fait, les failles accessibles lors de l'utilisation de la téléphonie sont aussi dangereuses sur les téléphones que sur les smartphones. Les vulnérabilités et attaques virales basées sur la réception et le transfert de fichiers sont plus dangereuses pour les téléphones mobiles que pour les smartphones. Le service Networking, qui est aussi un point sensible aux attaques, est plus fréquent sur les téléphones que sur les smartphones.

Pour ce qui est de nos tentatives « d'intercepter » un virus mobile, nous n'avons pas reçu de fichier infecté. Nous n'avons détecté aucune tentative de transfert de fichiers infectés. En même temps, nous recevons régulièrement des requêtes concernant l'envoi de fichiers en provenance de différents appareils, notamment au cours de nos tests dans les différents secteurs de la ville. Toutefois, ils se sont avérés ordinaires aussi bien à Londres qu'à Moscou. En réalité, le « Bluejacking » est très répandu, lorsque les utilisateurs s'échangent simplement des fichiers (musique, images, jeux), ou alors lorsque ces fichiers sont adressés par erreur. En revanche, un échange de fichiers aussi désordonné peut représenter un danger aussi bien pour celui qui envoie que pour celui qui reçoit. L'expéditeur peut envoyer un fichier important à un « mauvais » destinataire alors que le « bon » destinataire peut s'habituer à recevoir des fichiers anodins et finalement télécharger un ver ou un Trojan.

En conclusion, nos tests ont révélé qu'il est indispensable d'informer les utilisateurs sur les menaces collatérales liées à l'utilisation de la technologie Bluetooth. Les sociétés éditrices de téléphones et smartphones doivent à leur tour accorder toute l'attention nécessaire aux problèmes de sécurité consécutifs au développement du protocole Bluetooth et lors de la mise en place de services utilisés via ce protocole.

### ***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 et au Royaume-Uni.

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](mailto:Ebdc@mediasoft-rp.com)  
Peggy Lainé  
[Peggy.laine@mediasoft-rp.com](mailto: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](mailto:Jean.philippe.bichard@fr.kaspersky.com)  
Tél : 01 41 39 04 89