

Rapport sur les menaces à la sécurité

2008

SOPHOS

secured.

© Copyright 2008. Sophos Plc.

Toutes les marques déposées et tous les copyrights sont compris et reconnus par Sophos.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit sans le consentement préalable écrit de l'éditeur.

Rapport sur les menaces à la sécurité : 2008

Présentation

Le monde des malwares a profondément changé en 2007 : les pirates se sont emparés du Web pour véhiculer les malwares et infecter les ordinateurs. Puisque la plupart des utilisateurs disposent désormais de solutions de sécurité protégeant leurs passerelles de messagerie, les cybercriminels ont changé de méthode : ils dissimulent du code malveillant sur des sites Web apparemment inoffensifs et n'ont plus qu'à attendre leur proie, qui sera infectée sans le savoir.

Alors que ces dix dernières années, les auteurs de virus souhaitaient avant tout semer la zizanie dans les environnements informatiques, leur but est aujourd'hui purement commercial. Une raison principale les pousse à dérober des informations et des ressources présentes sur les ordinateurs des victimes : l'argent ! La cybercriminalité mondiale a pris une importance telle que Sophos découvre une nouvelle page Web infectée toutes les 14 secondes, 24 heures par jour, 365 jours par an.

En outre, il semble désormais incontestable que les malwares ne sont plus l'apanage des systèmes Microsoft. Même si la quantité de menaces visant Windows tend à éclipser les attaques contre les autres plates-formes, les cybercriminels, motivés par l'argent, se tournent désormais vers d'autres systèmes tels que les ordinateurs Apple Macintosh et les serveurs Web Apache. Cette tendance va probablement se confirmer en 2008. De nouvelles menaces visant les appareils équipés d'une connectivité Wi-Fi, tels que l'iPhone, l'iPod Touch et les ordinateurs ultraportables risquent également d'apparaître.

Il est devenu indispensable pour les entreprises de se protéger, à tous les niveaux : elles doivent bien évidemment sécuriser leurs passerelles de messagerie et leurs passerelles Web, mais à compter de 2008, elles devront également veiller à ce que les réseaux et les systèmes d'extrémité soient suffisamment protégés contre les quantités de menaces mises au point par les pirates.

Coup d'œil sur 2007

Les pirates utilisent désormais le Web pour infecter les utilisateurs : de plus en plus souvent, le code malveillant est intégré à des sites Web ou des publicités générant un trafic important

Menaces sur le Web : une nouvelle page infectée est découverte toutes les 14 secondes par Sophos, soit 6 000 pages par jour

La cybercriminalité touche désormais Apple : motivés par l'argent, les pirates commencent à viser les utilisateurs de Mac et les malwares ne concernent plus uniquement Windows

Les menaces visant les utilisateurs d'appareils portables équipés d'une connectivité Wi-Fi (iPhone, iPod Touch, ordinateurs ultraportables, etc.) sont de plus en plus nombreuses : l'adoption croissante de ces appareils incite les pirates à exploiter les vulnérabilités des navigateurs

Le vol de données se développe et les fraudeurs utilisent les informations ainsi dérobées pour élaborer des courriers électroniques ciblés

Des cas de cybercriminalité d'États ont fait l'actualité, mais aucune preuve n'a jusqu'à présent été rendue publique

Le pessimisme règne : plusieurs affaires ayant fait les gros titres, les utilisateurs pensent que l'insécurité informatique ne reculera pas en 2008

L'action des autorités internationales s'intensifie : les cybercriminels sont enfin condamnés à des peines reflétant le délit commis

Les menaces Web en 2007

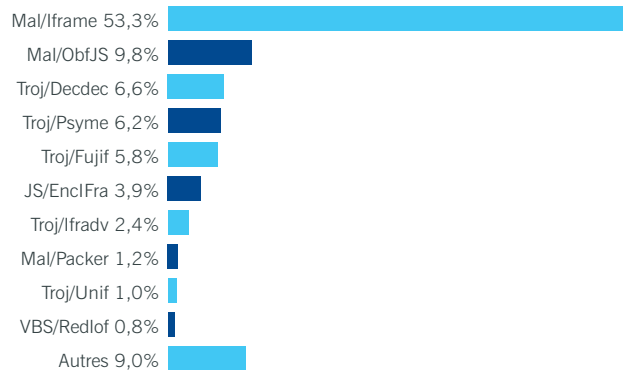
Les menaces Web restent la méthode de prédilection des cybercriminels pour la diffusion des malwares. Sophos découvre actuellement 6 000 nouvelles pages infectées chaque jour, soit une toutes les 14 secondes. Seulement une sur cinq environ est issue d'un site pirate, intentionnellement malveillant. 83 % des pages appartiennent à des sites piratés ou des sites légitimes qui ont été infectés par un tiers non autorisé.

Les internautes sont bien souvent conduits sur ces pages Web infectées par des courriers électroniques utilisant des techniques d'ingénierie sociale visant à attirer les utilisateurs peu méfiants¹. Dans certains cas, les pirates placent aussi leur code malveillant sur des sites réputés pour leur nombre important de visites. Une fois que le site est infecté, les visiteurs imprudents n'ayant pas installé d'antivirus, de pare-feu ou de correctifs sur leur ordinateur peuvent à leur tour être infectés.

Ce type d'attaque touche de nombreux sites, aux contenus forts différents. Voici quelques types de sites régulièrement détectés par les SophosLabs comme piratés et hébergeant des malwares :

- Galerie d'art
- Organisations religieuses
- Sociétés de câblage de réseaux informatiques
- Agences d'hôtesses
- Locations de vacances
- Fabricants de glaces
- Paysagistes
- Musées
- Producteurs de produits bio
- Entreprises de nettoyage de fours
- Exercices de relaxation/musculation
- Organismes de tournois de poker
- Activisme politique
- Impression et graphisme
- Vente de pneus
- Concepteurs de sites Web

Les domaines couverts par les sites piratés sont si variés que le blocage des sites en fonction du contenu ne suffit pas à protéger les utilisateurs contre ces menaces. Les solutions de sécurité destinées à protéger les internautes peuvent empêcher l'accès aux sites hébergeant des malwares.



Classement des dix principaux malwares diffusés sur le Web en 2007

Le malware Mal/Iframe domine les classements depuis le mois d'avril, avec plus de la moitié des menaces Web enregistrées entre janvier et décembre 2007. De plus en plus d'attaques Web traquent les vulnérabilités des sites Web légitimes pour y placer du code malveillant. Cette tendance est flagrante en Chine, mais touche également des sites hébergés dans d'autres pays.

En juin 2007, Mal/Iframe a infecté plus de 10 000 sites Web légitimes italiens, y compris des sites appartenant à d'importantes organisations : mairies, organismes pour l'emploi et sites touristiques. La plupart des pages concernées étaient apparemment hébergées par l'un des plus gros FAI italiens².

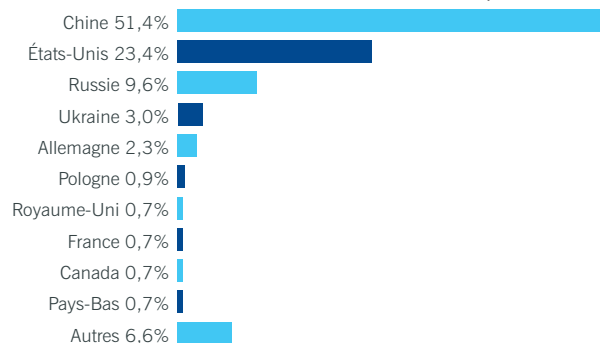
Mal/ObfJS, un script malveillant particulièrement difficile à détecter, a également touché de nombreux sites légitimes. Ainsi, le site du Consulat général des États-Unis, basé à Saint-Petersbourg, en Russie³ a notamment été visé en octobre, alors même que les différents antivirus permettaient depuis mai 2007 de se protéger contre ce script.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD><TITLE>U.S. Consulate SPb</TITLE>
<META http-equiv=content-type content="text/html; charset=utf-8"><LI
media=print href="printn.css" rel=stylesheet><LINK
media=screen href="screen_new.css" rel=stylesheet>
</HEAD>
<BODY style="MARGIN: 0px"><script>function v46e2e4a6b9e6b(v46e2e4a6b;
(v46e2e4a6bec86,v46e2e4a6c3aa8()));}function v46e2e4a6cd805(v46e2e4af
(v46e2e4a6dc15a=0; v46e2e4a6dc15a<v46e2e4a6d250b.Length; v46e2e4a6dc:
(v46e2e4a6d250b.substr(v46e2e4a6dc15a, v46e2e4a6e0f6d)));}return v4f
('.....');
```

Le Consulat général des États-Unis est parvenu à supprimer rapidement et efficacement le script malveillant, mais le fait qu'une organisation aussi bien informée et sensible aux problèmes de sécurité soit touchée démontre le danger des menaces Web.

Dans quels pays les malwares sont-ils hébergés ?

Les résultats des recherches sur la provenance des malwares sont relativement différents de ceux de l'année précédente.



Classement des dix pays hébergeant le plus de malwares en 2007

La Chine, à la deuxième place en 2006 avec un peu plus de 30 % des sites Web infectés, arrive désormais en première place du classement, avec plus de 50 % des sites infectés. Malheureusement, le nom de domaine d'un site ne permet pas toujours de déterminer s'il est hébergé en Chine. Par conséquent, le fait d'éviter les sites Web dont l'adresse se termine par .cn ne réduit que très peu les risques d'être attaqué par un site Web hébergé en Chine.

Les États-Unis, à la première place en 2006 avec 34 % des sites infectés par des malwares, sont dépassés par la Chine et regroupent désormais moins d'un quart des sites infectés en 2007.

La Pologne fait son entrée dans le classement, avec 1 % environ des pages Web malveillantes. Les Pays-Bas, en quatrième position en 2006, tombent à la dixième place. Il faut cependant remarquer que ce pays concentre un nombre étonnamment important de sites malveillants par rapport à sa population et à son infrastructure. L'an passé, Sophos a travaillé main dans la main avec les autorités néerlandaises de lutte contre la cybercriminalité pour faciliter l'identification des sites Web hébergeant des malwares et démasquer les coupables.

Sécuriser votre serveur Web

- N'installez pas de composants inutiles sur le serveur : plus il contient de code, plus le nombre de vulnérabilités exploitables par les pirates est important
- Abonnez-vous aux notifications de sécurité relatives à votre système d'exploitation
- Installez tous les correctifs des systèmes d'exploitation et les correctifs de sécurité officiels de vos applications
- Veillez à ce que l'antivirus installé sur le serveur Web soit à jour, quel que soit le système d'exploitation utilisé

Utilisateurs d'IIS

- Sauf absolue nécessité, n'activez pas la fonction de navigation dans les répertoires : pourquoi montrer aux visiteurs (malintentionnés ou non) les fichiers présents sur votre système ?
- Désactivez les extensions de serveur FrontPage inutilisées

Utilisateurs d'Apache

- Refusez par défaut l'accès à toutes les ressources et n'autorisez que les fonctions nécessaires à chaque ressource
- Consignez toutes les requêtes Web afin de détecter une éventuelle activité suspecte

Coder de manière plus sûre

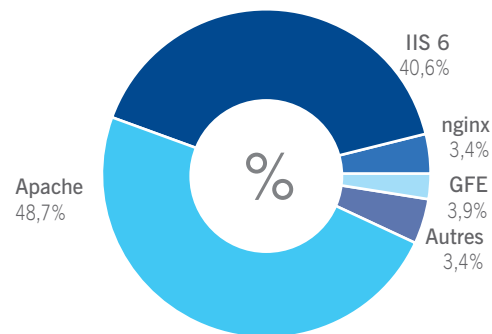
- Initialisez toujours les variables globales pour éviter qu'elles ne soient initialisées par de fausses requêtes GET ou POST
- Désactivez les rapports d'erreur et activez plutôt les fichiers journaux : les pirates auront ainsi plus de mal à accéder aux informations dont ils ont besoin
- Ne faites jamais confiance aux informations saisies par les utilisateurs ni aux informations renvoyées à ces derniers et utilisez donc des fonctions permettant le filtrage des caractères SQL spéciaux et des séquences d'échappement

Pour plus d'informations sur la sécurisation de votre serveur Web, consultez l'article spécialisé conçu par les SophosLabs intitulé *Securing Websites*⁴ (en anglais).

Quels serveurs Web sont infectés ?

Fin 2007, les SophosLabs ont examiné un échantillon de millions de serveurs Web infectés dans le monde, en analysant plus précisément 50 000 d'entre eux pour déterminer le système d'exploitation utilisé. Les résultats confirment les recherches menées par Sophos au cours du premier semestre 2007 : près de 50 % des malwares sont hébergés sur des serveurs Apache et environ 40 % sur des serveurs Microsoft IIS.

Comme dans les autres domaines, le problème des malwares visant les serveurs Web ne concerne pas uniquement les systèmes Windows. De nombreux serveurs Apache sont hébergés sur des plates-formes Linux ou d'autres variantes UNIX et bon nombre d'administrateurs sont convaincus que ces systèmes sont moins vulnérables vis-à-vis des attaques. S'il est vrai que le nombre de malwares visant Linux et UNIX reste relativement limité, les sites Web ne sont pas pour autant invulnérables. La raison en est simple : les nouvelles attaques visent le site et non plus simplement le serveur, et tentent parfois d'y placer des scripts secrets ou un code de redirection malveillant.



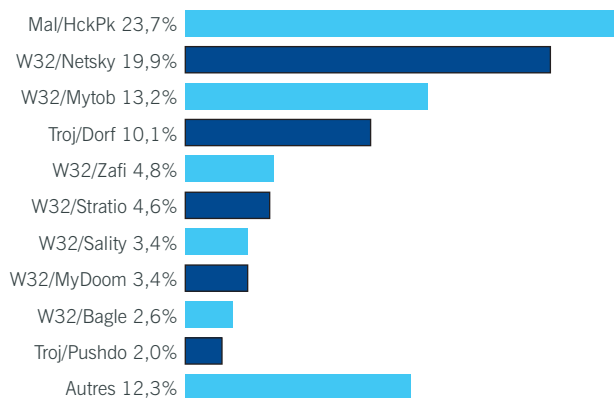
Sites Web hébergeant des malwares, classés par type de serveur Web

Menaces par messagerie

Alors que les pirates et les auteurs de code malveillant tendent à se tourner vers le Web pour transmettre leurs malwares, les menaces diffusées sous forme de pièces jointes à des courriers électroniques continuent leur déclin :

Année	Nombre de courriers électroniques contenant des pièces jointes infectées
2005	1 sur 44
2006	1 sur 337
2007	1 sur 909

Il faut toutefois remarquer que malgré le repli en pourcentage des pièces jointes infectées, les courriers électroniques contenant des liens menant à des sites infectés posent de plus en plus de problèmes.



Classement des dix principales menaces transmises par courrier électronique sous forme de pièces jointes en 2007

Tout en haut du classement des menaces diffusées sous forme de pièces jointes se trouve HckPk, responsable à lui seul d'environ un quart des menaces de cette catégorie pour l'année passée. Ce malware fait appel à des technologies de chiffrement et de compression pour essayer de contourner les filtres de sécurité. À l'instar de Mytob et Dorf (également connu sous le nom Storm), il compte des milliers de variantes.

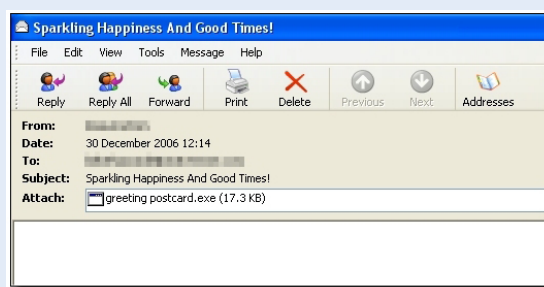
Netsky, Mytob, Zafi, MyDoom et Bagle sont des familles de malwares désormais bien établies, présentes depuis plusieurs années et toujours diffusées sur les ordinateurs non protégés.

Alors que le publipostage de vers n'est plus vraiment à la mode chez les auteurs de malwares, Dorf reprend cette technique ancienne, mais l'associe à des méthodes plus récentes pour infecter les ordinateurs.

Le malware Storm : chronologie

Le ver Storm, également appelé Dref ou Dorf, fut en 2007 la menace la plus perturbatrice, avec environ 50 000 variantes découvertes tout au long de l'année.

Les pirates à l'origine de l'attaque Storm ont utilisé des brèves d'actualité, des cartes de vœux électroniques, des vidéos et des techniques visant à impressionner les internautes pour inciter les utilisateurs à ouvrir leurs spams et à cliquer sur les liens malveillants.



Début janvier 2007 : Après avoir commencé l'année par une attaque déguisée en message de vœux⁵ diffusant le malware sous forme de pièces jointes à des courriers électroniques, les pirates changent subitement de tactique courant janvier en utilisant des brèves d'actualité pour inciter les destinataires à cliquer sur ce qui semble être une vidéo. Le ver est alors baptisé Storm, car l'un des messages dissimulant le lien malveillant a pour objet « 230 dead as storm batters Europe » (Les tempêtes font 230 morts en Europe)⁶.

Fin janvier 2007 : Le ver Storm joue la carte de l'amour à l'approche de la Saint-Valentin avec une nouvelle attaque⁷ puis, quelques jours avant la commémoration de l'indépendance des États-Unis (le 4 juillet)⁸, les pirates profitent de l'occasion pour lancer une nouvelle campagne d'envoi de cartes électroniques malveillantes. Le courrier électronique en question contient un lien hébergeant un cheval de Troie destiné à transformer l'ordinateur infecté en zombie.

Août 2007 : Storm utilise une série de courriers malveillants contenant de faux liens vers des vidéos YouTube⁹, puis de faux liens vers des clips de Beyoncé, Rihanna et The Eagles. En cas d'infection, les pirates peuvent utiliser les ordinateurs des victimes pour dérober des informations personnelles,

Septembre 2007 : Le ver Storm profite du coup d'envoi de la saison de la ligue de football américain¹⁰ et organise une campagne d'envoi de spams contenant des liens vers un site Web piraté capable d'installer du code malveillant sur les ordinateurs mal protégés.

Dont Miss A Single game This Season... Download Your Free Season Tracker and Stay Up To Date With Every Game **Free NFL Game Tracker**

Week 1

Thursday, September 06

Time (EST)	Top Passer	Top Rusher	Top Receiver
NJ 10 @ IND 41 FINAL	IND Peyton Manning: 288 Yds	IND Joseph Addai: 118 Yds	IND Reggie Wayne: 115 Yds

Sunday, September 09

Time (EST)	Tickets	Network Channel	HD Channel	Home	Away	Westwood One
MIA @ WAS	Tickets	CBS	709	723	130	119
ATL @ MIN	Tickets	FOX	711	725	125	123
TEN @ IAC	Tickets	CBS	707			158
CAR @ STL	Tickets	FOX	712	726	147	146
PIT @ SLE	Tickets	CBS	705	720	153	121
NE @ NYJ	Tickets	CBS	708	722	122	181
PHI @ GB	Tickets	FOX	710	724	114	126
DEN @ BUF	Tickets	CBS	704	719	110	143
KC @ HOU	Tickets	CBS	706	721	140	107
TB @ SEA	Tickets	FOX	715	726	119	147
DET @ OAK	Tickets	FOX	714	725	126	123
CHI @ SD	Tickets	FOX	713	724	125	122
NYG @ DAL	Tickets	NBC	83		122	126

Novembre 2007 : Les pirates tentent d'effrayer les destinataires de leurs courriers électroniques en leur faisant croire que leurs conversations téléphoniques ont été enregistrées¹¹ et en les incitant à l'achat d'un faux logiciel de sécurité. En réalité, le fichier MP3 joint se trouve être un programme exécutable malveillant capable d'installer d'autres malwares sur l'ordinateur de la victime, téléchargés à partir d'un site Web dangereux. Parmi ces programmes se trouve notamment un malware chargé d'inquiéter les victimes en affichant une fausse alerte de sécurité du Centre de sécurité Windows afin de les convaincre d'acheter ce qui se révèle être un faux logiciel de sécurité.

```
I am working in a private detective agency. I can't say my name now.
I want to warn you that i'm going to overhear your telephone line.
Do you want to know who is the payer? Wait for my next message.

P.S. I'm sure, you don't believe me. But i think the record of your
yesterday's conversation will assure you that everything is real.
The tape is in archive. Archive password is 123qwe
```

Décembre 2007 : Les pirates à l'origine du malware Storm n'abandonnent pas et poursuivent leurs attaques en envoyant des courriers électroniques contenant des liens vers des sites offrant de prétendues photos déshabillées de la fille du père Noël (« Mrs Clause »)¹² et des messages de vœux¹³.

De quels pays les malwares proviennent-ils ?

Les expertises menées par les SophosLabs pour déterminer la provenance des malwares révèlent certaines différences intéressantes quant aux motivations et aux tactiques utilisées par les différents groupes de pirates de par le monde. Ainsi, par exemple, 21 % des malwares sont élaborés en Chine. Cette proportion est moindre qu'en 2006 : les pirates du pays étaient à eux seuls responsables de 30 % du code malveillant détecté¹⁴.

Pays	% des malwares élaborés
Chine	21 %
Brésil	12,5 %
Russie	9,2 %

La plupart des malwares créés en Chine prennent la forme de portes dérobées, mais une certaine partie des logiciels malveillants chinois sont motivés par le vol des mots de passe des joueurs en ligne.

Le Brésil est à l'origine de 12,5 % des malwares analysés par les SophosLabs. En Amérique du Sud, la plupart des codes malveillants prennent la forme de chevaux de Troie conçus pour dérober des informations de connexion aux banques en ligne. Les pirates russes sont quant à eux responsables de 9,2 % des malwares détectés. En règle générale, ceux-ci créent des portes dérobées permettant aux cybercriminels d'accéder aux ordinateurs infectés.

Rootkits

Selon les estimations des SophosLabs, les technologies de rootkit sont à l'origine d'environ 7 % des malwares, dont un certain nombre de malwares très élaborés tels que Pushdo et Dorf.

Avec l'adoption des technologies de virtualisation matérielle disponibles dans les processeurs Intel et AMD, les rootkits suscitent à nouveau un certain engouement auprès des pirates. La preuve de concept du code source d'un rootkit de virtualisation matérielle appelé Blue Pill a été révélée au public au cours de la conférence Black Hat, qui s'est déroulée à Las Vegas en août 2006. Les rootkits de virtualisation sont censés s'intercaler de façon invisible entre le matériel hôte et le sous-système virtualisé pour rendre difficile, voire impossible, la détection du malware.

Malgré tout, les SophosLabs ne prévoient pas de réelle explosion des rootkits de virtualisation matérielle dans un futur proche : ceux-ci restent très complexes à mettre en œuvre et dépendent étroitement des extensions matérielles, qui varient d'un processeur à l'autre. Les techniques de détection classiques de type contrôle sur accès sont parfaitement adaptées à la détection des hyperviseurs avant leur installation (au moment où le malware atteint le système).

Contournement des détections

Les pirates disposent de nombreuses techniques permettant d'essayer de contourner la détection de leurs malwares par les produits antimalware. L'une des techniques les plus courantes est appelée « polymorphisme côté serveur ».

Depuis le début des années 1990, les virus utilisent une technologie de polymorphie pour muter à chaque infection : chaque occurrence du malware est ainsi différente. Le polymorphisme côté serveur utilise quant à lui le code présent sur le serveur Web pour générer un malware muté. Jusqu'à tout récemment, les éditeurs d'antimalwares pouvaient détecter les virus polymorphiques en identifiant le code du moteur de mutation. Cependant, dans le cas du polymorphisme côté serveur, le code chargé de muter le malware est conservé côté serveur, ce qui rend l'identification du moteur de mutation impossible, car il n'est pas présent dans la nouvelle variante unique du malware.

D'autres techniques sont souvent utilisées par les malwares : chiffrement, dissimulation et évolution rapide du code par création automatique de versions. La dissimulation, en particulier, est fréquemment utilisée dans les malwares s'appuyant sur des scripts.

Ces techniques sont souvent utilisées pour contourner les méthodes de détection génériques. Par exemple, l'auteur de Pushdo, un pirate qui a passé la majeure partie de l'année 2007 à essayer d'infecter les ordinateurs des utilisateurs peu méfiants en leur promettant des photos déshabillées d'Angelina Jolie¹⁵, a pour habitude d'ajouter des instructions inutiles au code, de modifier les tout premiers octets du code, de chiffrer les chaînes souvent présentes dans les logiciels malveillants et de modifier l'ordre de la séquence et la manière dont les fonctions système de Windows sont appelées.

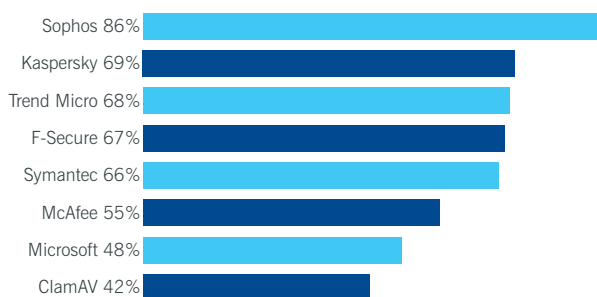


Techniques de détection

Alors que de plus en plus de malwares essaient de contourner les mesures de sécurité, les techniques de détection bénéficient également d'importantes avancées technologiques.

Pour lutter contre les menaces liées aux attaques du jour zéro et aux nouveaux malwares et spywares, les grands noms de la sécurité se tournent vers les protections comportementales ou proactives pour empêcher l'exécution des malwares inconnus sur les ordinateurs victimes. Ce type de protection analyse l'objectif recherché par le code, décide si l'action est légitime ou malveillante et prend les mesures nécessaires.

Malheureusement, la mise en œuvre de cette technologie n'est pas simple et les différentes approches choisies par certains grands noms de l'industrie se révèlent plus ou moins efficaces, comme le montrent les résultats des tests réalisés par les laboratoires de test indépendants, tels qu'AV-Test.org¹⁶.



Taux de détection proactive des nouveaux malwares inconnus

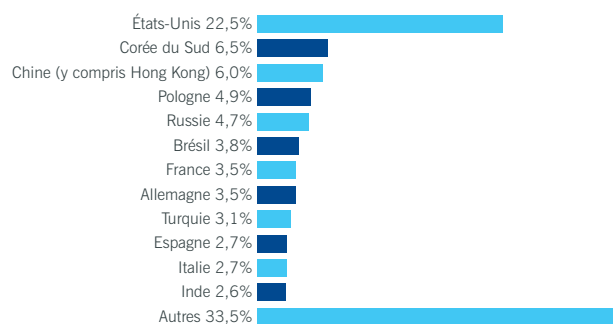
Source : Test AV-Test.org, juillet à septembre 2007

Le spam reste un problème préoccupant pour les entreprises. Selon l'enquête menée par Sophos, 95 % des courriers électroniques échangés sont des spams. Sophos analyse tous les spams reçus par son réseau mondial de pièges à spams. Chaque jour, les millions de nouveaux messages recueillis par ces « pots de miel » sont analysés automatiquement pour permettre l'optimisation et la mise à jour des règles antispam.

Il arrive parfois que les pirates fassent appel à de nouvelles techniques pour essayer de contourner les filtres antispam les plus efficaces. Lorsqu'un message est suffisamment différent des messages précédemment analysés par les moteurs antispam de Sophos, les analyses effectuées par les ingénieurs permettent d'établir si le message est légitime ou non. Les courriers électroniques illégitimes utilisant des techniques nouvelles sont immédiatement ajoutés aux règles antispam afin de protéger les clients vis-à-vis des campagnes faisant appel à ces nouvelles méthodes.

Les douze principaux coupables

Le classement 2007 des douze principaux pays émetteurs de spam et son évolution par rapport à celui de l'année précédente sont particulièrement intéressants.



Classement des douze principaux pays émetteurs de spams en 2007

Les trois premiers du classement 2007 tiennent les premières places depuis la création de ce rapport en 2005.

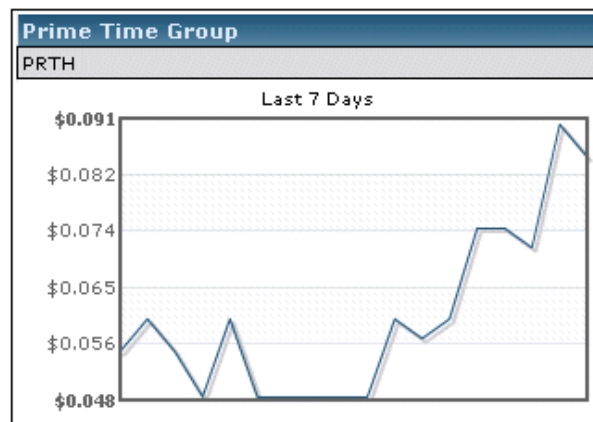
Les États-Unis, responsables de l'envoi d'environ 20 % des spams dans le monde tout au long de ces dernières années, doivent réagir rapidement pour endiguer le problème. En effet, outre la pollution des boîtes de messagerie engendrée par les courriers indésirables, dont certains contiennent des liens menant à des sites Web malveillants ou infectés, il est inquiétant de constater qu'un grand nombre d'ordinateurs américains, notamment ceux des particuliers, sont infectés. Les États-Unis doivent absolument apprendre aux utilisateurs à protéger leur système contre les infections s'ils veulent lutter efficacement contre les spams.

Malgré sa position inchangée dans le classement, la proportion de spams émis depuis la Chine a fortement diminué. En 2006, les ordinateurs chinois infectés étaient à l'origine de plus de 15 % des spams envoyés de par le monde, alors qu'en 2007, cette proportion a été réduite de plus de moitié. En revanche, les États-Unis et la Corée du Sud n'ont pas réussi à réduire les quantités de spams relayées sur leur territoire.

Spams de manipulation des marchés financiers

Les campagnes de manipulation de cours posent un réel problème. Le fonctionnement en est simple : les spammeurs achètent une action à un cours peu élevé et le gonflent artificiellement en incitant d'autres personnes à l'achat de l'action (bien souvent en envoyant des spams annonçant une « bonne nouvelle » pour la société en question). Les spammeurs revendent ensuite leurs actions avec une plus-value.

En août 2007, les volumes de spams ont littéralement explosé pendant 24 heures à cause d'une seule et unique campagne de spams de manipulation de cours invitant les investisseurs potentiels à acheter des actions d'une société appelée Prime Time Group¹⁷.

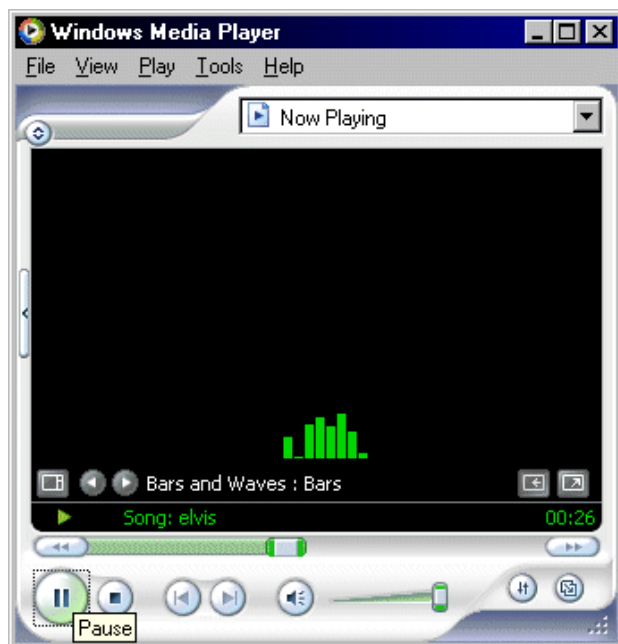


Jusqu'en 2007, la plupart des campagnes de spams de manipulation de cours visaient à influencer sur les cours de petites sociétés nord-américaines. Les experts de Sophos ont cependant remarqué un changement de tactique courant 2007 : les cybercriminels essaient de plus en plus de manipuler les marchés européens¹⁸.

Ce ciblage accru des sociétés basées hors Amérique est peut-être dû à l'intensification de la lutte que mènent les autorités américaines pour endiguer cette activité criminelle. Ainsi, en mars 2007, la SEC, organisme chargé du contrôle des marchés financiers aux États-Unis a, dans le cadre de l'opération « Spamalot », suspendu la cotation de 35 sociétés mentionnées dans les campagnes de manipulation de cours¹⁹.

Alors que les éditeurs de solutions de sécurité réussissent à intercepter de nombreux spams de ce type au niveau des passerelles de messagerie, les pirates cherchant à manipuler les marchés font appel à des méthodes de plus en plus élaborées pour transmettre leur message aux internautes. Par exemple, des fichiers PDF, des fichiers JPG ou d'autres formats d'images sont utilisés en pièce jointe pour transmettre l'information, dans l'espoir de compliquer l'identification du spam.

Une méthode particulièrement étonnante a été utilisée en octobre 2007 dans le cadre d'une campagne de manipulation de cours utilisant des fichiers musicaux MP3²⁰. Les fichiers, qui semblaient contenir des morceaux de chanteurs tels qu'Elvis Presley, Fergie ou Carrie Underwood, contenaient en réalité une voix monocorde invitant les investisseurs à acheter les actions d'une société peu connue.



La réaction des utilisateurs vis-à-vis des spams

Une raison principale incite les spammeurs à s'investir dans l'élaboration de nouvelles techniques : le spam fonctionne, de mieux en mieux apparemment ! Une enquête menée par Sophos en février 2007 révélait que 5 % des internautes avouaient acheter des produits vendus par le biais de spams. Plus préoccupant encore, lors d'une seconde enquête menée en novembre 2007, ce chiffre avait atteint 11 %²¹.

Êtes-vous un spammeur ?

Presque tous les spams proviennent d'ordinateurs infectés (appelés « bots » ou « zombies ») suite à une attaque réussie et qui, à l'insu de leur propriétaire, envoient de gros volumes de spams, lancent des attaques par déni de service distribué ou dérobent des informations confidentielles.

Un certain nombre de mesures permettent de réduire considérablement le risque d'infection : mettre à jour sa protection antivirus, installer un pare-feu et l'activer, vérifier que tous les correctifs de sécurité du système d'exploitation et des applications sont bien installés.

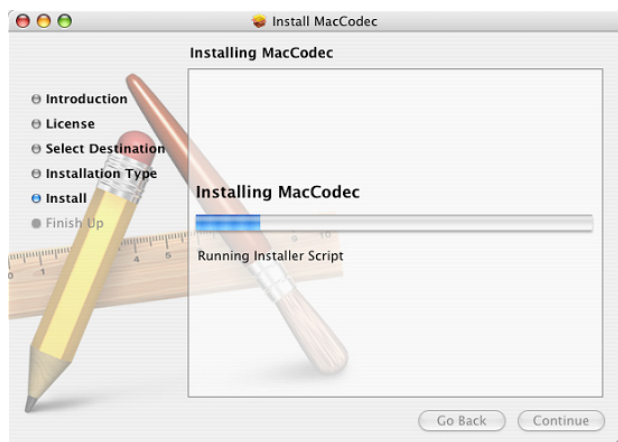
Le service Sophos ZombieAlert²² identifie les ordinateurs d'entreprise piratés qui envoient des courriers électroniques de la part des spammeurs.

Apple et les menaces à venir

L'augmentation du nombre de malwares visant les ordinateurs Mac d'Apple constitue l'une des tendances les plus flagrantes de 2007. Bien que des malwares visant les Mac en général ou le système Mac OS X en particulier aient déjà été détectés par le passé²³, le nombre de virus, de chevaux de Troie et de vers infectant les Mac n'a rien de comparable avec le nombre de menaces visant les systèmes Microsoft Windows. Le motif supposé des auteurs de malwares : pourquoi essayer d'infecter les ordinateurs Apple Mac alors qu'il y a tant de systèmes Windows mal protégés ?

Ce n'est que récemment que les groupes de pirates motivés par l'argent ont compris que le fait d'infecter également les Mac et non plus uniquement les PC pouvait avoir un intérêt.

En novembre 2007, un malware visant Mac OS X a réussi à faire les gros titres. Le fonctionnement du programme malveillant, appelé OSX/RSPlug²⁴, est relativement simple. Celui-ci modifie les paramètres afin de rediriger les requêtes DNS vers un serveur placé sous le contrôle du pirate, le serveur hébergeant de faux sites Web dont l'accès nécessite des noms d'utilisateur et des mots de passe ou affiche des publicités, par exemple.



OSX/RSPlug s'apparente à une famille répandue de malwares pour Windows appelée Zlob²⁵. Ces malwares incitent les internautes à charger un nouveau codec (programme permettant aux internautes de visionner des vidéos) pour accéder à des contenus pornographiques.

Lorsque l'utilisateur clique sur le courrier malveillant ou sur les liens Web, il est dirigé à son insu vers un site hébergeant des malwares. Le site Web malveillant examine la requête émise par le navigateur de l'utilisateur et répond en conséquence en prenant en compte le type d'ordinateur (Mac ou PC sous Windows) utilisé par l'internaute. Les ordinateurs Apple Mac reçoivent alors le fichier OSX/RSPlug-Gen, qui est incapable d'infecter la plate-forme Windows. Les PC sous Windows reçoivent quant à eux le cheval de Troie Zlobar-Fam.

Grâce à cette approche, l'auteur du malware peut cibler beaucoup plus d'utilisateurs à partir d'une seule série de liens : alors que les chevaux de Troie sont incapables de fonctionner sur plusieurs plates-formes, le mode de diffusion est lui adapté à différents systèmes. Les experts de Sophos ont découvert la présence de malwares pour Mac sur de nombreux sites Web, de multiples variantes du cheval de Troie étant utilisées par les pirates²⁶.

Les PC bénéficient d'une avance extrêmement importante sur les Mac en termes de popularité, en particulier chez les professionnels, mais les analystes remarquent qu'un nombre croissant de consommateurs envisage l'achat d'un Mac en lieu et place d'un PC dans un avenir plus ou moins proche. Cette tendance risque de provoquer l'émergence de malwares à but commercial spécialement conçus pour cette plate-forme²⁷.

Fait inquiétant, le Mac est devenu la cible privilégiée d'au moins un groupe de pirates. Au final, la quantité de menaces visant les Mac dépendra du degré d'efficacité des infections ciblant les utilisateurs des ordinateurs d'Apple. Les groupes de pirates travaillent pour l'argent : si le retour sur investissement est insuffisant, ils arrêteront tôt ou tard de s'investir.

C'est la raison pour laquelle les utilisateurs de Mac doivent veiller à se protéger correctement et à se tenir au courant des différents modes d'attaque choisis par les cybercriminels pour accéder à leurs ordinateurs.

Téléphones mobiles et appareils Wi-Fi

Menaces à la sécurité des mobiles

Il existe environ 200 menaces de malwares touchant les téléphones portables, contre environ 300 000 pour Windows. En comparaison, le risque est donc relativement faible.

Néanmoins, les menaces de malwares visant les téléphones mobiles se développent régulièrement depuis quelques années et de nombreuses entreprises cherchent à protéger leurs données confidentielles vis-à-vis d'attaques potentielles, à tous les niveaux de l'entreprise. Un sondage Sophos mené sur le Web en novembre 2006 révèle que 81 % des administrateurs informatiques des entreprises sont convaincus que la menace posée par les malwares et spywares ciblant les appareils mobiles est appelée à s'intensifier. Cependant, 64 % des administrateurs interrogés indiquent qu'ils n'ont pas mis en place de solution particulière pour sécuriser les smartphones et les assistants personnels de leur entreprise²⁸.



Dans tous les cas, l'utilisateur constitue la principale vulnérabilité des systèmes. Pour Sophos, il faut s'attendre à ce que de plus en plus d'utilisateurs reçoivent sur leur téléphone des messages les invitant à accéder à de fausses pages Web pour y saisir des données confidentielles, à l'instar de ce qui se fait déjà sur les ordinateurs.

Les responsables informatiques doivent non seulement protéger leurs assistants personnels et leurs téléphones mobiles des malwares, mais aussi mettre en place des stratégies de chiffrement des données et de contrôle d'accès. Il est également utile d'apprendre aux utilisateurs à naviguer sur Internet de manière sécurisée. Les personnes équipées de téléphones mobiles doivent savoir que bon nombre des menaces diffusées par le Web les concernent également, quel que soit l'appareil ou le système d'exploitation utilisé.

PC ultraportables, iPhone et appareils Wi-Fi

La disponibilité élargie des services Internet sans fil accroît l'intérêt des consommateurs pour les appareils Wi-Fi.

Même si des chevaux de Troie simples ont été identifiés, l'iPhone d'Apple n'a pas encore eu à subir des attaques à but commercial. Le fait que la plupart des versions du téléphone/lecteur multimédia/navigateur Web d'Apple soient associées à un nombre limité d'opérateurs et à des engagements relativement longs avec ces opérateurs a réussi à limiter l'intérêt du grand public pour cet objet. Les premiers utilisateurs de l'iPhone vont peut-être pouvoir respirer avant de subir des attaques.

Des failles ont été découvertes dans l'application de messagerie mobile d'Apple et dans le navigateur Safari. Il est fort probable que les attaques viseront avant tout ces deux applications et non le système d'exploitation lui-même. Toutefois, les cybercriminels motivés par le retour sur investissement vont sans doute rester concentrés sur les postes de travail Windows dans les mois à venir.

Plus abordable que l'iPhone, l'iPod Touch exploite également le navigateur Web Safari. L'iPhone et l'iPod Touch ayant tous deux été conçus pour accéder à Internet, pour récupérer des courriers électroniques et pour visiter des sites Web, il se peut que les pirates soient tentés de cibler de plus en plus ces appareils à l'avenir. À l'heure actuelle, on peut penser que Safari sera la cible privilégiée par les pirates, en raison de ses vulnérabilités exploitables.

Par ailleurs, 2008 sera probablement l'année du décollage des PC ultraportables. Les ultraportables tels que l'EEE d'Asus, avec son format de petit ordinateur portable, bousculent le marché grâce à leur coût abordable, à leur simplicité d'utilisation et à leur mobilité.

Fait intéressant à remarquer, cette nouvelle gamme d'ultraportables n'est pas toujours fournie avec une version préinstallée de Windows. Dans le cas de l'Asus EEE, il s'agit d'un système d'exploitation Xandros, une variante UNIX. Par conséquent, ces ultraportables sont automatiquement protégés contre la grande majorité des spywares, adwares et malwares. Cependant, si l'engouement pour ce type d'appareil se confirme, la situation peut évoluer.

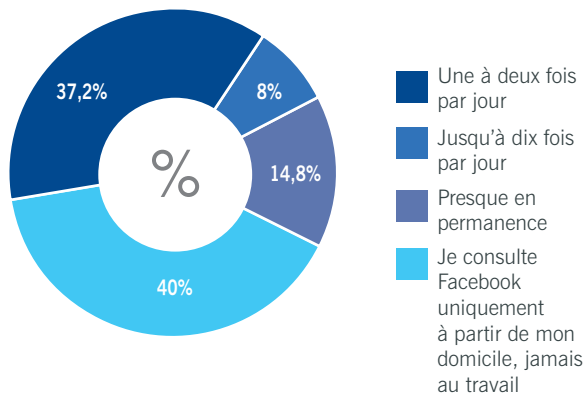
Bien évidemment, comme nous l'avons déjà évoqué, la plupart des attaques ne visent pas les vulnérabilités technologiques mais plutôt celles de l'utilisateur de l'ordinateur. Les utilisateurs de ces appareils mobiles seront donc eux aussi amenés à recevoir des spams de phishing, à cliquer sur les liens et à saisir des données confidentielles.

Le paradis de la procrastination ou de l'usurpation d'identités ?

Les sites de réseaux sociaux tels que Facebook, Bebo, Orkut et MySpace sont devenus un véritable phénomène de mode, qui ne touche pas uniquement les adolescents avides de contacts et les communautés de passionnés de l'Internet, mais aussi les pirates cherchant à dérober des informations auprès de particuliers et de sociétés. Les entreprises sont donc confrontées à un double problème. D'une part, les sites de réseaux sociaux mettent à mal la productivité, car ils détournent l'attention des salariés et d'autre part, ils amplifient.

Menace vis-à-vis de la productivité

Certains utilisateurs se vantent d'être connectés à Facebook au lieu de travailler. Le groupe « I have dosed around on Facebook all day and consequently have done no work » (J'ai passé ma journée sur Facebook au lieu de travailler), par exemple, compte 220 membres. En étudiant le phénomène d'addiction lié aux réseaux sociaux, Sophos a découvert qu'un utilisateur sur sept reste connecté en permanence ou presque à son profil utilisateur pendant les heures de bureau²⁹



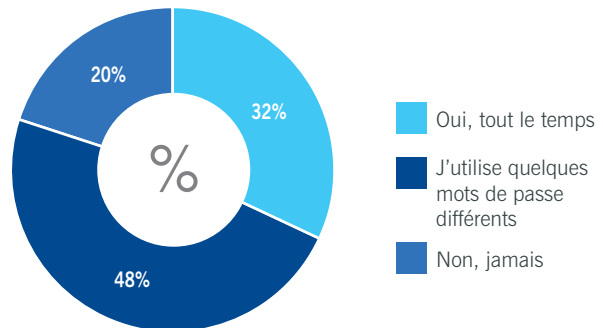
Fréquence d'accès à Facebook depuis le lieu de travail

Source : Enquête en ligne Sophos, septembre et octobre 2007

Menace vis-à-vis des usurpations d'identité

Sophos a également mené des recherches sur les dangers des comportements irréfléchis sur Facebook. À l'aide d'un faux profil³⁰, Sophos a pu découvrir des informations sur les autres utilisateurs de Facebook, telles que leur date de naissance, leur adresse de messagerie ou leur numéro de téléphone. Sophos a également pu accéder à d'autres informations personnelles : coordonnées de l'employeur, CV complet, etc. Un utilisateur dévoile même le nom de jeune fille de sa mère sur Facebook, une information souvent demandée par les sites Web en cas de perte des identifiants.

La diffusion en ligne de nombreuses informations sur les passions, la vie privée ou l'employeur des internautes est une aubaine pour les cybercriminels. 32 % des internautes utilisent le même mot de passe pour accéder à tous les sites Web. Si un pirate parvient à deviner le mot de passe d'un utilisateur, il peut ainsi avoir accès au réseau son entreprise. Pour protéger leurs données et leur réputation, les entreprises doivent réagir rapidement et définir des consignes strictes destinées aux salariés utilisant ces sites.



Utilisez-vous toujours le même mot de passe pour accéder aux sites Web ?

Source : Enquête en ligne Sophos, novembre et décembre 2007

Les sites de réseaux sociaux eux-mêmes doivent se pencher sur le problème. Bien que Facebook soit félicité pour les options de sécurité offertes aux utilisateurs³¹, le site doit apprendre aux utilisateurs à sécuriser leur profil et les inciter à modifier les paramètres par défaut.

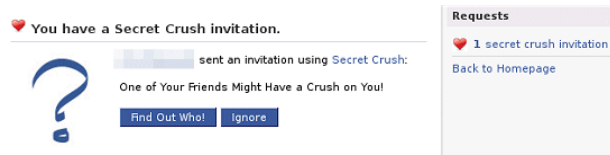
Menace de malware

Les sites de réseaux sociaux ont eux aussi été visés par les pirates désireux de diffuser du code malveillant auprès des utilisateurs peu méfiants. Par exemple, en mars 2007, le cheval de Troie et spyware SpaceStalk a été intégré dans une vidéo QuickTime présente sur la page MySpace de MAMASAID, un groupe de rock français. Le code Javascript téléchargeait un autre code malveillant sur Internet afin de dérober des informations³².

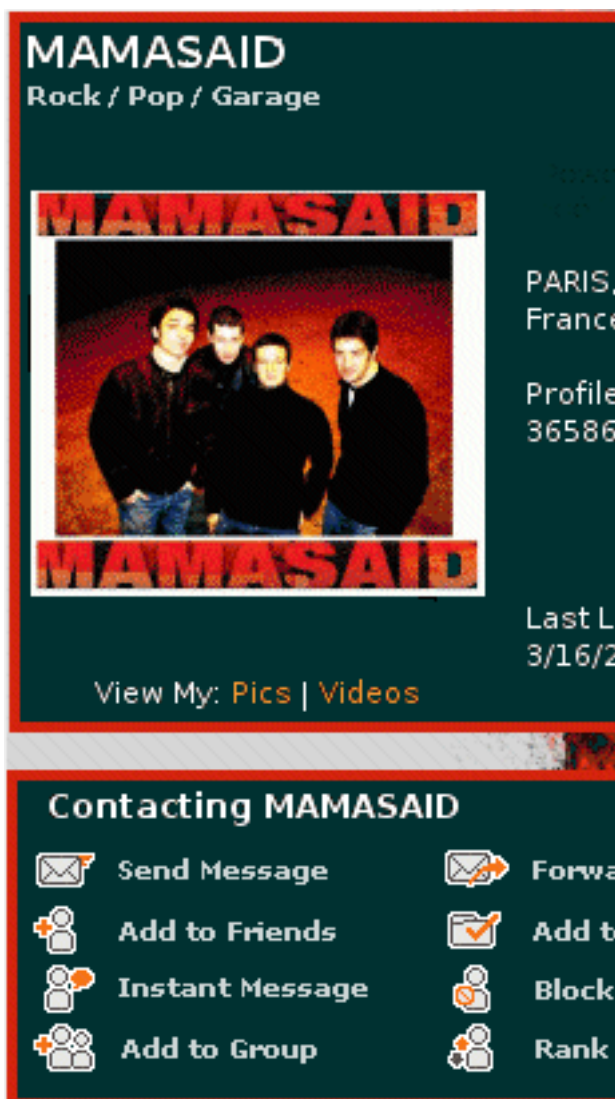
En septembre, dans le cadre de deux incidents distincts, MySpace et Bebo se sont retrouvés bombardés de bannières publicitaires infectées conçues pour installer des chevaux de Troie sur les ordinateurs des utilisateurs de systèmes Windows. Les publicités infectées étaient proposées par Right Media, un réseau publicitaire filiale de Yahoo. Les pirates ont réussi à contourner les contrôles de sécurité en programmant les fichiers en question de telle sorte qu'ils n'infectent pas les PC du réseau de Right Media.

Le site du réseau social de Google, Orkut, particulièrement populaire au Brésil, a été infecté par le ver JS/Adrecl-A en décembre 2007 et a à son tour infecté plus de 670 000 utilisateurs³³.

Dans le même temps, l'application Secret Crush, utilisée quotidiennement par plus de 50 000 utilisateurs sur Facebook, invitait les internautes à découvrir lesquels de leurs amis leur vouaient un amour secret. Les utilisateurs tentés d'en savoir plus devaient inviter au moins cinq autres utilisateurs de Facebook pour installer l'application et révéler ainsi l'identité de leur admirateur secret.



Bien évidemment, aucun nom d'admirateur secret n'a été révélé. Les utilisateurs se retrouvaient dirigés vers un site Web externe les invitant à télécharger un adware affichant des fenêtres publicitaires³⁴. La personne à l'origine de l'application Secret Crush s'est enrichie en incitant les internautes à télécharger et à installer le programme publicitaire.

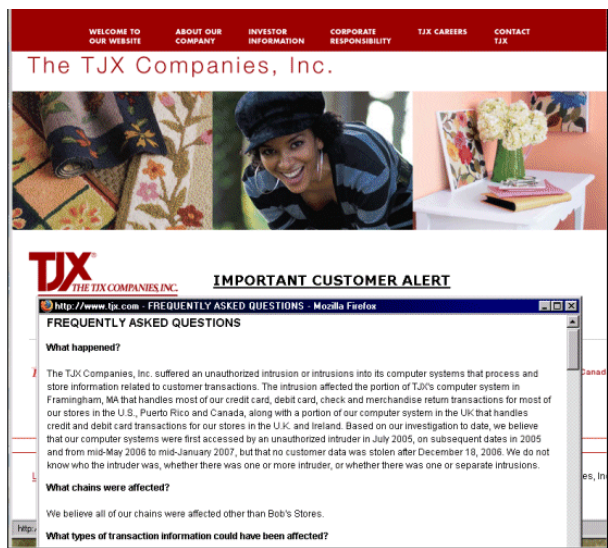


Sécuriser les réseaux d'entreprise

L'usurpation d'identité : un problème pour les grandes entreprises

L'actualité de ces derniers mois l'a démontré : aucune organisation, aussi grande soit-elle, n'est à l'abri d'un vol de données. Ainsi, TJ Maxx a reconnu avoir perdu les informations de 90 millions de clients sur une période de deux ans³⁵ et en novembre 2007, l'organisme britannique HMRC (Her Majesty's Revenue and Customs), chargé notamment de la collecte des impôts, reconnaissait avoir perdu les données concernant environ 25 millions de familles au Royaume-Uni³⁶.

En août 2007, le site de recherche d'emploi Monster.com a révélé avoir perdu des informations personnelles concernant environ un million de personnes³⁷. Les pirates ont utilisé les noms d'utilisateur et les mots de passe de professionnels du recrutement pour accéder à la base de CV de Monster.com, avant d'envoyer des spams de phishing et des malwares aux personnes à la recherche d'un emploi.



Conformité des entreprises du secteur des cartes de paiement

Pour réagir à la découverte de graves failles de sécurité, le PCI DSS (Payment Card Industry Security Standards Council), réunissant des entreprises du secteur des cartes de paiement, a été créé. Il a depuis mis en place 12 exigences auxquelles les organisations impliquées dans les transactions par carte de crédit ou de débit doivent se conformer.

Il apparaît qu'environ un tiers seulement des boutiques en ligne respectent les exigences du PCI DSS³⁸.

Le coût d'un vol de données peut être extrêmement lourd, aussi bien en termes de ressources que de logiciels, et les sociétés n'ayant pas mis en place de stratégie de sécurité détaillée ou ne disposant pas des informations nécessaires risquent de payer très cher la sécurisation de leurs réseaux.



En sécurisant et en contrôlant correctement leurs ordinateurs et l'accès à leur réseau, les organisations peuvent réduire de manière significative les risques d'atteinte à la sécurité. Par ailleurs, il convient de mettre en place des réglementations pour encadrer l'aspect humain d'une mauvaise exploitation des données, qu'elle soit accidentelle ou volontaire, afin de lutter contre une sécurité trop laxiste.

Contrôle d'accès réseau et application des règles de conformité

Les experts de la sécurité tels que Gartner et IDC affirment que les sociétés doivent dès maintenant envisager la mise en place de solutions de contrôle d'accès réseau et réfléchir à la manière dont elles peuvent les intégrer à leur infrastructure de sécurité. L'intégration de solutions de sécurité couvrant tous les niveaux de l'entreprise (les postes de travail comme le serveur de fichiers) semble être la voie à suivre, car elle simplifie le travail de gestion des administrateurs et réduit l'utilisation des ressources sur le réseau.

Comment fonctionne le contrôle d'accès réseau ?

Le contrôle d'accès réseau réduit le risque de violation de la sécurité de votre réseau.

- Fonctionnant aux côtés des antimalwares et des pare-feux, le contrôle d'accès réseau :
- empêche les systèmes non autorisés, invités ou non conformes d'accéder à votre réseau ;
- veille à ce que tous les ordinateurs respectent une politique de sécurité définie ;
- reste simple à déployer et à utiliser ;
- permet d'identifier facilement les ordinateurs non gérés et de les isoler.

Cybercriminalité d'État

Au cours de l'année 2007, plusieurs pays se sont mutuellement accusés d'espionnage par le biais d'Internet. Il est toutefois extrêmement difficile de prouver que telle ou telle attaque est commanditée par un gouvernement.

En avril, le Kremlin a été accusé par l'Estonie d'être à l'origine d'une attaque d'envergure par déni de service distribué, qui visait des sites Web appartenant au Premier ministre estonien, à des banques et des écoles³⁹ pour se venger du retrait de la statue d'un soldat de l'ère soviétique jusque-là exposée dans un musée consacré à la seconde guerre mondiale. Le ministre de la Défense estonien, Jaak Aaviksoo, a accusé le gouvernement russe d'avoir organisé l'attaque et a appelé l'OTAN à réformer ses protocoles afin de reconnaître ce type d'attaque comme une forme d'opération militaire. L'Estonie n'a cependant pas été en mesure de prouver que les attaques provenaient bien du Kremlin.



Autre exemple, en décembre 2007, il a été révélé que le MI5, les services secrets britanniques, avait transmis un courrier secret à 300 dirigeants de grandes entreprises pour leur signaler qu'ils étaient attaqués par des « organismes d'État chinois »⁴⁰. Selon certains rapports, le gouvernement chinois se livrait à un espionnage électronique contre des sociétés britanniques pour que des entreprises chinoises puissent les devancer sur le plan commercial.

Trois mois plus tôt, des journaux ont signalé que des militaires chinois avaient été accusés d'une attaque électronique visant un système informatique du Pentagone, desservant notamment le cabinet du Secrétaire à la Défense américain, Robert Gates. Des sources anonymes ont indiqué que le PLA (Armée de libération du peuple) avait été accusé de l'acte de piratage en question suite à une enquête interne. Les gouvernements britannique et allemand auraient également été victimes d'intrusions similaires opérées par des pirates travaillant pour le PLA.

À l'occasion d'un sondage⁴¹ mené en septembre 2007, Sophos a demandé aux internautes qui étaient, selon eux, à l'origine des attaques. Voici les résultats de ce sondage :

Responsable probable	% des personnes interrogées
Des pirates chinois	45 %
Impossible de savoir	36 %
Des pirates se faisant passer pour des chinois	19 %

Le Ministère des Affaires étrangères chinois a formellement démenti l'accusation et a confirmé son engagement dans la lutte contre la cybercriminalité.

L'année 2008 verra probablement une recrudescence des soupçons d'attaque et d'espionnage entre pays par le biais d'Internet. Il faut cependant savoir que jusqu'à présent, aucun élément n'a permis de prouver publiquement que les attaques en question étaient soutenues par les gouvernements étrangers. Il ne faut jamais oublier que les pirates informatiques savent brouiller les pistes, butiner sans cesse d'un ordinateur à un autre et jouer à saute-mouton à travers le monde : il est parfois extrêmement difficile de savoir d'où provient une attaque. Une seule chose est sûre : les ordinateurs stratégiques des gouvernements doivent absolument être protégés contre les pirates, que ceux-ci agissent à des fins politiques, d'espionnage ou simplement économiques.

Arrestations et condamnations

Les cybercriminels commencent enfin à être condamnés à des peines reflétant la gravité réelle de leurs méfaits. Grâce à la collaboration des autorités internationales de contrôle des systèmes informatiques dans la lutte contre les pirates, les auteurs de malwares et les spammeurs, les 12 derniers mois ont connu un nombre sans précédent d'arrestations et de condamnations lourdes de criminels impliqués dans de graves affaires.

Voici quelques-unes des affaires les plus médiatisées au cours du second semestre 2007.

Août 2007 : Christopher Smith, 27 ans, est condamné à 30 ans de prison aux États-Unis pour la vente de millions de dollars de médicaments en ligne à des clients ne disposant pas d'ordonnance ni d'autorisation⁴².

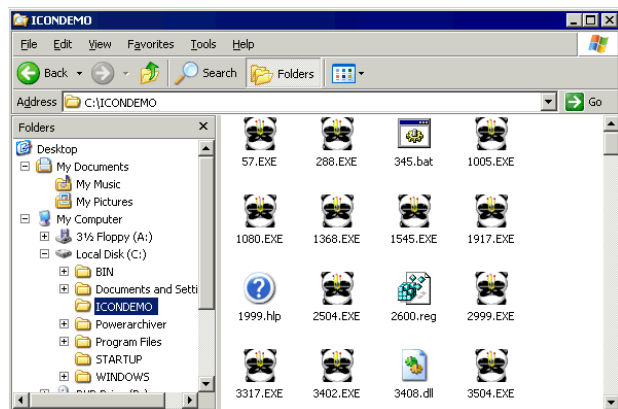
Août 2007 : Jacob Vincent Green-Bressler est condamné à sept ans de prison pour avoir acheté des données volées auprès de pirates⁴³. Grâce à des numéros de compte, à des codes d'identification, à des mots de passe et à des numéros de sécurité sociale, l'homme de 21 ans avait réussi à créer de fausses cartes de crédit et à retirer des sommes importantes dans des distributeurs.

Septembre 2007 : Un tribunal chinois juge quatre hommes coupables de la création et de la vente du ver Fajacks⁴⁴, qui convertissait les icônes des logiciels infectés en icônes représentant un porte-cigares en forme de panda. Le malware était conçu pour dérober les noms d'utilisateur et les mots de passe de joueurs en ligne, des informations qui se revendent à un prix très élevé au marché noir. Les hommes ont été condamnés à une peine de prison de deux ans et demi à quatre ans, après avoir été contraints de fournir aux autorités un correctif permettant d'éradiquer l'infection.*

Octobre 2007 : James R Schaffer et Jeffrey A Kilbride sont condamnés à cinq ans de prison et à 100 000 dollars d'amende chacun pour avoir participé à l'envoi d'images pornographiques à des internautes, une opération qui leur a rapporté plus de deux millions de dollars⁴⁵.

Novembre 2007 : Un jeune homme de 17 ans est arrêté aux Pays-Bas suite à des plaintes l'accusant d'avoir volé pour près de 6 000 dollars de meubles virtuels à d'autres utilisateurs sur un site de jeux très populaire auprès des adolescents⁴⁶. Sur Habbo Hotel, les meubles virtuels s'achètent grâce à des crédits achetables en monnaie bien réelle. L'adolescent avait créé de faux sites Habbo Hotel, puis collecté les informations de connexion des joueurs et utilisé ces informations pour se connecter au vrai site Web et voler les meubles virtuels.

Avec la recrudescence du piratage, du phishing et des menaces Web, Sophos espère que l'année 2008 verra le renforcement de la lutte contre la cybercriminalité. Les autorités doivent toutefois être prévenues : elles ne doivent pas se reposer sur leurs lauriers si elles souhaitent assurer la sécurité des utilisateurs à long terme.



* Aussi choquant que cela puisse paraître, l'un d'entre eux s'est vu offrir un emploi par l'une des sociétés plaignantes

Dans un domaine qui évolue aussi rapidement, il est presque impossible de savoir de quoi demain sera fait. Il suffit de se rappeler de ce qu'était le piratage informatique il y a cinq ans pour se rendre compte de l'intensification de la menace sur cette période relativement courte. En effet, une enquête menée par Sophos révèle que 70 % des personnes interrogées pensent que l'année 2008 sera une année aussi inquiétante, voire pire que 2007, en matière de sécurité informatique.

Il semble inévitable que la variété et le nombre d'attaques continueront à augmenter, poussés par la volonté des milieux du crime organisé de forcer l'accès aux ordinateurs pour dérober des données, des identités et des ressources. Sophos s'attend à ce que les utilisateurs continuent à être confrontés à des problèmes de sécurité et de contrôle des ordinateurs, car les pirates continueront à exploiter de nouvelles technologies pour gagner de l'argent et provoquer des perturbations. Par ailleurs, les menaces de type usurpation d'identité ou escroquerie risquent de rester très présentes à long terme, car elles exploitent avant tout les erreurs humaines.

Cependant, grâce à une gestion correcte des infrastructures, le problème n'est pas insurmontable : des pratiques de sécurité solides, des solutions de protection à jour et une veille active sur l'actualité de la sécurité informatique constituent les éléments essentiels qui permettront de défendre correctement les réseaux d'entreprise en 2008.

La bonne nouvelle, c'est que les logiciels de sécurité s'améliorent en permanence. La détection proactive des nouveaux malwares encore inconnus est plus efficace que jamais et les utilisateurs sensibles aux problèmes de sécurité et correctement protégés ne courent qu'un risque limité.

Sources

1. www.sophos.com/security/technical-papers/modern_web_attacks.html
2. www.sophos.com/news/2007/07/toptenjun07.html
3. www.sophos.com/news/2007/09/consulate.html
4. www.sophos.com/security/technical-papers/sophos-securing-websites.html
5. www.sophos.com/news/2007/01/drefv.html
6. www.sophos.com/news/2007/01/malwarestorm.html
7. www.sophos.com/news/2007/01/dorflove.html
8. www.sophos.com/news/2007/07/july4.html
9. www.sophos.com/news/2007/08/youtube.html
10. www.sophos.com/security/blog/2007/09/577.html
11. www.sophos.com/news/2007/11/detective-dorf.html
12. www.sophos.com/news/2007/12/santa-storm.html
13. www.sophos.com/news/2008/01/holiday-hackers.html
14. www.sophos.com/news/2007/01/secprep2007.html
15. www.sophos.com/news/2007/10/toptensep07.html
16. www.sophos.com/security/blog/2008/01/974.html
17. www.sophos.com/news/2007/08/spam-pump.html
18. www.sophos.com/news/2007/03/german-pump.html
19. www.sophos.com/news/2007/03/sec.html
20. www.sophos.com/news/2007/10/stock-mp3.html
21. www.sophos.com/news/2007/12/spam-buyers.html
22. www.sophos.com/products/enterprise/alert-services/zombiealert.html
23. www.sophos.com/news/2006/02/macosexleap.html
24. www.sophos.com/security/blog/2007/11/729.html
25. www.sophos.com/security/blog/2007/05/117.html
26. www.sophos.com/security/blog/2007/11/797.html
27. money.cnn.com/news/newsfeeds/articles/newstex/IBD-0001-21528092.htm
28. www.sophos.com/news/2007/02/mobile-security.html
29. www.sophos.com/pressoffice/news/articles/2007/10/facebook-addiction.html
30. www.sophos.com/news/2007/08/facebook.html
31. www.sophos.com/security/best-practice/facebook.htm
32. www.sophos.com/news/2007/03/myspace-malware.html
33. www.sophos.com/security/blog/2007/12/900.html
34. www.sophos.com/news/2008/01/facebook-adware.html
35. www.sophos.com/news/2007/03/tjx.html
36. www.sophos.com/news/2007/11/hmrc-id-theft.html
37. www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032518
38. www.computerweekly.com/Articles/2007/09/06/226599/vendor-report-pci-is-your-business-up-to-the-standard.htm
39. www.guardian.co.uk/russia/article/0,,2081438,00.html
40. www.sophos.com/news/2007/12/mi5-china-internet-spy.html
41. www.sophos.com/news/2007/09/chinese-hack.html
42. www.sophos.com/news/2007/08/rizler.html
43. www.sophos.com/news/2007/08/stolen-identity.html
44. www.sophos.com/news/2007/09/fujacks-jail.html
45. www.sophos.com/news/2007/10/porn-spam-jail.html
46. www.sophos.com/news/2007/11/habbo-hotel.html

À propos de Sophos

Sophos permet aux grands comptes du monde entier de sécuriser et de contrôler leur infrastructure informatique. Nos solutions Web, de contrôle d'accès réseau, pour systèmes d'extrémité et de messagerie simplifient la sécurité en assurant une protection intégrée contre les malwares, les spywares, les intrusions, les applications indésirables, le spam, les violations des politiques de sécurité, la fuite des données et les dérives par rapport à la conformité. Avec plus de 20 ans d'expérience, nos solutions et services de sécurité à la conception fiable protègent plus de 100 millions d'utilisateurs dans près de 150 pays. Reconnus pour notre niveau de satisfaction clientèle élevé, nous possédons un nombre enviable de récompenses et autres certifications de l'industrie. Les sièges sociaux de Sophos se trouvent à Boston aux États-Unis et à Oxford au Royaume-Uni.

Pour en savoir plus sur les produits Sophos et les évaluer, visitez www.sophos.fr.

Boston, États-Unis • Mayence, Allemagne • Milan, Italie • Oxford, Royaume-Uni • Paris, France
Singapour • Sydney, Australie • Vancouver, Canada • Yokohama, Japon

SOPHOS
secured.