Rapport

Rapport de McAfee sur le paysage des menaces : 1er trimestre 2009

McAfee® Avert® Labs

Sommaire

Ce *Rapport de McAfee sur le paysage des menaces* présente les dernières statistiques et analyses concernant les menaces véhiculées par le Web et la messagerie électronique. Ce rapport trimestriel est le fruit du travail des chercheurs de McAfee Avert Labs, qui, grâce à une équipe répartie aux quatre coins de la planète, offrent un point de vue unique sur le paysage actuel des menaces et leurs cibles — des particuliers aux grandes entreprises — ainsi que les régions du monde dans lesquelles elles font rage. Découvrez avec nous les principaux problèmes de sécurité qui ont surgi ces trois derniers mois. Pour plus d'informations, vous pouvez également consulter McAfee Threat Center à l'adresse http://www.mcafee.com/us/threat_center/default.asp ou www.trustedsource.org.

Au cours du 1er trimestre 2009, le paysage des menaces a connu des changements spectaculaires par rapport à l'année dernière ou même à il y a quelques mois. Personne n'aurait parié sur une diminution du volume de spam en circulation, mais avec la fermeture de McColo en novembre 2008, c'est pourtant ce qui s'est passé. Le nombre de messages de spam demeure 30 % en-deçà de son pic, et nous n'avons pas assisté à l'augmentation qui caractérise toujours le mois de mars. La question n'est pas tant de savoir *si* le spam atteindra à nouveau les niveaux antérieurs, mais plutôt *quand*. Diverses données concernant le développement de nouveaux zombies et réseaux de robots (botnets) donnent à penser que cela ne devrait pas tarder.

Le nombre de sites web malveillants est en hausse, à l'instar des sites hébergeant des logiciels malveillants (malwares), qui sont plusieurs milliers à faire leur apparition chaque jour. De nouvelles formes de logiciels malveillants sont par ailleurs créées quotidiennement, et celles qui ont atteint les niveaux de prévalence les plus élevés sont présentées dans ce rapport.

Ces derniers temps, le ver Conficker, connu officiellement sous le nom de W32/Conficker.worm, a mobilisé énormément d'attention par rapport aux autres menaces de sécurité. Ce rapport tentera de déterminer s'il ne s'agit que de pur battage médiatique ou d'une menace bien réelle. Nous examinerons également les menaces qui ne sont pas autant relayées par les médias, alors, qu'en fait, elles pourraient s'avérer plus dangereuses que celles qui défraient davantage la chronique.

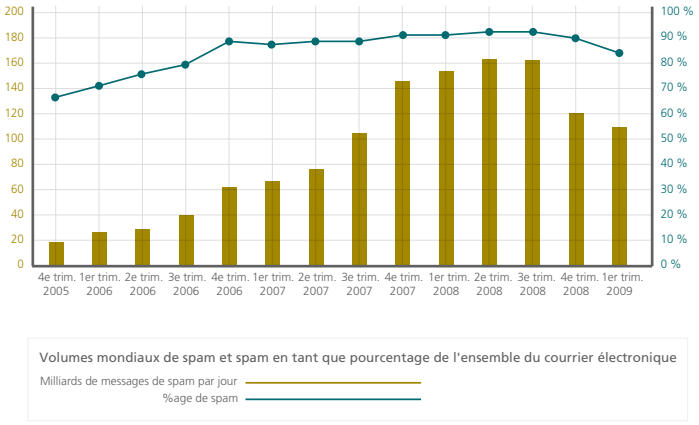
La répartition géographique des menaces ne cesse d'évoluer, raison pour laquelle ce rapport propose une analyse des facteurs géographiques liés au développement des menaces, en analysant notamment l'origine du spam, les sources de zombies et l'emplacement des sites malveillants, en plus d'identifier les acteurs émergents du marché des menaces. Certaines données très intéressantes contenues dans ce rapport laissent par ailleurs entendre que les pays générateurs de menaces ne font pas grand cas du fait que celles-ci sont exploitées contre des entités nationales.

Pour terminer, nous passerons en revue une série de prévisions établies dans notre rapport *Paysage des menaces : prévisions pour 2009*, publié en janvier, afin de voir si et comment elles se réalisent. Parmi les principales tendances mises en lumière, citons l'utilisation de l'actualité récente et des réseaux sociaux pour prendre au piège des utilisateurs trop confiants.

Le spam toujours au centre des préoccupations à l'échelle mondiale

Quelle récession ?

De manière générale, le volume d'e-mails et de spam au cours du 1er trimestre 2009 a atteint des niveaux que nous n'avions plus vus depuis quasiment deux ans. Les spammeurs sont-ils, à l'instar du reste de l'économie, victimes d'une conjoncture économique difficile ? La question ne se pose pas réellement en ces termes. Le fait est que le spam ne s'est pas encore entièrement remis du démantèlement de McColo, intervenu en novembre 2008. Le volume enregistré au 1er trimestre 2009 est 20 % plus bas qu'au cours du même trimestre de l'année dernière, et 30 % plus bas qu'au cours du 3e trimestre 2008, qui a affiché les volumes trimestriels les plus élevés à ce jour. Si le volume de spam en circulation a d'ores et déjà regagné environ 70 % depuis la déconnexion de l'hébergeur, il n'est toujours pas revenu à ses niveaux antérieurs.



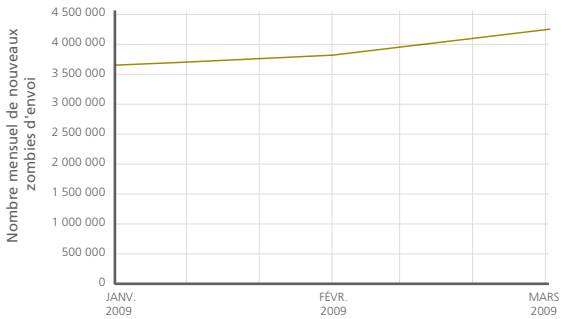
Ces dernières années, le mois de mars a battu tous les records en termes de volume de messages, mais nous sommes loin du compte cette année : en mars de l'année dernière, 153 milliards de messages par jour en moyenne ont été envoyés contre seulement une centaine de milliards cette année.

Le pourcentage de spam par rapport à l'ensemble des messages envoyés est tombé sous la barre des 90 %, du jamais vu depuis 2006. Pour l'ensemble de l'année 2008, nous avons évalué le spam à 90 % du volume total des e-mails, contre 86 % ce dernier trimestre. D'après les estimations, même si les comptes de messagerie et leur activité respective varient considérablement, les utilisateurs reçoivent de six à douze fois moins d'e-mails par jour comparé à l'année dernière.

D'après nous, les volumes de spam devraient atteindre à nouveau les niveaux de 2008, mais la réorganisation des centres de commande et des réseaux de robots par les spammeurs après le démantèlement de McColo a pris plus de temps que beaucoup ne l'avaient pensé au départ. En fin de compte, c'est avant tout une question de retour sur investissement pour les spammeurs, de même que dans toute autre activité.

Les zombies pullulent et font grimper la production

Au cours du dernier trimestre, nous avons identifié près de douze millions de nouvelles adresses IP « zombies », c'est-à-dire d'ordinateurs sous le contrôle de spammeurs et autres pirates. Il s'agit d'une augmentation importante, de près de 50 %, par rapport au dernier trimestre 2008. Malgré un nombre record de nouveaux zombies enregistré au 3e trimestre 2008, les chiffres de ce trimestre placent la barre encore plus haut, avec un million de zombies supplémentaires. Et bien que le volume de spam n'ait pas encore rejoint les niveaux d'avant la fermeture de McColo, le niveau d'activité des nouveaux zombies et le zèle avec lequel les spammeurs s'efforcent de retisser leur toile laissent à penser que cela ne saurait tarder.



Une ventilation des systèmes infectés par pays montre qu'au cours du dernier trimestre, 63 % des nouveaux zombies sont apparus dans les dix pays les plus touchés par ce phénomène, soit une légère diminution par rapport aux deux précédents trimestres. Il semble que les spammeurs s'attaquent aux ordinateurs d'un nombre toujours plus grand de pays pour nourrir leurs efforts.

1er trim. 2009		4e trim. 2008		3e trim. 2008	
Pays	Pourcentage d'adresses IP	Pays	Pourcentage d'adresses IP	Pays	Pourcentage d'adresses IP
Etats-Unis	18,0	Chine	15,8	Chine	20,4
Chine	13,4	Etats-Unis	15,4	Etats-Unis	16,5
Australie	6,3	Allemagne	6,5	Allemagne	6,8
Allemagne	5,3	Royaume-Uni	6,0	Royaume-Uni	6,0
Royaume-Uni	4,7	Brésil	4,9	Brésil	4,8
Brésil	4,0	Espagne	4,3	Espagne	3,7
Inde	3,1	Australie	4,1	Inde	2,5
Espagne	3,0	Italie	3,5	Russie	2,4
Corée du Sud	2,8	Russie	3,1	Corée du Sud	2,4
Russie	2,5	Corée du Sud	2,4	Italie	2,2
Total	**63,3**	**Total**	**66,0**	**Total**	**67,5**

La Chine et les Etats-Unis ont tour à tour occupé le haut du tableau au cours de ces trois derniers trimestres et dominent le classement en termes de nombre d'ordinateurs zombies sous le contrôle des spammeurs. L'Australie a quant à elle connu une évolution notable, puisqu'elle n'apparaissait pas dans le top dix au troisième trimestre 2008, mais occupe la troisième place depuis les deux derniers trimestres, avec 6 % du nombre total de nouveaux zombies. Le cinquième continent semble être un terrain propice au recrutement de zombies.

1er trim. 2009		4e trim. 2008	
Pays	%age du total	Pays	%age du total
Etats-Unis	35,0	Etats-Unis	34,3
Brésil	7,3	Brésil	6,5
Inde	6,9	Chine	4,8
Corée du Sud	4,7	Inde	4,2
Chine	3,6	Russie	4,2
Russie	3,4	Turquie	3,8
Turquie	3,2	Corée du Sud	3,7
Thaïlande	2,1	Espagne	2,4
Roumanie	2,0	Royaume-Uni	2,3
Pologne	1,8	Colombie	2,0
	70,0		**68,3**

Spam par pays : les Etats-Unis à nouveau au premier rang mondial

Si la situation des constructeurs automobiles américains en termes de production et de ventes est inconfortable, pour ce qui est de la production de spam, les Etats-Unis demeurent en tête du classement mondial avec 35 % du spam généré à l'échelle de la planète. Et bien que les opérations de commande et de contrôle du spam fassent appel à une infrastructure internationale, les spammeurs continuent de privilégier l'utilisation d'ordinateurs américains pour émettre du spam. Les dix principaux pays dominent largement en termes de production de spam, puisqu'ils représentent près de 70 % du total et distancent de loin les 200 et quelque autres pays du monde.

Les données recueillies lors des deux derniers trimestres montrent que c'est l'Inde qui a connu la croissance la plus forte en termes de pourcentage, puisqu'elle génère désormais près de 7 % du spam mondial, soit une multiplication par deux de sa production de spam par rapport au trimestre précédent. Le spam semble être le dernier secteur d'activité en date à miser sur la délocalisation en Inde.

La Thaïlande, la Roumanie et la Pologne font également leur entrée dans le classement des dix plus gros producteurs de spam, ce qui vient appuyer la théorie selon laquelle les spammeurs cherchent tous azimuts de nouvelles sources pour alimenter leurs moteurs de spam.

1er trim. 2009		4e trim. 2008		3e trim. 2008	
Médicaments délivrés sur ordonnance	25,0	Médicaments délivrés sur ordonnance	37,0	Amélioration des performances sexuelles pour l'homme	31,2
Publicité	21,9	Publicité	19,3	Publicité	19,3
Produits de contrefaçon	18,8	Amélioration des performances sexuelles pour l'homme	16,8	Médicaments délivrés sur ordonnance	10,7
Amélioration des performances sexuelles pour l'homme	17,5	Notification de l'état de remise	9,5	Tempête	8,0
Notification de l'état de remise	7,1	Rencontres	3,9	Notification de l'état de remise	7,7
Tempête	1,6	Produits de contrefaçon	2,6	Informations de dernière minute	6,7
Diplômes	1,1	Emploi	1,7	Produits de contrefaçon	6,0
Logiciels	1,1	Logiciels	1,5	Prêts	1,6
Prêts	1,0	Prêts	1,2	Services bancaires	1,1
Autre	4,9	Autre	6,5	Autre	7,7
	100,0		**100,0**		**100,0**

Spam par type : sexe, drogue et plus encore

Le spam portant sur l'amélioration des performances sexuelles pour l'homme, les médicaments délivrés sur ordonnance et la publicité générale continuent d'occuper le haut du classement des types de spam envoyé. Ces trois formes représentent à elles seules environ 60 % du spam envoyé au cours des trois derniers trimestres. On pourrait croire que le slogan « sexe, drogue et rock 'n' roll » se perpétue à travers le spam. C'est presque cela. Sans doute les choses ont-elles quelque peu évolué... Car aujourd'hui, le message pourrait être « sexe, drogue et économie ».

Le spam relatif aux produits de contrefaçon (principalement des montres) a fait un important bond en avant ce trimestre et représente désormais près de 19 % du spam total. Il est devenu très populaire l'année dernière, mais a également connu une croissance importante au cours de ce dernier trimestre, ce qui amènerait à penser que, dans un contexte économique difficile, les spammeurs nous aident à augmenter notre pouvoir d'achat en proposant des affaires à prix défiant toute concurrence.

Le spam lié aux notifications de l'état de la remise reste quant à lui stable (8 % du spam total). Ces messages sont presque toujours associés à des attaques de type phishing et se présentent sous la forme d'un avis retourné après usurpation de l'adresse électronique de la victime. Le phishing est donc clairement toujours d'actualité et se porte bien. Bon nombre de ces messages sont conçus dans le but de réaliser un profit financier et de soutirer des informations personnelles.

Les spammeurs ne respectent la souveraineté d'aucun pays — pas même du leur

Si l'on en croit un mythe répandu au sein de la communauté de la cybersécurité, les cybercriminels, qui résideraient en grand nombre en Europe de l'Est, privilégient les cibles situées dans des pays occidentaux et rechignent à attaquer les citoyens ou les sociétés de leur propre juridiction. Diverses sources et données viennent toutefois démolir ce mythe. Internet ne connaît pas de frontières géographiques. Il est désormais évident que les cybercriminels s'attaquent à toutes les cibles qu'ils rencontrent sur leur chemin. Ainsi, nous disposons de preuves démontrant que les cybercriminels s'en sont pris à des organismes gouvernementaux et des entreprises russes et d'Europe de l'Est de premier plan, ainsi qu'à des responsables et cadres de ces entités.

McAfee TrustedSource™ a récemment observé une série d'e-mails et de messages de spam véhiculant des logiciels malveillants émanant de divers organes gouvernementaux et institutions bancaires russes. D'après notre analyse, les principales banques russes compromises sont les suivantes :

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- The Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

Les données recueillies suggèrent également que les systèmes informatiques des services gouvernementaux russes suivants sont contrôlés par des gangs de cybercriminels :

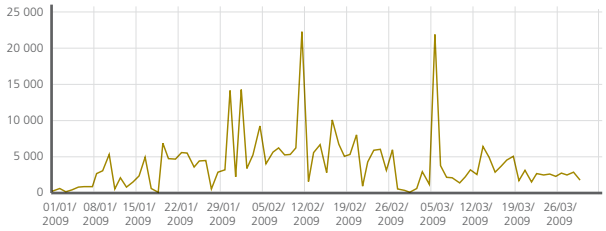
- Ministère des finances de la région de Nazran
- Réseau Internet de l'Etat russe
- Institut régional des finances et de l'économie
- Joint Institute for Nuclear Research (JINR)
- Centre médical du département du président de la Fédération de Russie
- Caisse de retraite de la Fédération de Russie
- Réseau personnel du ministère de la Justice de la Fédération de Russie
- Réseau de communication cellulaire tchétchène JSC

Ces données sur la Russie laissent à penser que les cybercriminels ratissent large et attaquent tout type d'organisation présentant un intérêt financier ou autre. Bien que ce type d'activités (et le volume de spam qu'elles produisent) soit clairement dominé par la Russie, notre étude montre l'existence d'activités similaires dans d'autres pays de l'ancienne Union soviétique, dont l'Ukraine, la Biélorussie, l'Arménie, l'Azerbaïdjan, la Géorgie, le Kazakhstan, le Kirghizstan, la Moldavie, le Tadjikistan, le Turkménistan et l'Ouzbékistan.

Web : de nouveaux sites à la réputation malveillante apparaissent chaque jour

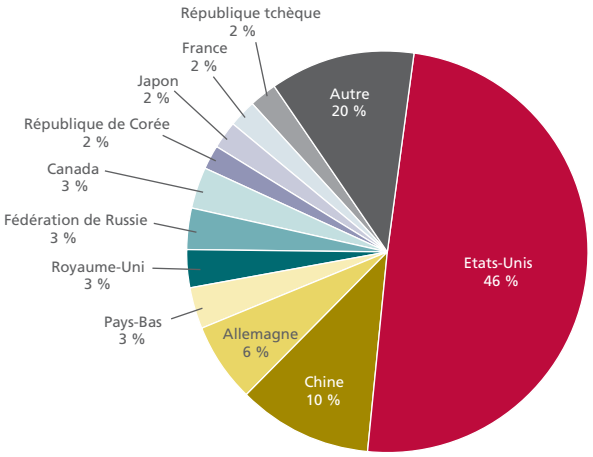
Durant ce trimestre, nous avons assisté à une recrudescence de bon nombre des menaces apparues au cours du dernier trimestre 2008. Bien que le battage médiatique se soit essentiellement focalisé sur le ver Conficker, celui-ci est loin d'être la seule menace à s'être propagée au cours de ce trimestre. En effet, même en faisant abstraction de Conficker, une légère augmentation de l'activité au fil des ans et une hausse manifeste par rapport aux précédents trimestres sont perceptibles. Les applications antivirus malveillantes ont fait naître diverses inquiétudes sur le Web et provoqué une hausse des fraudes et du phishing.

A l'exception du graphique « Répartition des sites web de réputation malveillante », les graphiques ou données d'évolution quotidienne de cette section n'incluent pas les domaines malveillants que Conficker devait contacter. En effet, bien que les données sur Conficker constituent un pan important du paysage des menaces, elles ont tendance à fausser la réalité de l'activité malveillante. De nombreuses autres menaces dont la prévalence s'intensifie sont bel et bien présentes. Les auteurs de logiciels malveillants et autres spécialistes de l'arnaque en ligne profitent en effet du contexte économique dégradé et de nos préoccupations pour développer des sites à des fins d'escroquerie. Ils affirment, entre autres arguments, pouvoir vous éviter une saisie hypothécaire et créent des sites de phishing sur tous les thèmes possibles, allant jusqu'à offrir des cartes de fidélité dans des magasins. Les sites antivirus malveillants continuent d'abuser les utilisateurs trop confiants. Qui plus est, les méthodes utilisées pour attirer les internautes sur des sites web ne cessent d'évoluer. Même en faisant abstraction de toute l'activité liée à Conficker, les sites qui franchissent la ligne les séparant du statut de sites de réputation « malveillante » (ou « rouges ») ont connu une hausse notable par rapport aux deux derniers trimestres 2008.



Nombre de nouveaux sites web de réputation malveillante apparaissant chaque jour

Où se développent tous ces sites de mauvaise réputation web ? Certainement pas à l'endroit où on pourrait le croire.



Distribution des sites web de réputation malveillante

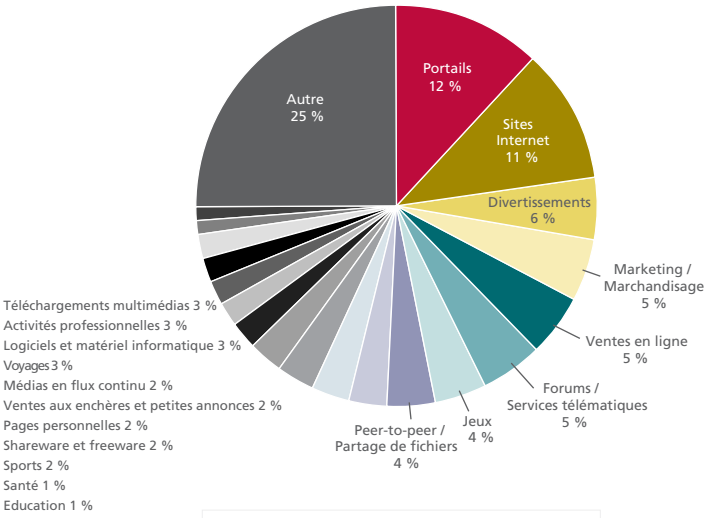
Comment expliquer ce changement soudain dans ce que nous considérions jusqu'à présent comme la « norme » (avec les Etats-Unis, la Chine et la Russie en tête du classement) concernant l'activité web malveillante[1] ? Ce bouleversement ne signifie nullement que le nombre de sites à la réputation

1. Au 3e trimestre 2008, le classement s'établissait comme suit : les Etats-Unis avec 41 %, la Chine avec 12 %, la Russie avec 7 %, l'Allemagne et les Pays-Bas avec 5 %, la Corée du Sud avec 4 %, Hong Kong avec 3 %, Taïwan, le Canada et la République tchèque avec 2 %, les pays restants représentant 17 %.

malveillante a diminué dans ces pays. Simplement, l'augmentation de ces sites a été plus rapide dans d'autres pays. Cette croissance est en grande partie liée à l'endroit où Conficker a implanté certains des domaines qu'il prévoit de contacter ou a contacté. En fait, Conficker est responsable à lui seul du classement des Pays-Bas en quatrième position (ex aequo avec d'autres pays). Bien que les Pays-Bas constituent depuis longtemps un terrain de prédilection pour les sites de phishing, Conficker a provoqué une hausse importante du nombre de sites web infectés par des logiciels malveillants et d'autres types de contenu malveillant. Ce changement ne peut cependant pas être entièrement imputé à Conficker. Le Canada doit son entrée dans le peloton des dix principaux pays hébergeant des serveurs web malveillants à l'éventail de logiciels malveillants et de logiciels espions (spywares) présents sur ces sites.

L'une des principales conclusions que nous pouvons tirer est que ces mêmes pays se retrouvent également sur les listes établies pour plusieurs vecteurs d'attaque : sites malveillants, sites hébergeant des logiciels espions et publicitaires (adwares), phishing et spam. Les sept premiers pays hébergeant des sites web de réputation malveillante figurent également parmi les dix premiers pays abritant des sites de phishing, de spam et de logiciels malveillants/espions.

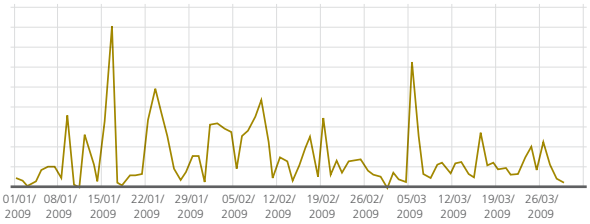
Les objectifs visés par les sites de réputation malveillante varient considérablement : activités légitimes, opérations douteuses ou fraudes. Le risque encouru sera toujours plus grand si vous visitez un site pornographique ou de jeux de hasard qui n'est associé à aucune activité légitime ou reconnue. Cependant, tous les sites sont vulnérables et les contenus consultés par les utilisateurs constituent autant d'opportunités exploitables par les distributeurs de logiciels malveillants.



20 principales catégories légitimes ayant la réputation de « sites web malveillants » d'après TrustedSource

Ce trimestre, les serveurs de contenu ont bénéficié d'un regain d'intérêt de la part des distributeurs de logiciels malveillants en tant qu'outil de diffusion de contenu malveillant et illégal. Cette tendance est perceptible tant sur les sites détenus et gérés par des fournisseurs digne de confiance et très respectés que sur les sites moins connus et plus suspects. Cette menace associée à la généralisation de l'utilisation des blogs et à l'optimisation des moteurs de recherche accentue la nécessité de doter chaque ordinateur d'une solution complète de sécurisation de l'environnement web.

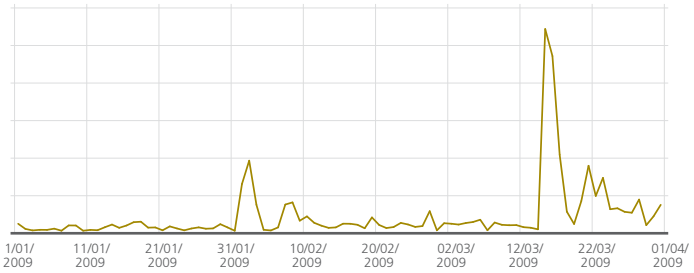
Maintenant que nous avons abordé l'aspect *géographique*, penchons-nous sur les *types* de menaces identifiés. Outre Conficker, un très grand nombre de nouveaux logiciels malveillants et d'exploits ont fait leur apparition sur le Web au cours de ce trimestre.



Nombre de nouveaux sites web hébergeant des logiciels malveillants et des programmes potentiellement indésirables

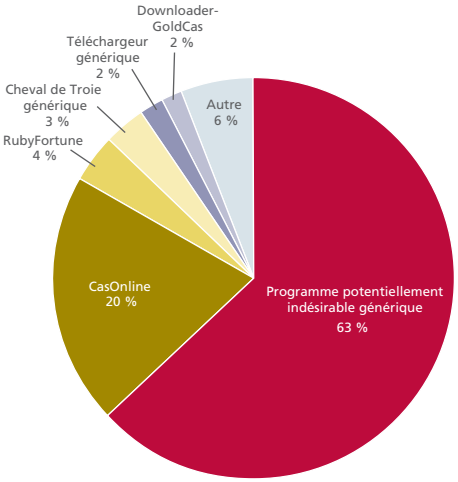
Le graphique ci-dessus montre le nombre de sites web propageant des logiciels malveillants et des programmes potentiellement indésirables détectés au cours de ce trimestre par le réseau McAfee TrustedSource. (Le graphique montre les sites qui hébergent des logiciels malveillants et reflète le trafic des internautes sur ces sites. Il n'inclut pas les sites légitimes utilisés pour rediriger les internautes vers des sites malveillants. De plus, pour son élaboration, nous avons renoncé à notre méthodologie de recherche proactive afin de proposer une image exacte des nouvelles menaces uniques apparaissant dans le cadre d'une navigation standard — que ce soit à l'école, à la maison ou au bureau.)

De leur côté, les graphiques ci-dessous reflètent les résultats obtenus à l'aide de notre méthodologie proactive concernant les téléchargements uniques de nouveaux logiciels malveillants fournis par différents sites web. C'est ainsi qu'apparaissent quelques pics intéressants dus à de nouveaux exploits ou à la découverte de « mines d'or » de téléchargements malveillants et de programmes potentiellement indésirables.



Téléchargements de logiciels malveillants et de programmes potentiellement indésirables identifiés de manière proactive par jour

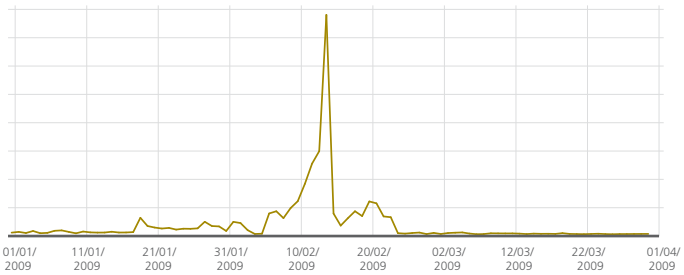
Nos observations proactives, combinant le balayage et la vérification régulières des sites web et des méthodes uniques de repérage de nouvelles informations malveillantes, font apparaître un pic particulièrement intense dans les téléchargements de logiciels malveillants de type jeux de casino vers la fin du mois de janvier et le début du mois de février, ainsi qu'un autre dans les programmes génériques potentiellement indésirables vers la fin du trimestre. Cette activité correspond aux quatre types principaux de téléchargement de logiciels malveillants au cours de ce trimestre (voir le graphique suivant). Un autre logiciel malveillant à ne pas négliger est le cheval de Troie Vundo omniprésent, dont l'activité s'est intensifiée ces trois derniers mois.



Prévalence du téléchargement de logiciels malveillants et de programmes potentiellement indésirables – par type

Parmi les menaces web amorphes auxquelles nous sommes confrontés figurent les *exploits*, une notion qui peut revêtir de très nombreux sens, souvent différents, pour les chercheurs et les utilisateurs. Avert Labs suit la trace des nouvelles pages hébergeant des exploits de navigateur à mesure que nous analysons et surveillons le Web, ce qui nous permet d'identifier régulièrement de nouvelles failles au niveau de la sécurité des navigateurs. Les navigateurs (et leurs plug-ins) qui ne sont pas mis à jour constituent des terrains de jeu privilégiés pour les auteurs de logiciels malveillants. Une fois les navigateurs sous contrôle, l'introduction d'un code de programmation permettant des infections par des logiciels publicitaires, l'espionnage des frappes et d'autres activités malveillantes sur l'ordinateur de l'utilisateur devient un jeu d'enfant.

Les navigateurs (et leurs plug-ins) qui ne sont pas mis à jour constituent des terrains de jeu privilégiés pour les auteurs de logiciels malveillants.



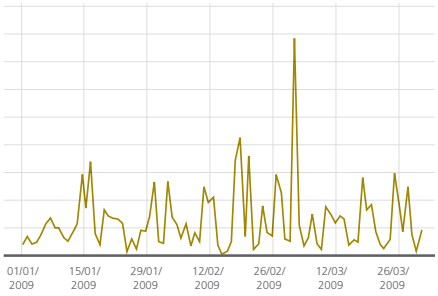
Sites web hébergeant des exploits de navigateurs détectés

Activité des anonymiseurs

Les auteurs de logiciels malveillants intensifient leurs attaques à coup d'URL de redirection, que ce soit par le biais d'un anonymiseur ou d'une interface Web 2.0 utilisant un serveur de contenu, leur but étant de contourner les outils de détection standard (en présentant une URL intégrée plutôt qu'une URL source) ou de profiter de la réputation du site à partir duquel le logiciel malveillant donne l'impression d'être lancé.

Un anonymiseur est un outil qui dissimule l'identité des internautes lorsqu'ils sont en ligne. La plupart des anonymiseurs ne sont pas malveillants, ce qui explique qu'ils n'aient pas été abordés lors de nos précédentes discussions sur les risques pour la sécurité. L'utilisation d'un anonymiseur peut toutefois

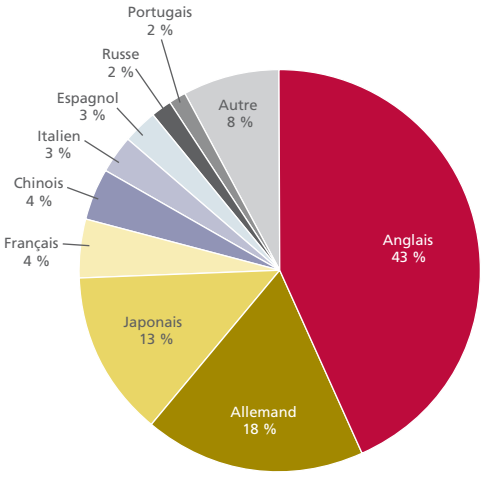
ouvrir la voie à une attaque de l'intercepteur (« man-in-the-middle »), qui consiste à injecter un code dans les messages échangés entre l'utilisateur et le serveur par le biais d'un anonymiseur malveillant ou piraté. En plus de créer un risque pour la sécurité de l'utilisateur, ce type d'attaque fait courir un danger à des hôtes et des réseaux pourtant protégés. De manière générale, une augmentation de l'activité des anonymiseurs a été enregistrée par rapport au trimestre précédent. Une légère augmentation est également constatée par rapport au même trimestre de l'année dernière.



Nombre de nouveaux anonymiseurs par jour

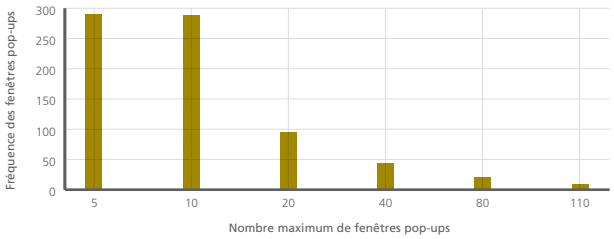
Tendances générales du Web

Le Web est une communauté mondiale. Il suffit de regarder le trafic sur les sites de réseaux sociaux ou professionnels ou encore le nombre croissant de langues prises en charge par les pages web pour s'en rendre compte. Les attaques via les blogs ne sont pas en reste : les attaques menées à l'encontre de sites américains renommés sont également diffusées par l'intermédiaire de blogs chinois, brésiliens, etc. Et les attaques d'aujourd'hui utilisent un réseau toujours plus vaste. En outre, les distributeurs de logiciels malveillants tirent parti de la notoriété de grandes marques (dans le cadre de grands événements sportifs, par exemple) et des logiciels malveillants intégrés dans des tableaux de compétition et les fichiers JPG des joueurs pour toucher le public dans différentes langues.



Distribution des langues dans le contenu web

Les désagréments occasionnés par les pop-ups n'ont pas connu de fléchissement. A cet égard, on notera avec intérêt que, malgré les programmes de blocage des pop-ups et d'autres outils similaires, la plupart des sites web continuent d'y avoir recours. Ainsi, nous avons dénombré pas moins de 116 fenêtres de ce type sur un site web.



Distribution des fenêtres pop-ups dans les sites en contenant au moins cinq

Ainsi, les sites de commerce électronique exigent autant de circonspection qu'un colporteur se présentant à votre porte.

Nous continuons d'assister à une généralisation de l'utilisation de sites Web 2.0 et professionnels légitimes pour la propagation de logiciels malveillants. Il y a dix ans ou plus de cela, il était possible de rester protégé simplement en se tenant à l'écart de certains types de contenu, mais il semble aujourd'hui que les menaces parviennent à nous trouver quels que soient les sites Internet que nous visitons. Tout site susceptible d'être exploité (via une faille quelconque) l'est. Les administrateurs constatent qu'ils reçoivent des « coups de sonde » de pirates tentant d'exploiter leurs serveurs. A cet égard, il est intéressant de noter la fréquence élevée de ce type de sondage malveillant provenant de sites et de serveurs associés à des logiciels illégaux, des sites malveillants et des anonymiseurs. Lorsqu'un site web à fort trafic est vulnérable, la question n'est pas de savoir s'il sera exploité, mais quand.

Une hausse marquée des fraudes sur le Web a été constatée. D'après nous, ce phénomène devrait s'intensifier, les arnaqueurs profitant des préoccupations de la population mondiale pour lancer des attaques via le spam et le Web. Il est parfois très difficile de déterminer si une organisation est légitime. Ainsi, les sites de commerce électronique exigent autant de circonspection qu'un colporteur se présentant à votre porte. Les internautes doivent savoir qu'une fois qu'ils ont communiqué des informations de carte de crédit à un fraudeur pour un soi-disant don en ligne ou un faux service, celles-ci sont perdues à jamais.

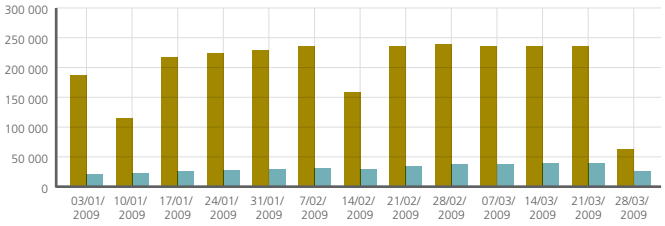
Nos recherches laissent cependant entrevoir une lueur d'espoir pour l'économie. Les sites immobiliers ont connu une croissance marquée au cours de ce trimestre et figurent désormais parmi les dix principales catégories de contenu accessibles aux utilisateurs (au détriment des sports, qui ont quitté le peloton de tête).

Logiciels malveillants : un Conficker surmédiatisé face à la menace bien réelle des logiciels à exécution automatique

Conficker a fait couler beaucoup d'encre ces derniers mois. Pour un peu, on pourrait même croire qu'il s'agissait de la seule menace dont il faille s'inquiéter. Les chiffres font toutefois apparaître une toute autre réalité. Il est en effet déraisonnable de brosser un tableau apocalyptique de Conficker.

Conficker a vu son importance croître pour diverses raisons : il a infecté de nombreux hôtes, son développement et sa maintenance ont été très actifs, et il a fait l'objet de nombreux débats. Mais le nombre de détections réelles n'est pas aussi important qu'on pourrait le croire au vu de l'attention énorme accordée à ce logiciel malveillant.

Nous avons par ailleurs assisté à l'émergence de plusieurs logiciels malveillants très inquiétants au cours de ce trimestre. C'est ainsi que des logiciels malveillants basés sur la fonction d'exécution automatique AutoRun, qui utilisent principalement des clés USB ou des mémoires Flash pour se répliquer, ont été détectés dans des proportions beaucoup plus grandes que Conficker. Comparons-les côte à côte :



Nombre d'ordinateurs sur lesquels des logiciels malveillants à exécution automatique et Conficker ont été détectés

Logiciels malveillants à exécution automatique

Conficker

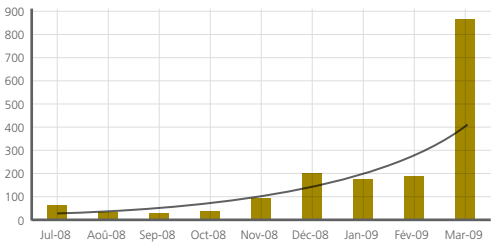
Ces 30 derniers jours, les vers à exécution automatique ont représenté moins de 10 % des détections signalées. Parti d'environ 1 %, Conficker s'est quant à lui multiplié par 12, mais il continue de représenter moins de 15 % du nombre de vers à exécution automatique détectés à leur niveau le plus haut.

Mise à jour des prévisions

McAfee Avert Labs a publié en début d'année son rapport intitulé *Paysage des menaces : prévisions pour 2009*[2]. Plusieurs de nos hypothèses se sont concrétisées ce trimestre.

Quand un tir ami fait de nombreuses victimes

Ces dix dernières années, le vecteur de menace populaire consistant à propager les virus d'ordinateur en ordinateur par l'intermédiaire des cercles d'amis a été en grande partie abandonné. Cette méthode d'attaque traditionnelle a toutefois connu un regain de vitalité avec l'arrivée des environnements Web 2.0. C'est ainsi que, durant ce trimestre, des variantes de Koobface ont pris des milliers d'utilisateurs par surprise, les infectant avec des virus provenant de leurs amis sur Facebook. Les liens associés aux messages envoyés par le virus conduisaient les victimes à leur insu vers des sites web distribuant le ver, de sorte que leurs ordinateurs ne mettaient pas longtemps à contracter le virus et à envoyer eux aussi des messages infectés à leurs cercles d'amis. Les réseaux sociaux demeurent donc un vecteur populaire pour les attaques par ingénierie sociale.



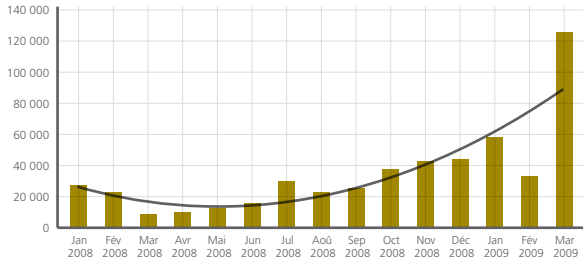
Fichiers binaires Koobface uniques découverts

Des sites web trompeurs à l'échelle mondiale

En février dernier, Facebook a été exploité par des pirates ayant réussi à créer de fausses applications à l'aide de la plate-forme Facebook. De nombreux utilisateurs ont mordu à l'hameçon et installé ces applications. Ces événements ont attiré l'attention des médias, ce qui a amené McAfee Avert Labs à percer à jour une vaste boucle d'optimisation d'un moteur de recherche visant les principaux mots clés de recherche de Google. Les pirates n'ont pas seulement dérobé du matériel sous copyright de sites très connus : ils ont également exploité d'autres sites populaires, tels que Democrats.org, pour faire grimper

2. McAfee Avert Labs Threat Center. http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report_fr.pdf

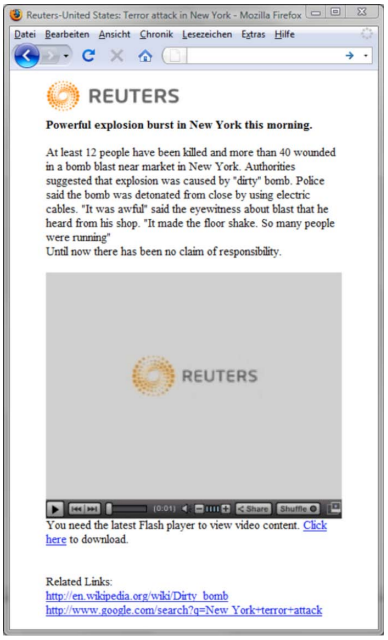
leur classement dans Google. Le but qu'ils poursuivaient en optimisant les résultats de recherche était d'installer un logiciel antivirus factice. C'est exactement ce que faisait une de ces applications Facebook trompeuses, qui renvoyait des résultats de recherche « falsifiés » et, partant, aiguillait les utilisateurs vers un faux logiciel de sécurité. Tous ces incidents soulignent la nécessité de sécuriser la navigation Internet.



Faux fichiers binaires antivirus uniques découverts

Des menaces qui vous parlent

Les pirates savent que plus une attaque est pertinente et contextuelle, plus l'utilisateur sera porté à effectuer l'action voulue : cliquer sur un lien, saisir un nom d'utilisateur et un mot de passe, installer une application, etc. Le récit d'un événement qui s'est produit à notre porte a plus de chances d'attirer notre attention que celui d'un événement qui a lieu à l'autre bout du monde. Ce concept a été exploité en février et mars derniers par les cybercriminels à l'origine du virus Waledac, qui dirigeait des utilisateurs peu méfiants sur des sites web personnalisés en fonction de la localisation géographique de la victime, afin de renforcer son sentiment d'authenticité. Et tandis que les utilisateurs lisaient les « nouvelles locales », le site web tentait d'installer le virus à leur insu via un code d'exploit de téléchargement automatique.



Blog McAfee Avert Labs

Google et le détournement du moteur de recherche

Google. Ce nom évoque à lui seul bien des choses dans l'esprit de nombreuses personnes. Pour les chercheurs d'emploi, il est un moyen d'accès aux dernières offres d'emploi. Pour les employeurs, il représente une solution pour trouver des employés qualifiés en ligne. Pour les acheteurs, c'est un outil efficace pour localiser les articles recherchés au prix le plus intéressant. Et pour les pirates et les cybercriminels, c'est un outil de plus en plus efficace pour diffuser des logiciels malveillants et commettre toutes sortes de crimes et délits informatiques. Etant donné que les moteurs de recherche génèrent une grande partie de l'activité Internet à l'heure actuelle, il semble logique que les auteurs de logiciels malveillants cherchent à exploiter leur puissance pour distribuer leurs logiciels. Nous vous invitons à parcourir les quelques articles suivants du blog McAfee Avert Labs consacrés à ce sujet :

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/

- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

Compte tenu de la puissance de l'indexation et des mots clés populaires conjuguée aux promesses d'argent facile pour les cybercriminels, ce type d'abus a encore de beaux jours devant lui.

L'économie et les craintes

La récession économique mondiale en inquiète plus d'un, tandis que d'autres restent préoccupés par les questions de sécurité et de terrorisme. Pour les auteurs de logiciels malveillants et les cybercriminels, il est très facile de convertir ces craintes en profits. Cette tendance économique, que nous avions épinglée dans notre rapport intitulé *Paysage des menaces : prévisions pour 2009*, a été exploitée tout au long de ce trimestre par de nombreux procédés dérangeants. La crainte constitue en effet une puissante motivation pour les cybercriminels qui en tirent parti dans le cadre d'attaques par ingénierie sociale :

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/
- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

Les fraudes, le spam et le phishing fonctionnent déjà très bien sous des cieux cléments — mais mieux encore en des temps difficiles. N'oubliez jamais que les personnes mal intentionnées lisent les mêmes nouvelles que nous et n'hésiteront pas à retourner les gros titres et l'actualité contre nous si nous baissons la garde.

A propos de McAfee Avert Labs

McAfee Avert Labs est le centre de recherche mondial de McAfee, Inc. Grâce à des équipes de chercheurs spécialisés dans les logiciels malveillants, les programmes potentiellement indésirables, les intrusions sur l'hôte et sur le réseau, les logiciels malveillants visant l'environnement mobile et la divulgation des vulnérabilités conformément à l'éthique, Avert Labs bénéficie d'une extrême visibilité sur la sécurité. Cette vision globale permet aux chercheurs de McAfee d'optimiser en permanence les technologies de sécurité et de mieux protéger le grand public.

A propos de McAfee, Inc.

Basé à Santa Clara en Californie, McAfee, Inc. est la plus grande entreprise au monde entièrement vouée à la sécurité informatique. McAfee consacre tous ses efforts à trouver des réponses aux plus grands défis de sécurité de notre époque. A cette fin, notre société fournit des solutions et des services proactifs réputés assurant la sécurisation des systèmes et des réseaux dans le monde entier. Les utilisateurs peuvent ainsi se connecter à Internet, surfer et faire des achats en ligne en toute sécurité. Grâce au soutien d'une équipe de recherche saluée par de nombreux prix, McAfee développe des produits novateurs qui aident les particuliers, les entreprises, le secteur public et les fournisseurs de services à se conformer aux réglementations, à protéger leurs données, à prévenir les perturbations dans le flux des activités, à identifier les vulnérabilités ainsi qu'à surveiller et à améliorer en continu leurs défenses. http://www.mcafee.com/fr.

McAfee®

McAfee SAS
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

5395rpt_avert_quarterly-threat_0409