

viruses

DDoS attacks

phishing

BHOs

Le petit livre vert de la sécurité Internet



keyloggers

trojans

pharming

backdoors

spyware

spam

worms



NORMAN®

www.norman.com

Le petit livre vert de la sécurité Internet

Norman ASA ne peut être considéré comme responsable des pertes ou dommages causés par l'utilisation de cette documentation, ou par des erreurs ou déficiences du produit.

Les informations de ce document peuvent faire l'objet de modifications sans préavis. Aucune partie de ce document ne peut être reproduite, transmise sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris les systèmes de photocopie, d'enregistrement ou de stockage d'informations, pour toute utilisation autre que l'usage personnel de l'acheteur, sans une autorisation écrite de Norman ASA.

Le logo Norman est une marque déposée de Norman ASA.
Les noms des produits cités dans ce document sont déposés et sont la propriété de leurs auteurs respectifs. Ils sont uniquement mentionnés à des fins d'identification.

Copyright © 2006 Norman ASA.
Tous droits réservés.

Table des matières

Une présence sécurisée sur Internet 4

Pour une utilisation mieux protégée.....	5
Pour les utilisateurs de réseaux sans fil.....	10

Quelques menaces courantes 12

Malware (code nocif).....	13
Virus informatique.....	13
Un virus peut apparaître sous différents formats.....	13
Ver.....	14
Cheval de Troie.....	15
Logiciels espions.....	15

Il existe plusieurs catégories d'espions.....	15
Logiciels publicitaires.....	17
Portes dérobées (Backdoor).....	17
Combinaisons de code nocif.....	18

Autres types de menaces.....	18
Spam.....	18
Phishing.....	19
Pharming.....	20
Attaques de refus de service répartis.....	20
Outils de mémorisation de la frappe.....	21
Objets tiers des navigateurs.....	21

Solutions proactives vs antivirus traditionnels 22

Solutions antivirus traditionnelles.....	22
Solutions proactives.....	23

Une présence sécurisée sur Internet

Il n'est pas simple de retracer l'évolution des crimes et de la sécurité informatique. Cependant, le besoin d'une sécurité efficace est évident et une connaissance de base des menaces les plus répandues est impérative. Le but de cette brochure est d'identifier : les menaces actuelles les plus cour-

antes, les méthodes employées par le code nocif pour affecter l'utilisateur et les mesures à prendre pour vous protéger.

Les virus informatiques et autres menaces contre la sécurité informatique sont un problème que nous connaissons bien depuis longtemps déjà. Le premier virus informatique a été découvert il y a 20 ans, et ce problème a évolué à une vitesse alarmante au fil des ans. Les premiers virus étaient conçus pour détruire

et bloquer les machines, mais les créateurs de programmes nocifs sont bien plus « raffinés » et leurs motivations sont surtout économiques. Les auteurs de virus les plus actifs sont souvent très organisés et ils utilisent des méthodes sophistiquées pour la propagation du code nocif. Les hackers peuvent voler vos informations privées pour des raisons économiques, ou ils peuvent contrôler vos habitudes de navigation sur Internet pour vous proposer des publicités personnalisées. Certains hackers collectent les adresses e-mail de votre système pour les vendre à d'autres sociétés.

REMARQUE

La criminalité informatique est de mieux en mieux organisée et crée des menaces plus sophistiquées.

Ils doivent arrêter leur connexion Bluetooth quand elle ne sert pas. La première chose que les intrus potentiels recherchent est le nom de réseau (SSID) – qui est introuvable lorsque la connexion est arrêtée.

L'autre danger potentiel est le risque de perte physique de données. Avec l'accroissement du nombre de personnes qui travaillent à domicile et hors des locaux de la société, le risque de vol physique se développe. Choisissez avec prudence les endroits où vous posez votre ordinateur portable et les mémoires externes.

Pour une utilisation mieux protégée

Internet vous expose à de nombreux dangers. Les utilisateurs de réseaux sans fil (WLAN) et de Bluetooth sont plus exposés aux menaces que les autres. Les adeptes des technologies mobiles doivent être particulièrement attentifs aux risques potentiels qui compromettent leur sécurité.

Des virus et des points de vulnérabilité ont déjà été détectés sur les téléphones portables. L'un des exemples est le virus Cabir, qui peut se répandre d'un téléphone à un autre.

Consultez également la section consacrée aux utilisateurs de réseaux sans fil.

Voici quelques conseils généra-



ques pour continuer à utiliser Internet en toute sécurité.

- 1 **N'invitez pas d'étrangers chez vous**
Soyez attentif à la configuration de votre PC avant de vous connecter sur Internet. Il est vital d'avoir conscience des ressources et dossiers partagés. Vous n'avez probablement pas l'intention de partager vos données privées avec la communauté Internet, ce qui aurait pour effet de les exposer d'une manière peu sûre. C'est une des failles sécuritaires les plus dangereuses des systèmes Windows, et elle est fréquemment exploitée par les intrus. Vous devez également arrêter votre PC lorsque vous ne l'utilisez pas.

- 2 **Utilisez des outils de « nettoyage » professionnels**
L'installation d'un logiciel antivirus est une mesure de sécurité obligatoire. Notez qu'il est également important de mettre à jour régulièrement votre logiciel antivirus, de préférence automatique-

ment lors de la connexion à Internet.

L'installation de produits contre l'espionnage et les publicités vous aidera à garder une machine propre et à éloigner les logiciels espions et publicitaires. Il est également judicieux de permettre à une société spécialisée dans la lutte antivirus d'analyser votre courrier entrant avant d'autoriser les messages à entrer sur votre système.

- 3 **Mettez régulièrement à jour votre système d'exploitation**
Le système d'exploitation est le cœur des activités de votre PC. Un système exempt de bogues à 100 % n'existe pas. Les auteurs de virus profitent souvent des bogues logiciels, aussi, veillez à télécharger et installer régulièrement toutes les mises à jour sécuritaires importantes.

- 4 **Soyez critique envers le « service postal »**
Appliquez quelques règles de bon sens. Si une seule des situations suivantes est

vraie, détruisez tout simplement le message :

- l'expéditeur est inconnu
- le champ objet n'a aucun sens
- le message contient un lien, et vous ignorez où il va vous mener sur Internet
- le message lui-même est suspect
- le message contient une pièce

REMARQUE

Les éditeurs de logiciels ne distribuent JAMAIS les mises à jour sécuritaires en masse par e-mail.

jointe suspecte

- le message semble provenir d'un éditeur de logiciels et contient un programme joint, supposé être une mise à jour sécuritaire. Les éditeurs de logiciels ne distribuent JAMAIS les mises à jour sécuritaires en masse par e-mail !

L'emploi de la fonction d'aperçu des clients de messa-



gerie est un risque sécuritaire. Vous devez la désactiver, donc être capable de supprimer les messages indésirables sans qu'il soit nécessaire de les ouvrir.

Un filtre anti-spam vous fera gagner beaucoup de temps et vous évitera les frustrations liées au nettoyage des messages indésirables, qui contiennent souvent du code nocif. Vous ne devez JAMAIS répondre aux messages de spam.

Vous devez crypter les informations confidentielles avant leur expédition.

5 Procurez-vous un « concierge » digne de confiance

Votre ordinateur dispose de nombreuses « entrées » (ports) dédiées à différentes tâches. Les ports ouverts constituent un accès illimité aux ressources de votre machine. Par exemple, le port 25 sert généralement au courrier, et c'est le plus utilisé

REMARQUE

Utilisez de discernement avant de révéler des informations personnelles sur Internet.

par les spammers. Le port 80 est l'entrée web normale. Le principal objectif d'un pare-feu personnel est de protéger votre ordinateur contre les « visiteurs » – c'est-à-dire les attaques – venant d'Internet. La plupart des pare-feu peuvent également être paramétrés pour bloquer les accès ayant certaines adresses pour origine.

6 Protégez les informations sensibles contre les « agences de filature »

Sécurisez le stockage de vos données confidentielles. Ceci est particulièrement important pour les machines portables, qui sont plus susceptibles de s'égarer. La meilleure solution consiste à utiliser des outils de cryptage capables de gérer les dossiers et les fichiers individuels.

7 Ne laissez personne entrer

Paramétrez votre navigateur web pour qu'il vous demande d'autoriser le « contenu actif ».

De nombreux sites web utilisent les scripts et autres types de programmes pour améliorer votre pratique de la navigation. Cependant, cette pratique constitue un risque sécuritaire, car elle implique l'exécution de code sur votre ordinateur. Soyez sélectif envers les sites web auxquels vous permettez l'accès à votre ordinateur, et soyez critique envers les programmes que vous téléchargez et les programmes peer-to-peer (P2P ou égal à égal).

8 Demandez conseil au personnel qualifié

Si vous travaillez à domicile ou si vous utilisez un ordinateur portable pour vos tâches quotidiennes, vous devez d'abord et avant tout vous familiariser avec les consignes de votre employeur et les réglementations applicables à la sécurité informatique dans ces situations. Vous éviterez bien des problèmes en consultant le personnel informatique de votre société.



- 9 Évitez de divulguer des informations vous concernant
Ne révélez JAMAIS d'informations de nature personnelle si ce n'est pas absolument nécessaire. Il est judicieux d'utiliser des adresses e-mail distinctes pour formuler des demandes différentes.

- 10 Sauvegardez les informations pertinentes
Les effacements de données peuvent se produire par accident, par activité virale ou d'un autre code nocif, ou par l'action de personnes malfaisantes qui y ont accès. Sauvegardez régulièrement vos données vitales. Les fichiers de données les plus précieux sont ceux dont la création vous a demandé beaucoup de temps et d'efforts. Les logiciels et autres fichiers système peuvent être réinstallés s'ils sont endommagés.

Pour les utilisateurs de réseaux sans fil

Les utilisateurs de réseaux sans fil (WLAN) doivent prendre des précautions supplémentaires pour rester protégés. Un réseau sans fil est simple et efficace pour ses utilisateurs, mais il est également très accessible, donc vulnérable aux intrus et autres utilisateurs illégitimes. Si vous ne protégez pas ou ne verrouillez pas votre système

REMARQUE

Éteignez toujours votre ordinateur lorsqu'il ne sert pas.

réseau, il est accessible à votre insu et peut être employé pour des usages illégaux, par exemple,

pour distribuer du spam. Dans le pire scénario, des intrus peuvent accéder à votre ordinateur.

Voici quelques conseils pour les utilisateurs de réseaux sans fil :

Protégez votre réseau avec un code d'accès

La documentation vous indique la marche à suivre. C'est une procédure simple à la portée de tous ; il suffit d'entrer le bon code pour accéder au



réseau.

Lorsque vous activez un code d'accès, vous avez l'assurance que seuls les ordinateurs munis de la bonne « clé » peuvent accéder à votre réseau personnel, et que le trafic du réseau est crypté. Les méthodes de cryptage les plus courantes sont WEP et WPA.

Utilisez des programmes antivirus

Comme tous les utilisateurs de

réseau, les utilisateurs de réseaux sans fil doivent être protégés par un programme antivirus. Les réseaux sans fil sont particulièrement vulnérables, et les logiciels antivirus vous protègent des virus, vers, chevaux de Troie et autres codes nocifs. Les meilleurs programmes sont les solutions antivirus proactives, qui ne reposent pas sur la technologie classique basée sur les signatures. Les solutions antivirus proactives détectent

les virus nouveaux et inconnus, protégeant ainsi votre ordinateur plus efficacement.

Utilisez des programmes contre les espions et les publicités

Ces programmes suppriment les espions et empêchent le contrôle de votre activité Internet.

Cryptez vos données personnelles

Vous ne souhaitez pas partager vos données avec tout le monde. Le meilleur moyen d'entretenir

vos confidentialité est de crypter vos fichiers. Vous pouvez installer des programmes de cryptage et chiffrer vos messages, vos fichiers personnels, vos informations d'entreprise, vos données confidentielles et vos pièces jointes de messagerie.

Quelques menaces courantes

Plusieurs menaces peuvent vous nuire en tant qu'utilisateur. Voici les plus courantes :

Malware (code nocif)

« Malware » est le terme générique qui désigne le code nocif conçu pour perturber ou détruire un système informatique. Vous trouverez ci-dessous une brève description de la plupart des types de code nocif courants.

1 Virus informatique

Un virus est un programme conçu pour se copier et se propager, généralement en s'attachant aux applications.

Lorsqu'une application infectée est exécutée, elle peut infecter d'autres fichiers. Une intervention humaine est nécessaire pour qu'un virus se propage sur les machines et les systèmes. Ceci peut se faire par téléchargement de fichiers, échange de disquettes et de clés USB, copie de fichiers vers ou depuis un serveur, ou envoi de pièces jointes infectées par courrier électronique.

REMARQUE

Les meilleurs programmes sont les solutions antivirus proactives, qui ne reposent pas sur la technologie classique basée sur les signatures..

Un virus peut apparaître sous différents formats :

Virus de fichier :

Un virus de fichier est attaché à un fichier programme, en principe, un fichier .EXE ou .COM. Il emploie différentes techniques pour infec-

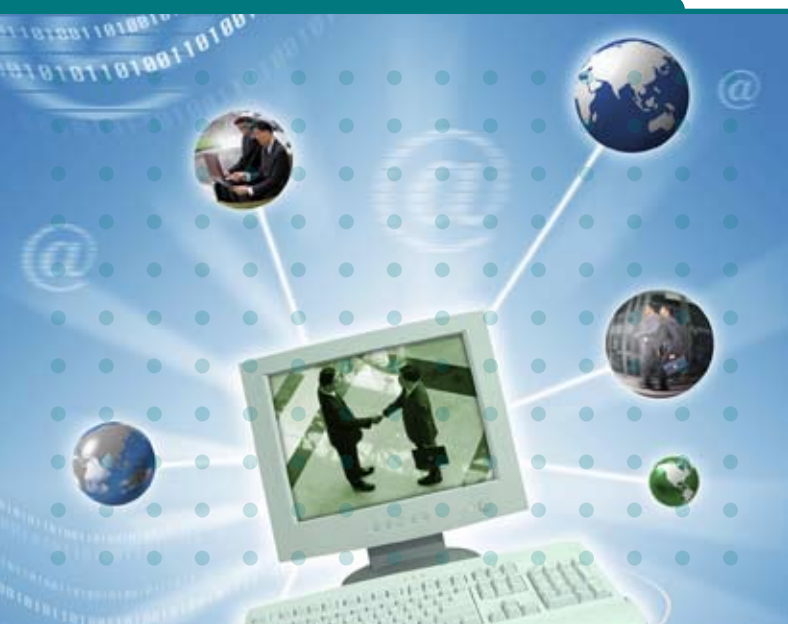
ter d'autres fichiers programmes. Ce type de virus peut être transféré vers/depuis tous les supports de stockage (depuis un CD-ROM) et sur un réseau.

Virus système :

Les virus systèmes (aussi appelés virus d'amorçage) sont souvent présents sur les disquettes à l'insu de l'utilisateur. Lorsque l'utilisateur démarre ou redémarre l'ordinateur, le virus système infecte le secteur d'amorçage principal (MBS) si le disque infecté est dans le lecteur de disquettes.

Virus dropper :

Un dropper est un programme créé ou modifié pour « installer » un virus sur l'ordinateur cible. Le drop-





per est comme l'enveloppe dans laquelle se trouve le virus. L'infection est effective lorsque le virus s'installe sur l'ordinateur. C'est le virus proprement dit qui se propage, et non le dropper. Le dropper peut avoir un nom comme LISEZMOI.exe, qui attire la curiosité de l'utilisateur et l'incite à ouvrir le fichier. En réalité, un dropper est un cheval de Troie qui tente d'installer un virus.

Virus de macro :

Les virus de macros peuvent être stockés dans tous les types de fichiers utilisant un langage macro, tels que Word, Excel, Access et Word-Pro. Ce virus se propage d'un document à un autre, et l'infection se produit lors de l'ouverture du document.

2 Ver

Un ver de réseau infecte les autres ordinateurs et se propage automatiquement

dans un réseau sans intervention de l'utilisateur. Le fait qu'aucune intervention humaine ne soit nécessaire à sa propagation lui permet de se répandre plus rapidement qu'un virus.

Les vers sont transférés par courrier, souvent à l'insu de l'utilisateur infecté. L'un des comportements caractéristiques du ver de message est qu'il s'envoie à toutes les adresses qu'il trouve sur le PC infecté. Le message semble alors avoir été émis par l'utilisateur infecté, qui est généralement une personne de votre connaissance, ce qui peut vous faire baisser la garde.

3 Cheval de Troie

Un cheval de Troie semble ne présenter aucun danger à première vue. Il peut même sembler utile et vous incite par cette ruse à l'employer. Mais alors, pendant que le programme fonctionne, il ouvre une porte dérobée, exposant votre ordinateur au piratage.

REMARQUE

Les programmes d'espionnage sont, pour la plupart, très difficiles à éliminer..

4 Logiciels espions

Les espions (spyware) sont une forme de technologie employée pour collecter des informations sur une personne ou une société à leur insu. Les espions sont souvent installés secrètement, soit pendant le téléchargement d'un fichier ou lorsque vous cliquez sur une publicité. Les espions peuvent aussi être implantés d'origine sur votre matériel.

Il existe plusieurs catégories d'espions :

Réseaux publicitaires :

La colonne vertébrale de l'espionnage est constituée par les réseaux publicitaires qui rémunèrent, sur la base des téléchargements, les éditeurs de jeux, d'utilitaires et de lecteurs de musique et

vidéo pour inclure leurs programmes d'affichage publicitaire.

Traqueurs :

Désigne un certain nombre de programmes permettant aux réseaux publicitaires de fonctionner sur les machines de bureau. Ils sont parfois livrés avec des programmes populaires et sont présentés, au cours de l'installation, comme des extensions très attractives à l'hôte du cheval de Troie. Ils collectent tous

des informations.

Backdoor Santas:

Programmes autonomes dont l'approche est similaire à celle des chevaux de Troie, mais sans liens vers les réseaux publicitaires, et collectant des informations sur l'utilisateur.

Cookies:

Certains navigateurs continuent à envoyer les cookies existants, même après leur désactivation dans les

paramètres. Vous devez supprimer manuellement les éventuels fichiers de cookies de votre système pour éviter d'être « suivi » par des tiers, des réseaux, ou des fournisseurs de logiciels espions ou publicitaires.

Les programmes espions peuvent réinitialiser votre signature automatique, désactiver ou contourner les fonctions désinstallées, surveiller ce que vous frappez au clavier, analyser les fichiers de votre lecteur, changer votre page d'accueil et, bien entendu, afficher des publicités, que vous soyez connecté ou non.

Ils peuvent lire, écrire et supprimer des fichiers, et même reformater votre disque dur,

pendant qu'ils envoient un flux d'informations à la personne qui les contrôle. Une fois qu'ils sont installés, il est très difficile de supprimer ces programmes en employant des méthodes normales. Ils laissent souvent des composants derrière eux pour continuer à contrôler votre

REMARQUE

Les sondages montrent que plus de 50 % des messages reçus sont du spam.

comportement et se réinstaller par eux-mêmes.

Les espions ne sont pas intégrés dans les logiciels officiels, mais ils peuvent être installés sur votre machine pendant vous surfez sur Internet !

5 Logiciels publicitaires

Les logiciels publicitaires (adware) sont étroitement liés aux logiciels espions ; nombre de ces derniers sont implantés pour permettre l'exécution de programmes publicitaires. Ces logiciels affichent des publicités, le plus souvent sous la forme de fenêtres de type 'pop-up'.

Elles sont parfois personnalisées, sur la base de vos habitudes sur Internet ou de votre comportement général.

6 Portes dérobées (Backdoor)

C'est un programme qui ouvre, sur votre ordinateur, un accès que vous n'avez pas l'intention d'autoriser. Il peut donc permettre un accès à distance, con-



tournant les dispositifs d'authentification que vous avez mis en place pour la sécurité.

Le backdoor ouvre, en général, certains ports auxquels l'auteur tente de se connecter. Si quelqu'un « réussit » à infecter plusieurs ordinateurs avec ces programmes, il peut les analyser intégralement afin de les identifier et de les employer pour des tâches spécifiques, par exemple, pour en faire des zombies (voir ci-dessous).

7 Combinaisons de code nocif

R é c e m m e n t , nous avons constaté l'émergence rapide de code nocif combinant plusieurs des menaces mentionnées ci-dessus.

Des vers sont employés pour répandre des virus qui installent des portes dérobées et des espions ; des logiciels espions dirigent des publicités d'un type spécifique vers votre machine ou se servent de votre PC comme serveur

REMARQUE

Les cibles favorites du phishing sont les utilisateurs de services bancaires en ligne.

de messagerie pour envoyer du SPAM (voir ci-dessous), etc.

Les différences entre ces types de menaces deviennent plus floues.

Autres types de menaces :

1 Spam

Le spam peut être défini comme étant des messages indésirables expédiés aléatoirement par lots. C'est une méthode extrêmement efficace et économique de marketing des produits. La plupart des utilisateurs sont exposés au spam, ce qui est confirmé par des sondages qui montrent que le spam constitue plus de 50 % de tous les messages électroniques reçus.

Le SPAM n'est pas une menace directe, mais le volume de messages générés et le temps perdu pour les utilisateurs à le signaler et le supprimer en fait un élément très ennuyeux pour les utilisateurs d'Internet.

Le Spam est également employé pour propager les différents types de menaces expliqués ci-dessus.

2 Phishing

Le phishing est une acquisition frauduleuse d'informations personnelles sensibles – telles que les mots de passe, les éléments d'une carte de crédit – par le biais de messages à l'aspect officiel d'entités dignes de confiance demandant des informations légitimes. Les cibles les

plus populaires sont les utilisateurs des banques en ligne et des sites d'enchères.

Les 'adeptes' de cette technique envoient généralement un grand nombre de courriers (spam) à leurs victimes potentielles. Ces messages dirigent le destinataire vers une page web qui semble être celle de sa banque en ligne, par exemple, mais, en réalité, elle capture les informations du compte pour un emploi illégitime.



3 Pharming

Le pharming est une forme de phishing très sophistiquée. Ses 'adeptes' exploitent le système DNS, c'est à dire le système qui permet de transformer l'adresse d'un ordinateur en adresse de protocole Internet (IP). Ce faisant, les « pharmers » peuvent créer, par exemple, un site factice ressemblant à un vrai – comme un site de banque en ligne – puis collecter des informations que les utilisateurs pensent donner à leur véritable

banque. Auparavant, le pharming était appelé « empoisonnement DNS ».

4 Attaques de refus de service répartis

Plusieurs sites web haut de gamme ont été attaqués par ces types de refus de service. (DDoSAttacks). Ces attaques proviennent souvent de plusieurs robots qui envoient en même temps un fort volume de requêtes à une machine particulière du réseau. Par conséquent, la surcharge

étrangle le réseau ou la machine et empêche son utilisation légitime. Ces assaillants – les robots – sont souvent des ordinateurs sur lesquels des portes dérobées sont ouvertes dans ce but particulier. La plupart des utilisateurs de ces ordinateurs ne sont sans doute pas au courant de cet état de fait, et les machines infectées sont souvent appelées des « zombies ».

REMARQUE

Norman propose plusieurs produits garantissant votre sécurité sur Internet. Pour en savoir plus, consultez www.norman.com

Elles sont paramétrées pour être prêtes à agir dès que le pirate appuie à distance sur la bonne touche. Votre machine peut être utilisée pour accomplir des actions illégales.

5 Outils de mémorisation de la frappe

Les outils de mémorisation de la frappe enregistrent la frappe des utilisateurs, soit sur une application spécifique, soit, plus généralement sur tout le système. Ces outils permettent aux malfaiteurs de rechercher des portions d'information

spécifiques, qui peuvent servir aux usurpations d'identité, aux vols de propriété intellectuelle ou aux actions frauduleuses.

Cette méthode permet de voler des numéros de cartes de crédit, des mots de passe et autres informations sensibles. Ils peuvent être installés sur votre ordinateur par le biais de pièces jointes ou, plus fréquemment, par des virus ou des vers. Certains sites web pratiquent aussi ce type d'installation sur la machine du visiteur, mais leur durée de vie n'est, généralement, pas très longue.

6 Objets tiers des navigateurs / nettleserhjelpere

Les objets de navigateur (Browser Helper Objects ou BHO) sont des modules destinés à Internet Explorer. Un BHO a un accès total à tout ce qui se passe dans la session de navigation en

cours ; il peut voir les pages qui s'affichent, leur mode d'affichage et il peut (ce qu'il fait) en modifier les bords avant leur apparition. Malgré leur mauvaise réputation, les BHO ont souvent une utilisation légitime, telles que le téléchargement, l'affichage de conseils, et la suppression des popup.

Solutions proactives vs antivirus traditionnels

La différence entre les solutions antivirus traditionnelles basées sur les signatures et les technologies proactives peut être la vie ou la mort de vos systèmes informatiques.

Les solutions proactives sont capables de détecter les nouvelles menaces dont les solutions à base de signatures ne peuvent pas se charger. Les auteurs de virus devenant de plus en plus performants et les nouvelles variantes de virus inondant le web,

les solutions traditionnelles ne suffisent plus. Le besoin de solutions proactives est urgent.

Voici une brève description de ces deux technologies.

Solutions antivirus traditionnelles

Avec les solutions antivirus traditionnelles à base de signatures, un virus doit être découvert par quelqu'un, identifié comme

étant un virus et analysé avant que l'industrie antivirus puisse offrir une solution adaptée.

Seulement après ces étapes initiales nécessaires, un fichier de signature virale peut être publié. En moyenne, la distribution d'un fichier de signatures mis à jour demande entre 6 et 24 heures. Ce fichier sert à la mise à jour du programme antivirus de chaque client, qui pourra alors détecter et stopper les tentatives d'infection à partir de ce moment. Manifestement, la période séparant la publication du virus et la distribution du fichier de signatures mis à

REMARQUE

Le solutions antivirus proactives peuvent détecter les virus nouveaux et inconnus..

jour est critique pour les utilisateurs, qui restent exposés au risque potentiel d'infection.

Solutions proactives

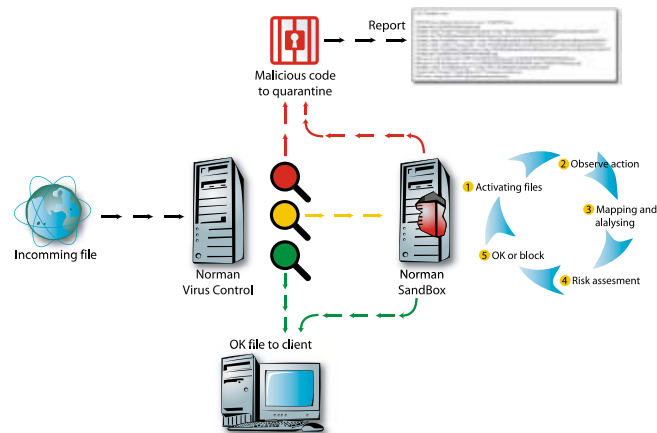
Une solution antivirus proactive détecte les fichiers nouveaux et inconnus sans faire appel aux fichiers de signatures mis à jour. Norman propose une solution proactive unique – Norman Sandbox. C'est, en réalité, un environnement informatique totalement simulé, isolé du véritable

REMARQUE

Vous pouvez tester gratuitement vos fichiers dans l'espace Norman SandBox Center. Testez cette fonction sur <http://sandbox.norman.no/>

environnement de traitement.

Tous les fichiers entrants accèdent à un environnement factice (sandbox). Là, les fichiers sont contrôlés et, en cas de découverte d'actions suspectes, le fichier est stoppé et l'accès au véritable environnement lui est refusé. Si son comportement est normal, il peut accéder à l'ordinateur. Les attaques de type Jour Zéro – celles qui se produisent le jour même où une vulnérabilité logicielle est révélée, et qui entraînent la création d'un programme exploitant cette faille – sont une menace croissante. Seules les solutions proactives peuvent se charger de cette menace.



Norway

Norman ASA
Strandvn. 37
Postboks 43
1324 Lysaker
Tel: +47-67 10 97 00
norman@norman.no
www.norman.no

Denmark

Norman Data Defense Systems A/S
Blangstedgårdsvej 1
5220 Odense SØ
Tel: +45-63 11 05 08
info@normandk.com
www.norman.com/dk

Sweden

Norman Data Defense Systems AB
Västgötegatan 7
SE-602 21 Norrköping
Tel: +46-011-230 330
sales.se@norman.no
www.norman.com/se

UK

Norman Data Defense Systems (UK) Ltd
15 Linford Forum
Rockingham Drive
Linford Wood
Milton Keynes
MK14 6LY
Tel: +44 1908 678496
norman@normanuk.com
www.normanuk.com

Germany

Norman Data Defense Systems GmbH
Gladbecker Strasse 3
40472 Düsseldorf
Germany
Tel: +49-211 586 990
norman@norman.de
www.norman.de

Switzerland

Norman Data Defense Systems AG
Münchensteinerstrasse 43
4052 Basel
Switzerland
Tel: +41-61 317 25 25
norman@norman.ch
www.norman.ch

Benelux

Norman / SHARK BV
Postbus 159
2130 AD Hoofddorp
The Netherlands
Tel: +31-23 789 02 22
info@norman.nl
www.norman.nl

Italy

Norman Data Defense Systems
Centro Direzionale Lombardo
Via Roma, 108
20060 Cassina de'Pecchi (MI)
Tel: +39 02 951 58 952
Fax: +39 02 951 38 270
www.normanit.com

Spain

Norman Data Defense Systems
Camino Cerro de los Gamos, 1, Ed. 1
28224 Pozuelo de Alarcón. Madrid
Tel: +34 91 790 11 31
Fax: +34 91 790 11 12
www.normandata.es

France

Norman Data Defense Systems
8 Rue de Berri
75008 Paris
Tel: +33 1 42 99 94 14
Fax: +33 1 42 99 95 01
info@norman.fr



NORMAN®

www.norman.com