Initiation à la prévention des virus informatiques

Serge Ballini, Sophos France

Première publication : Août 2000
Révision 1.1 Octobre 2000

RÉSUMÉ

Ce livre blanc décrit la situation actuelle concernant les virus informatiques, leurs points d'entrée les plus courants, les procédures pour empêcher les infections, les types de logiciel antivirus, le déploiement et l'administration des logiciels antivirus ainsi que les mesures de traitement d'une attaque virale

Les virus aujourd'hui

Plus de 50 000 virus en août 2000.

Le nombre de virus connus a dépassé les 50.000 en août 2000. La grande majorité (74%) correspond aux virus parasites (attaquant les codes exécutables), viennent ensuite les virus macros (19%) puis les virus de secteurs de démarrage (7%). En mai 2000, 88% des infections rapportées à Sophos étaient dues aux virus macros, 9% aux virus parasites et seulement 3% aux virus de secteur de démarrage. Remarquez qu'une infection rapportée n'est comptée qu'une seule fois, que le virus infecte une seule machine ou 10 000 machines : les statistiques citées ne sont qu'indicatives et permettent de se faire une idée de la situation actuelle.

Le nombre de nouveaux virus découverts continue de croître. Lors du second trimestre 2000, le laboratoire de Sophos a traité 800 nouveaux virus par mois.

Il est impossible de prédire quel nouveau virus sera "en liberté" et cela pose problème. Ils doivent tous être analysés et leurs détections/désinfections inclues dans le logiciel antivirus.

Les éditeurs de logiciels antivirus sont tous confrontés au dilemme qui consiste à déterminer la priorité qu'ils doivent affecter à chaque signature de détection de virus arrivant dans les laboratoires de recherche. Il est impossible de prédire lequel de ces nouveaux virus sera mis "en liberté" (si c'est le cas) et cela commence à poser des problèmes : les nouveaux virus doivent simplement être analysés et leur signature pour détection / désinfection incluse dans le logiciel antivirus. Cependant, un groupe de virus possède un potentiel de propagation plus rapide que les autres. Les virus qui sont "activés par Internet" et qui exploitent certaines formes de facteur d'ingénierie sociale de base (tel que le virus LoveLetter) font, bien entendu, partie de cette catégorie.

Procédures antivirales

L'utilisation d'un logiciel antivirus ne devrait pas être l'unique composant d'une défense antivirale efficace. Les quelques recommandations qui suivent doivent être prises en considération dans la mise en place d'une stratégie de protection globale.

N'utilisez plus le format DOC

Arrêtez d'utiliser les formats de fichiers DOC et XLS. Utilisez plutôt les formats de fichiers RTF et CSV.

Utilisez plutôt les fichiers Rich Text Format (RTF). Tout le formatage Word du texte est préservé mais les fichiers RTF étant incapables de contenir des macros, ils sont donc incapables de propager des virus. Attention néanmoins : un fichier Word reçu avec une extension RTF n'est pas nécessairement un fichier Rich Text Format. Word peut sauver des fichiers dans le format Word (c'est à dire : avec des macros) sous n'importe quelle extension.

N'utilisez plus le format XLS pour Excel.

Utilisez plutôt le format CSV. Celui-ci a des propriétés similaires pour EXCEL à celles des fichiers RTF pour Word.

Utilisez PowerPoint 7 ou une version inférieure.

PowerPoint 7 ou versions inférieures ne supportent pas les macros. Il est donc insensible aux virus. Malheureusement, l'apparence visuelle des présentations de PowerPoint 8 est meilleure que celle de PowerPoint 7. Par conséquent, il est difficile de convaincre l'utilisateur qu'il est préférable d'utiliser un environnement moins attrayant mais plus sûr.

Utilisez des visionneuses, pas les applications

La plupart des systèmes sont configurés pour démarrer l'application associée au type du fichier lorsque l'utilisateur ouvre une pièce jointe. Par exemple, un fichier DOC démarrera Word, un fichier XLS Excel etc. Cela pose problème dans la mesure où, ces applications exécuteront aussi les macros présentes dans le fichier reçu, permettant ainsi l'infection par un virus.

La plupart des applications de courrier électronique peuvent être configurées pour afficher le contenu d'un fichier reçu en utilisant une 'visionneuse'. Les visionneuses n'ont, normalement, pas la possibilité d'exécuter les macros. Si un fichier infecté est examiné de cette façon, le virus n'infectera pas l'environnement. Les utilisateurs n'ayant généralement pas besoin d'éditer les pièces jointes reçues, cette technique est une méthode antivirale très efficace.

Bloquez l'envoi / réception de code exécutable

Les utilisateurs n'ont normalement pas besoin d'envoyer ou de recevoir de code exécutable. Lorsque des fichiers de données compressés ZIP sont envoyés, l'utilisation de ZIP compressés statiquement est une meilleure solution.

Les utilisateurs n'ont, le plus souvent, aucun besoin réel d'envoyer ou de recevoir du code exécutable par courrier électronique. Dans la plupart des entreprises, c'est également illégal, et transgresse généralement les termes du copyright logiciel. Certaines personnes aiment à utiliser des fichiers ZIP auto-extractibles pour envoyer des fichiers de données compressés : pour des raisons de sécurité, l'utilisation de fichiers ZIP compressés de façon statique (qui nécessitent PKUNZIP pour être décompressés) est une meilleure solution.

Il est souvent préférable de bloquer tout transfert de code exécutable au niveau d'une passerelle Internet. Malheureusement, il est impossible de déterminer à 100% si un code est exécutable ou non en analysant soit le contenu du fichier soit l'extension du fichier. Cependant, bloquer les fichiers portant des extensions exécutables telles que EXE, VBS, SHS etc., contribue grandement à l'efficacité des mesures antivirales en général. Il est également judicieux de bloquer les pièces jointes à double extension (Lovelet.txt.vbs par exemple), celles-ci n'ayant pas de raison légitime d'exister et étant fréquemment utilisées par les vers attachés à des e-mail.

L'éducation de l'utilisateur joue aussi un rôle significatif dans la prévention des infections par code exécutable reçu via e-mail ou téléchargés : il peut être très tentant pour un utilisateur de PC qui ignore les risques encourus d'installer un bel écran de veille ou un jeu. Il convient de lui faire développer un sain niveau de paranoïa consistant à considérer toute pièce jointe ou tout exécutable téléchargé comme pouvant potentiellement véhiculer un virus.

Changez la séquence de démarrage du CMOS

La plupart des PC sont configurés, tels qu'ils ont été livrés par les constructeurs, pour démarrer d'abord à partir du lecteur A: puis, seulement s'il n'y a pas de disque système dans le lecteur, à partir du lecteur C:. Si un utilisateur laisse une disquette infectée dans le lecteur de disquette, le PC deviendra lui même infecté et infectera ensuite toute autre disquette inscriptible.

Démarrer le PC du lecteur C: élimine complètement le danger d'une infection par pur virus de secteur de démarrage.

Sur les PC modernes, la séquence de démarrage est stockée dans la mémoire CMOS et il est très facile de la changer. Changer la séquence pour que le PC démarre du disque dur élimine complètement les risques d'infections par de purs virus de secteur de démarrage. Si jamais le PC avait besoin d'être démarré à partir d'une disquette, la séquence de démarrage peut être facilement inversée pour cette occasion.

Cependant, la plupart des entreprises n'utilisent pas cette technique simple.

Désactivez Windows Scripting Host

Windows Scripting Host devrait être désactivé.

Si Windows Scripting Host (WSH) n'est d'aucune utilité dans le cadre des applications de l'utilisateur, il devrait être désactivé. Ceci élimine tout risque de contamination par les virus de type VBS (Visual Basic Script) et SHS (Scripting Host System), qui représentent les virus plus courants de nos jours. La procédure pour désactiver WSH est décrite (en anglais) à l'adresse http://www.sophos.com/support/faqs/wsh.html.

Tenez-vous informé des bulletins de sécurité

Jusqu'en novembre 1999, les experts antivirus affirmaient haut et fort qu'un PC ne pouvait pas être infecté par la simple lecture d'un e-mail. Bien entendu, ils avaient analysé les spécifications techniques de l'époque et avaient déterminé qu'apparemment, il n'était pas possible d'infecter un PC en lisant simplement un e-mail. Malheureusement, il y avait une différence entre les spécifications de Microsoft Outlook et ce que le code réalisait réellement (en fait, il s'agissait d'un bug de programmation), ce qui a permis l'infection par le virus BubbleBoy lorsqu'un utilisateur lisait simplement un e-mail. Microsoft a publié un patch qui corrigeait le problème (voir Microsoft Security Bulletin MS99-032) mais très peu d'utilisateurs l'ont implémenté. Kakworm, qui exploite la même faille, est encore l'un des virus les plus courants aujourd'hui alors que le patch de Microsoft existe depuis plus d'un an.

Kakworm, qui exploite une faille de sécurité, est l'un des virus les plus courants d'aujourd'hui.

La demande sans fin de nouvelles fonctionnalités, graphiques attrayants et sophistication supérieure a engendré le niveau de complexité des logiciels d'aujourd'hui et résulte en une conception logicielle plus rapide mais moins efficiente (réduisant ainsi le niveau moyen de compétence des programmeurs et la qualité des logiciels). Il est malvenu de se plaindre du manque de fiabilité du système d'exploitation Windows et de ses logiciels : la demande du marché est de loin la principale coupable provoquant indirectement cette non-fiabilité.

La situation ne devrait pas s'améliorer. Les entreprises doivent donc maintenir une veille attentive des divers bulletins de sécurité publiant les failles de sécurité et y palier le plus tôt possible.

Sauvegardes

La corruption de données est pire que la destruction de données. Il est souvent difficile de la détecter, cela peut prendre des mois avant qu'elle ne soit remarquée.

La destruction de données n'est qu'un des effets secondaires provoqués par les virus. Ce n'est pas nouveau et ce n'est pas non plus la pire chose qu'il puisse arriver aux données. Les sauvegardes ont été une composante de sécurité depuis les premiers jours des ordinateurs, protégeant des pannes inévitables de divers éléments pouvant causer des pertes de données.

La corruption de données est bien pire que la destruction de données. Il est souvent difficile de la détecter, ce qui signifie qu'il peut s'écouler plusieurs mois avant qu'elle ne soit remarquée. Généralement, le recours aux sauvegardes pour récupérer les données est impossible car les documents et les feuilles de calcul changent et les documents issus des sauvegardes peuvent être trop vieux pour pouvoir être utilisés.

Néanmoins, les sauvegardes continuent à être une défense efficace contre les virus informatiques et sont donc nécessaires.

Types d'antivirus

Scanners

Les scanners sont de loin le type de logiciel antivirus le plus utilisé de nos jours. Ils contiennent des informations de détection / désinfection pour tous les virus connus. Ils sont faciles à utiliser et capable d'identifier un virus (par ex. "ABC.DOC est infecté par le virus 'xxxx'"). Ils sont également capables de désinfecter certains types de fichiers contaminés.

Les scanners ont un inconvénient principal : ils ont besoin d'être mis à jour avec les dernières informations virales de façon à rester efficaces.

Checksummers (Programmes utilisant des sommes de contrôle)

Les Checksummers (programmes utilisant des sommes de contrôle) reposent sur la détection des modifications de fichiers. Lorsqu'un virus infecte un objet, celui-ci est modifié. Cette modification sera détectée par le scanner. Si le virus modifie un objet surveillé par le programme, ce dernier détectera aussi bien les virus connus que les virus inconnus.

Lors de l'utilisation d'un Checksummers, la principale difficulté est de pouvoir distinguer une modification légitime d'une modification virale. En d'autres termes, les résultats trouvés par le Checksummers ont besoin d'une interprétation experte (généralement non disponible au niveau utilisateur). Un autre problème se pose, ce genre d'outil ne détectera un virus qu'après infection. Il ne peut pas être utilisé à titre préventif. L'utilisation d'une simple détection de présence de virus n'est évidemment pas la meilleure solution.

Heuristiques

Les heuristiques (provenant du grec heuriskein, découvrir, trouver) sont un ensemble de règles, stratégies, méthodes ou astuces utilisées pour améliorer l'efficacité d'un système essayant de découvrir les solutions à des problèmes complexes. Dans le contexte des logiciels antivirus, les méthodes heuristiques sont utilisées par les logiciels qui appliquent des règles d'étude du comportement des programmes afin de différencier les virus des programmes légitimes. Au premier abord, il peut être tentant pour l'utilisateur d'opter pour un logiciel heuristique car celui-ci est souvent présenté comme n'ayant pas besoin de mises à jour.

Un logiciel basé sur les méthodes heuristiques utilise des règles pour distinguer les virus des non-virus. Malheureusement, ce n'est pas sans problème.

Malheureusement, les logiciels utilisant une méthode heuristique ne sont pas sans problème. Leur principal inconvénient est que la communauté des créateurs de virus apprend très rapidement les règles utilisées par les logiciels heuristiques et commence alors à écrire des virus les évitant. Les entreprises antivirales reformulent alors les règles et rééditent le logiciel, etc., rendant ainsi caduque l'argument " pas de mises à jour ". De par leur principe de fonctionnement, ils sont généralement incapables d'identifier avec précision le virus en cause et encore moins de décontaminer les objets infectés.

Les logiciels heuristiques ont également une forte propension à générer de fausses alertes, c'est à dire à déclarer des objets comme virus alors qu'ils ne le sont pas. C'est la raison pour laquelle les logiciels heuristiques sont peu choisis en environnement d'entreprise.

Points d'entrées des virus

De façon à déterminer les points stratégiques où le logiciel antivirus devrait être déployé dans une entreprise, il est important d'identifier les points d'entrée les plus courants des virus.

E-mail

Une très importante proportion des infections d'aujourd'hui est provoquée par des pièces infectées jointes aux e-mail.

Aujourd'hui, une très grande proportion d'infections est provoquée par des pièces infectées jointes aux e-mail. La facilité avec laquelle un utilisateur peut cliquer sur une pièce jointe et lancer une application est un facteur significatif de la vitesse de propagation des virus e-mail. Si le contenu de l'e-mail est suffisamment attrayant (par ex. 'kindly check the attached LOVELETTER coming from me') et l'extension visible de la pièce jointe assez innocente aux yeux d'un utilisateur moyen (par ex. LOVE-LETTER-FOR-YOU.TXT.vbs - les fichiers texte ne peuvent pas provoquer d'infection), la tentation de l'utilisateur peut devenir irrésistible.

Le danger d'infection par pièces jointes n'est, bien entendu, pas limité aux e-mail. Les messages de forums de discussion sont aussi capables de transporter des pièce jointes et le nombre de nouvelles pièces jointes infectées actuellement découvertes par les scanners automatisés sur les forums est d'environ 10 par jours.

World Wide Web

Le web 'fourmille' de sites contenant des documents infectés par des virus. L'accès au web depuis un bureau est non seulement possible technologiquement mais également perçu comme 'normal' dans le cadre du travail. Malheureusement, il est trop facile d'y télécharger des fichiers potentiellement infectés.

Plusieurs entreprises ont trouvé que fournir des PC physiquement séparés pour accéder au web est une bonne solution.

Plusieurs entreprises ont cependant déterminé que la meilleure solution pour accéder à Internet était de le faire à partir de PC physiquement séparés du réseau interne. De cette manière, non seulement le web est physiquement séparé du réseau principal de l'entreprise mais aussi, les employés perdent beaucoup moins de temps à 'surfer' sur des sites qui ne sont pas en rapport avec leur travail car il est aisé de les remarquer quand ils ne sont pas assis à leur bureau.

Disquettes et CD

L'utilisation des disquettes a été considérablement réduite avec l'apparition des réseaux mais la plupart des PC sont encore pourvus, en standard, de lecteurs de disquettes. De nos jours, 3% des infections sont dues aux virus de secteur de démarrage, ce qui montre que les disquettes ne sont pas mortes (pas encore). Les CD (en particulier les CD distribués avec les magazines) transportent aussi très fréquemment des virus.

Points de déploiement d'un logiciel antivirus

Un logiciel antivirus devrait être déployé sur les passerelles Internet, les serveurs et les stations de travail.

Il existe trois points stratégiques où il est important de déployer un logiciel antivirus : sur la passerelle Internet, sur les serveurs et sur les stations de travail.

Passerelle Internet

La passerelle Internet est le nœud d'interconnexion d'Internet et du réseaux interne de l'entreprise. C'est un bon emplacement pour installer un logiciel antivirus, qui vérifiera les pièces jointes entrantes et sortantes.

L'utilisation d'un logiciel antivirus sur une passerelle présente l'avantage principal suivant : les pièces jointes infectées envoyées à de multiples adresses e-mail génèreront une seule alerte virale (sur la passerelle) au lieu de multiples alertes si l'e-mail infecté était autorisé à parvenir jusqu'aux stations de travail.

Le principal désavantage de l'utilisation d'un logiciel antivirus sur la passerelle est le ralentissement du débit d'e-mail provoqué par le logiciel au niveau de la passerelle.

Pour le moment, relativement peu d'e-mail sont cryptés et l'efficacité du contrôle passerelle est bonne. Cela déclinera dans l'avenir.

Il est important de garder à l'esprit l'un des problèmes liés à l'utilisation d'un logiciel antivirus sur la passerelle : l'utilisation croissante du cryptage. Il n'est pas possible de vérifier les pièces jointes cryptées car les virus seront cachés dans le cocon du cryptage. Pour le moment, un nombre relativement faible d'e-mail sont cryptés et l'efficacité du contrôle antiviral au niveau de la passerelle est bonne. Cela déclinera à l'avenir.

Serveurs

L'utilisation d'un logiciel antivirus sur les serveurs pour contrôler les fichiers qui sont stockés, de façon centralisée, par les stations, présente plusieurs avantages par rapport au contrôle des fichiers stockés sur disques réseau à partir d'une station de travail. En premier lieu, le trafic réseau est minimisé car le processus de contrôle s'exécute localement sur le serveur. De plus, les mécanismes de furtivité d'un virus sont inefficaces car le virus n'est jamais 'actif' sur le serveur.

A remarquer cependant : les serveurs d'entreprise sont souvent de type Unix, Linux, Netware, OS2, OpenVMS ou autre système d'exploitation, bien qu'ils contiennent la plupart du temps les fichiers de stations Windows ou Macintosh. Il peut être difficile de trouver un antivirus pour ces plates-formes dans la mesure ou la majorité des produits sur le marché ciblent essentiellement les plates-formes Windows.

La plupart des entreprises déploient un logiciel antivirus pour contrôler leurs serveurs à intervalles réguliers, généralement lors de périodes de faible activité.

Stations de travail

Le contrôle de virus sur la station de travail est probablement la partie la plus importante des trois points d'entrées stratégiques.

Le contrôle de virus sur les stations de travail est de loin le plus important de ces trois points stratégiques de contrôle. Même si le virus pénètre la passerelle Internet en arrivant par un e-mail crypté, même s'il n'est pas détecté par le scanner du serveur (qui ne contrôle pas les e-mail), il sera intercepté par la station de travail avant qu'il ne puisse l'infecter.

Très souvent, maintenir à jour le logiciel antivirus de la station de travail est l'une des tâches les plus ardues de l'administrateur système. Ceci est spécialement le cas sur les stations de travail qui ne sont pas connectées en permanence au réseau, tels que les portables.

Administration du logiciel antivirus

Comme l'efficacité de l'utilisation du logiciel antivirus dépend de la fréquence des mises à jour, il est très important que des outils efficaces soient disponibles pour déployer, mettre à jour et administrer le logiciel antivirus dans toute l'entreprise.

Mises à jour par internet

La mise à jour automatique du logiciel antivirus par Internet est un concept attrayant pour les administrateurs système. Cependant, il a des implications au niveau de la sécurité de l'entreprise car le contrôle est décentralisé vers le fournisseur du logiciel antivirus.

Un logiciel antivirus se mettant automatiquement à jour via Internet est un concept très attrayant pour les administrateurs système (charge de travail nulle). Il a, cependant, de profondes implications dans la sécurité globale de l'entreprise car il décentralise de fait, vers le fournisseur du logiciel antivirus les processus de contrôle et de décision concernant l'installation du logiciel sur le réseau de l'entreprise. Peu d'entreprises en sont satisfaites, préférant interposer un spécialiste humain dans le processus. Le spécialiste peut alors décider ce qui doit être mis à jour, quand et comment le faire. Cela permet également de tester tout nouvel élément du logiciel avant de le déployer sur l'ensemble des plates-formes de l'entreprise

Administration

L'administrateur d'un logiciel antivirus, dans une installation importante, a besoin d'outils puissants pour communiquer efficacement avec le logiciel antivirus. (admin->logiciel->admin). Le logiciel a besoin d'être maintenu à jour (admin->logiciel) tandis que l'administrateur système doit bénéficier d'un retour d'informations d'alertes virales et autres informations sur l'état de la protection (logiciel->admin).

Trois techniques principales sont utilisées pour distribuer les mises à jour à travers le réseau de l'entreprise : push, pull et combinaison de push / pull. Chacune à ses avantages et ses inconvénients et la décision de la meilleure technique à adopter dépend considérablement de la structure du réseau, de la bande passante, de l'utilisation du réseau, etc.

Guérison d'une attaque virale

Si un virus réussit à pénétrer les défenses placées sur son chemin, l'entreprise doit avoir en place des procédures efficaces pour contenir l'infection sur un nombre minimum de PC.

Si l'impensable survient et qu'un virus réussit à pénétrer toutes les défenses placées sur son chemin, l'entreprise doit avoir mis en place des procédures efficaces pour contenir l'infection afin de minimiser le nombre de PC infectés ainsi que pour les restaurer en l'état avant infection. Ceci est un sujet relativement complexe sans solutions aisées.

Une entrée de virus se produit généralement quand le logiciel antivirus utilisé ne reconnaît pas un virus particulier. Avoir de bonnes relations avec le fournisseur du logiciel antivirus et savoir qu'il réagira en cas d'urgence sont des éléments importants de la stratégie antivirale de l'entreprise.

Le traitement des effets d'un virus qui a pénétré dans l'entreprise engendrera un coût bien plus élevé que celui de n'importe quel logiciel antivirus. La dépense principale sera le temps car il sera probablement nécessaire d'intervenir sur chaque station de travail infectée pour effectuer la désinfection et la restauration dans son état initial.

Si l'entreprise dispose de configurations logicielles standard, et de façon complémentaire, d'un logiciel de création d'image disque, la restauration des stations de travail infectées en leur état initial en est grandement facilitée.

Le présent document est disponible à l'adresse :
http://www.sophos.com/pressoffice/resources/fr/

SOPHOS

Sophos Plc • The Pentagon • Abingdon • Oxfordshire • OX14 3YP • UK • Tél +44 01235 559933 • Fax +44 01235 559935
Sophos Inc • 50-S Audubon Road • Wakefield • MA 01880 • USA • Tél 781 213 3456 • Fax 781 213 5466
Sophos Pty Ltd • Level 4 • 725 George Street • Sydney • NSW 2000 • Australie • Tél 02 9212 1600 • Fax 02 92121788
Sophos Sarl • 1-3 Place Victor Hugo • 92400 Courbevoie • France • Tél 01 41 99 94 20 • Fax 01 41 99 94 49
Sophos GmbH • IT Park • Am Hahnenbusch • 55268 Nieder-Olm • Allemagne • Tél 06136 91193 • Fax 06136 911940

www.sophos.com