Gestion des menaces

Enjeux et Solutions

Menaces Web

Un White Paper Trend Micro I Février 2008

SOMMAIRE

TREND MICRO™

SYNTHÈSE

Motivés par la revente fort profitable d'informations confidentielles détournées, les cybercriminels ont fait du Web le principal terrain de leurs exactions. Les menaces Web se caractérisent par une activation concomitante de plusieurs techniques, et se déclinent en de multiples variantes, qui, pour certaines, sont localisées géographiquement et linguistiquement. Les conséquences de tels actes sont nombreuses : détournements d'identifiants, fuite d'informations confidentielles de l'entreprise, impact négatif sur l'image de marque et confiance érodée du grand public vis-à-vis du commerce électronique. Face à ces enjeux, l'utilisation généralisée du Web et la complexité de la protection contre les menaces Web constituent sans doute le plus grand défi de ces dix dernières années en matière de sécurité et de confidentialité des informations personnelles et professionnelles. Les moyens classiques, qui se contentent d'une couche ou d'une technologie de sécurité peinent à garantir une protection adéquate face à ces menaces, ce qui plaide en faveur d'une approche de sécurité multicouche. Ce livre blanc décrit les menaces Web, leur fonctionnement et leurs impacts, ainsi que les limites des méthodes traditionnelles de protection face à ces menaces. Le document dévoile également les principes d'une nouvelle approche, plus que jamais nécessaire, qui instaure différentes couches de sécurité.

INTRODUCTION : UN SCÉNARIO FÂCHEUX

Robert, avocat au département juridique d'une grande société pharmaceutique, arrive à son bureau lundi matin, s'identifie sur son ordinateur, et comme à son habitude, commence par consulter ses nouveaux emails. Fan de basket-ball, Robert a assisté la veille à un match à la télévision. Avec ce match en tête, il remarque un court email d'un de ses amis. L'email mentionne un lien vers un nouveau site Web présentant des informations sur l'une des plus grandes stars actuelle du basket. Robert clique sur le lien et se retrouve sur un site particulièrement complet sur le joueur, avec photos, vidéos et autres informations. L'avocat télécharge une des photos via son navigateur, et, à son insu, un script malveillant contenu dans le fichier jpg initie une commande de téléchargement d'un fichier exécutable, qui s'installe automatiquement sur son ordinateur. Ce logiciel pirate recueille certains types de fichiers prédéfinis stockés sur le disque dur de Robert, les comprime, les crypte, et les envoie à une adresse email précise : celle du cybercriminel. Ces fichiers contiennent, pour certains d'entre eux, des informations ultra-confidentielles sur différents dossiers de brevet pilotés par Robert. En envoyant ce même email à une liste de collaborateurs de diverses entreprises pharmaceutiques, le cybercriminel cible spécifiquement ce secteur d'activité pour obtenir des informations confidentielles, qui seront revendues à bon prix par la suite. Ainsi, en cliquant sur un lien apparemment inoffensif, Robert a déclenché fortuitement un processus permettant à des informations professionnelles et confidentielles de se retrouver dans de mauvaises mains. Cet acte expose potentiellement sa société, entre autres conséquences, à une perte de ses brevets et avantages concurrentiels et à un contentieux juridique.

Ce même lundi matin, l'administrateur réseau de la société pharmaceutique contrôle le trafic réseau. Sa société s'est récemment équipée d'un outil de filtrage d'URL à base de liste noire, qui vient compléter la protection antivirale des postes clients. L'administrateur ne décèle pas d'activité inhabituelle sur sa console. Le téléchargement du programme malveillant et le détournement des fichiers de Robert échappent en effet à toute détection, et ce, pour plusieurs raisons liées aux pratiques actuelles des cybercriminels. En premier lieu, les auteurs du logiciel malveillant ont mis en ligne le site Web incriminé le matin de l'attaque, pour éviter qu'il ne soit inclus dans la liste noire de l'outil de filtrage. Les pirates ont ensuite intégré des instructions dans le programme malveillant afin d'exporter progressivement les fichiers de Robert, évitant ainsi tout pic de trafic réseau qui attirerait l'attention de l'administrateur. La société pharmaceutique étant dépourvue d'outil d'analyse comportementale à l'échelle de sa passerelle Internet, les emails avec pièces jointes envoyées par l'ordinateur de l'avocat n'ont éveillé aucun soupçon.

TREND MICRO™

De tels scénarios sont communs dans le monde entier, au sein de multinationales, comme des PME. Un nombre important et croissant de menaces Web, similaires à celle décrite ci-dessus, se décline en de multiples variantes pour commettre leur forfait. Les cybercriminels détournent ainsi les listes de numéros de sécurité sociale d'organismes de santé, les numéros de cartes de crédit d'institutions financières, et les informations ultra-confidentielles d'entreprises technologiques. Cette pratique est également en train d'éroder la confiance des consommateurs quant à la protection de leur information confidentielle, et met directement en péril des secteurs d'activité comme la banque en ligne, les transactions sur Internet et le commerce électronique.

CONTEXTE

Au cours des 15 dernières années, les menaces sur la sécurité des informations ont montré de multiples visages. Les virus intégrés dans des fichiers exécutables téléchargés ont fait place à des virus Macro dans des fichiers et documents de travail, suivis quelques années plus tard des menaces envoyées par email (par ex., les virus « I Love You » et « Melissa »). Dans chacun de ces cas, les auteurs de ces logiciels malveillants ont sélectionné le support le plus utilisé et le moins protégé. Les logiciels malveillants tirent encore avantage de l'utilisation généralisée de la messagerie électronique, mais ce vecteur devient de plus en plus protégé, et témoigne d'une prise de conscience des entreprises face à ce danger. Aujourd'hui, une nouvelle vague de menaces émerge, utilisant le Web comme vecteur de propagation.

Dans le droit fil des menaces historiques, les menaces Web gagnent du terrain, à une période où l'utilisation de leur support - le Web - est plus que jamais un moteur de croissance des échanges commerciaux. La plupart des collaborateurs d'entreprise débutent leur journée en ouvrant le navigateur de leur ordinateur de bureau. Les réseaux sociaux tels que Myspace et YouTube, et le comportement des internautes qui privilégie une utilisation locale du Web, témoignent d'un Web qui s'utilise, certes de manière différente, mais tout aussi frénétiquement.

Et pourtant, le Web reste relativement mal protégé, par rapport à la messagerie notamment, et devient un vecteur de choix pour diffuser les logiciels malveillants. Pour IDC, « jusqu'à 30 % des entreprises de 500 personnes et plus ont été infectées suite à une navigation sur le Web, alors que seules 20 % à 25 % d'entre elles ont été victimes de virus et de vers informatiques à partir d'emails ». [1] Le Web est plus difficile à protéger, puisqu'il requiert une bande passante beaucoup plus importante pour filtrer ses flux de données, par rapport à la messagerie qui contient jusqu'à mille fois moins de données que le Web. Les logiciels antivirus traditionnels installés sur les postes clients, bien que cruciaux pour la protection de ces machines, affichent leurs limites face aux menaces Web, un état des lieux qui facilite davantage la prolifération des menaces Web : un support relativement peu ou prou protégé, mais largement et régulièrement utilisé, car essentiel à la productivité des entreprises. Il est urgent que la sécurité des informations prenne le virage d'une nouvelle approche qui soit réellement adaptée à ces nouvelles menaces.

Un état des lieux qui facilite davantage la prolifération des menaces Web : un support relativement peu ou prou protégé, mais largement et régulièrement utilisé, car essentiel à la productivité des entreprises

DÉFINITION DES MENACES WEB

Les menaces Web constituent un vaste ensemble de menaces issues d'Internet. Elles associent des techniques et des supports différents, plutôt qu'un support ou une approche unique, pour concrétiser des approches sophistiquées. Les auteurs d'une menace Web changent constamment de versions ou les utilisent sous différentes variantes. Les menaces Web sont stockées dans un lieu fixe sur un site Web, plutôt que sur la machine infectée de l'utilisateur, et les scripts sont constamment modifiés afin d'éviter toute détection. Au cours de ces dernières années, les pirates, auteurs de virus, spammers et autres concepteurs de logiciels espions se sont progressivement hissés au rang de cybercriminels qui activent les menaces Web principalement pour des raisons de profit financier. Ils sont à l'origine d'infections simplement par le biais de visites d'utilisateurs sur des pages Web infectées, et utilisent ensuite diverses techniques furtives permettant de se « cacher » sur un ordinateur ou sur le Web. Une fois actif et en place, les scripts malveillants détournent lentement et discrètement les fichiers de l'utilisateur et consomment les ressources CPU de son poste client.

Types de menaces web

Voici quelques exemples concrets de ces menaces, selon les différentes étapes qui leur permettent de se concrétiser, de la mise à disposition de liens web malveillants aux conséquences de l'infection :

- Envoi de liens web :
  - Spam, phishing (escroquerie par hameçonnage) par email, annonces de gains financiers majeurs et autres messages avec liens qui dirigent l'utilisateur vers un site malveillant.
  - Un serveur de nom de domaine piraté (via pharming, une technique de piratage qui exploite les vulnérabilités DNS), ou un site web qui redirige l'utilisateur vers un site frauduleux, en lieu du site légitime, ou vers un serveur proxy. L'objectif est de détourner les données de l'utilisateur ou d'infecter son équipement.
  - Certains sites de réseaux sociaux et toute autre exaction qui visent à infecter l'utilisateur.
- Utilisation d'un site Web
  - Utilisation des failles du navigateur vis-à-vis des fichiers multimédia (image, animation, vidéo, et audio) pour introduire/télécharger des fichiers malveillants.
  - Contrôles ActiveX ou téléchargements ad hoc : l'utilisateur doit télécharger un composant avant de visualiser un fichier ou tentative d'injection d'un tel fichier si le navigateur n'est pas à jour de ses patchs de sécurité.
- Infection
  - Infection véhiculée par des applications qui introduisent des fichiers malveillants dans le système.
  - Mises à jour automatique de ces menaces via un téléchargement web en plusieurs fichiers pour éviter toute détection par les outils d'analyse classiques.
- Conséquences de l'infection
  - Spyware ou applications malveillantes qui détournent les données et informations d'un système pour les transmettre à un tiers.
  - Adware, logiciel de datamining et autres fenêtres pop-up à objectif commercial.
  - Micrologiciels intégrés au navigateur qui altèrent les résultats des moteurs de recherche, profilent les habitudes de navigation des utilisateurs et recueillent des informations sur leurs centres d'intérêt (produits et services notamment), pour cibler plus finement les campagnes marketing.
  - Bots et zombies (postes clients infectés et gérés à distance), qui reçoivent des instructions via le web.

- **Des méthodes sophistiquées**
  La majorité des menaces web tirent avantage du port 80, quasiment toujours ouvert pour communiquer aux utilisateurs les informations du Web et concrétiser les promesses de productivité et de convivialité d'Internet (le scénario précédent illustre parfaitement cette approche). Les menaces web ont tendance à cibler des infections à l'échelle locale ou régionale (via notamment des sites Web localisés ou qui ciblent un groupe démographique/ethnique en particulier), une approche plus appropriée que les infections de masse du passé. Les auteurs des logiciels malveillants capitalisent également sur l'actualité et des événements sociaux, repris par exemple dans les sujets des spams envoyés (avec souvent une adresse web vers un site qui injecte un logiciel malveillant) avec référence à des vacances, des personnalités connues, au sport, à la pornographie et autres sujets d'intérêt.

IMPACTS ET ÉTENDUE DES MENACES WEB

Les menaces web, générées par les cybercriminels, ont des objectifs précis. Le plus commun d'entre eux est de détourner de l'information pour la revendre. Les fuites de données qui résultent de tels actes conduisent à un vol ou une utilisation frauduleuse des informations confidentielles de l'utilisateur infecté, ou facilitent les opérations de phishing qui visent à récupérer toujours plus d'information. Ces menaces sont susceptibles de peser sur la confiance des utilisateurs vis-à-vis du commerce électronique et des transactions sur Internet. Un second objectif de ces menaces est de détourner des ressources systèmes de l'utilisateur et de les utiliser dans le cadre d'opérations rentables comme un envoi de spam, des attaques généralisées de déni de services, ou des opérations permettant aux auteurs de se rémunérer au clic.

Les profits générés par ces menaces web sont colossaux. Jeanson James Ancheta, par exemple, a détourné 60 000 USD en gérant un réseau de 400 000 PC Botnet [2]. Ivan Maksakov, Alexander Petrov et Denis Stepanov ont extorqué 4 millions USD via une attaque généralisée de type déni de service sur les sociétés de pari sportif au Royaume-Uni [3]. Un logiciel aussi puissant que celui utilisé par ces protagonistes vaut de 1 000 à 5 000 dollars américains sur le marché noir, une fourchette de prix qui permet de s'offrir un Cheval de Troie capable de détourner des informations de compte clients [4]. Les chiffres restent néanmoins rares pour évaluer précisément l'étendue des profits dans un secteur où l'opacité règne.

Le coût financier de ces menaces web a, en revanche, été évalué par de nombreux acteurs. Consumer Reports USA indique que les attaques de phishing sur le grand public américain ont coûté 630 millions $ en 2005 [5]. En Allemagne, l'utilisation de numéros d'authentification de transactions en conjonction avec les noms d'utilisateur et les mots de passe, n'a pas empêché les banques du pays d'être victimes du phishing. La police de Munich estime que cette fraude en ligne a coûté un million d'euro entre janvier et juillet 2006, sur cette seule ville [6]. Selon Asia.Internet, Gartner estimerait le coût total des attaques de phishing en 2006 à 2,8 milliards $ [7].

Les schémas 1 et 2 (en page 7) proposent des estimations sur le coût financier des différentes menaces web, des chiffres qui témoignent de leur dynamisme (voir schéma 3 en page 8). Standard Bank, estime que le nombre de spyware a bondi de 50 % en 18 mois et que la création de virus a été multipliée par 16 sur les trois dernières années [8]. Une étude démontre que les auteurs de phishing arrivent à leurs fins sur prés de 14% de leurs messages infectés envoyés, 24 heures seulement après leur émission. Ce chiffre superforme d'ailleurs ceux avancés par plusieurs observateurs et professionnels de la sécurité réseau [9].

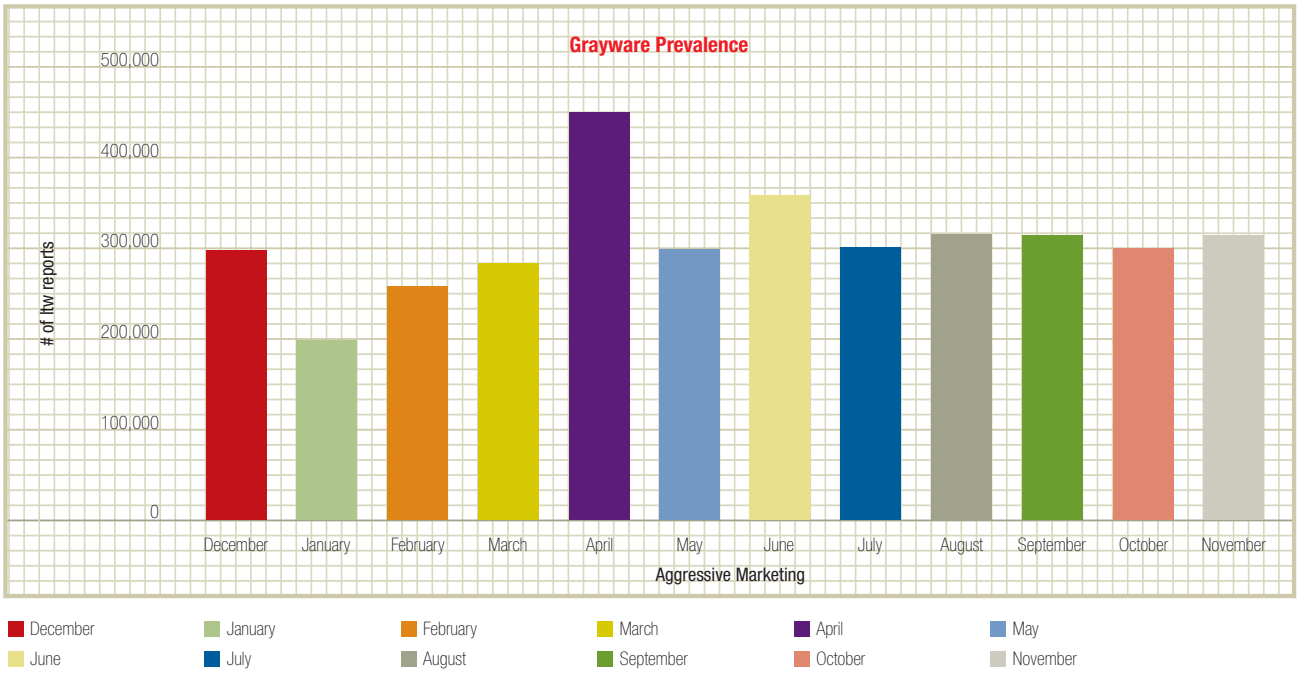

Schéma 1. Le Grayware (scripts parasites, mais non malveillants) s'est considérablement développé en 2006. Ces chiffres sont inquiétants : Trend Micro a effectivement constaté une forte évolution du Greyware vers des logiciels malveillants qui visent à générer des revenus au clic réalisé. *Source : Trend Micro*

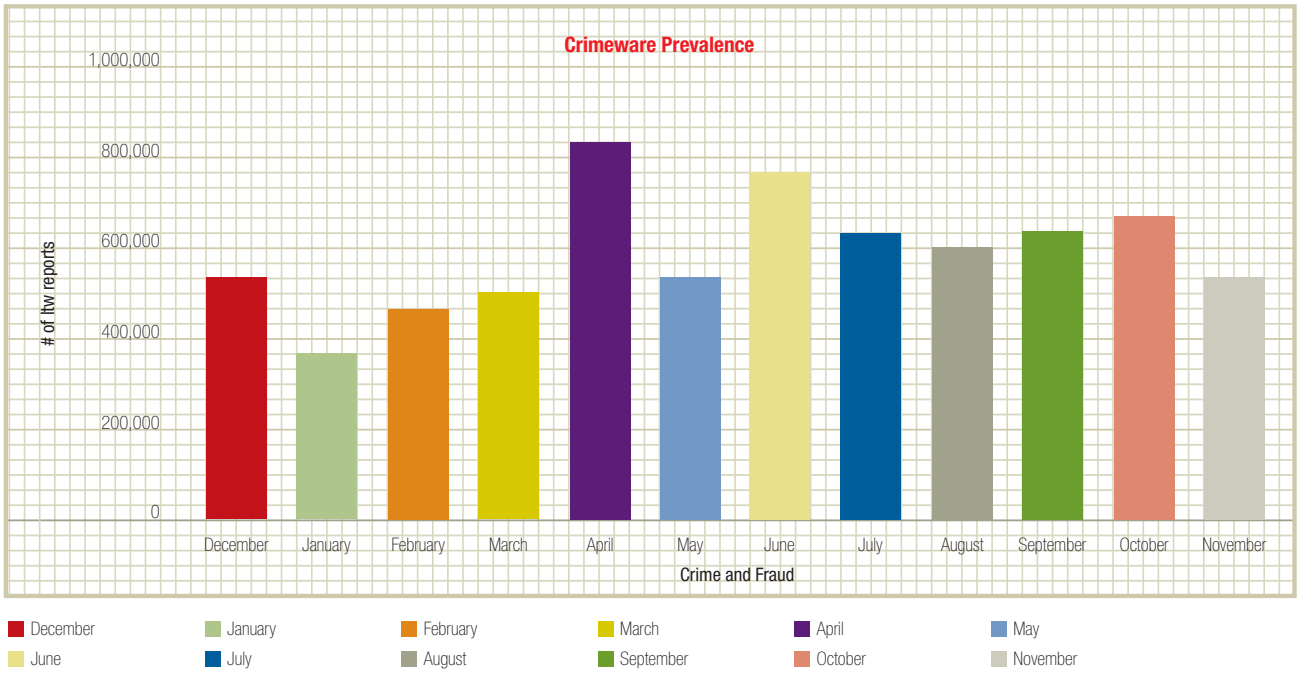

Schéma 2. En 2006, les crimewares (logiciels à objectif criminel qui tentent d'automatiser les fraudes financières) ont été particulièrement actifs. Source : *Trend Micro*

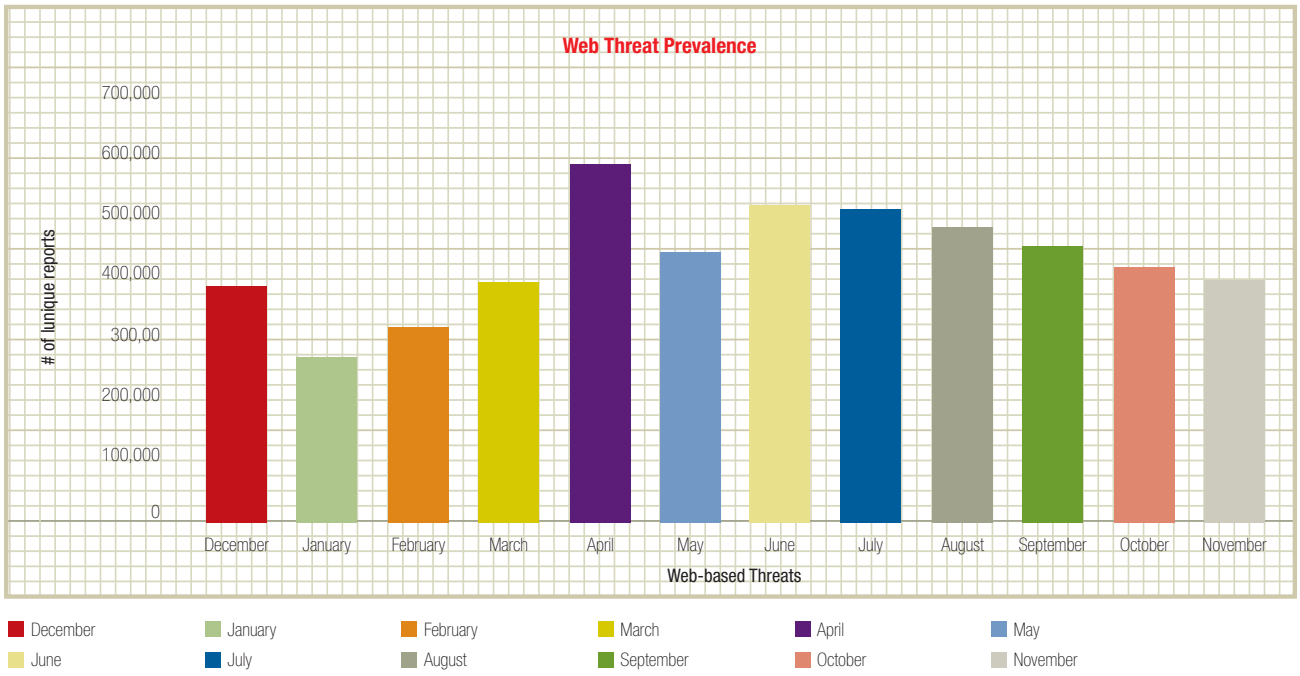

Schéma 3. Après l'email, le second vecteur de prolifération des logiciels malveillants est le Web. *Source : Trend Micro*

ÉCHEC DES MÉTHODES CLASSIQUES CONTRE LES MENACES WEB

L'approche antivirus classique consiste à analyser les virus actifs sur le web, et à concevoir des signatures virus qui seront distribuées aux utilisateurs. Cette approche reste limitée pour juguler les menaces web, pour différentes raisons. Les menaces donnent en effet lieu à des attaques ciblées avec de multiples variantes, et l'échantillonnage de ces virus est donc rarement pertinent. Les variantes utilisent différents vecteurs de propagation (spam, messagerie instantanée et autres sites web), ce qui rend l'échantillonnage classique et le processus de création de signature imparfaits. Les menaces web associent de nombreuses tactiques (attaques locales et régionales, spam en langue locale/régionale, site web localisés, etc.) et une seule solution de sécurité ne suffit pas à maîtriser toutes ces menaces : un échantillon de virus recueilli lors d'une attaque localisée n'est pas entièrement représentatif des autres attaques localisées.

Les menaces web privilégient la discrétion pour éviter de se faire repérer, et sont donc difficiles à détecter via les techniques antivirus classiques. Dans certains cas, les menaces web aboutissent à une infection généralisée du système (exemple d'un kit "racine" qui remplace le file system) qui empêche la désinstallation ou les méthodes classiques de nettoyage. Une restauration complète est alors nécessaire, avec formatage du disque dur, puis réinstallation du système d'exploitation, des applications et des données utilisateur. Les cybercriminels tirent aussi avantage du port 80 qui est ouvert pour assurer les communications légitimes, en contournant le pare-feu client. Les pirates les plus aguerris profitent du délai entre l'identification d'un virus et la mise à disposition du patch de sécurité approprié pour lancer leurs attaques. Parallèlement, les cybercriminels ciblent et tente d'infecter de nombreuses plateformes, dont Windows Web Server, et s'adaptent à différentes technologies. Les serveurs Web Linux, considérés comme moins vulnérables à une époque, sont désormais menacés. Lorsqu'un logiciel malveillant est installé, il incite les autres applications à transgresser les règles de prévention des intrusions sur le système hôte. L'excès de faux-positifs en matière d'alerte finit par lasser l'utilisateur au point qu'il désactive sa protection et permet ainsi au virus de s'exécuter. Dans ce cas de figure, le virus contourne les techniques de protection et de détection d'intrusion en place.

Les programmes personnels de téléchargement, cibles favorites des menaces web, paraissent innocents au premier abord. Pourtant, ils pèsent sur les analyses heuristiques de fichiers en multipliant les faux-positifs ou en rendant cette analyse inefficace. Les menaces web contribuent également à multiplier les faux-positifs en coordonnant des attaques multicouches et multiprotocoles qui ne sont pas détectés par les outils de sécurité traditionnels. C'est l'exemple du pirate qui inclut un lien web dans un email ou message instantané. L'utilisateur clique sur ce lien et se retrouve sur un site légitime…mais piraté quelques heures auparavant. Des tests de contrôle Active X évaluent alors la vulnérabilité du navigateur de l'utilisateur. Le logiciel malveillant passe à l'attaque dès qu'une faille est détectée, en téléchargeant un fichier, puis en cherchant de nouvelles failles pour télécharger de nouveaux fichiers, et ainsi de suite. Chacun de ces flux peut apparaître bénin individuellement, mais ils constituent une attaque ciblée lorsque pris dans leur globalité.

UNE NOUVELLE APPROCHE : UNE PROTECTION INTÉGRÉE ET MULTICOUCHE

Une nouvelle approche de sécurité est nécessaire pour traiter cette nouvelle menace et venir au renfort des techniques actuellement en vigueur. L'approche la plus efficace met en jeu plusieurs couches de sécurité de défense et intègre un ensemble de mesures de sécurité. Par ailleurs, la nature versatile des menaces Web impose un partage des informations, où les données recueillies à l'échelle d'une couche vont mettre à jour les informations des autres couches de sécurité. Une approche efficace doit également se pencher sur tous les protocoles utilisés, qui sont autant de vecteurs d'infection potentielle. La coordination de ces mesures de protection doit être gérée centralement et doit cibler les différentes régions du monde pour identifier les versions locales de ces menaces.

Une approche multicouche est essentielle pour déjouer ces menaces et implique une protection à trois niveaux différents (schéma 4) : "In-the-cloud" (analyse des données Web en amont de la passerelle Internet d'entreprise), surveillance de la passerelle Internet, et analyse des données sur le poste client. Les menaces Web utilisent souvent un email pour mettre à disposition le lien Web incriminé. L'interception de cet email dans la zone « in-the-cloud » allège le trafic email au niveau de la passerelle, libère de la bande passante, consomme moins de ressources de traitement et d'archivage (ces emails n'ont pas besoin d'être archivés selon les réglementations en vigueur), et se veut donc plus économique.

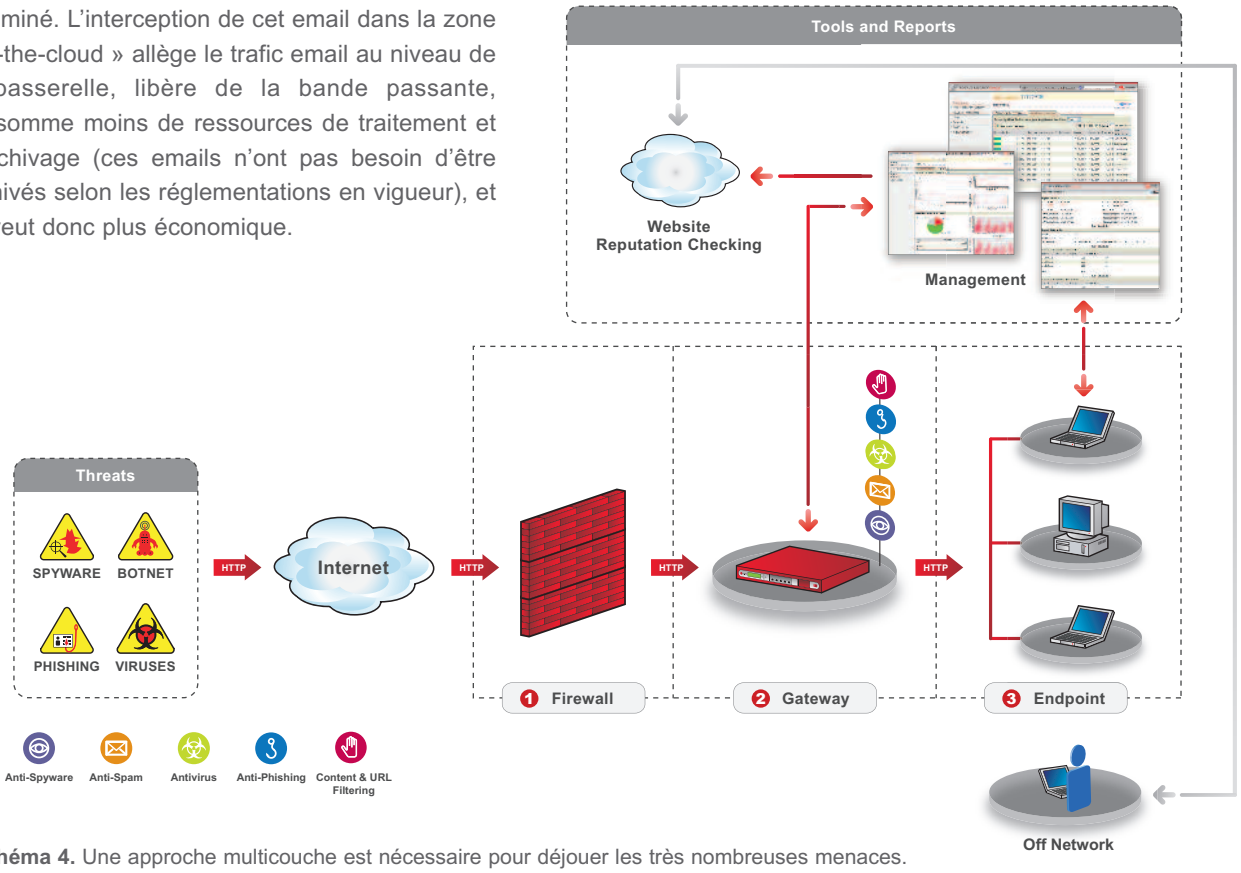

Schéma 4. Une approche multicouche est nécessaire pour déjouer les très nombreuses menaces.

In-the-Cloud.

Cette couche de protection va essentiellement valider la « réputation » de chaque site Web avant que l'utilisateur y accède, une opération assez similaire aux vérifications d'usage avant l'octroi d'un crédit par une institution financière. Ce contrôle de la « réputation Web » fait intervenir une base de données de filtrage d'URL, mais avec 5 000 nouveaux domaines créés chaque jour, le contrôle de la réputation d'un site exige des mesures supplémentaires : vérification auprès d'une base de « notation de sécurité », conçue à partir d'une évaluation périodique des sites web et de leur intégrité, et auprès de bases qui répertorient les URL impliquées dans des attaques de phishing ou victimes de pharming. Les cybercriminels modifient souvent l'emplacement physique de leurs adresses IP pour éviter de se faire repérer, ce qui implique de vérifier dans la zone in-the-cloud la localisation d'une adresse IP associée à une URL. Pour optimiser l'efficacité, une analyse sur les domaines de premier niveau est également nécessaire (les lettres d'une adresse URL à la droite du dernier point, code pays compris - voir schéma 5)..

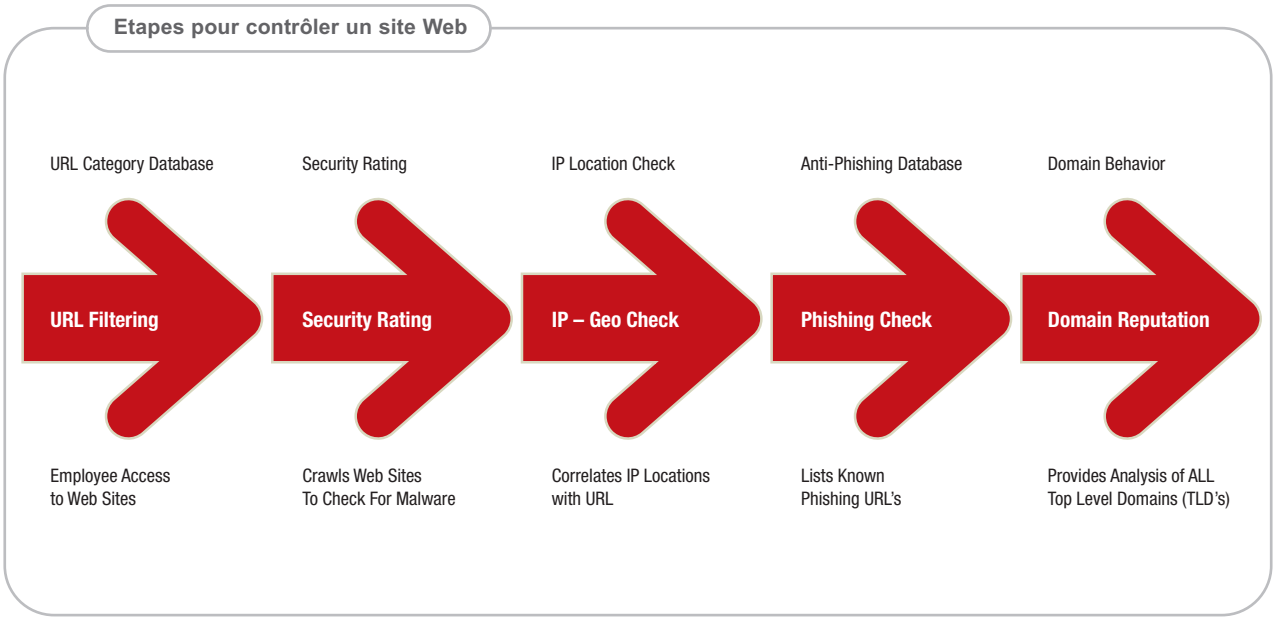

Schéma 5. Vérification In-the-cloud de la réputation de chaque site web via un processus en plusieurs étapes.

Au niveau de la passerelle Internet

Des analyses précises doivent également être menées sur la seconde des trois couches de sécurité, à savoir la passerelle Internet. Ces analyses, exécutées via un outil logiciel ou un matériel dédié, porteront sur les fichiers, en vérifiant la « réputation » de chaque fichier avant d'autoriser son téléchargement par l'utilisateur. Une analyse des données et de la réputation de chaque fichier du site Web doit s'effectuer régulièrement pour établir et maintenir à jour une base de données de réputation des fichiers. Ce contrôle des fichiers vient renforcer le contrôle de réputation Web dans la zone In-the-cloud, et déjouer les tentatives des cybercriminels qui déplacent souvent les fichiers à contenu malveillant d'un site Web à un autre.

Le second levier de protection au niveau de la passerelle est une analyse comportementale capable d'identifier et de corréler des activités distinctes et ainsi statuer sur leur animosité. Cette analyse s'adosse à une échelle de gravité pour chaque combinaison d'activités et neutralise ces activités associées dès le franchissement d'un seuil prédéfini sur cette échelle. Cette analyse identifie également les déclencheurs d'attaques, des éléments factuels liés aux données et aux protocoles utilisés et qui révèlent des activités suspectes. De plus, cette approche va définir des règles qui associeront différents déclencheurs. Ces déclencheurs correspondent à des conditions prédéfinies qui valident l'existence d'une activité malveillante à l'échelle de la passerelle.

Sur le poste client

Les mesures mises en œuvre dans la zone In-the-cloud et sur la passerelle Internet doivent s'accompagner d'une troisième couche de protection à l'échelle des postes clients. Aux États-Unis, les portables représentent près des deux tiers des ventes d'ordinateurs [10]. Ces portables doivent être protégés : ils se connectent à différents réseaux, tandis que les visiteurs et le personnel externe/intérimaire les sortent du périmètre physique d'une entreprise. Les règles de sécurité d'entreprise doivent donc être appliquées, que l'utilisateur soit connecté ou pas au réseau d'entreprise. D'où l'intérêt d'une solution de protection des postes clients (contrôle d'accès et analyse du poste), capable de nettoyer et de restaurer la machine en cas d'infection. Ainsi, si un PC portable infecté fait partie d'un réseau de bot, il est susceptible de tenter de se connecter à son bot herder (personne contrôlant le réseau de bot). Un autre exemple est celui des spywares qui tentent de transférer l'information recueillie à leur propriétaire. Dans ces deux cas, l'activité peut être détectée et neutralisée, et une opération de nettoyage activée le cas échéant. L'arsenal de sécurité pour les postes clients doit comprendre un filtrage d'URL, des fonctionnalités de vérification de la réputation de site Web, et l'enregistrement d'un point de restauration en amont de toute session de navigation. Si une activité anormale est détectée après le téléchargement d'un fichier ou la navigation sur Internet, l'ordinateur sera ainsi restauré à son point initial enregistré.

Parmi les autres moyens de prévention, notons la création d'un « environnement virtuel » dédié à la navigation sur le Web, qui sert de zone tampon pour éviter que les menaces web ne prolifèrent jusqu'au poste de l'utilisateur. Les postes clients doivent également être équipés d'outils de nettoyage sous deux formats : nettoyage via un agent logiciel installé et nettoyage sans agent logiciel. L'agent logiciel, lorsqu'installé sur un poste client, va piloter les opérations de nettoyage. Le nettoyage sans agent logiciel est nécessaire pour les portables d'un visiteur ou d'un personnel externe. Le nettoyage est alors réalisé à la demande avec un contrôle d'accès réseau (accès limité au réseau pour réaliser le nettoyage). Un mécanisme de restauration complète sera activé lorsque le nettoyage n'est pas possible, après une infection à la racine du poste client par exemple.

Une information relayée et mise en boucle

Le schéma 6 illustre cette approche multicouche et souligne un aspect important de sa mise en œuvre. L'intégration des protections In-the-cloud, de la passerelle Internet et à l'échelle du poste client implique de relayer l'information entre ces couches. Parallèlement, le retour d'information d'une couche à une autre s'adosse à un mécanisme de boucle : ainsi, les informations d'analyse de comportement recueillies sur la passerelle seront acheminées via une boucle pour mettre à jour les bases de réputation web et les fonctionnalités de sécurité du poste client. Les informations recueillies à l'échelle du poste client seront utilisées par les outils d'analyse qui protègent la passerelle et la base de réputation Web In-the-cloud.

Les techniques de relais et de mise en boucle sont nécessaires pour pérenniser la protection. Toutes ces fonctionnalités et les règles associées doivent être gérées à partir d'une console d'administration centralisée. D'autre part, des équipes spécifiques doivent être dédiées aux différentes régions du monde pour réaliser les opérations de veille, d'échantillonnage, de prévention, de restauration, et de coordination avec les équipes et avec les autorités légales, pour ainsi optimiser la lutte contre les menaces Web. Cette approche exhaustive favorise une réponse plus rapide, des solutions personnalisées et une meilleure sensibilisation à la problématique des menaces web.

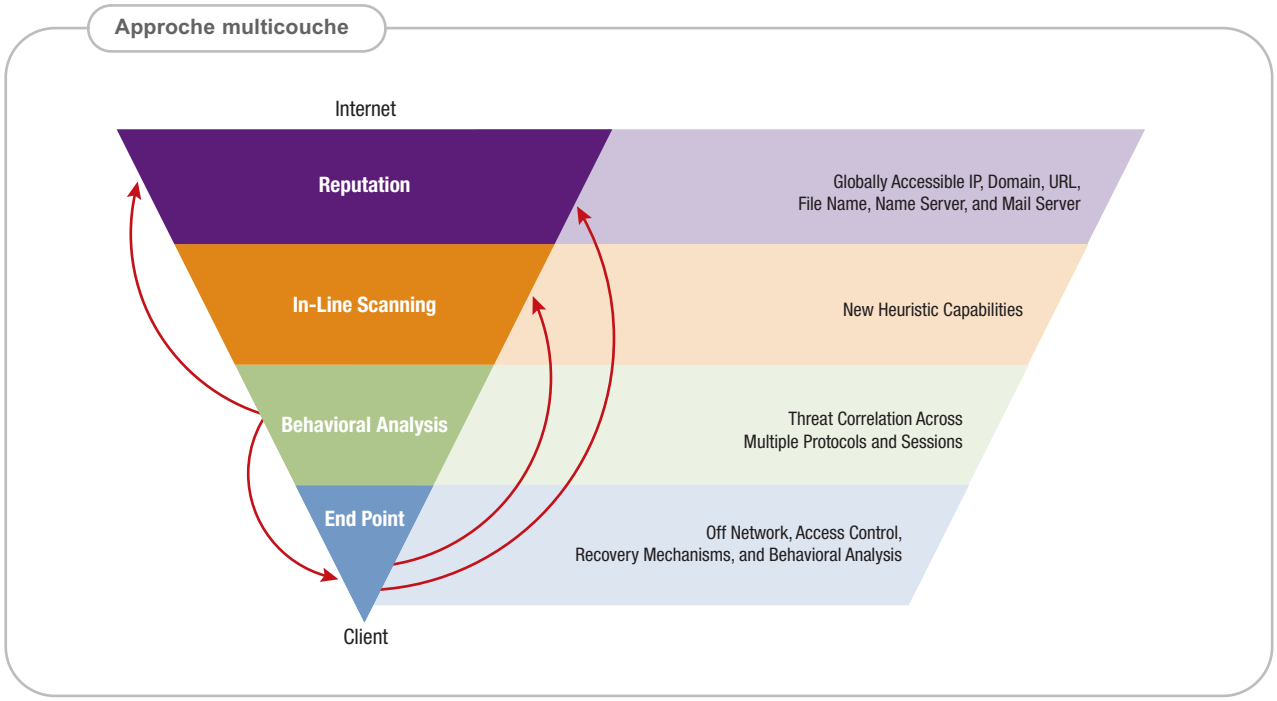

Schéma 6. Le relais (approche descendante) et la mise en boucle (flèches) d'informations de sécurité améliorent l'approche multicouche qui protège la zone In-the-cloud, la passerelle Internet, le réseau interne et le client final.

UNE APPROCHE QUI VISE AUSSI LA SÉCURITÉ EMAIL

Cette approche multicouche gagnera à sécuriser la messagerie électronique également. Une protection In-the-cloud active est essentielle dans l'univers de la messagerie : lorsqu'un email se présente à la passerelle Internet, les réglementations en vigueur exigent un archivage de ce message sur une période pouvant atteindre 10 ans. Ainsi, un filtrage In-the-cloud préserve la bande passante, réduit les espaces de stockage et les coûts de maintenance, et améliore la protection. À ce niveau, la protection doit s'adosser à de nombreux tests : réputation de l'IP de l'émetteur, réputation de l'IP du nom de domaine, pare-feu email, filtrage antispam et antivirus (avec 0 faux-positifs pour ces tests de premier niveau). Le pare-feu email doit être hébergé en amont du serveur de messagerie pour contrer les attaques généralisées de type déni de service ou de piratage d'annuaire (attaque qui collecte des adresses de messagerie valides).

Au niveau de la passerelle Internet, des solutions antivirus et antispam doivent analyser et détecter le spam évolué, généré automatiquement, comportant des images pour tenter de légitimiser le message, gros consommateur d'espace de stockage et contenant généralement un logiciel malveillant. À ce niveau, un moteur de règles est requis pour faire le lien entre les serveurs email et l'annuaire (LDAP par exemple). Des technologies d'analyse comportementales détectent si un utilisateur ne répond pas à un message répété, ce qui classe ce message dans la catégorie des spams. L'analyse du contenu des e-mails peut également être réalisée à cette étape pour garantir que les collaborateurs ne divulguent aucune information confidentielle à des tierces parties illégitimes. Cette fonctionnalité doit également crypter les messages sortants et assurer un archivage des messages conformes au cadre réglementaire.

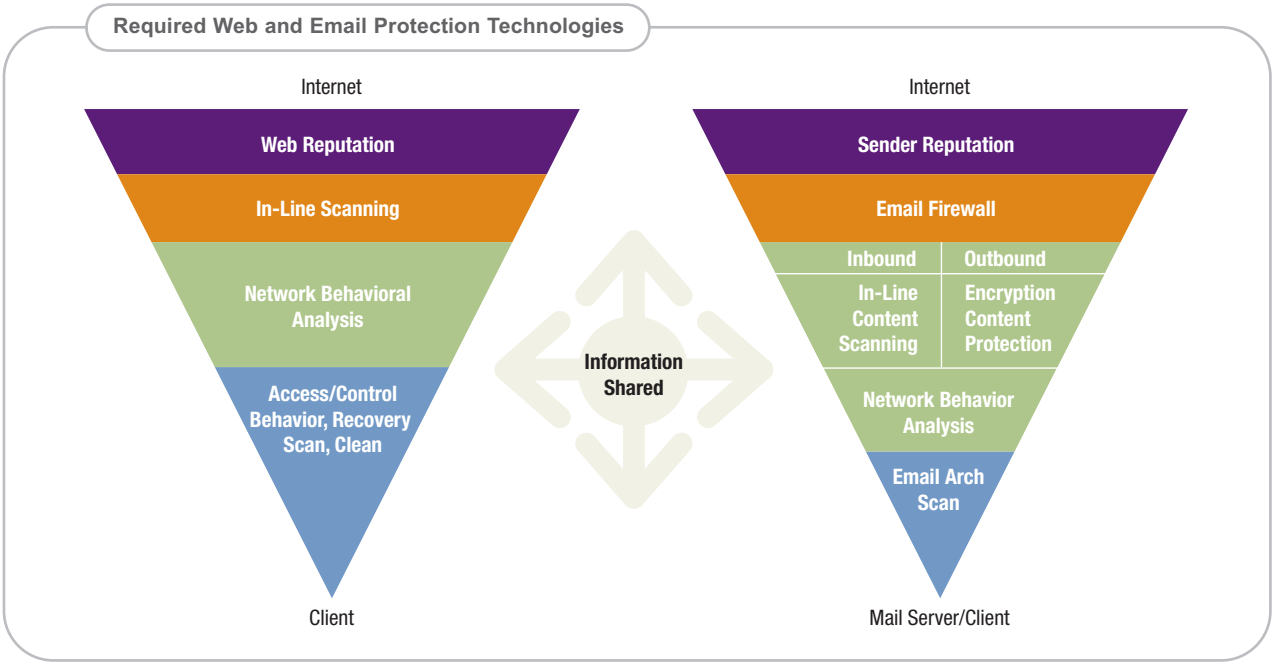

Schéma 7. Trend Micro recommande des solutions qui favorisent un partage d'information entre les technologies de protection du Web et de l'email, et une gestion centralisée de la protection des réseaux contre ces menaces.

LA STRATÉGIE TREND MICRO

La stratégie de protection de Trend Micro face aux menaces Web constitue une solution exhaustive et multicouche pour se prémunir contre de très nombreuses menaces Web (voir Schéma 8). Trend Micro offre ainsi ses services de réputation pour la protection In-the-cloud. Au niveau de la passerelle Internet, les solutions logicielles et matérielles de Trend Micro (dont InterScan Web Security Suite et InterScan Web Security Appliance, l'appliance de sécurité), proposent un filtrage des fichiers et une analyse des comportements pour identifier toute activité malveillante. Enfin, au niveau du poste client, Trend Micro propose ses solutions primées OfficeScan et Anti-Spyware Enterprise Edition pour gérer le contrôle d'accès et les analyses. Les solutions conviviales et ciblées de Trend Micro proposent une protection exhaustive et intégrée contre les menaces web et émergentes, conçue spécifiquement pour les entreprises dont les équipes informatiques sont limitées.

Trend Micro propose également des services de nettoyage et de restauration adossés à des processus de relais et de mise en boucle de l'information de sécurité, ainsi qu'une gestion centralisée des outils de sécurité via Trend Micro Control Manager. Ces fonctionnalités sont proposées dans des formats et outils parfaitement adaptés aux grandes entreprises, aux PME, aux fournisseurs de services et au grand public. Parallèlement, TrendLabs constitue une solution novatrice pour répondre aux menaces web, via un réseau de laboratoires régionaux, plus de 800 ingénieurs, une exploitation 24 heures sur 24, 7 jours sur 7, et des ressources dédiées à la prévention des menaces web.

CONCLUSION

Les menaces web sont plus que jamais virulentes dans leur nombre et leur impact. Leur complexité et variantes, l'utilisation de différents vecteurs de propagation, et l'exploitation de la moindre faille des médias actuellement utilisés, font des menaces web le plus grand défi actuel qui pèse sur les entreprises, les fournisseurs de services et le grand public. Le coût de ces menaces s'évalue compte tenu du nombre des fuites d'information confidentielle, de leur impact direct sur l'image de marque et en matière de contentieux judiciaire et/ou de la divulgation d'éléments de propriété intellectuelle aux concurrents. Les approches classiques connaissent des limites dans la protection contre ces menaces web et le secteur de la sécurité informatique s'interroge toujours sur les méthodes les plus efficaces. Sur le terrain, les entreprises comme les fournisseurs de services sont invités à mettre en œuvre une approche en plusieurs couches de sécurité différenciées pour mieux contrer ces menaces.

RÉFÉRENCES

1. IDC, press release, July 18, 2006, "Private Internet Use by Staff Threatens IT Security in Danish Companies, Says IDC," http://www.idc.com/getdoc.jsp?containerId=pr2006_07_14_125434.
2. Gregg Keizer, TechWeb Technology News, January 24, 2006, "Botnet Creator Pleads Guilty, Faces 25 Years," http://www.techweb.com/wire/security/177103378
3. Marius Oiaga, Softpedia, October 4, 2006, "Hacking Russian Trio Gets 24 Years in Prison," http://news.softpedia.com/news/Hacking-Russian-Trio-Gets-24-Years-in-Prison-37149.shtml.
4. Byron Acohido and Jon Swartz, USA TODAY "Cybercrime flourishes in online hacker forums," October 11, 2006, http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm
5. Consumer Reports, "Don't bite at phishers' e-mail bait," September 2006, http://www.consumerreports.org/cro/personal-finance/news/september-2006/dont-bite-at-phishers-e-mail-bait-9-06/overview/0609_dont-bite-at-phishers-email-bait_ov.htm.
6. Police of the City of Munich, August 25, 2006, http://www.sueddeutsche.de/,tt3m3/muenchen/artikel/612/83529/
7. "Scammers Hooking Bigger Phish," Asia.Internet, November 9, 2006, http://asia.internet.com/news/article.php/3642971.
8. Herman Singh, Standard Bank, "Next Generation Internet Fraud and Techniques to Combat This," BMI-T Annual Banking Forum, October 19, 2006, Johannesburg, http://www.bmi-t.co.za/presentations/bf/links/presentations/Herman%20Singh.pdf.
9. Markus Jakobsson, Jacob Ratkiewicz, "Designing Ethical Phishing Experiments: A study of (ROT-13) rOnl query features," International World Wide Web Conference Committee, WWW 2006, May 23-26, 2006, Edinburgh, Scotland, ACM 1-59593-323-9/06/0005, http://www.informatics.indiana.edu/markus/papers/ethical_phishing-jakobsson_ratkiewicz_06.pdf.
10. Tom Krazit, Cnet, "Two in three retail PCs are notebooks," December 20, 2006, http://news.com.com/Two+in+three+retail+PCs+are+notebooks/2100-1044_3-6144921.html.

TREND MICRO INC.
85 Avenue Albert 1er
92500 Rueil Malmaison

Tél : 01 76 68 65 00
Fax : 01 76 68 65 05
www.trendmicro.com