

Navigation Web : allier sécurité et productivité dans un environnement de plus en plus dangereux – un véritable défi pour les entreprises

Avec une nouvelle page Web infectée toutes les 14 secondes, le Web est aujourd'hui le principal vecteur d'attaques de piratage en ligne. Il représente aussi une menace pour la productivité de nombreuses entreprises. Pourtant, la plupart des entreprises ne sont pas protégées contre les malwares modernes. Rares sont celles qui déploient un dispositif de protection proactive pour combattre ces dangers et protéger la sécurité du réseau ainsi que la productivité du personnel. Ce livre blanc met en évidence les six principaux stratagèmes utilisés par les pirates, et décrit les trois éléments de protection clés que les entreprises doivent mettre en œuvre pour protéger leurs systèmes et ressources.

Navigation Web : allier sécurité et productivité dans un environnement de plus en plus dangereux – un véritable défi pour les entreprises

Malwares Web : la nouvelle arme

Traditionnellement, les cybercriminels utilisaient plutôt la messagerie comme vecteur d'attaque. Toutefois, au fur et mesure que les entreprises ont été sensibilisées à ce danger et ont pris des mesures pour protéger leurs systèmes de messagerie, les pirates se sont tournés vers le Web, qui est aujourd'hui encore très peu protégé. Ils se sont mis à installer des malwares Web pour dérober directement des informations confidentielles ou pour établir des botnets – qui sont des réseaux d'ordinateurs piratés – permettant de diffuser des spywares, des virus, du spam et d'autres menaces.

Les pirates ne cessent d'exploiter les vulnérabilités des nouvelles infrastructures ou des nouveaux systèmes de navigation pour diffuser du code malveillant sur des sites Web légitimes. Au début de l'année 2008, on dénombrait 6000 pages Web infectées par jour, soit une toutes les 14 secondes¹. Ce problème atteint une telle ampleur que le deuxième code malveillant bloqué par Sophos en 2007 a été Mpack, kit de création de malwares pour pages Web, qui peut être téléchargé gratuitement sur Internet.

Aujourd'hui, seulement 15 % des entreprises disposent d'un système de protection proactive sur leur passerelle Web². De plus, très souvent, les correctifs des navigateurs Web ne sont pas à jour. Aussi est-il facile pour les pirates d'infecter des milliers de systèmes chaque jour via le Web.

Cette activité est extrêmement lucrative pour les criminels : un seul ordinateur compromis peut donner accès à des milliers d'enregistrements. Elle est aussi extrêmement coûteuse pour les entreprises. On estime à 197 dollars US le coût de chaque enregistrement client compromis en 2007³.

Outre ces risques de sécurité importants, les entreprises doivent faire face à l'impact négatif pour la productivité de l'explosion de popularité des réseaux sociaux et des autres sites qui ne sont pas stratégiques pour l'activité de l'entreprise. Quand le personnel navigue sur des sites Web interdits, cela peut ralentir le réseau, réduire la productivité de l'entreprise et accroître les risques de sécurité (et d'infractions à la loi) si des informations sensibles, professionnelles ou personnelles sont envoyées en ligne.

“

Une nouvelle page Web infectée est découverte toutes les 14 secondes.

”

Rapport Sophos 2008 sur les menaces de sécurité¹

Un nouvel éventail d'astuces

Le succès ou l'échec d'un logiciel malveillant dépend de l'association d'un certain nombre de facteurs, comme la manière dont ce logiciel est diffusé, la personne à laquelle il est envoyé, la manière dont il s'exécute, la rapidité à laquelle il se propage ou encore sa capacité à déjouer les mécanismes de détection. Les pirates ont recours à un nouvel éventail de stratagèmes pour maximiser le taux d'infection de leurs malwares.

PREMIER STRATAGÈME

Accroissement de la portée des infections grâce au détournement de réputation

83 pour cent des pages Web infectées par des malwares se trouvent sur des sites Web parfaitement légitimes¹. Pour les auteurs de malwares, la manière la plus efficace et la moins coûteuse d'infecter des ordinateurs par l'intermédiaire du Web consiste à héberger leurs malwares à l'endroit où le plus grand nombre de personnes les verront. C'est précisément ce qu'ils font quand ils détournent la réputation de sites Web existants en attirant des utilisateurs qui se méfient d'autant moins qu'ils font confiance à la popularité et à la crédibilité de ces URL qui semblent sûres.

Bien que certains pirates créent également spécialement de nouveaux sites Web infectés à l'aide de services d'hébergement Web gratuits ou, plus généralement, en utilisant un nom de domaine similaire à une marque légitime qui existe déjà, cette pratique est beaucoup moins répandue que le détournement de réputation.



83 pour cent des pages Web infectées par des malwares se trouvent sur des sites Web parfaitement légitimes



Rapport Sophos 2008 sur les menaces de sécurité¹

La balise HTML <IFRAME> est un mécanisme très pratique pour les cybercriminels qui souhaitent infecter un site Web. En 2007, elle a représenté plus de 50 % des malwares Web⁴. En visant un serveur Web non sécurisé ou en exploitant d'autres nouvelles vulnérabilités avant que les correctifs soient disponibles, les pirates peuvent injecter rapidement et facilement de nombreuses pages sur une multitude de sites Web à l'aide d'une balise iFrame malveillante. Comme ce code est quasiment invisible, voire complètement invisible (il peut être réduit à 1 pixel x 1 pixel, ou même paramétré sur 0), il permet de charger du contenu sans même que l'administrateur du site ou le visiteur en soit informé.



Infection d'une page Web par plusieurs balises iFrame

Dans l'exemple ci-dessus, chacun des rectangles représente une balise iFrame d'une largeur et d'une hauteur de 3 pixels. Si la largeur ou la hauteur était de 0, il n'y aurait aucun indicateur visible permettant de savoir que cette page est compromise.

Une fois chargé à l'insu de l'administrateur et du visiteur, le malware peut exécuter sa charge sur l'ordinateur de l'utilisateur. Ce type de menace peut se multiplier extrêmement rapidement et avoir un effet véritablement dévastateur. En Chine, fin 2006, le virus parasite Fujacks a infecté plusieurs millions d'ordinateurs. Pour se répandre aussi rapidement, il ordonnait à chaque ordinateur infecté d'injecter une balise iFrame malveillante dans tous les fichiers HTML et tous les autres fichiers Web auxquels il avait accès. Ainsi, de nombreux sites Web d'entreprise ont été infectés par l'intermédiaire des ordinateurs de leurs propres employés.

En concentrant leurs efforts pendant une période prolongée pour infiltrer des sites recevant un grand nombre de visiteurs, les pirates ont atteint des résultats largement à la hauteur de leurs espoirs. Parmi les sites de réseaux sociaux affectés en 2007 figuraient MySpace, Facebook et Orkut, de Google. Ce dernier a infecté plus de 670 000 utilisateurs⁵. Le site Web des Miami Dolphins a été pris pour cible quelques jours avant que le stade de l'équipe accueille la Superbowl, au mois de février 2007, et il a infecté des milliers d'ordinateurs.

Aucun secteur n'est épargné par les attaques. De nombreux sites officiels, comme celui du Consulat américain en Russie, ont été infectés. Même celui de Computer Associates, éditeur de solutions informatiques, a été infecté pendant une courte durée, redirigeant les visiteurs sur du contenu malveillant⁶. Les sites moins en vue et les pages Web d'amateurs sont eux aussi susceptibles d'être infectés. Ainsi des communautés chrétiennes, des entreprises agroalimentaires organiques, des paysagistes et même des fabricants de glaces ont-ils été pris pour cible.

DEUXIÈME STRATAGÈME

Dissimulation de l'attaque derrière un téléchargeur

Au lieu de placer directement leur code malveillant sur une page Web, de nombreux cybercriminels insèrent des « téléchargeurs ». Ces chevaux de Troie sont conçus pour éviter la plupart des mécanismes de défense. Ils contiennent très peu de code et ne contiennent pas par eux-mêmes de charge malveillante. Ce n'est qu'une fois installés sur un ordinateur qu'ils téléchargent cette charge à partir d'un autre site Web, souvent via un port différent. Dans certains cas de figure plus complexes, le mécanisme d'infection peut impliquer d'autres composants de téléchargeurs, qui récupèrent alors du contenu à partir de plusieurs domaines Web, ou qui peuvent même télécharger des malwares en plusieurs éléments afin de déjouer les systèmes de détection, puis les réassembler au niveau du point d'entrée. La charge peut aussi être différée. Il est alors plus difficile pour l'utilisateur et pour les technologies de sécurité de comportement de détecter les activités suspectes.

Il existe de nombreuses familles de téléchargeurs. Clagger, qui a fait son apparition au mois de février 2007, a été si efficace qu'il a été révisé 80 fois dans de nouvelles attaques.

TROISIÈME STRATAGÈME

Infection silencieuse par téléchargement passif

Pour que ce type d'infection se produise, il suffit qu'un utilisateur navigue sur le Web et visite une page infectée à l'aide d'un navigateur auquel aucun correctif n'a été appliqué. L'utilisateur n'a même pas besoin de cliquer sur des liens particuliers, ni d'ouvrir des fichiers précis. Son ordinateur devient infecté simplement parce qu'il a visité un site sur lequel les vulnérabilités connues du navigateur sont exploitées par l'auteur d'un malware.

Le problème, pour les administrateurs, est qu'il est beaucoup plus délicat de mettre à jour les correctifs de navigateurs et de modules complémentaires que les correctifs de système d'exploitation. Il peut y avoir plusieurs correctifs de navigateurs et de modules externes par mois, et ils peuvent provenir d'éditeurs différents. A titre d'exemple, au début de l'année 2008, des contrôles ActiveX de téléchargement d'images vulnérables utilisés par MySpace et Facebook ont exposé les utilisateurs à des attaques⁷.

Souvent utilisé en combinaison avec le piratage de réputation, qui constitue un moyen aisé d'atteindre la victime, le téléchargement passif fait partie des outils très efficaces de l'arsenal du pirate.

QUATRIÈME STRATAGÈME

Exploitation des noms de domaine résultant de fautes de frappe

Les pirates ont eu l'idée de créer des noms de domaine ressemblant à des sites parfaitement légitimes (par exemple, « Goggle » au lieu de « Google », ou un « .tv » à la fin au lieu de « .com »), ce qui leur permet d'utiliser des fautes de frappe courantes pour faire atterrir très simplement des utilisateurs sur leurs pages Web. Ces pages sont en quelque sorte des pièges, qui n'attendent que des proies à capturer et à infecter. Comme ces sites ressemblent généralement au site initialement souhaité, il est très facile d'obtenir du visiteur qu'il ouvre ou télécharge du contenu, d'autant que ce contenu semble sûr.

CINQUIÈME STRATAGÈME

Utilisation d'attaques de spam à flux rapide pour envoyer des malwares

Alors qu'ils envoyaient souvent les malwares sous forme de pièces jointes aux messages électroniques, les pirates tendent aujourd'hui à envoyer des messages électroniques contenant des liens qui conduisent à des pages Web infectées. Derrière ces liens se cachent des armées d'ordinateurs infectés, appelés « botnets », qui font office d'hôtes Web. Les auteurs de malwares alternent constamment entre ces différents ordinateurs pour fournir une page d'accueil infectée toujours différente aux personnes qui suivent un lien. Cette opération consistant à modifier rapidement l'adresse IP de l'ordinateur qui héberge le malware est appelée « flux rapide ». Elle complique la tâche aux filtres en charge de détecter et de bloquer les attaques de spam correspondantes.

De la même manière que des astuces d'ingénierie sociale sont utilisées pour convaincre les utilisateurs de cliquer sur les pièces jointes, des méthodes similaires sont employées pour les convaincre de cliquer sur les liens de pages Web. Le ver Storm (ou Dorf), qui a constitué la première menace Web en 2007, utilisait des sujets d'actualité, des cartes de vœux virtuelles, des faux messages YouTube et des événements sportifs.

SIXIÈME STRATAGÈME

Toujours avoir une longueur d'avance sur les systèmes de défense de sécurité

Contrairement aux virus et aux vers véhiculés par messagerie, qui cessent d'être dangereux une fois qu'ils ont été éradiqués, les menaces Web modernes ne cessent d'être adaptées et modifiées afin d'esquiver les systèmes de défense. En présentant continuellement les menaces sous une forme différente, les pirates peuvent créer de nombreuses variantes mineures, dont certaines ne sont pas reconnues par les solutions de sécurité. Ce processus peut même être automatisé, ce qui permet aux criminels de générer plusieurs variantes d'un même malware le même jour.

Famille	Vitesse de mise à jour (jours)
Mal/ObfJS	< 1
Mal/Clagger	1,5
Mal/Dorf	< 1
Mal/Dropper	3
Mal/DownLdr	3,5
Troj/Pushdo	4

Source : SophosLabs

Exemples de familles de malwares fréquemment mis à jour

Cette modification constante du code permet non seulement aux pirates de compromettre plus d'ordinateurs, mais elle leur assure aussi qu'ils resteront infectés plus longtemps. En modifiant constamment les caractéristiques de leur code, les pirates peuvent déjouer les moteurs de détection de malwares utilisant la signature (ou ceux qui reposent sur des fonctions d'analyse peu évoluées) et ajouter d'autres malwares, tels que des spywares ou des adwares, à l'ordinateur. Les ordinateurs compromis peuvent aussi être utilisés pour lancer des campagnes de spam répétées ou des attaques de déni de service distribuées.

Les trois éléments clés de la protection Web moderne

Les menaces Web actuelles évoluent très rapidement, et les auteurs de malwares exploitent immédiatement la moindre vulnérabilité détectée dans les navigateurs. Aussi les entreprises ne peuvent-elles pas se contenter de protéger leur messagerie et leurs systèmes d'extrémité. Elles doivent prendre des mesures pour s'assurer que les utilisateurs qui naviguent sur le Web ne compromettent pas la sécurité informatique de l'entreprise, les ressources réseau ni la productivité du personnel. Ces mesures passent tout d'abord par la prévention, avec l'application systématique des correctifs disponibles, et la sensibilisation des utilisateurs aux risques inhérents à la navigation Web, mais les entreprises doivent aussi mettre en œuvre une solution de sécurité Web exhaustive, intégrant trois éléments clés :

- **Un filtrage reposant sur la réputation**
- **Un filtrage prédictif en temps réel des menaces**
- **Un filtrage reposant sur le contenu**

PREMIER ÉLÉMENT DE SÉCURITÉ CLÉ Filtrage reposant sur la réputation

Les filtres reposant sur la réputation constituent le premier élément clé à mettre en œuvre pour contrecarrer les menaces Web. Ils empêchent d'accéder à un catalogue de sites connus pour héberger des malwares ou une autre forme de contenu indésirable, en filtrant leur URL suivant que leur réputation est « bonne » ou « mauvaise ». Ils ont fait leurs preuves et protègent efficacement contre les menaces Web déjà connues et bien localisées. Ils permettent en outre d'optimiser les performances du réseau et la productivité du personnel en bloquant l'accès au contenu Web illégal, inapproprié ou non stratégique pour l'entreprise.

Bien que ces filtres d'URL traditionnels se connectent souvent à de puissantes bases de données, régulièrement mises à jour, de sites connus pour héberger des malwares ou du contenu suspect, ils ont un gros défaut, d'ailleurs bien connu des cybercriminels : ils n'offrent aucune protection contre les malwares hébergés par des sites

légitimes, jusqu'alors considérés comme sûrs mais qui viennent d'être piratés, ni contre les sites qui viennent d'être créés. Le trafic en provenance de ces sites n'est pas bloqué, et les malwares récents ou anciens peuvent donc entrer dans l'entreprise.

DEUXIÈME ÉLÉMENT DE SÉCURITÉ CLÉ Filtrage prédictif en temps réel des menaces

Le filtrage prédictif en temps réel des menaces comble une grande partie des lacunes des filtres reposant sur la réputation. L'ensemble du trafic Web passe par un analyseur conçu pour identifier les malwares connus, ainsi que ceux qui émergent seulement. Le moteur de malwares est optimisé pour réaliser une analyse à faible latence, et chaque fois qu'un utilisateur accède à un site Web, quelle que soit sa réputation ou sa catégorie, le trafic est analysé à l'aide d'une combinaison de signatures et de technologies d'analyse de comportement.

Il faut souligner que ce type d'analyse en temps réel présente un autre avantage par rapport aux filtres d'URL traditionnels : par définition, la filtration est bidirectionnelle. Elle porte à la fois sur la requête envoyée par l'utilisateur au serveur Web et sur les informations renvoyées par le serveur Web à l'utilisateur. Cette filtration bidirectionnelle détecte non seulement les malwares connus au fur et à mesure qu'ils infectent des sites légitimes, mais elle protège aussi contre les nouvelles menaces où qu'elles soient hébergées.

Le filtrage prédictif en temps réel des menaces reste peu répandu au sein des solutions de sécurité majeures disponibles sur le marché actuellement. De nombreux éditeurs de solutions de sécurité se contentent d'analyser les signatures. D'autres, apparus plus récemment sur le marché, prétendent offrir des solutions complètes, mais ne sont pas en mesure de prouver qu'ils offrent une protection pleinement proactive.

Questions clés à poser à un fournisseur potentiel de solutions de sécurité

- La base de données d'URL utilisée pour votre filtrage de réputation a-t-elle une couverture mondiale ?
- A quelle fréquence cette base de données est-elle mise à jour pour inclure les nouvelles menaces ?
- Comment identifiez-vous les nouveaux hôtes de menaces Web ?
- Combien de nouveaux sites hébergeant des menaces identifiez-vous chaque jour ?
- Comment puis-je bloquer ou autoriser les utilisateurs par catégorie de pages Web ?
- Puis-je personnaliser les privilèges de navigation groupe de travail par groupe de travail ou individu par individu ?
- Puis-je définir des politiques permettant de restreindre la navigation sur les sites récréatifs en fonction de l'heure en cours ?
- Votre solution analyse-t-elle l'ensemble du trafic entrant pour détecter les malwares ?
- Votre solution analyse-t-elle le contenu réel des fichiers, ou se fie-t-elle simplement à l'extension ou au type MIME ?
- Utilisez-vous votre propre technologie pour l'analyse des malwares ou utilisez-vous des technologies de tiers ?
- Quel est l'impact de votre solution globale sur les performances ?
- Faut-il prévoir un coût supplémentaire pour le filtrage en temps réel des menaces ?
- Etes-vous en mesure de démontrer votre expertise dans le domaine de la recherche appliquée aux menaces Web ?
- Disposez-vous de statistiques réalisées par un organisme indépendant sur le taux de détection de menaces Web de votre solution ?
- Puis-je voir une démonstration de la console d'administration pour juger de sa convivialité ?
- Votre solution intègre-t-elle des agents de surveillance matériels pour contrôler l'état des logiciels, du matériel et du trafic ?
- Comment les problèmes sont-ils signalés à l'administrateur ? Par messagerie électronique ? Par téléphone ?
- Proposez-vous une surveillance de la disponibilité en temps réel afin de garantir un fonctionnement 24 heures sur 24, 7 jours sur 7 ?

TROISIÈME ÉLÉMENT CLÉ

Filtrage reposant sur le contenu

Le filtrage reposant sur le contenu analyse l'ensemble du trafic réseau pour déterminer le véritable type de fichier du contenu qui revient d'un site Web. Il peut ensuite autoriser ou interdire ce trafic en fonction de la politique de l'entreprise.

Les filtres de contenu analysent le contenu réel d'un fichier au lieu de ne s'intéresser qu'à l'extension du fichier ou au type MIME signalé par le serveur Web. Ils peuvent aussi identifier et bloquer les types de fichiers qui semblent légitimes et inoffensifs mais qui dissimulent en fait du contenu interdit. A titre d'exemple, un fichier peut porter une extension .TXT mais contenir en fait un fichier exécutable.

En n'autorisant que le contenu de nature professionnelle, cet élément de protection clé permet aux entreprises d'élaborer des politiques autour des différents types de contenu qui peuvent servir à envoyer des malwares. Il contribue donc à réduire les risques d'infection. Par exemple, les exécutables Windows et les économiseurs d'écran peuvent être interdits. Le filtrage reposant sur le contenu optimise aussi la bande passante en bloquant le contenu volumineux ou gourmand en ressources, comme la vidéo en continu.

Former les utilisateurs pour mieux vous défendre

De nombreuses entreprises ont déjà réussi à apprendre à leurs employés à identifier les menaces liées au courrier électronique. La lutte contre les menaces Web fait intervenir des technologies plus évoluées encore, et les utilisateurs peuvent, et même doivent, là aussi s'engager dans le combat.

De nombreuses entreprises appliquent des procédures définissant les sites Web jugés appropriés, mais rares sont celles qui mettent à jour ces procédures pour inclure des conseils sur la manière d'éviter les infections en navigant sur le Net.

Une bonne politique de sécurité doit indiquer clairement que :

- Les employés ne doivent jamais ouvrir les messages électroniques de spam.
- Les employés ne doivent jamais cliquer sur des liens inclus dans des messages électroniques envoyés par des expéditeurs inconnus.
- Le service informatique doit faire en sorte que les correctifs disponibles pour les navigateurs Web de l'entreprise soient appliqués systématiquement.
- Les employés doivent minimiser la navigation Web extraprofessionnelle, non seulement pour des raisons de sécurité mais aussi par souci de productivité.

Les utilisateurs peuvent également encourager les utilisateurs à signaler les comportements inhabituels (voire exiger d'eux qu'ils les signalent), notamment si leur ordinateur devient soudain anormalement lent, si la page d'accueil change quand ils lancent leur navigateur sans qu'ils aient rien fait à cet effet, ou si rien ne se passe quand ils ouvrent un fichier.

Conclusion

Chaque heure, et même chaque minute, des cybercriminels cherchent à exploiter le trafic Web pour en tirer un profit financier. La navigation Web fait aujourd'hui partie intégrante des activités professionnelles de la plupart des entreprises, et elle doit bénéficier du même niveau de protection que les passerelles de courrier électronique et les systèmes d'extrémité. Pour se protéger de la menace croissante que représentent les malwares diffusés sur le Web, les entreprises doivent surtout disposer d'une solution qui offre à la fois des fonctions de sécurité éprouvées, des contrôles de sites et de contenu puissants, et un système d'administration efficace, sans pénaliser les performances informatiques globales. En effet, parallèlement, l'utilisateur final a besoin d'applications rapides et efficaces. Au final, les solutions qui ne répondent pas à ces critères de sécurité, de contrôle et de performances mettent en danger l'entreprise.

Solution Sophos

Incluse dans Web Security and Control, la Sophos Web Appliance protège contre les spywares, les adwares, les virus, le code malveillant, les applications indésirables et le contenu indésirable. Elle intègre un moteur d'analyse large spectre novateur capable de détecter toutes les menaces grâce à une approche unique combinant un filtrage de réputation, un filtrage prédictif en temps réel des menaces et un filtrage de contenu. Sa console de gestion conviviale et ses puissants outils de création de rapports, qui informent rapidement l'administrateur de la nature du trafic Web, des menaces et des comportements d'utilisateurs, permettent une navigation Web sécurisée sans la complexité supplémentaire des filtres traditionnels. En tant qu'appliance administrée, la Sophos Web Appliance offre des services à distance de surveillance continue et d'assistance à la demande garantissant la sécurité Web la plus fiable du marché.

Sources (en anglais)

- 1 Rapport Sophos 2008 sur les menaces de sécurité
www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-report-08.pdf
- 2 Marketscope for URL filtering 2006. Lawrence Orans et Arabella Hallawell. Gartner, Inc. March 2006
- 3 2007 Annual Study : Cost of a Data Breach – Ponemon Institute, novembre 2007
- 4 Modern web attacks, Sophos Labs technical paper, Fraser Howard
www.sophos.com/security/technical-papers/modern_web_attacks.pdf
- 5 www.sophos.com/security/blog/2007/12/900.html
- 6 www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9055599
- 7 www.theregister.co.uk/2008/02/01/myspace_image_uploader_bug/

A 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, de 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 infractions aux politiques de sécurité, les fuites de données et les dérives par rapport à la conformité. Fruit de plus de 20 ans d'expérience, nos solutions et services de sécurité reposent sur une conception fiable et protègent plus de 100 millions d'utilisateurs dans près de 150 pays. Nous sommes reconnus pour notre niveau de satisfaction clientèle élevé et avons à notre actif un nombre important de récompenses et d'autres certifications de l'industrie. Les sièges sociaux de Sophos se trouvent à Boston aux Etats-Unis et à Oxford au Royaume-Uni.

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

© 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.

SOPHOS
WWW.SOPHOS.COM