FROST & SULLIVAN

UNE APPROCHE PLUS SÉCURISÉE FACE AUX MENACES WEB DYNAMIQUES

Livre blanc par Frost & Sullivan
Parrainé par Google

Analyste et auteur : Terrence Brewton, Analyste, Sécurité des réseaux

"Former des partenariats avec des clients en vue de créer des stratégies de croissance innovantes"

TABLE DES MATIÈRES

INTRODUCTION

Quelle que soit leur taille, les organisations dépendent d'Internet pour leurs activités commerciales, l'accès au Web étant en effet devenu incontournable. Or, selon une estimation du FBI (Bureau fédéral d'investigation des États-Unis), le piratage informatique coûte chaque année aux entreprises américaines environ 67,2 milliards de dollars.[1] Contrairement à ce que l'on pourrait croire, ce ne sont plus seulement les sites traditionnellement malveillants (tels que les sites pornographiques) qui sont utilisés pour exploiter les vulnérabilités des internautes peu suspicieux. Il s'agit de plus en plus de sites a priori anodins tels que MySpace ou YouTube, des clients Web ou encore des systèmes de messagerie instantanée et de messagerie Web.

Il est inquiétant, bien que peu étonnant, de savoir que ces pirates sont affiliés à des syndicats du crime organisé. De tels groupes profitent en effet de l'expertise de "hackers" talentueux pour s'immiscer dans les failles des réseaux d'entreprise et exploiter les informations cruciales afin de les voler et de les revendre. Les logiciels malveillants les plus récents qui circulent actuellement sont capables de s'adapter rapidement aux contre-mesures anciennes et actuelles. Ils peuvent ainsi les éviter et quelques secondes leur suffisent ensuite pour infecter une entreprise. C'est pourquoi la stratégie de protection des entreprises qui auparavant s'appuyait sur des pare-feu, des correctifs, des listes de blocage d'URL et des signatures antivirus n'est plus efficace aujourd'hui pour faire face aux menaces nées sur le Web. Une nouvelle approche qui puisse répondre aux menaces dynamiques en temps réel est indispensable pour sécuriser ce canal de communication essentiel.

PROTÉGER L'ENTREPRISE : UN PARCOURS SEMÉ D'EMBÛCHES

Protéger une entreprise est de nos jours synonyme de nombreux défis. Même s'il est entendu qu'il s'agit d'une priorité de premier ordre, de nombreuses idées reçues subsistent encore au sein de l'entreprise. Ces croyances peuvent être pernicieuses, car nombre d'entre elles contribue à tort à créer un sentiment de sécurité.

Les technologies d'hier sont inefficaces contre les logiciels malveillants d'aujourd'hui

Les technologies de filtrage plus anciennes, telles que les serveurs proxy et les filtres d'URL, sont efficaces pour mettre en œuvre des stratégies d'utilisation acceptable : elles empêchent en effet des employés de consulter des sites à caractère pornographique ou incitant à la haine, et limitent ainsi le risque de procès souvent coûteux. De nos jours cependant, les filtres d'URL ne garantissent pas la sécurité, car ils reposent essentiellement sur une analyse passée et non sur une analyse en temps réel. Ils sont tout simplement incapables de protéger l'entreprise contre des sites Web malveillants et dynamiques qui peuvent modifier leur contenu instantanément.

Aujourd'hui, les pirates informatiques sont plus soucieux de leur portefeuille que de leur notoriété publique. Ainsi, pour éviter d'être repérés et pour augmenter leurs revenus, les pirates et autres créateurs de logiciels malveillants développent des outils s'appuyant sur

1. Joris Evers : "La criminalité informatique coûte 67 milliards de dollars", selon le FBI.

Sites pornographiques et autres URL malveillantes : entre mythe et réalité

MYTHE : SI JE NE CONSULTE PAS DE SITES À CONTENU PORNOGRAPHIQUE, SITES DE JEUX OU DE PIRATAGE, JE NE M'EXPOSE À AUCUN LOGICIEL MALVEILLANT.

RÉALITÉ : DES SITES DE GRANDES ENTREPRISES TELLES QUE TOM'S HARDWARE ET AMD ONT PAR LE PASSÉ ÉTÉ PIRATÉS ET D'AUTRES SOCIÉTÉS IMPORTANTES LE SERONT DANS LE FUTUR.

MYTHE : MON FILTRE D'URL BLOQUE TOUS LES SITES WEB MALVEILLANTS. JE SUIS DONC SÛR QUE TOUS LES SITES AUXQUELS JE SUIS AUTORISÉ À ACCÉDER NE SONT PAS INFECTÉS.

RÉALITÉ : LES FILTRES D'URL NE SONT PAS MIS À JOUR EN TEMPS RÉEL ALORS QUE LES EXPLOITS « ZERO-DAY » SONT EUX PUBLIÉS CHAQUE JOUR SUR LE WEB. C'EST POURQUOI N'IMPORTE QUEL SITE PEUT ÊTRE INFECTÉ ET IL EST SOUVENT TROP TARD QUAND VOUS VOUS EN RENDEZ COMPTE.

MYTHE : SI JE DISPOSE DES CORRECTIFS ET DES MISES À JOUR ANTIVIRUS LES PLUS RÉCENTS, MON ENTREPRISE EST PROTÉGÉE.

RÉALITÉ : BIEN QUE LES CORRECTIFS LOGICIELS ET SIGNATURES ANTIVIRUS LES PLUS RÉCENTS PROTÈGENT LES ENTREPRISES CONTRE LES PROBLÈMES CONNUS, ILS NE LES PROTÈGENT PAS CONTRE LES EXPLOITS « ZERO-DAY » ET LES VIRUS INCONNUS.
CES DERNIERS SONT EN EFFET DIFFICILES À DÉTECTER, ET UNE FOIS QU'ILS LE SONT, IL FAUT DES JOURS VOIRE DES SEMAINES POUR DÉVELOPPER ET PUBLIER UN CORRECTIF OU UNE SIGNATURE ANTIVIRUS.

des exploits « zero day » et des vulnérabilités inconnues. Très souvent, ces vulnérabilités et outils malveillants ne sont pas partagés publiquement, pas même au sein de la communauté des hackers, et lorsque les fournisseurs découvrent et publient enfin des correctifs et signatures antivirus, les pirates ont déjà exploité et tiré parti des réseaux vulnérables.
Même si, de nos jours, les attaques de virus à grande échelle se font rares, des sites Web de renom continuent de faire l'objet de piratages. Par exemple :

- Le site Web du stade Dolphin (Miami) a été la cible d'un pirate avant le Super Bowl 2007. En effet, le site Web a renvoyé des milliers de visiteurs vers des sites de phishing et autres sites malveillants.

- En 2007, Tom's Hardware, un site Web grand public portant sur les technologies, a infecté ses utilisateurs pendant plusieurs jours avec des chevaux de Troie qui ont eu pour effet de voler les informations personnelles contenues sur les ordinateurs de ces internautes.

Menaces Internet : un paysage en constante évolution

Menaces internes

Il est courant de penser que les attaques internes sont systématiquement lancées par des employés mécontents ou ayant fait l'objet d'un licenciement. Rien n'est plus faux. La majorité des menaces internes sont le fait de travailleurs efficaces qui, à leur insu, contournent des mesures de sécurité pour télécharger des photos de famille, écouter leur émission Web préférée ou cliquer sur un lien vers une carte de vœux. En ne tenant pas compte des contrôles et des mesures de sécurité, ils utilisent sur le réseau des applications nécessitant une bande passante très importante, de même qu'un nombre inquiétant d'applications malveillantes. Autant d'éléments susceptibles de compromettre le réseau. Les menaces internes peuvent s'avérer très coûteuses pour une organisation et on estime que pour une société de taille moyenne, les frais engagés pour résoudre ce type de menaces avoisinent par an les 14 millions de dollars.[3]

La plupart des spécialistes en sécurité informatique s'accordent à dire que l'éducation à la sécurité combinée à des technologies de filtrage de contenu en temps réel constitue la méthode la plus efficace pour se protéger contre les menaces internes et externes qui exploitent les vulnérabilités des entreprises.

Attaques par évasion

Une autre menace de plus en plus courante est l'utilisation de méthodes d'attaque évasives. Cette nouvelle technique est utilisée par les pirates pour contourner la technologie de filtrage par signatures et bases de données d'URL. Les pirates informatiques configurent des serveurs Web qui proposent au visiteur des annonces ou du contenu légitimes. Cependant, ces annonces ou ce contenu contiennent un logiciel malveillant qui est injecté dans l'ordinateur de l'internaute, à la première visite. Lors des visites suivantes, l'utilisateur

Comme l'a souligné le rapport Google intitulé "The Ghost in the Browser" [2] il existe quatre méthodes d'infection à partir de sites Web :

1) Sécurité du serveur Web : c'est dans ce cas la vulnérabilité d'un ite Web qui est exploité par un pirate.
2) Contenu fourni par l'utilisateur : les blogs, profils, ou ommentaires modifiés par l'utilisateur cachent bien souvent autre chose.
3) Publicité : les liens vers des publicités sont en réalité des scripts Javascript qui renvoient vers des scripts Javascript qui eux-mêmes renvoient vers d'autres scripts Javascript… tout au long de la chaîne, ces scripts peuvent être compromis.
4) Widgets tiers : les widgets sont des liens externes vers des applications que des webmasters utilisent pour améliorer l'utilité ou la valeur de leur site Web (compteurs de visites, calculatrices, etc.)

Quelle que soit la technique utilisée, la tendance actuelle qui se dégage est la suivante : un volume de contenu de plus en plus important est généré par des sources de plus en plus nombreuses. Cette évolution a pour effet de fragiliser la chaîne de confiance qui au final se brise pour laisser entrer des virus, des enregistreurs de frappe et des chevaux de Troie sur votre réseau. Notons toutefois que vos utilisateurs n'ont, en aucun moment violé votre politique d'utilisation.

2. Rapport Google "Ghost in the Browser 2007"
3. Étude annuelle 2006 : Cost of Data Breach, Ponemon Institute

n'est pas infecté car son adresse IP a été enregistrée. En outre, cette technologie échappe aux procédés de filtrage et aux services de réputation car elle identifie l'adresse IP et les méthodes heuristiques du service, et présente un contenu légitime. Ainsi, les pirates évitent de se retrouver sur des listes noires ou grises, ce qui leur permet de poursuivre leur mission d'infection.

Menaces mixtes

Les menaces multi-canaux ou mixtes sont des attaques de réseau présentant les caractéristiques des vers et des virus informatiques.Cette méthodologie mixte exploite les vulnérabilités connues ou non documentées des systèmes ou des réseaux informatiques. Avant de déployer leurs méthodologies d'attaque, les pirates téléchargent les signatures de virus les plus récentes et simulent leurs méthodologies pour vérifier la rapidité ou la méthode avec laquelle l'attaque sera détectée. Cette simulation leur fournira les informations nécessaires pour perfectionner leurs attaques. Le virus Storm Worm est un exemple de ce type d'attaque : il comprend de nombreuses variantes qui ont frappé le réseau Internet fin 2006, et a continué d'évoluer jusqu'en septembre 2007.

Web 2.0

La croissance et la puissance des sites de réseaux sociaux, des wikis et des blogs sont essentiellement dues au Web 2.0, terme utilisé pour désigner le contenu riche fourni par les utilisateurs. Cette technologie présente cependant de nouvelles vulnérabilités qui peuvent vous exposer sur votre lieu de travail à des attaques Internet. Le Web 2.0 repose dans une large mesure sur des modèles de programmation légers tels que le langage XML (Extensible Markup Language), très vulnérable au piratage de session. Les structures asynchrones JavaScript et XML (Ajax), autre technologie Web 2.0 populaire, présentent de graves défauts en matière de codage qui pourraient facilement être exploités par un pirate expérimenté grâce à des méthodologies d'attaque évasives. En décembre 2006, le site MySpace a supprimé des centaines de profils d'utilisateur infectés par un ver qui exploitait une vulnérabilité Ajax pour rediriger ces internautes vers des sites de phishing les invitant à confirmer leurs nom d'utilisateur et mot de passe.

QUAND LES SERVICES À LA DEMANDE PERMETTENT DE RELEVER LES DÉFIS DU FILTRAGE DE CONTENU

Face à la mutation progressive du paysage des menaces, sous l'influence de pirates audacieux qui développent de nouvelles attaques ultrarapides pour rendre visibles les vulnérabilités d'une entreprise, les responsables informatiques ne peuvent plus compter sur les technologies actuelles, comme le filtrage d'URL ou les solutions basées sur des applications. Qui plus est, la majorité des mécanismes de défense de réseau tels que les pare-feu, les UTM et autres technologies de filtrage de réseau est incapable de contrecarrer et d'empêcher les attaques dues à l'absence de signatures, de correctifs et de listes de blocage d'URL à jour. Le coût de propriété en termes de frais d'abonnement, de surplus de matériel et de main d'œuvre requise pour assurer la maintenance des technologies matérielles est tout simplement faramineux. Ainsi, un service hébergé ou à la demande peut constituer un moyen efficace de parer les menaces Internet tout en maintenant les coûts de propriété à un niveau minimum.

Il s'avère que les services à la demande constituent l'une des approches les plus efficaces pour les entreprises qui souhaitent une solution flexible de défense contre des menaces en constante évolution. Elles peuvent ainsi espérer réguler l'utilisation abusive de la bande passante pour empêcher toute fuite de données. Les responsables des technologies de l'information et des services informatiques doivent prendre en compte les points suivants lorsqu'ils envisagent d'intégrer leur réseau à un service géré :

- Le service doit s'intégrer facilement à celui de l'entreprise et entraîner un temps d'arrêt nul ou très court.
- Le service doit réduire le coût total de propriété en termes de matériel et de main d'œuvre.
- Le service doit fournir une protection évolutive contre les menaces connues et inconnues, notamment les exploits « zero-day ».
- Les outils de gestion doivent être disponibles en toute sécurité 24h/24 et 7j/7, n'importe où dans le monde.

Analyse de la fonctionnalité de technologie de filtrage du Web

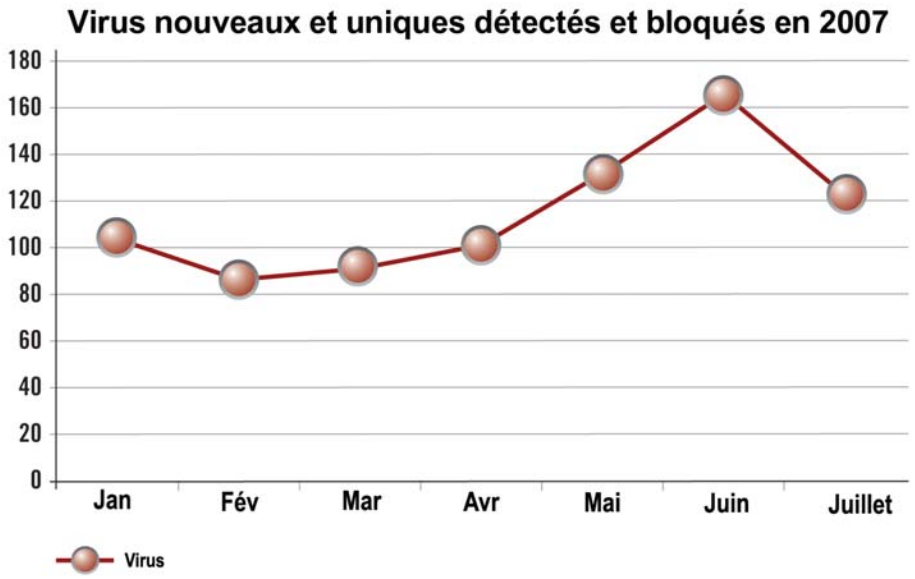
	Solutions URL	Solutions UTM	Solutions basées sur des applications	Solutions à la demande
Efficacité contre les vulnérabilités connues et les exploits « zero day »	Faible	Modéré	Modéré	Élevé
Fournit des mises à jour sur les menaces en temps réel	Non	Non	Non	Oui
Automatise les restrictions de navigation	Oui	Oui	Oui	Oui
Coût de propriété	Modéré	Élevé	Élevé	Faible
Niveau de mise en œuvre initial, assistance continue et coûts de main d'œuvre	Modéré	Élevé	Modéré	Faible
Évolutivité	Modéré	Faible	Faible	Élevée

SÉCURITÉ WEB POUR L'ENTREPRISE DE GOOGLE

La sécurité Web pour l'entreprise de Google, fournie par Postini, offre aux entreprises souhaitant se protéger contre les attaques Web une passerelle à la demande et sécurisée. En utilisant le service à la demande de Google, une entreprise peut profiter des avantages suivants :

- **Protection en temps réel**
  La sécurité Web pour l'entreprise de Google fournit une protection dynamique et en temps réel 24h/24 et 7j/7 par une analyse du trafic destinée à détecter les logiciels malveillants avant qu'ils ne pénètrent dans le réseau ou les informations sensibles avant qu'elles ne quittent ce même réseau. La solution de détection des menaces de Google dépasse le simple cadre du déploiement de correctifs et de mises à jour de signatures. Le service utilise le système d'analyse heuristique contrôlé de l'ordinateur pour détecter les activités "zero-day" et déployer des contre-mesures dans les minutes ou les heures qui suivent (et non plusieurs jours après). Il s'oppose ainsi aux technologies traditionnelles basées sur les signatures qui requièrent l'apparition de l'attaque pour que des contre-mesures puissent être développées.

Virus nouveaux et uniques détectés et bloqués en 2007



Source : Postini

- **Filtrage d'URL de première classe**
  La sécurité Web pour l'entreprise de Google permet d'accéder à un contenu Web professionnel en adaptant la liste d'URL aux besoins de l'entreprise et bloque l'accès aux autres sites. Ainsi, le service réduit le risque d'entrée de contenu offensant et à forte utilisation de bande passante sur le réseau. En réduisant ce risque, le service limite les éventuels procès et le coût associé à une bande passante supplémentaire.

Frost & Sullivan

Un antivirus installé sur votre poste de travail ou au niveau de la passerelle vous protège-t-il vraiment ?

Le graphique ci-contre affiche le nombre de virus nouveaux et uniques que le service de sécurité Web pour l'entreprise de Google a détecté et arrêté AVANT que les moteurs antivirus ne proposent des signatures pour ces nouvelles attaques malveillantes. Les entreprises qui avaient fait confiance aux antivirus installés sur leurs postes de travail ou au niveau de la passerelle pour se protéger ont fait l'objet de nombreuses infections (sans compter les problèmes de dépannage s'y afférent) avant que leurs bases de données de signatures ne puissent être mises à jour.

- **Performances élevées**
  La plate-forme de sécurité Web pour l'entreprise de Google, fournie par Postini, est conçue spécialement pour le trafic Web. Elle utilise un traitement de mise en parallèle extrême pour optimiser le débit. La redondance très élevée offerte aux clients permet de garantir qu'ils disposent d'au minimum deux fois plus d'espace sur chaque serveur. Toutes les données sont réparties localement sur deux centres de données afin de réduire le temps de latence et d'optimiser la disponibilité.

- **Une évolutivité en toute simplicité**
  La sécurité Web pour l'entreprise de Google est extensible à l'infini de sorte qu'il est possible d'ajouter instantanément des utilisateurs à un coût fixe. Aucune planification de capacité supplémentaire n'est requise en cas de redimensionnement de l'entreprise, ce qui vous permet de déployer les services sur plusieurs filiales ou sites internationaux, sans délai d'exécution ou dépenses supplémentaires, ou autres coûts de configuration ou d'administration. Comme pour l'ensemble des services de sécurité et de conformité Google, la sécurité Web pour l'entreprise de Google intègre des fonctions de redondance, de disponibilité et de reprise sur incident, réduisant ainsi les ressources nécessaires et les coûts des interruptions planifiées ou non planifiées.

- **Un faible coût total de propriété**
  La sécurité Web pour l'entreprise de Google est la réponse au problème des responsables informatiques qui souhaitent fournir des solutions de qualité avec un budget de plus en plus restreint.Les services à la demande de Google sont conçus pour s'intégrer en toute transparence à l'architecture de réseau existante, ce qui réduit les besoins d'implémentation.Ainsi, le coût total de propriété est limité, car aucun logiciel, matériel ou membre de personnel supplémentaire n'est requis pour déployer et maintenir la solution.

- **Composant essentiel pour une sécurité élargie des communications**
  Grâce aux services de sécurité et de conformité Google, vous pouvez sécuriser toutes les communications électroniques (e-mail et Web) et gérer des stratégies de communication à partir d'un emplacement central.

CONTACTEZ-NOUS

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

Londres

Oxford

Francfort

Paris

Israël

Pékin

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapour

Sydney

Tokyo

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303, États-Unis
Tél. 650.475.4500
Télécopie 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616,
États-Unis
Tél. 210.348.1000
Télécopie 210.348.1003

Londres
4, Grosvenor Gardens,
Londres SWIW ODH, Royaume-Uni
Tél 44(0)20 7730 3438
Télécopie 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

À PROPOS DE FROST & SULLIVAN

Basé à Palo Alto, dans l'État de Californie, Frost & Sullivan est un leader international du conseil en croissance stratégique. Ce livre blanc s'inscrit dans le cadre d'une recherche stratégique discontinue de Frost & Sullivan dans les secteurs des technologies de l'information. Frost & Sullivan publie régulièrement des analyses stratégiques portant sur les principaux marchés de produits associés au stockage, à la gestion et à la sécurité des données. Frost & Sullivan fournit également des conseils en croissance personnalisés à un large éventail d'entreprises nationales et internationales.

Les informations contenues dans ce document sont basées sur des recherches et des entretiens menés exclusivement par Frost & Sullivan, et peuvent par conséquent faire l'objet de modifications. Frost & Sullivan ne saurait être tenu responsable de l'inexactitude des informations fournies par les fabricants et utilisateurs finaux.

WP37-0709