

SOPHOS

Rapport Sophos 2005 sur la gestion des menaces à la sécurité

2005



Rapport Sophos 2005 sur la gestion des menaces à la sécurité

Bilan de l'année 2005

Les responsables de la protection des réseaux ont eu à faire face cette année à des défis nouveaux et sophistiqués.

La complexité croissante des demandes exercées sur les systèmes informatiques, en matière de mobilité, de flexibilité ou d'interaction entre les différents logiciels et matériels, a conduit à une explosion du nombre de voies d'accès exploitées par les menaces.

L'année dernière, on a assisté à une augmentation du nombre et des types de logiciels malveillants. Le détournement des systèmes en ordinateurs zombies est devenu la pierre angulaire de nombreuses attaques et, face à la diffusion rapide des nouvelles menaces, les médias ont dû créer à la hâte des termes pour les décrire ("phishing", "pharming" ou encore "spearphishing"). La distinction entre les différents types de menaces est devenue plus floue. Dans l'ensemble, les menaces sont devenues plus discrètes et difficiles à déceler. Les spywares en particulier constituent l'un des plus importants défis auxquels l'entreprise doit désormais faire face.

Tendances des nouvelles menaces

Un rapport publié en novembre 2005 par Financial Insights, une société du groupe IDC, estime que, à cause du phishing,

les institutions financières internationales ont perdu à elles seules près de 400 millions de dollars US en 2004.¹

L'année dernière, les collusions criminelles et lucratives entre auteurs de virus, spammeurs et pirates ont foisonné sous des formes de plus en plus sophistiquées. Dans un environnement en perpétuelle évolution, les criminels ont collaboré pour créer des campagnes mêlant attaques virales, spam, phishing et spywares, brouillant les distinctions entre les types de menaces.

Le vandalisme aveugle des générations précédentes a fait place à des activités criminelles aux objectifs précis, qui s'appuient sur la création et la diffusion de multiples variantes d'une même menace pour essayer de contourner les protections antivirus à base de signatures et les techniques antispam traditionnelles.

En comparaison avec les vers à diffusion de masse du passé, les attaques actuelles à base de codes malveillants ciblent un nombre réduits de victimes afin de ne pas attirer inutilement l'attention sur elles.

Egalement, le nombre d'ordinateurs ciblés par chaque attaque de spam a été réduit pour que la menace se glisse au-dessous du seuil de détection des radars antispam mesurant le volume des échanges de messages électroniques.

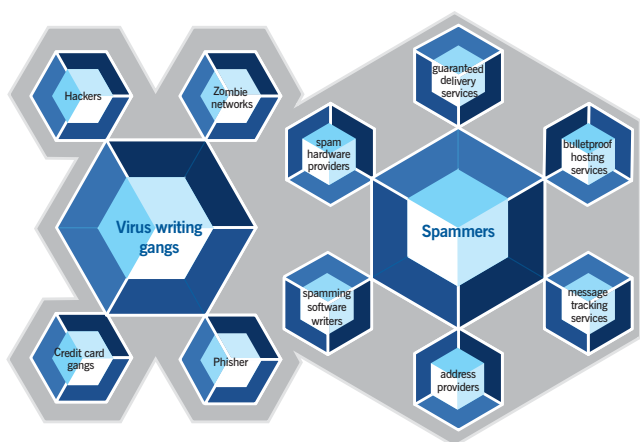


Figure 1 : L'écosystème des menaces

2005 en quelques chiffres

- 48 % d'augmentation des nouvelles menaces par rapport à l'année précédente
- 1 courriel sur 44 est viral
- Le nombre des nouveaux chevaux de Troie dépasse celui des vers dans une proportion de 2 contre 1
- La spam à caractère médical reste le plus répandu, avec une recrudescence du contenu pornographique et des escroqueries financières
- Collaboration des cybercriminels pour combiner les techniques d'attaques

Fort taux de croissance des menaces

Le nombre des nouvelles menaces a continué d'augmenter dans des proportions autrefois jugées impossibles à contenir. En décembre 2005, Sophos Anti-Virus identifiait et offrait une protection contre plus de 114 000 différents virus, vers, chevaux de Troie et autres logiciels malveillants.

Sur la période janvier–novembre 2005, le nombre de nouvelles menaces virales, de vers, chevaux de Troie et spywares a augmenté de 48 % comme suit :

- 2004 : 10 724 nouvelles menaces
- 2005 : 15 907 nouvelles menaces

Le trait le plus remarquable de cette évolution est l'augmentation systématique, mois après mois, du nombre des nouvelles menaces malveillantes. Pour le seul mois de novembre 2005, 1 940 nouvelles menaces malveillantes ont été découvertes ! Il s'agit à ce jour du plus grand chiffre mensuel de nouvelles menaces contre lesquelles Sophos offre une protection ! La Figure 2 compare les mesures de 2005 avec celles de l'année dernière.

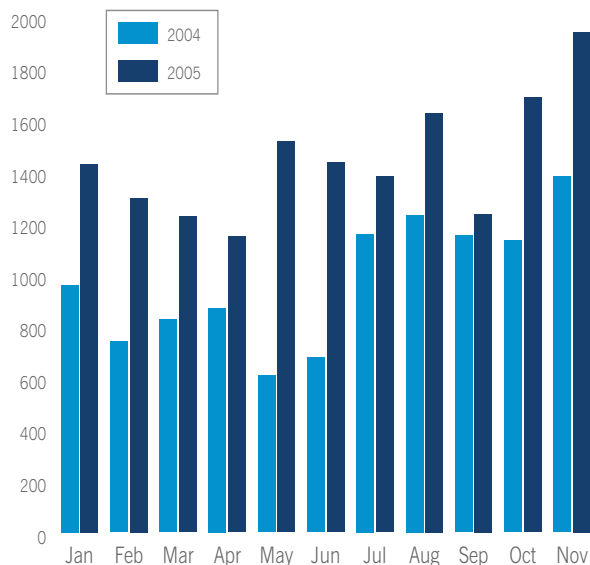


Figure 2 : Nouvelles menaces malveillantes
Comparaison 2004 et 2005

On peut attribuer cette augmentation à l'intérêt croissant des criminels pour la création de logiciels malveillants. L'appât du gain les a conduits à concevoir davantage de virus, de vers ou de chevaux de Troie pour dérober et extorquer de l'argent à des entreprises ou des utilisateurs innocents.

La quantité et la variété des menaces ne sont pas seules à augmenter sans cesse. C'est aussi le cas de la vitesse à laquelle les nouvelles attaques émergent et se diffusent.

Cette année, 1 courriel sur 44 en moyenne était infecté par un virus. En période d'épidémie majeure (comme lors de l'irruption de Sober-Z fin novembre 2005), ce chiffre a atteint 1 sur 12². Les vers à diffusion de masse parviennent ainsi à gravement perturber les communications sur Internet, inondant les utilisateurs particuliers, les entreprises et les fournisseurs d'accès de messages à contenus indésirables et dangereux.

En outre, les auteurs de logiciels malveillants ont tenté de rendre la vie des spécialistes de la lutte antivirus plus difficile en diffusant brutalement de nouvelles versions de leurs virus et chevaux de Troie, en grand nombre et dans une période de temps très courte³. En "emballant" leur code malveillant sous des habillages différents, leur but est d'éviter la détection par les éditeurs de solutions antivirus, en remplaçant rapidement les anciennes versions du ver ou du cheval de Troie par une nouvelle version dès que la précédente est neutralisée par les protections mises en place.

Pour cette raison, de plus en plus d'entreprises adoptent des protections proactives afin de bloquer le plus grand nombre possible de menaces virales dès leur première apparition, avant même que des mises à jour antivirus soient disponibles.

Sophos a complété cette approche en introduisant sa technologie de détection par Génotype™ viral, qui permet de déterminer si un nouveau logiciel malveillant est apparenté à d'anciens membres de la même famille de virus, pour l'empêcher de percer les défenses de l'entreprise.

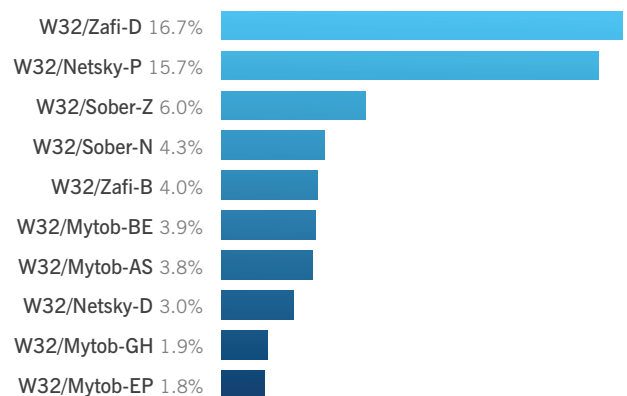


Figure 3 : Top Ten des virus signalés à Sophos en 2005

Top Ten des menaces

Sophos dispose d'un réseau global de dizaines de milliers de stations de surveillance qui capturent les données sur les plus récents virus se propageant par courriel. Il offre une mesure précise de la santé des systèmes de messagerie et fournit des alertes avancées sur l'apparition de crises épidémiques virales.

Bien que les pirates utilisent de plus en plus de techniques antispam pour diffuser les chevaux de Troie, ces derniers n'ont pas le même impact que les vers et les virus, qui ont la capacité de se propager via les systèmes de messagerie.

Pour de nombreux utilisateurs, particuliers ou entreprises, les codes malveillants figurant dans ce Top Ten sont les plus visibles, car ils apparaissent dans leurs boîtes de messagerie ou sont bloqués au niveau des passerelles de messagerie de l'entreprise.

Curieusement, ce classement est dominé par des virus apparus depuis longtemps. Ceci vient confirmer que les attaques les plus récentes ont été plus insidieuses, infectant de façon subtile de plus petits groupes de victimes dans l'espoir d'éviter d'attirer l'attention sur eux.

Le ver Zafi-D, qui sévit depuis longtemps, représente plus de 16,7 % de tous les virus signalés à Sophos ces douze derniers mois. Ce ver hongrois se dissimule sous les traits d'un message de vœux de Noël pour amener l'utilisateur à ouvrir sa pièce jointe infectée⁴.

Un autre "vétérain", Netsky-P, qui avait frappé le plus durement en 2004⁵, a régné très longtemps au sommet du Top Ten des virus. Sven Jaschan, un adolescent allemand qui a reconnu avoir écrit les vers Netsky et Sasser, est sorti libre du tribunal avec 30 heures de travaux d'intérêt général et une mise en liberté surveillée⁶. Il est intéressant de noter que la plupart des observateurs s'accordent à penser que l'auteur du ver Sober se trouve en Allemagne et que la peine de Jaschan n'a donc probablement pas été réellement dissuasive.

S'il avait eu plus de temps, le ver Sober-Z aurait dominé le tableau, mais son apparition fin novembre 2005 l'a empêché de prendre la tête du classement. Le ver utilise un certain nombre de déguisements (il se fait notamment passer pour un message provenant d'un enquêteur du FBI ou de la CIA) et accuse le destinataire de visiter des sites web illégaux afin de l'inciter à exécuter la pièce jointe malveillante.

Le ver bilingue Sober-N a émergé pour la première fois en mai. Se faisant passer pour des tickets offerts pour la Coupe du monde 2006 en Allemagne, Sober-N a infecté des milliers de PC dans 40 pays⁷.

Sober-N attendait en silence en tâche de fond des PC infectés, avant de se mettre à niveau vers une version plus récente pour générer une série de spams nationalistes allemands depuis les ordinateurs zombies compromis.

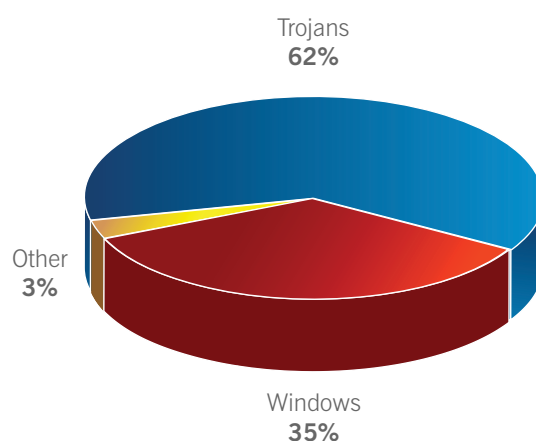


Figure 4 : Types de nouvelles menaces en 2005

Chevaux de Troie

En 2005, il y a eu chaque mois plus de chevaux de Troie écrits que de vers Windows. Comme le montre la Figure 4, les chevaux de Troie représentent en fait près des deux tiers de tous les logiciels malveillants signalés à Sophos.

Ceci vient confirmer que les auteurs de logiciels malveillants se tournent davantage vers des attaques ciblées contre des petits groupes de personnes plutôt qu'un bombardement en masse des utilisateurs Internet.

Il se peut que les criminels Internet abandonnent les attaques à grande échelle parce qu'ils ne souhaitent pas attirer l'attention sur leurs efforts, mais aussi parce qu'ils ne parviennent pas, en pratique, à gérer la quantité de données volées qu'ils reçoivent s'ils ont infecté des centaines de milliers d'ordinateurs en une journée.

Comme il est beaucoup plus simple de dérober de l'argent depuis 200 comptes bancaires que depuis 200 000, les criminels restent mesurés dans leurs attaques et utilisent des chevaux de Troie pour s'assurer qu'ils volent à un petit groupe de personnes faciles à manœuvrer plutôt qu'à un nombre ingérable de victimes inconnues.

A la différence d'un virus et d'un vers, un cheval de Troie ne se réplique pas tout seul. C'est la raison pour laquelle il doit être envoyé en masse sous forme de spam depuis d'autres systèmes. C'est ce à quoi servent principalement les réseaux de zombies (la principale caractéristique de toutes les menaces signalées à Sophos l'an dernier), que nous allons décrire maintenant.

Caractéristiques principales des menaces

Ces douze derniers mois, les cybercriminels ont usé de moyens de plus en plus astucieux pour infecter les ordinateurs et parvenir à leurs fins.

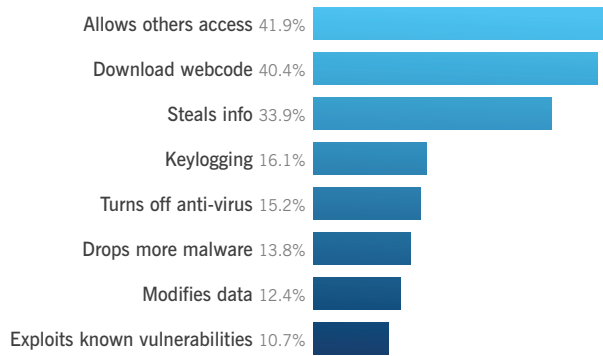


Figure 5 : Principales caractéristiques des menaces

Comme le montre la Figure 5, ils ont, par exemple, dérobé des informations en désactivant le logiciel antivirus d'un ordinateur et en injectant du code malveillant utilisé ensuite pour différentes tâches. Presque aussi dangereux que les zombies, certains codes malveillants téléchargent du code web, ce qui souligne la nécessité d'installer des pare-feu sur les postes de travail et les portables. Etendre la protection à l'ensemble du réseau est indispensable car la plupart des logiciels malveillants présentent plus d'une des caractéristiques ci-dessus.

Zombies

Un ordinateur est transformé en zombie lorsqu'un "bot", ou programme automatisé, y est installé, donnant l'accès à l'ordinateur ainsi que son contrôle au pirate, qui crée ainsi un réseau de zombies, ou botnet. L'un des botnets les plus en vue de l'année a été créé par le ver Zotob qui s'est fait une réputation mondiale en août lorsque des sociétés de médias éminentes⁸, dont ABC, The Financial Times et The New York Times, en ont été victimes. CNN, autre victime du ver Zotob, a été infecté lors d'une émission en direct, perturbant son programme télé et faisant la une de l'actualité.

La plupart des virus du Top Ten signalés à Sophos entre janvier et novembre 2005 pouvaient ouvrir à des tiers l'accès aux ordinateurs infectés, c'est-à-dire créer des zombies.

Les recherches menées par Sophos ont démontré que plus de 60 % de la totalité du spam provient d'ordinateurs piratés, qui sont ensuite utilisés pour commettre un grand nombre de crimes comme le lancement d'attaques par déni de service distribué sur des serveurs web (en utilisant http) ou sur des serveurs de messagerie (en utilisant SMTP). Cette réelle menace à la réputation des entreprises a conduit Sophos à lancer en juillet 2005 son service ZombieAlert™ qui alerte l'entreprise dès que l'un de ses ordinateurs commence à envoyer du spam⁹.

Une grande proportion de logiciels malveillants tente aussi de télécharger du code malicieux depuis le web, ce qui souligne la nécessité de se protéger avec un pare-feu, non seulement à la

périphérie du réseau, mais aussi sur les systèmes d'extrémité et tout particulièrement sur les portables.

Spyware

L'émergence en force des spywares constitue une des principales nouveautés de cette année. Ces programmes - qui s'installent secrètement sur les ordinateurs, enregistrent les frappes au clavier, dérobent des informations et ouvrent les réseaux à d'autres attaques - posent de nouveaux défis aux entreprises. En s'installant sur les ordinateurs de manière furtive, en cachette ou par ingénierie sociale, ils envoient des informations depuis ces systèmes à des tiers sans le consentement ou à l'insu des utilisateurs.

La Figure 6 indique le niveau de menace des spywares en 2005, en pourcentage du nombre total de logiciels malveillants analysés par les SophosLabs™. Leur proportion n'a cessé de croître, passant de 54,2 % en janvier à 66,4 % en novembre.

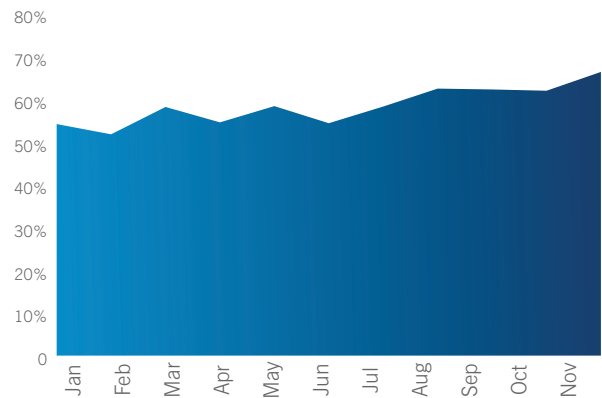
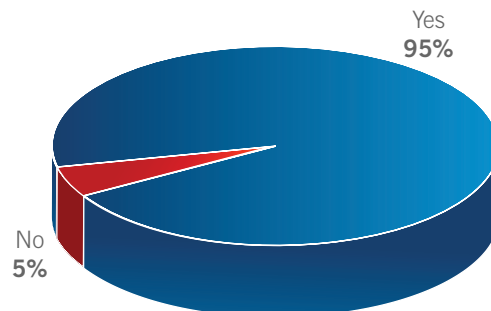


Figure 6 : Proportion des spywares parmi les menaces

Les entreprises prennent de plus en plus conscience du problème des spywares. Parmi celles qui ont répondu au sondage web de Sophos, une majorité écrasante a indiqué souhaiter que leur logiciel antivirus assure une protection simultanée contre le spyware, comme l'indique la Figure 7.



Source : sondage web Sophos

Figure 7 : Personnes interrogées estimant qu'un logiciel antivirus devrait offrir une protection contre les spywares

Au cours de l'année 2006, Sophos prévoit que les éditeurs qui fourniront uniquement une protection antispyware se retrouveront sur un marché de plus en plus concurrentiel, sauf s'ils collaborent avec des éditeurs de solution antivirus. Il est vraisemblable que le marché se consolidera et que certains acteurs offrant seulement une protection contre les spywares ne parviendront pas à conserver leurs parts de marché.

Méthodes de propagation

Les logiciels malveillants utilisent une grande variété de méthodes pour se propager. Il est assez habituel d'observer des combinaisons de virus et de vers selon différentes techniques pour augmenter la diffusion et les probabilités d'infection.

La Figure 8 montre les différentes techniques utilisées par les logiciels malveillants pour se propager et le pourcentage des menaces qui les utilisent. Ce tableau ne reflète pas nécessairement le succès de chaque méthode, mais simplement le fait que des auteurs de logiciels malveillants l'intègrent dans leur code. Il n'inclut pas non plus les chevaux de Troie, qui n'ont pas de technique de propagation propre.

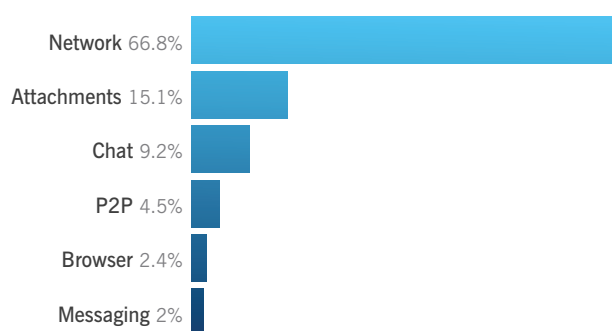


Figure 8 : Méthodes de propagation

Dans les stratégies de protection, l'accent est toujours fortement mis sur le blocage des menaces à la passerelle de messagerie. Cependant, bien qu'étant une part essentielle de toute stratégie de défense, ceci ne procure aucune protection contre les menaces utilisant d'autres voies de communication.

Les entreprises sont aussi vulnérables à un grand nombre d'autres menaces qui ignorent la passerelle. Les vers de réseau représentent une menace interne réelle pour les entreprises, et le contenu malveillant actuel peut tout aussi bien pénétrer dans l'entreprise par l'intermédiaire des navigateurs web, des protocoles de discussion Internet et des applications de messagerie instantanée comme AIM et MSN Messenger.

En outre, la surveillance de chaque CD-ROM, système de stockage USB, carte mémoire, assistant personnel ou lecteur MP3 se connectant aux ordinateurs de l'entreprise, où qu'ils se trouvent, est quasiment impossible. Ce sont pourtant tous des

points d'entrée potentiels de contenus à caractère malveillant, d'où la nécessité de mettre l'accent sur le besoin de protéger aussi bien le poste de travail que tous les autres niveaux de l'infrastructure informatique.

En novembre 2005, ce sujet est brutalement réapparu à l'ordre du jour lorsqu'il s'est avéré que certains CD musicaux Sony introduisaient, via leur dispositif anti-copie, une faille qui était exploitée par un certain nombre de chevaux de Troie¹¹.

La variété des tactiques utilisées par les pirates pour propager le code viral oblige plus que jamais à utiliser des codes de conduite et souligne l'importance d'éduquer les utilisateurs, d'appliquer des politiques de sécurité de l'entreprise, d'utiliser systématiquement des correctifs contre les failles et d'adopter une approche multiniveau pour la protection virale.

Motivations des créateurs de codes malveillants

Autrefois, les motivations de la plupart des auteurs de virus étaient identiques à celles de ceux qui maculent les murs de graffitis. Les auteurs de virus, qui étaient dans en grande majorité des adolescents ou des personnes moralement immatures, écrivaient des programmes malveillants pour flatter leur estime de soi ou impressionner leurs collègues. Certains auteurs de virus laissaient même dans leurs codes des messages ou des indices destinés aux enquêteurs.

Ces virus n'étaient pas inoffensifs (ils utilisaient les ressources du système et posaient des problèmes pour les entreprises et les particuliers) mais ils n'avaient pas d'objectif clair.

Aujourd'hui, de plus en plus de logiciels malveillants sont manifestement conçus pour des motivations financières. Des organisations criminelles s'aperçoivent qu'Internet peut être utilisé de nombreuses façons pour dérober l'argent d'autrui.

Le phishing, le spam, les menaces de chantage par déni de service, les arnaques par courriel, le spyware ou le pharming ont tous pour but de soutirer de l'argent à leurs victimes.

En outre, des industries parallèles ont poussé comme des champignons dans l'écosystème des menaces : par exemple, certains développeurs vendent des logiciels qui aident les spammeurs à coordonner des ordinateurs zombies pour lancer leurs campagnes.

Il y a eu également des cas d'associés travaillant pour des éditeurs de logiciels adwares soupçonnés d'avoir abusé des directives définies par ces société en installant illégalement des adwares sur des milliers d'ordinateurs.

On a même assisté à une recrudescence du nombre de vers et de chevaux de Troie volant les codes d'accès à des participants de jeux MMORPGs (Massively Multiplayer Online Role Playing Games) dans le but de dérober et de vendre des articles virtuels permettant de réaliser des bénéfices bien réels. Même si ces articles n'ont pas d'existence physique, ils peuvent être vendus, et cela a déjà occasionné quelques arrestations¹².

Ce passage au vol de biens virtuels n'est pas très surprenant quand on voit les sommes d'argent échangées pour des articles virtuels dans ces mondes virtuels. Un citoyen de Miami, par exemple, a récemment dépensé 100 000 dollars américains pour acheter une station spatiale virtuelle¹³.

En revanche, la plus grande part des activités criminelles reste dans le domaine des spywares, du phishing et de la fraude Internet. Les cybercriminels partagent leur savoir-faire et travaillent en étroite collaboration pour soutirer de l'argent à des utilisateurs de PC innocents.

Les spammeurs

Le spam à caractère médical (couvrant à l'origine des médicaments pour améliorer les performances sexuelles, suivre un régime ou prendre des hormones de croissance) reste le type de spam le plus répandu. On a même eu droit cette année à des campagnes de spam qui exploitaient les inquiétudes liées à la grippe aviaire en commercialisant en ligne des remèdes censés offrir une protection antivirale¹⁴. Cette catégorie de spam est restée stable tout au long de l'année et n'a pas, comme le montre la Figure 9, augmenté de manière sensible.

Le spam à contenu pornographique a connu une hausse sensible à partir d'août 2005, hausse que l'on peut attribuer à une classification améliorée de cette catégorie de spam par les stations de surveillance Sophos au cours du dernier trimestre de l'année. En matière de prévalence, le spam à caractère

adulte et sexuel est longtemps resté en seconde place derrière la délivrance de médicaments.

Le spam à caractère financier (bourse, actions), lui, a augmenté de façon considérable : il a représenté près de 13,5 % du spam en novembre 2005, contre seulement 0,8 % en début d'année.

Dans les escroqueries à caractère financier ("pump-and-dump") envoyées en masse et constatées cette année, des courriels soutiennent par exemple que certaines entreprises ont mis au point des médicaments efficaces contre la grippe aviaire¹⁵.

Dans le même temps, les catégories des produits et des logiciels ont connu un sérieux déclin. Les spammeurs font de la publicité pour des produits de moins en moins légitimes. A noter également une augmentation au cours de l'année du spam concernant les montres Rolex, bien qu'il soit impossible de savoir s'il s'agissait ou non de marchandises légitimes.

Phishing

L'une des formes les plus lucratives de spamming, le phishing, est aussi un moyen de plus en plus répandu de vol en ligne. Sophos constate de plus en plus de courriels de phishing associés à PayPal, mais aussi eBay et Amazon. Des institutions financières éminentes apparaissent elles aussi régulièrement.

Il suffit d'amener un petit nombre de destinataires à cliquer sur un lien menant vers un site Web falsifié pour que l'escroquerie soit rentable.

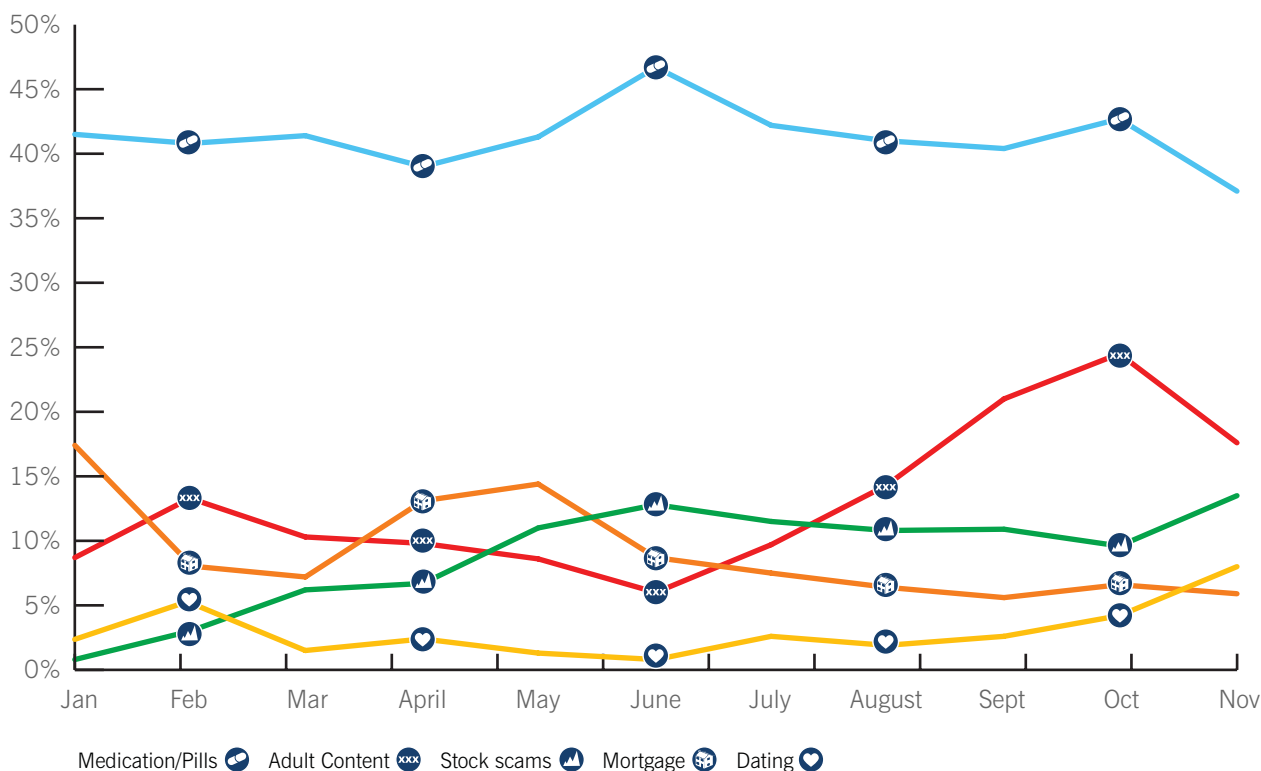


Figure 9 : Catégories de spam

Certaines escroqueries par phishing sont particulièrement retorses. Par exemple, en août 2005, des phishers se sont fait passer pour une vieille dame en fauteuil roulant cherchant un article sur eBay, afin de profiter des bons samaritains¹⁶.

La toute dernière technique dans ce domaine s'appelle le "spear phishing". Il s'agit d'une campagne de phishing ciblant délibérément un petit groupe d'utilisateurs, par exemple les employés d'une entreprise donnée, dans le but d'accéder sans autorisation à des données confidentielles. En utilisant une tactique d'ingénierie sociale et en falsifiant l'adresse électronique utilisée dans ce type d'attaque pour qu'elle semble provenir d'un individu connu du destinataire, les occasions de réussir ces méfaits sont démultipliées.

Escroqueries

On a recensé près de 419 escroqueries connues (comme Advanced Fee Fraud ou Letters from Nigeria) qui continuent de se propager au milieu du spam normal. Ces douze derniers mois, Sophos a intercepté un grande variété d'escroqueries de messagerie envoyées en masse à un grand nombre de gens. On trouvait parmi ces derniers les courriels prétendant provenir de victimes de la catastrophe du tsunami dans l'Océan Indien¹⁷, de parents présumés d'un homme tué pendant les attaques terroristes à Londres en 2005¹⁸ et même d'une fausse loterie du club de football de Liverpool¹⁹.

Les douze principaux pays émetteurs de spam

La Figure 10 révèle les principaux pays d'origine des systèmes émetteurs de spam. Les Etats-Unis restent en tête, mais relaient une part du spam mondial bien moindre qu'en 2004²⁰. Sophos a établi que plus de 60 % du spam est désormais généré par des zombies, c'est-à-dire des ordinateurs piratés infectés par du code malveillant.

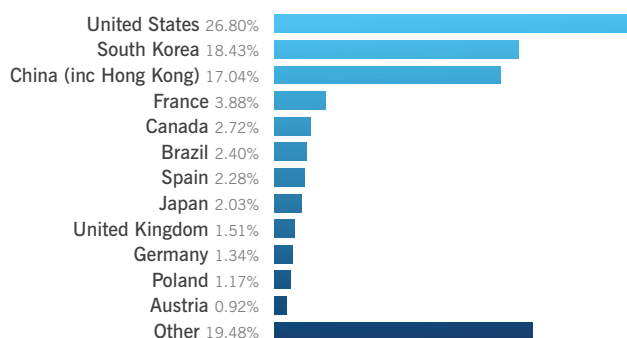


Figure 10 : Les douze principaux pays émetteurs de spam

Cette technique signifie qu'il n'est pas nécessaire que les coupables se trouvent dans le même pays que les ordinateurs innocents utilisés pour envoyer leur spam. Alors que les Etats-Unis, la Corée du Sud et la Chine sont à l'origine de plus de 50 % du spam, les USA et le Canada ont fait d'énormes efforts

2006 et au-delà

Spyware et adware

Le spyware semble promis à une augmentation en 2006 et on constate l'émergence de pirates commençant à utiliser des zombies pour installer sur le réseau des adwares et des programmes potentiellement indésirables. Si l'adware n'est pas toujours illégal, son statut légal est détourné et exploité pour générer des recettes²¹. La menace des spywares et des adwares continuant de croître, il est vraisemblable qu'en 2006 les entreprises recherchent des solutions intégrées avec gestion centralisée plutôt que de logiciels d'utilisation domestique.

Aucune fin en vue pour le spam

Le 24 janvier 2004, Bill Gates prévoyait que, d'ici deux ans, le spam ne serait plus qu'un mauvais souvenir²². Pourtant, le 24 janvier 2006 approche, et les rumeurs sur la fin du spam semblaient sérieusement exagérées. Malgré l'augmentation des mesures prises contre les spammeurs et l'amélioration constante des logiciels antispam, la menace reste bien présente.

Les H-IPS (Host Intrusion Prevention Systems)

Les H-IPS couvrent un grand nombre d'approches sécuritaires comme le confinement comportemental et l'inspection des applications, mais aussi des approches plus traditionnelles comme la protection virale et la mise en place de pare-feu personnel. Sophos estime que les utilisateurs ont intérêt à sérieusement considérer le type de protection dont ils ont besoin pour protéger leurs entreprises, plutôt que de se précipiter sur un produit qui promet de résoudre tous les problèmes de sécurité.

Virus de téléphones mobiles

Bien qu'une augmentation du nombre de virus pour téléphones mobiles ait été constatée, ce nombre reste insignifiant²³ par rapport au nombre beaucoup plus important de virus ciblant les postes de travail Windows. Les auteurs de virus, décidés à voler de l'argent et des ressources aux utilisateurs d'Internet, trouvent l'agression des ordinateurs Windows facile et rentable. D'après un sondage web réalisé par Sophos, 70 % des entreprises pensent que certains distributeurs antivirus font une promotion excessive de la menace virale sur les téléphones mobiles.

Microsoft

Il est vraisemblable que le projet de Microsoft de commercialiser des logiciels antivirus pour les particuliers affecte les éditeurs de sécurité qui protègent les utilisateurs à domicile. Ce sera toutefois pour Microsoft un défi considérable de se faire accepter comme éditeur de sécurité crédible auprès des entreprises. D'après un sondage Sophos effectué après l'irruption du ver Zotob, 35 % des personnes interrogées ont estimé que Microsoft était responsable, le ver ayant exploité une faille de sécurité critique dans le code Windows²⁴.

Il est aussi possible qu'à l'avenir, nombre de virus soient créés pour détériorer spécifiquement le produit antivirus de Microsoft, comme ce fut le cas pour ses produits antispyware et pare-feu²⁵.

Auteurs de code malveillant

Les auteurs de virus continueront d'utiliser d'autres méthodes pour gagner de l'argent avec leurs codes malveillants, que ce soit par le vol d'informations confidentielles, l'utilisation d'ordinateurs exploités sous la forme d'usines à spam²⁶ ou pour les attaques par déni de service distribué (DDoS)²⁷ ou la pose d'adwares sur les PC infectés. De plus en plus, il faudra s'attendre à une diminution de l'impact des vers de messagerie traditionnels, et à une augmentation de l'utilisation de chevaux de Troie dans les attaques ciblées²⁸.

Exploitation des failles

Bien que Microsoft continue à voir ses failles exploitées par des auteurs de codes malveillants, nous risquons d'assister à une augmentation des attaques profitant des failles de sécurité d'autres produits très utilisés (outils du bureautique, navigateurs web alternatifs, logiciels de passerelle de messagerie, etc).

Zombies

Comme de plus en plus d'utilisateurs particuliers passent à Windows XP SP2 et bénéficient de sa sécurité améliorée (pare-feu de base, téléchargement automatique de correctifs de sécurité), les pirates ne peuvent plus seulement compter sur les vers Internet pour s'engouffrer sur les ordinateurs et les compromettre. Désormais, ils vont utiliser l'ingénierie sociale pour pénétrer dans les systèmes et désactiver la protection de l'intérieur, permettant ainsi le téléchargement d'un composant zombie.

pour réduire leur contribution au problème. Grâce à un certain nombre d'initiatives (peines de prison infligées aux spammeurs, législation plus ferme et meilleure sécurité des systèmes) la chute du pourcentage de spam envoyé depuis les ordinateurs d'Amérique du Nord a été sensible.

Des efforts, tels que l'initiative des FAI pour offrir leurs services afin d'agir sévèrement contre les spammeurs ou encore l'application par les autorités de la législation CAN-SPAM, ont aidé l'Amérique du Nord à maîtriser les spammeurs basés sur leur territoire. Certains des plus prolifiques spammeurs ont ainsi été obligés d'abandonner leur activité ou de partir à l'étranger.

L'arrivée de Windows XP SP2 en 2004, offrant une sécurité améliorée, a également aidé à protéger les particuliers contre le piratage informatique.

Il est évident maintenant qu'il ne faut plus considérer Boca Raton en Floride comme la capitale mondiale du spam et que la Russie est aujourd'hui un havre pour nombre de spammeurs. Malheureusement, quel que soit l'endroit où il se trouve, le spammeur peut exploiter toutes les connexions ADSL mal sécurisées du monde pour envoyer ses messages indésirables.

Un besoin de protection

Les ordinateurs insuffisamment protégés sont assaillis plus rapidement que jamais. Profitant des failles logicielles, le code malveillant peut se propager sans intervention humaine. Des vers Internet comme Zotob utilisent des failles présentes dans le système d'exploitation Windows, infectant potentiellement des centaines de milliers d'ordinateurs dans le monde. De plus en plus, le pirate crée du code malveillant avant que l'utilisateur n'ait pu appliquer le correctif de sécurité Microsoft ou même, parfois, avant qu'un correctif ne soit publié.

Microsoft a publié 29 correctifs indispensables entre janvier et novembre 2005, soit une moyenne de 2,4 par mois, ainsi que de nombreux autres correctifs essentiels à la sécurité.

Les recherches menées par Sophos ont montré que le risque d'infection par un ver lorsqu'on connecte à Internet un ordinateur sous Windows XP (sans SP2) non protégé et sans correctifs était d'environ 40 % après environ 10 minutes, atteignant 94 % après 60 minutes (voir la Figure 11). Dans beaucoup de cas, cela ne laisse même pas suffisamment de temps pour télécharger et installer les correctifs de sécurité ou un pare-feu. Les ordinateurs doivent donc être protégés avant d'être mis en ligne.

La bonne nouvelle est qu'un système utilisant Windows XP SP2 et convenablement protégé avec les correctifs adaptés bénéficie d'une protection beaucoup plus solide contre les vers Internet, réduisant ainsi de façon drastique la possibilité de pénétration de votre PC par l'un d'entre eux. Malheureusement, il se crée de plus en plus de codes malveillants qui, s'ils arrivent sur le bureau de l'utilisateur via un téléchargement web ou une pièce

jointe à un courriel, désactivent instantanément la sécurité de Windows XP SP2 pour autoriser l'entrée de menaces externes.

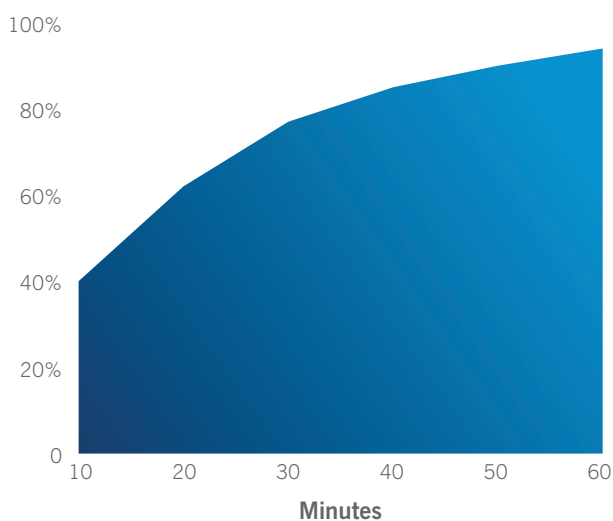


Figure 11 : Risque d'infection par un ver Internet si l'ordinateur n'est pas protégé

Les cinq plus importantes menaces véhiculées par Internet entraînant ces infections apparaissent dans la Figure 12.

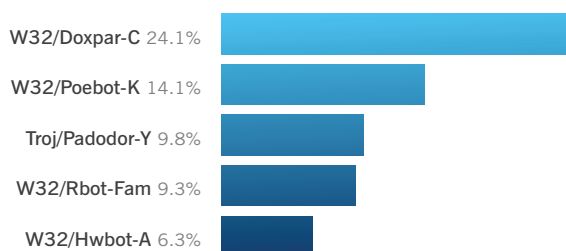


Figure 12 : Top des menaces véhiculées par Internet

Le danger des vers Internet est qu'ils ne nécessitent aucune intervention de l'utilisateur. Il n'est pas nécessaire que l'utilisateur visite un site Web ou ouvre un courriel pour être infecté. Il suffit de relier un ordinateur non protégé à Internet pour mettre le PC en danger.

L'infection est silencieuse et invisible. L'utilisateur ne sait pas que son ordinateur a été compromis et qu'il est susceptible de transmettre des infections à d'autres utilisateurs du net, d'être espionné ou d'envoyer du spam au nom de pirates.

Conclusion

La quantité croissante des nouvelles menaces, leur vitesse de diffusion et la tâche complexe d'assurer la protection des réseaux contre ces menaces vont avoir des implications fortes pour les entreprises en 2006.

La combinaison des techniques de diffusion et l'action à plusieurs niveaux de nombreuses menaces signifie que les entreprises vont s'adresser de plus en plus à des éditeurs disposant d'une expertise complète et de solutions consolidées pour protéger leurs systèmes, leurs données et la continuité de leurs services.

Sophos est l'un des plus grands éditeurs mondiaux de solutions de gestion intégrée des menaces pour les entreprises, le secteur public et l'enseignement. Fiables et simples à utiliser, nos produits protègent plus de 35 millions d'utilisateurs dans plus de 150 pays. Nos 20 ans d'expérience, la combinaison d'un savoir-faire antivirus et antispam développé en interne et notre réseau mondial de centres d'analyse des menaces, nous permettent de répondre rapidement à l'émergence des menaces, quelle que soit leur complexité, et d'atteindre le plus haut niveau de satisfaction clients du marché.

SOPHOS
WWW.SOPHOS.COM

Références

- 1 IDC - Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc, Nov 2005
 - 2 Sober-Z worm poses as bogus email from FBI or CIA
www.sophos.com/pressoffice/news/articles/2005/11/soberfbi.html
 - 3 Genotype technology defends against Mytob mass attack, Sophos reports on multitude of worms
www.sophos.com/pressoffice/news/articles/2005/04/va_mytobmultitude.html
 - 4 Latest Zafi worm spreading in the wild as email Christmas greeting
www.sophos.com/pressoffice/news/articles/2004/12/va_zafid.html
 - 5 War of the worms: Netsky-P tops list of year's worst virus outbreaks
www.sophos.com/pressoffice/news/articles/2004/12/pr_uk_20041208yeartopten.html
 - 6 Sasser worm writer walks free from court, Sophos comments on conviction of Sven Jaschan
www.sophos.com/pressoffice/news/articles/2005/07/va_sasserfree.html
 - 7 Sober-N worm seen in over 40 countries, shows no sign of disappearing
www.sophos.com/pressoffice/news/articles/2005/05/va_sobern2.html
 - 8 Breaking news: worm attacks CNN, ABC, The Financial Times, and The New York Times
www.sophos.com/pressoffice/news/articles/2005/08/va_breakingnews.html
 - 9 Sophos ZombieAlert Service identifies spammer-controlled computers on business networks
www.sophos.com/pressoffice/news/articles/2005/07/pr_uk_20050713zombiealert.html
 - 10 95% say anti-virus software should also stop spyware
www.sophos.com/pressoffice/news/articles/2005/07/va_pollspyav.html
 - 11 Un cheval de Troie exploite une vulnérabilité de DRM, la protection anti-copie de CD de Sony
www.sophos.fr/pressoffice/news/articles/2005/11/stinx.html
 - 12 Suspected gang who stole from online game players arrested in Korea
www.sophos.com/pressoffice/news/articles/2005/07/va_krarrests.html

Trojan steals usernames and passwords for fantasy role-playing game
www.sophos.com/pressoffice/news/articles/2005/01/va_legmiry.html
 - 13 Man spends \$100,000 on virtual space station in online game
www.informationweek.com/story/showArticle.jhtml?articleID=173601281
 - 14 Sophos issues health warning after spammers peddle drugs to combat bird flu
www.sophos.com/pressoffice/news/articles/2005/10/sa_tamifluspam.html
 - 15 Spammers sell drugs and pump stocks on back of bird flu fears
www.sophos.com/pressoffice/news/articles/2005/10/sa_tamifluspam.html
 - 16 Selon Sophos, les phishers utilisent une vieille dame en chaise roulante pour cibler les bons samaritains d'eBay
www.sophos.fr/pressoffice/news/articles/2005/08/sa_samaritan.html
 - 17 Sophos hoax description: Letter from tsunami victim
www.sophos.fr/virusinfo/hoaxes/tsunami.html
 - 18 Sick 419 scammers use name of London bombing victim in attempt to steal money
www.sophos.com/pressoffice/news/articles/2005/08/sa_419bombscam.html
 - 19 Bogus Liverpool Football Club emails aim to steal money from the unwary
www.sophos.com/pressoffice/news/articles/2005/11/liverpoolfc.html
 - 20 The «Dirty Dozen» 2004: Sophos reveals the top spamming countries
www.sophos.com/pressoffice/news/articles/2004/12/sa_dirtydozenyear.html
-

-
- 21 FBI arrests 20-year-old suspected zombie king
www.sophos.com/pressoffice/news/articles/2005/11/ancheta.html
 - 22 Gates forecasts victory over spam
news.bbc.co.uk/1/hi/business/3426367.stm
 - 23 Customers unlikely to encounter Mibir mobile phone worm
www.sophos.com/pressoffice/news/articles/2005/04/va_mibir.html
 - 24 PC users point the finger at Microsoft over latest virus outbreak
www.sophos.com/pressoffice/news/articles/2005/08/va_zotobpoll.html
 - 25 First Trojan to attack Microsoft anti-spyware product discovered
www.sophos.com/pressoffice/news/articles/2005/02/va_bankash.html
 - 26 Spammer Sober-Q Trojan horse stopped proactively by Sophos Genotype technology
www.sophos.com/pressoffice/news/articles/2005/05/va_soberq.html
 - 27 Suspected zombie kings who ran botnet of 100,000 PCs arrested
www.sophos.com/pressoffice/news/articles/2005/10/va_dutchbotarrests.html
 - 28 Des pirates s'attaquent aux infrastructures gouvernementales et industrielles du Royaume Uni
www.sophos.fr/pressoffice/news/articles/2005/06/va_niscc.html
-