IBM Internet Security Systems
Évolution des menaces.

Des menaces en mutation : combattre les maliciels de nouvelle génération

Sommaire

L'évolution galopante des menaces Internet

Les méthodes d'attaque Internet ont discrètement évolué depuis 2005. Et si cette évolution est demeurée subtile jusqu'à présent, les entreprises qui l'ignorent s'exposent à des risques sérieux. Les motivations des pirates ont changé : leurs attaques ne visent plus la gloire et la célébrité, mais le profit. Les tentatives de gains financiers les mieux organisées mobilisent les talents de la communauté des pirates pour mettre au point de nouvelles stratégies et développer des logiciels malveillants innovants capables de pénétrer les systèmes des entreprises sans être détectés. Les solutions de sécurisation classiques protégeaient les organisations contre des pirates qui ambitionnaient de faire la une grâce au succès d'une attaque par saturation ou à la défiguration d'un site Web. Aujourd'hui, les attaquants ont des motivations pécuniaires ou politiques et font appel à des technologies de pointe pour s'insinuer dans les réseaux en y restant le plus longtemps possible incognito – de manière à multiplier leurs chances de succès dans le vol d'informations et d'autres activités lucratives.

La Figure A montre les différences entre les attaques observées durant les précédentes décennies et les nouvelles formes d'attaque.

Figure A

Caractéristiques	Avant	Aujourd'hui
Motivation	Gloire et célébrité	Profit
Complexité	Monodimension	Multiforme
Portée	Large – pour se faire de la publicité (technique du tapis de bombes ou du tir d'arrosage)	Ciblée – pour passer inaperçues (technique du tireur d'élite ou des frappes chirurgicales)
Principal risque	Blocage du réseau (le temps de nettoyer et de réparer)	Pertes financières directes, vol de secrets de fabrication ou d'informations stratégiques, divulgation des données clients
Cibles	Très visibles, indifférenciées	Individualisées (entreprise ou personnes déterminées)
Défense efficace	Signatures antivirus, actions correctives	Protection multifonction, nécessité d'une approche préventive et comportementale
Remède	Analyse et éradication	Pas toujours possible, peut nécessiter le chargement d'une nouvelle image système
Types d'attaque	Virus, vers, logiciels espions	Virus sur mesure, dissimulation d'activité, chantage, harponnage
Mode opératoire	Trafic réseau – L'attaque est volontairement rendue visible	Code malveillant – On recherche la furtivité pour opérer incognito

Face à ces nouvelles attaques motivées par le profit, les organisations doivent évaluer la pertinence des plates-formes de sécurisation en place. Ce dossier décrit les menaces de nouvelle génération qui s'appuient sur des programmes malveillants – un domaine où nombre d'entreprises présentent un niveau d'exposition sans précédent.

Ma solution actuelle est-elle efficace contre les programmes malveillants de nouvelle génération ?

Votre plate-forme de sécurisation est-elle à la hauteur ?

Les programmes malveillants employés dans les attaques modernes ont des effets plus dévastateurs que les vers et virus antérieurs, très visibles. Nombre des systèmes de protection existants ne sont pas capables de stopper les "maliciels" de nouvelle génération. Ces solutions de sécurisation s'appuient généralement sur les signatures des attaques connues : quand elles détectent l'une de ces signatures, elles déclenchent l'alarme et peuvent essayer de bloquer l'attaque. Une protection fondée sur les signatures ne peut cependant que prévenir les attaques répertoriées. Conscients de la faiblesse d'une telle défense, les pirates se sont mis à développer des attaques "jour 0".

La question que doivent se poser les responsables de la sécurité est la suivante : Ma solution actuelle protège-t-elle mon organisation contre les programmes malveillants de nouvelle génération ?

Les attaques modernes surclassent les technologies de sécurisation traditionnelles

Ces vingt dernières années, les systèmes antivirus (AV) basés sur les signatures étaient généralement efficaces. Pendant plus de deux décennies, ils ont réussi à contenir la propagation des virus. Le code malveillant moderne présente cependant des caractéristiques très différentes des virus du passé. Un virus se définit comme un code autoreproducteur, le plus souvent conçu pour perturber ou bloquer un réseau. Le code malveillant d'aujourd'hui est discret, très ciblé, et peut ou non se reproduire. Les pirates développent de nouveaux programmes capables de déjouer les logiciels AV classiques. Les attaques modernes pénètrent les systèmes de protection classiques basés sur les signatures en employant des techniques multiformes conçues pour pirater les systèmes à des fins lucratives.

Menaces et défenses de ces 20 dernières années

Menaces de nouvelle génération et défenses classiques

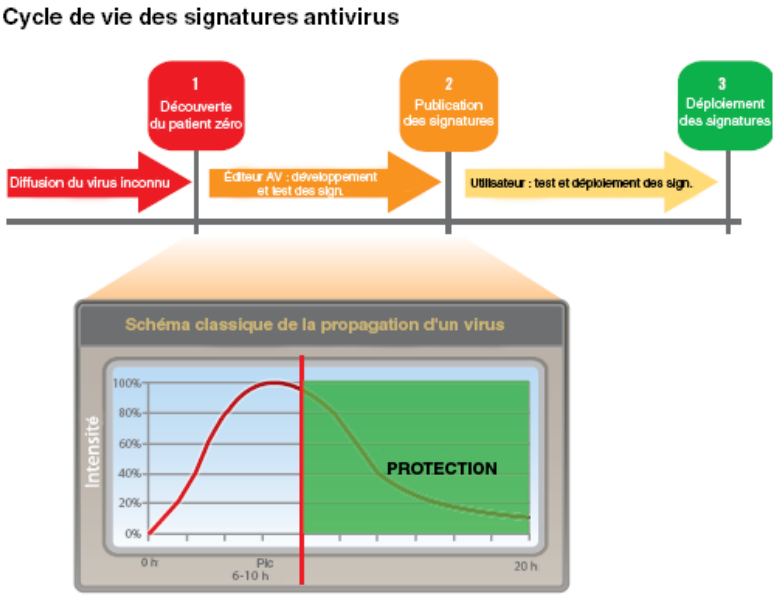
Pendant plus de 20 ans, les systèmes antivirus basés sur les signatures ont protégé les entreprises contre la plupart des attaques. Mais les menaces modernes sont multiformes et plus puissamment armées, et font l'objet d'un déploiement stratégique pour contourner les systèmes de protection classiques.

Le cycle de protection classique

Des cyberdélinquants inventifs ont étudié le fonctionnement des solutions de sécurité classiques afin de mettre au point de nouveaux "maliciels" capables de tirer parti de leurs angles morts. Prenons le cas d'une épidémie virale. Dès lors que le virus se propage, le processus de défense par signature se déroule en trois phases :

1. Découverte
2. Développement et publication de la signature
3. Déploiement de la signature

Dans la première phase de l'attaque, un nouveau virus "autoreproducteur" pénètre le réseau et s'exécute. Ces attaques étant conçues pour provoquer des problèmes réseau très visibles, les virus étaient généralement découverts rapidement.



Après la découverte d'un virus, les éditeurs de logiciels AV passent à la phase suivante : le développement et la publication de la signature. Ils conçoivent une signature capable d'offrir une protection contre de futures attaques. Une fois la signature mise au point, elle est déployée dans le cadre des mises à jour régulières communiquées aux utilisateurs. Ce processus est systématique, mais les phases de développement et de déploiement peuvent prendre des heures, voire des jours, les entreprises restant sans défense entre-temps. L'entreprise a de plus ses propres délais de déploiement pour tester et mettre en œuvre la nouvelle signature. Les délais de développement et de déploiement de la signature sont souvent conditionnés par la nocivité et la vitesse de propagation d'un virus.

Le code malveillant déjoue le cycle traditionnel de défense par signature

Les menaces modernes sont conçues pour s'attaquer aux systèmes de sécurisation classiques ainsi qu'aux réseaux et aux données qu'ils protègent. Pour commencer, un maliciel capable de différer ou d'éviter sa découverte déjoue l'ensemble du processus. Du fait de sa furtivité et de sa précision, le code malveillant ne répond pas au premier critère de hiérarchisation de la majorité des logiciels AV, puisqu'il n'infecte pas un grand nombre de systèmes. En contournant ou en retardant la phase de découverte, les nouveaux

maliciels portent un coup terrible à la stratégie de défense obsolète des antivirus basés sur les signatures.

En second lieu, les pirates utilisent activement la technologie pour créer des variantes d'attaques multiformes. Les attaques les plus complexes associent plusieurs techniques – "maliciels ciblés" (designer malware), chantage (ransomware), outils de dissimulation d'activité (rootkits), chevaux de Troie... Ces attaques multiformes renforcent les chances de contournement et d'évitement des systèmes AV existants. Les menaces de nouvelle génération mettent systématiquement en œuvre une méthode ou une caractéristique spécifique qui accroît l'exposition de l'entreprise. Pour réduire les chances de succès des attaques "malicielles", les responsables de sécurité doivent connaître l'ennemi. Et pour renforcer leurs défenses, ils doivent comprendre les attributs, les caractéristiques et les scénarios de déploiement possibles de ces attaques modernes.

Découvrez vos nouveaux ennemis

Maliciel ciblé (designer malware) : *Code malveillant conçu pour infecter ou menacer une organisation ou un petit nombre d'organisations ayant un profil similaire. Par exemple, un cheval de Troie écrit spécialement pour une banque déterminée.*

Les menaces émanant de ce type de maliciel sont très spécifiques. Comme les attaques ciblées, elles font appel à une méthode très spécifique et, au niveau le plus simple, peuvent viser une entreprise ou une population d'utilisateurs déterminée. Les logiciels AV traditionnels ayant l'habitude de hiérarchiser les menaces en fonction du "nombre total" de systèmes infectés, les maliciels ciblés tirent parti de cette conception dépassée des risques pour passer à travers les mailles.

Il est possible de développer des signatures antivirus pour ce type de logiciel. Mais les pirates ont bien compris les mécanismes de défense classiques et conçoivent des attaques qui évitent soigneusement les points déclencheurs. Une attaque qui ne se propage pas au-delà d'un petit cercle d'utilisateurs a peu de chances d'être détectée.

Si la plupart des pirates modernes préfèrent le profit à la gloire, certains maliciels ciblés sont à l'origine de nombre d'attaques retentissantes. En Israël, une attaque lancée au moyen d'un cheval de Troie à des fins d'espionnage industriel est restée invisible pendant 18 mois. Cette affaire reflète la

tendance des nouvelles attaques : déjouer les défenses existantes et voler des informations pendant le plus longtemps possible avant d'être découvert.

Avec les millions de dollars investis dans des recherches propriétaires, le secteur des biotechnologies est une cible privilégiée des "designer malware". On imagine sans peine la valeur que peut avoir la formule du futur médicament miracle. Deux firmes de biotechnologie ont été victimes de maliciels spécialement conçus pour dérober les secrets de laboratoire de nouveaux projets. Les logiciels malveillants de ce type ont la capacité de voler des découvertes et des secrets commerciaux en relativement peu de temps sans être découverts.

Harponnage (spear phishing) : *Cette technique qui conjugue hameçonnage et "ingénierie sociale" (ou piratage psychologique) vise un individu ou un groupe d'individus. L'attaque est d'autant plus crédible qu'elle est extrêmement ciblée.*

Le harponnage allie le hameçonnage classique à des techniques de piratage psychologique pour construire des attaques très ciblées. Il est très employé dans la cyberpiraterie d'État et dans les attaques dirigées contre les institutions financières. L'attaquant utilise des informations privées ou publiques sur des individus pour rédiger un e-mail personnalisé qui semble provenir d'une source légitime et incite la victime à répondre en fournissant ses informations personnelles (nom d'utilisateur, mot de passe...). Exemple : le nom et les coordonnées professionnelles de Jean Dupont sont publiés dans un magazine spécialisé faisant état de sa récente promotion. Le pirate utilisera ces informations pour envoyer à l'intéressé un e-mail contrefait mais d'allure officielle concernant un prétendu service et l'invitant à activer un nouveau compte complémentaire. En répondant, Jean Dupont permet à l'attaquant d'installer un cheval de Troie ou une porte dérobée sur son ordinateur – ou fournit un identifiant et un mot de passe qui peuvent être les mêmes que ceux qu'il utilise pour accéder en ligne à son compte bancaire.

Chantage (ransomware) : *Ce logiciel malveillant effectue l'archivage chiffré de fichiers importants et efface les fichiers originaux, qui deviennent ainsi inaccessibles à moins du versement d'une rançon. Des formes de chantage plus perfectionnées mettent en œuvre diverses formes de manipulation et d'extorsion.*

Le chantage représente une tendance marquée. L'attaquant chiffre les documents d'un utilisateur et oblige ce dernier à verser une rançon s'il veut pouvoir accéder de nouveau à ses fichiers au moyen d'un mot de passe qui lui sera fourni. Généralement, l'utilisateur paie la rançon en "achetant" un produit coûteux sur un site Web conçu par le pirate.

Ce type d'attaque recourt également à l'intimidation en disant aux victimes qu'elles se sont mises dans cette situation parce qu'elles ont visité des sites Web indécents ou qu'elles ont stocké des contenus pornographiques sur leur ordinateur. Que ces accusations soient vraies ou fausses, elles peuvent dissuader les utilisateurs de rechercher l'assistance des responsables de la sécurité. Ces nouvelles menaces, fondées non seulement sur la technologie mais aussi sur l'implication directe de l'utilisateur, ont une capacité de nuisance qui dépasse le strict cadre d'Internet, auquel sont confinés les vers traditionnels.

Certains "ransomware" emploient des méthodes furtives entraînant l'autodestruction du code après le chiffrement des contenus de l'utilisateur, ce qui rend encore plus difficile le déverrouillage des fichiers sans le concours de l'attaquant.

Outils de dissimulation d'activité (rootkits) : *Capables de rendre un programme malveillant totalement invisible pour le système d'exploitation et les analyseurs de signatures AV, les outils de dissimulation d'activité peuvent être associés à plusieurs types de maliciel pour pirater les systèmes de l'entreprise et lancer des attaques multiformes.*

Les "rootkits" représentent aujourd'hui l'une des principales menaces du fait de leur caractère furtif et de leur aptitude à s'associer avec d'autres logiciels malveillants. Il s'agit en fait d'une technologie de dissimulation qui contribue à rendre n'importe quel type de maliciel indétectable par l'analyse de signatures AV. En s'insinuant dans le système d'exploitation du système infecté, ces "outils" peuvent empêcher la détection des activités qu'ils veulent

masquer. Des commandes courantes comme le listage des fichiers d'un répertoire peuvent perdre toute fiabilité, car des fichiers peuvent être cachés.

Le dépistage de tels programmes ressemble à un jeu de cache-cache. Si vous voyez la personne se cacher, vous avez bien plus de chances de la trouver. Mais si vous n'avez pas vu où elle s'est cachée, il est possible que vous ne puissiez jamais la trouver. Les technologies de protection comportementales peuvent permettre d'identifier des rootkits avant qu'ils s'installent. Une fois qu'un rootkit s'est dissimulé, il risque d'être trop tard et les dégâts peuvent être irrémédiables.

Nombre d'entreprises essaient d'éliminer les programmes de dissimulation après une infection, mais les bonnes pratiques préconisent plutôt de recréer une image du système pour le restaurer. Pourtant, même si l'on prend le temps de restaurer le système, le mal est souvent déjà fait. Si le rootkit a permis le vol d'informations stratégiques ou de secrets commerciaux, l'entreprise ne peut plus récupérer des informations rendues publiques ou communiquées à la concurrence.

Cheval de Troie (trojan) : *Les chevaux de Troie n'ont rien de nouveau, mais ils reviennent au premier plan. Il s'agit de programmes qui incitent l'utilisateur à les exécuter pour effectuer des opérations apparemment anodines, mais qui conduisent en réalité des activités clandestines nuisibles.*

Les chevaux de Troie jouent un rôle grandissant dans les menaces modernes axées sur le profit. En 2006, ils ont constitué 75 % des maliciels. Leur caractère furtif facilite le vol de données ou l'accès à des systèmes en vue d'une exploitation future. Exemple : les enregistreurs de frappe (keyloggers) et les récupérateurs de mots de passe qui permettront d'accéder frauduleusement à des comptes pour réaliser des gains financiers.

La plupart des logiciels AV basés sur les signatures sont peu efficaces contre les chevaux de Troie, car ils sont conçus avant tout pour détecter des programmes malveillants autoreproducteurs. À défaut de méthodes comportementales efficaces pour détecter les chevaux de Troie, des organisations comme les institutions financières sont particulièrement exposées.

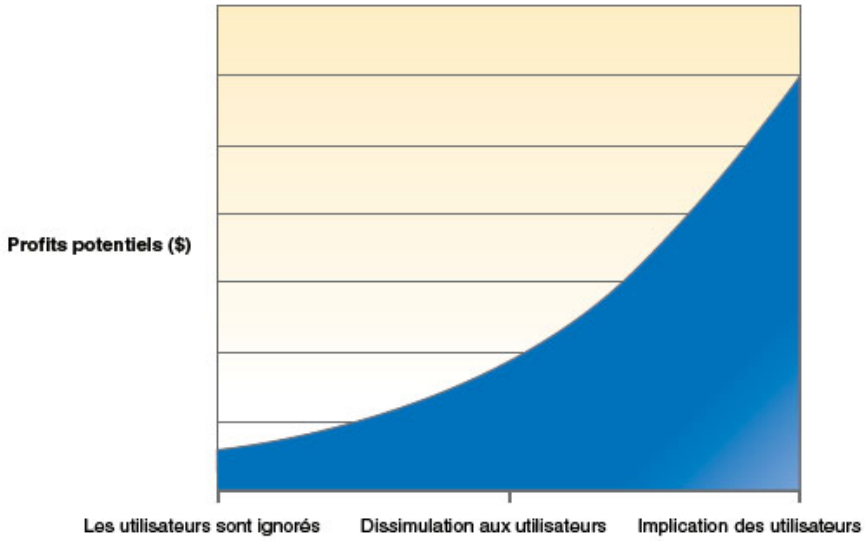
La crise que traverse le secteur bancaire brésilien illustre bien l'efficacité des nouveaux chevaux de Troie. Des pirates utilisent des chevaux de Troie personnalisés pour vider les comptes des clients. Les attaques courantes recourent à des techniques de hameçonnage pour installer un cheval de Troie sur les ordinateurs des utilisateurs. Une fois les machines infectées, le code malveillant guette le moment où l'utilisateur visite le site d'une banque; il affiche alors une page d'accueil contrefaite ou capture les informations de connexion. La grande innovation des chevaux de Troie modernes est l'utilisation de sites Web authentiques. En effet, les utilisateurs se laissent difficilement tromper par un site factice. Les nouveaux chevaux de Troie s'ingénient donc à leur dérober des informations d'identification lorsqu'ils visitent le vrai site d'une institution financière.

Les banques brésiliennes n'ont réussi à détecter la présence d'un nouveau cheval de Troie personnalisé qu'après le signalement de la fraude par un client. Une fois le problème identifié, un éditeur AV peut développer une nouvelle signature, mais cette signature sera inopérante contre un autre cheval de Troie personnalisé. Dans ce scénario, on parle aussi de "maliciel ciblé" (designer malware).

Un mode opératoire qui évolue

Les règles du jeu ont changé : les menaces continuent à évoluer, et les cyberdélinquants ne sont plus motivés par la gloire, mais par le profit. Faute d'une défense adéquate contre les nouvelles menaces innovantes, les organisations et leurs utilisateurs s'exposent à des risques bien réels.

Les menaces ne sont plus simples : la plupart des attaques modernes conjuguent plusieurs techniques à la fois et, pour offrir une protection efficace, vos défenses doivent couvrir tout le spectre. Le seul recours à des systèmes comme l'analyse des signatures sera généralement insuffisant face aux nouvelles attaques. Les entreprises qui se polarisent sur les menaces connues seront sans défense devant des pirates qui inventent et développent sans cesse des maliciels capables de déjouer les technologies de protection traditionnelles et les analyses de signatures AV existantes. Et si les technologies proprement dites évoluent, la façon dont les logiciels malveillants sont mis en œuvre pour manipuler leurs victimes évolue elle aussi.



Les attaques antérieures ignoraient les utilisateurs et recherchaient la gloire et la notoriété en provoquant des pannes à grande échelle. Puis, les attaques ont commencé à se faire plus discrètes tandis que des possibilités de gains financiers se faisaient jour. Aujourd'hui, le déploiement créatif de maliciels peut impliquer directement les utilisateurs pour maximiser les profits potentiels.

Le virus Satan est un exemple de déploiement créatif de code malveillant pour générer du profit. L'université de Cambridge a signalé dans un rapport que le virus Satan développait des interactions étroites avec l'utilisateur pour rester actif et accroître les profits.

Le virus Satan

Les interactions de l'utilisateur avec le virus Satan jouent sur les émotions. Tout d'abord, l'attaquant va convaincre un utilisateur qu'il peut retirer un avantage de l'exécution du virus. Par exemple, le virus peut offrir à un employé la capacité de voir les fichiers ou les e-mails de son supérieur. Et si l'employé accepte l'offre et déploie le virus, il pourra effectivement accéder à ces documents.

Par la suite, le virus enregistre la fréquence à laquelle l'employé visualise les e-mails ou les fichiers de son chef, puis il utilise ces informations pour faire chanter l'employé. Ce dernier devra maintenir le virus en vie, faute de quoi il lui faudra répondre de ses actes. Dans la mesure où il s'agit au départ d'un virus très ciblé, l'attaquant doit recourir au chantage pour propager le virus, au lieu d'en retirer un profit immédiat. Et il pourra exiger de l'employé qu'il démarche des collègues afin de développer les activités de chantage ainsi que les profits pouvant en résulter.

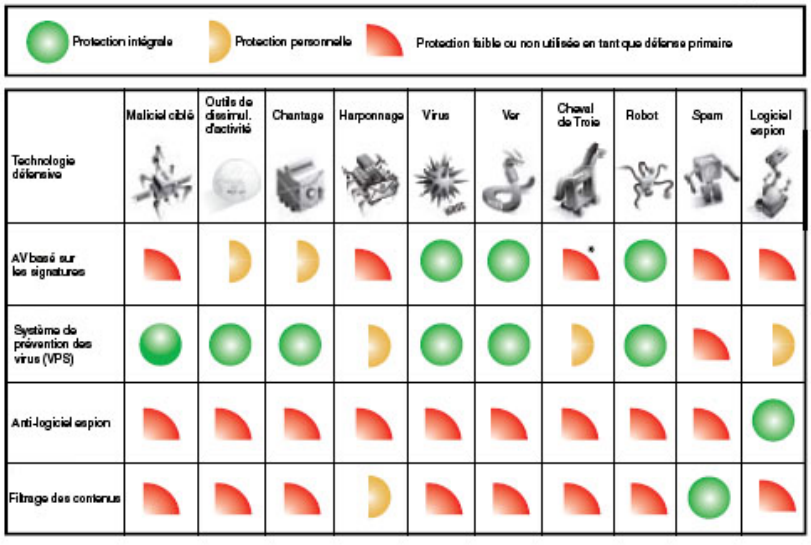
Comment se protéger contre les nouvelles menaces

Compte tenu des progrès de la technologie et de la façon dont les menaces sont mises en œuvre, les systèmes d'entreprise doivent déployer plusieurs couches de défense pour réduire les risques. Face à l'augmentation du nombre des attaques multiformes, il y a en effet des chances qu'une forme finisse par réussir – à moins d'une défense appropriée.

La Figure B montre les niveaux de protection que peut fournir une technologie défensive face à chaque type de menace. Chacune de ces technologies est conçue pour fournir une protection contre certains types de menaces, mais peut aussi servir contre d'autres types de menaces dans certaines situations.

Pour donner une vue générale des fonctionnalités, ce tableau présente trois niveaux de protection :

Figure B



** Si certains éditeurs de logiciels AV basés sur les signatures offrent une certaine protection contre les chevaux de Troie, cette protection intervient souvent après l'infection et ne s'applique qu'aux clients de l'éditeur. Ce niveau de protection n'est pas toujours efficace contre les menaces de nouvelle génération*

Historiquement, les éditeurs de systèmes AV basés sur les signatures ont réussi à éviter la propagation de la plupart des attaques dès lors qu'une signature avait été développée. Le principe même de cette technologie la rend efficace contre les virus, les vers ou les robots. Mais elle est moins probante contre les chevaux de Troie. De fait, en général, les certifications AV ne testent pas la capacité des moteurs d'analyse à détecter les chevaux de Troie susceptibles de véhiculer des menaces ciblées. Les responsables sécurité doivent donc vérifier le niveau de protection dont ils bénéficient réellement contre un maliciel ciblé ou des chevaux de Troie personnalisés. Par exemple, les laboratoires ICSA ne testent que les maliciels autoreproducteurs, tandis que la WildList et WildCore testent uniquement les virus et les vers.

Les technologies anti-logiciel espion et de filtrage des contenus sont efficaces contre les logiciels espion et les pourriels (spam), respectivement, mais n'offrent pas de réelle protection contre les menaces de nouvelle génération dont nous traitons ici.

IBM Virus Prevention System (VPS) est une technologie antivirus comportementale conçue pour stopper les attaques "jour 0" par une pré-exécution du code dans un espace virtuel, le maliciel étant bloqué avant de toucher sa cible s'il manifeste un comportement malveillant. Ce type de détection est crucial dans la lutte contre les menaces actuelles les plus avancées. Grâce à la technologie comportementale, VPS fournit une protection renforcée et élargie contre les attaques.

Principales différences entre VPS et les AV basés sur les signatures

Protection contre les menaces de nouvelle génération	 Maliciel ciblé	 Chantage	 Outils de dissimulation d'activité
Virus Prevention System (VPS)	Peut protéger le patient zéro	Détention proactive	Prévient l'installation de rootkits
AV basé sur les signatures	A d'abord besoin d'un patient zéro	Peut détecter mais ne peut pas nettoyer après l'infection (les données sont volées)	Ne peut pas nettoyer après l'installation

IBM Internet Security Systems (ISS) : une plate-forme de protection intégrale

La plate-forme de protection IBM est une solution simple et intégrée qui met la défense proactive à la portée de toutes les organisations soucieuses de leur sécurité.

Étant donné la forte motivation des pirates, les entreprises doivent se doter d'une plate-forme de protection capable d'évoluer et de s'adapter constamment aux nouvelles menaces. Les produits et les services avancés de sécurité d'IBM interagissent comme un système intégré. Chaque module assure individuellement une protection efficace contre différents types de menaces et de situations, mais la protection est encore plus efficace quand le module est mis en œuvre dans le cadre de la plate-forme de protection intégrée.

Les solutions de protection IBM combattent les nouvelles menaces avec les technologies de sécurisation les plus perfectionnées. La technologie antivirus brevetée Virus Prevention System (VPS) d'IBM est conçue pour détecter les comportements malveillants et ne nécessite pas de mise à jour des signatures. L'approche proactive d'IBM est entièrement axée sur la prévention des comportements malveillants plutôt que sur une protection contre les seules menaces connues. La plate-forme de protection d'IBM couvre la totalité de l'entreprise avec des solutions pour les postes de travail, les serveurs, les réseaux et les passerelles – le tout géré centralement à partir d'une unique console. Les caractéristiques de cette plate-forme capable de prévenir efficacement les menaces de nouvelle génération sont les suivantes :

- Technologie VPS – une technologie exclusive qui agit de façon proactive contre les programmes suspects même avant qu'ils ne soient connus publiquement. VPS analyse le code et le "pré-exécute" dans un environnement virtuel : il n'y a donc pratiquement aucun risque de contamination du vrai système ni de dommages collatéraux pendant la détection. En mettant en œuvre une technologie de détection comportementale, au lieu de la reconnaissance de signatures connues, VPS offre une puissante protection même contre les plus menaces les plus récentes – maliciels ciblés, outils de dissimulation d'activité et chantage. La technologie VPS est intégrée dans de nombreux produits IBM, dont IBM Proventia® Desktop Endpoint Security, Proventia Network Mail Security System et Proventia Network Multi-Function Security (MFS).

- IBM Proventia Desktop est une solution multifonction qui assure une protection proactive contre plusieurs types de menaces à la fois. Proventia Desktop mérite sa réputation d'agent de protection multifonction le plus complet, avec pare-feu personnel, prévention des intrusions fondée sur les vulnérabilités, prévention des attaques par dépassement de mémoire, contrôle des applications, antivirus basé sur les signatures et technologie VPS. Toutes ces technologies coopèrent pour bloquer les menaces Internet avant qu'elles n'atteignent les postes de travail et puissent causer des dommages – pannes, manque à gagner ou installation de code malveillant susceptible de voler des informations ou de provoquer des pertes financières directes.

- IBM Proventia Server Intrusion Prevention est une solution multifonction de prévention des intrusions sur les serveurs conçue pour bloquer proactivement plusieurs types de menaces à la fois. Les menaces hybrides et les attaques sophistiquées d'aujourd'hui déjouent les défenses traditionnelles. Grâce à son architecture multifonction, Proventia Server peut faire intervenir une autre technologie si une technologie de protection ne suffit pas contre une menace donnée.

- IBM Proventia Network Mail assure la protection proactive de l'infrastructure de messagerie de l'entreprise, avec contrôle des spams. Son évolutivité lui permet de prendre en charge les grands environnements avec un déploiement d'outils limité. Proventia Network Mail met en œuvre la technologie VPS pour bloquer les codes malveillants et le trafic suspect.

- IBM Proventia Network MFS est un système de sécurité réseau multifonction qui allie la puissante technologie de prévention des intrusions d'IBM aux capacités des logiciels AV classiques et à l'approche comportementale de VPS. Il inclut également pare-feu, filtrage Internet et technologie anti-spam pour parer de façon proactive à toute une série de menaces – accès illicites, attaques réseau, code malveillant et menaces multiformes.

Des services de protection contre les menaces de nouvelle génération

IBM Professional Security Services et IBM Managed Security Services apportent une protection renforcée contre les menaces les plus récentes. Dans le cadre de ses services gérés, IBM est en première ligne pour observer les nouveaux programmes malveillants et leurs tendances comportementales, et peut ainsi offrir des services de protection efficaces.

IBM Professional Security Services fournit des services de conseil expert pour aider les entreprises de toutes tailles à réduire les risques, à répondre aux exigences de la réglementation, à préserver leur continuité opérationnelle et à répondre à leurs besoins de sécurité. Spécialisés à 100 % sur les problèmes de sécurité, ces consultants de haut niveau s'appuient sur des méthodes validées fondées sur les bonnes pratiques ISO 17799 et bénéficient du soutien de l'équipe de recherche et développement IBM Internet Security Systems X-Force®. Ils font appel à des outils internes, aux connaissances les plus pointues et aux contre-mesures les plus perfectionnées pour développer des programmes de sécurisation capables de fiabiliser l'exploitation des entreprises en luttant efficacement contre des menaces qui évoluent en permanence.

IBM Managed Security Services est une solution idéale pour les organisations qui veulent optimiser la sécurité de leurs informations. IBM fournit l'expertise, le savoir-faire et l'infrastructure nécessaires pour protéger le patrimoine informationnel de l'entreprise contre les attaques Internet – 24 heures sur 24, 7 jours sur 7, 365 jours par an.

En savoir plus sur la prévention des menaces de nouvelle génération

Pour en savoir plus sur les menaces de nouvelle génération et sur les produits et les services conçus pour les empêcher d'affecter les réseaux des entreprises, visitez :
ibm.com/services/fr.

Pour accéder à des contenus de formation et de sensibilisation, avec des fiches solutions, des forums stratégiques régionaux et des actualités sur les menaces de nouvelle génération discutées dans ce dossier, visitez : www.iss.net/evolvingthreat/.

Des menaces en mutation – Mini-glossaire

Vous trouverez ici une brève définition des principales menaces présentées dans ce dossier.

Logiciel antivirus basé sur les signatures (Signature Anti-virus - AV) – *Programme informatique conçu pour détecter et neutraliser des logiciels malveillants comme des virus et des vers. Les réactions peuvent consister à bloquer l'accès des utilisateurs aux fichiers infectés, à nettoyer les fichiers ou les systèmes infectés ou à informer les utilisateurs de la détection d'un programme infecté.*

Menaces multiformes (Blended Threats) – *Association de plusieurs types de code malveillant visant à accroître l'efficacité et les chances de succès d'une attaque.*

Maliciel ciblé (designer malware) – *Code malveillant conçu pour infecter ou menacer une organisation ou un petit nombre d'organisations ayant un profil similaire. Par exemple, un cheval de Troie écrit spécialement pour une banque déterminée.*

Code malveillant ou maliciel (malcode) – *Programme dont l'exécution permet à un pirate de conduire des activités malveillantes.*

Chantage (ransomware) – *Code malveillant consistant le plus souvent à protéger des fichiers par mot de passe sur le système d'un utilisateur jusqu'au paiement d'une rançon. Des formes de chantage plus perfectionnées mettent en œuvre diverses formes de manipulation et d'extorsion.*

Outils de dissimulation d'activité (rootkit) *– Programmes capables de rendre un logiciel malveillant invisible pour le système d'exploitation, l'utilisateur et les fonctions de protection. Il existe de nombreux types de "rootkits" – dans l'espace utilisateur, dans l'espace noyau, sur une machine virtuelle, au niveau de l'hyperviseur, dans la couche NDIS (Network Driver Interface Specification), et même dans la mémoire EEPROM (mémoire morte programmable effaçable électriquement) et dans la mémoire vidéo.*

Harponnage ou filoutage (spear phishing) *– Technique associant hameçonnage et "ingénierie sociale" (ou piratage psychologique) et visant un individu ou un groupe d'individus. L'attaque est d'autant plus crédible qu'elle est extrêmement ciblée.*

Attaque ciblée (Targeted Attacks) *– Analogue à un maliciel ciblé, une attaque ciblée peut aussi viser une population d'utilisateurs spécifique.*

Cheval de Troie (trojan) *– Programme qui incite l'utilisateur à l'exécuter pour effectuer des opérations apparemment anodines, mais qui conduit en réalité des activités clandestines malveillantes comme l'enregistrement de touches (keylogging) ou le vol de mot de passe.*

Virus *– Réplication, via des fichiers hôtes, de code implanté illégalement dans un programme informatique, généralement en vue d'endommager ou de bloquer un système ou un réseau.*

Ver (worm) *– Programme autoreproducteur qui utilise un réseau pour transmettre des copies de lui-même à d'autres terminaux. À la différence d'un virus, un ver n'a pas besoin de s'adjoindre à un programme existant et ne requiert pas d'intervention de l'utilisateur pour se propager. Un ver peut perturber le réseau (par exemple, en consommant de la bande passante), alors que les virus infectent ou altèrent toujours les fichiers d'un ordinateur cible.*

Compagnie IBM France
Tour Descartes - La Défense 5
2, avenue Gambetta
92066 Paris La Défense Cedex

Imprimé en France
01-08

GTW03007-FRFR-00