Bitdefender®

Rapport sur l'état des e-menaces au 1er semestre 2012

Auteur :
Bogdan BOTEZATU – Analyste senior des e-menaces

Collaborateurs :
LiviuARSENE – Analyste des menaces mobiles
Loredana BOTEZATU – Spécialiste en communication
Adrian MIRON – Responsable de la recherche antispam
Dragoș GAVRILUȚ – Responsable de la recherche antimalware
Dan BERBECE - Administrateur de la base de données RTVR

Table des matières

Table des matières 3
Introduction : Bienvenue dans l'ère des attaques commanditées par les États 4
Zoom sur les malwares 5
Analyse des malwares 6
Menaces sur les réseaux sociaux 10
Analyse du spam 13
Phishing et usurpation d'identité 17
Le paysage Android 20
Les vedettes du premier semestre 21
Top 10 des menaces Android au 1er semestre 2012 22
Top 10 des pays touchés par les malwares Android 25
Prévisions 26

Légendes des figures

Figure 1 - Analyse des malwares au 1er semestre 2012 6
Figure 2 - Evolution des malwares aux 1er et 2nd semestres 2011 et au 1er semestre 2012. 9
Figure 3 - Analyse des malwares du 1er semestre 2012 – Les exploits sont le vecteur privilégié des infections. 9
Figure 4 - Le modificateur de thème Facebook délivre des add-ons malveillants aux utilisateurs de Chrome et de Firefox. 10
Figure 5 - Fausses applications Facebook redirigeant le trafic des mobiles Android. 11
Figure 6 - PinPal Bot, un outil polyvalent d'abus. 12
Figure 7 - Répartition du spam par catégories. 13
Figure 8 - Modèle de spam de Canadian Pharmacy. 14
Figure 9 - Message de spam de confirmation de réservation de billet contenant Zeus. 14
Figure 10 – Arnaque mail qui usurpe l'identité d'un FAI. 15
Figure 11 - La vague de spam [sans objet] se répand comme une traînée de poudre. 16
Figure 12 - Top 10 des pays hébergeant des pages de phishing au 1er semestre 2012. 17
Figure 13 - Top 10 des marques visées par le phishing au 1er semestre 2012. 18
Figure 14 - Page de phishing PayPal. 18
Figure 15 – De prétendue demande de changement de mot de passe par Linkedln. 19

© 2012 Bitdefender

Introduction : Bienvenue dans l'ère des attaques commanditées par les États

Non seulement la découverte de Stuxnet avait pris par surprise l'industrie de la sécurité en 2010, mais elle avait aussi éclairé d'un jour nouveau ce que l'on appelait la « cyber-guerre » : un combat, avec Internet pour théâtre, comportant des attaques à motivation politique visant des données et des systèmes d'information.

Le premier semestre de cette année a apporté de nouvelles surprises en termes de cyber-guerre avec la découverte de Flamer – l'une des e-menaces les plus puissantes et complexes connues à ce jour. Conçu pour fonctionner furtivement et collecter des données au moyen d'un nombre stupéfiant d'approches, Flamer a réussi à déjouer les détections antivirus pendant environ cinq ans.

Flamer est à ce jour l'un des malwares les plus volumineux : il est composé de plus de 63 fichiers différents, y compris composants principaux et plugins. Son architecture modulaire lui permet de déployer rapidement ses fonctionnalités par l'ajout de code LUA.

Des gouvernements ont continué d'utiliser le malware à des fins de cyber-espionnage pendant toute la première moitié de 2012. Des cybercriminels chinois ont tenté d'atteindre des personnels militaires avec des spams ciblés véhiculant des exploits Flash de type « zero-day ».

© 2012 Bitdefender

Zoom sur les malwares

- Au cours des six premiers mois de 2012, le paysage des malwares est resté relativement stable, avec Trojan.AutorunInf, Win32.Worm.Downadup et Exploit.CplLnk constituant les trois menaces les plus importantes dans le monde. Les deux premiers ont plus de quatre ans d'existence et, bien que les vulnérabilités qui leur permettent d'infecter les systèmes aient été identifiées, ils continuent de faire des victimes.

- Le premier semestre 2012 a également été riche en violation et divulgation de données. La sécurité de services Internet très populaires, comme Last.FM, LinkedIn et Yahoo Voice, et aussi des forums très fréquentés (comme les forums Android de Phandroid) a été compromise, les bases de données de leurs utilisateurs ayant été volées et partagées en ligne. Dans certains cas, les fuites de bases de données ont été suivies par des tentatives de phishing auprès des victimes.

- Les utilisateurs d'ordinateurs connectés en permanence à Internet ont à relever plus de défis que ceux qui passent moins de temps sur le Web. D'après le **Cloud Bitdefender**, le risque qu'affrontent le plus fréquemment les utilisateurs connectés en permanence est nommé 'Application.InstallCore', un module qui est connu pour être installé par d'autres malwares et qui affiche des publicités, sans le consentement de l'utilisateur. TrojanAutorunInf, ainsi qu'Exploit.CplLnk et Win32.Worm.Downadup constituent d'autres risques.

- Les malwares orientés vers des gains financiers directs gagnent sans cesse du terrain. En dehors des célèbres chevaux de Troie 'bancaires', les créateurs non autorisés de monnaie Bitcoin se sont multipliés depuis leur découverte mi-2011. Les cybercriminels échangent ces Bitcoins contre des monnaies locales, ou les utilisent pour trafiquer sur des forums underground.

- Les malwares à finalité commerciale ont également joué un rôle clé au cours du premier semestre 2012 lorsque des gangs, comme ceux impliqués dans Carberp ou le scandale du malware pornographique Android au Japon, ont été arrêtés.

- La première moitié de l'année s'est terminée par la chute de l'infrastructure DNS Changer exploitée par la corporation cybercriminelle estonienne Rove Digital, démantelée par le FBI en novembre 2011. La fermeture des serveurs DNS malveillants a contraint le FBI à utiliser des serveurs DNS propres aux mêmes adresses IP pour préserver la connexion à Internet des hôtes infectés. Conformément à la décision du tribunal, l'utilisation des serveurs DNS de remplacement devait se poursuivre jusqu'au 9 juillet, même si plus de 350.000 hôtes utilisaient encore les serveurs DNS pirates pour se connecter.

© 2012 Bitdefender

Analyse des malwares

Le panorama des e-menaces a relativement peu changé au cours de la première moitié de 2012 en ce qui concerne les trois principales menaces. L'une des préoccupations particulières est l'augmentation de l'activité de Win32.Sality.3, une variante du célèbre botnet Sality dont on estime qu'il a compromis plus d'un million d'ordinateurs dans le monde. Trojan.FakeFolder.B a également grimpé de la neuvième à la cinquième place en moins de six mois, le nombre d'ordinateurs atteints ayant presque doublé.

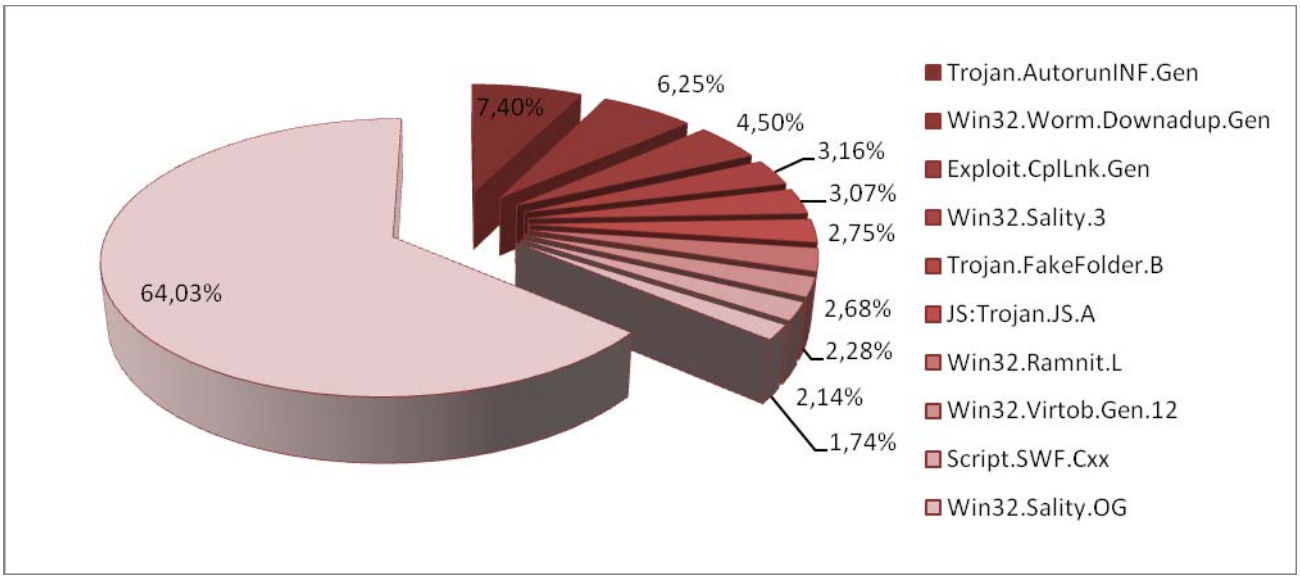


Figure 1 - Analyse des malwares au 1er semestre 2012.

1. Trojan.AutorunINF.Gen– 7,40 % (-1,14 / -)

Trojan.AutorunInf n'est plus à présenter – il a été l'une des trois principales e-menaces pendant environ quatre ans. Cette détection fonctionne avec de faux fichiers Autorun créés par différentes familles de malwares pour faciliter la propagation via des supports amovibles. Bien que les fichiers autorun.inf ne soient pas malveillants par défaut, ils sont fréquemment créés par d'autres e-menaces possédant des capacités analogues à celles d'un ver et copiés sur des clés USB, avec le véritable malware. Dès que le support amovible est connecté sur un ordinateur avec l'Autorun activé, le fichier autorun.inf exécute automatiquement le malware, ce qui infecte l'ordinateur. Cette fonction a été supprimée de Windows Vista SP1 et des plus récents systèmes d'exploitation, mais les systèmes plus anciens restent vulnérables.

2. Win32.Worm.Downadup – 6,25 % (+0,58 / -)

Le ver Downadup a fait son apparition début 2008 et a provoqué la plus grande épidémie de tous les temps, puisqu'il a réussi à infecter plus de 12 millions d'ordinateurs en moins de 24 heures. Le ver exploite une vulnérabilité sur RPC du service Serveur de Microsoft Windows (aussi connue sous le nom de MS08-67) pour se diffuser sur les réseaux locaux. Les ordinateurs infectés se voient refuser l'accès aux mises à jour

© 2012 Bitdefender

de sécurité, aux sites de vendeurs d'antivirus ou à ceux proposant un support technique. Le botnet a été utilisé pour installer de faux antivirus et d'autres e-menaces, mais le ver Downadup ne semble pas avoir progressé au cours des deux dernières années.

3. ExploitCPLLnk – 4,50 % (+0,11 / -)

Exploit.CplLnk.Gen est le composant de Stuxnet qui lui permet de se lancer lui-même dès qu'une clé USB infectée est branchée. La clé utilise des fichiers lnk (raccourcis) qui déclenchent un exploit dans la manière dont les systèmes d'exploitation Windows affichent les éléments du Panneau de configuration. Ce piège est un des cinq exploits de type zero-day que Stuxnet utilisait pour se diffuser et fonctionne dans toutes les versions du système d'exploitation Windows. Les cybercriminels responsables de l'opération Stuxnet ont probablement préféré un exploit zero-day à l'Autorun.inf pour une infection via USB, de manière à limiter les risques de repérage.

4. Win32.Sality.3 – 3,16 % (-0,03 / +1 place)

Win32.Sality.3 représente 3,19 % de l'ensemble des infections du premier semestre 2012. Ce malware infectieux extrêmement agressif s'attache à d'autres fichiers scr et exe sur le PC de la victime, et tente d'infecter d'autres systèmes sur le même réseau. Le virus Sality dispose d'un cryptage puissant pour échapper à la détection antivirus. Il est également équipé d'un composant rootkit utilisé pour détruire les solutions antivirus (qui sont autrement hors d'atteinte du malware). Le botnet Sality compte à cette date plus d'un million d'ordinateurs infectés, qui peuvent être administrés à distance par le botmaster.

5. Trojan.FakeFolder.B – 3,07 % (+1,49 / +4 places)

Trojan.Fake.Folder.B a enregistré une croissance explosive en moins de six mois, passant de la neuvième à la cinquième position. Cette e-menace relativement récente est un composant du cheval de Troie Dorkbot, qui l'utilise pour maintenir le malware actif dans la mémoire de l'ordinateur. Le Dorkbot fait la liste des dossiers présents sur le PC infecté, crée un raccourci vers ces derniers, puis les masque. A chaque fois que l'utilisateur tente d'accéder à un dossier, le raccourci ouvre également le composant malveillant situé dans le dossier Recycler.

6. JS:Trojan.JS.A– 2,75 % (nouveau / nouveau)

Occupant la 6ème place du classement des e-menaces pour le premier semestre 2012, Trojan.JS.A est un élément crypté en code JavaScript qui s'ajoute à des pages HTML ou à d'autres snippets de JavaScript. Il est alors utilisé pour rediriger l'utilisateur vers une page qui héberge d'autre e-menaces, particulièrement des exploits Web visant le navigateur et Java Runtime Environment. Ces pages de destination récoltent également des informations sur les systèmes compromis, comme le nom de domaine, le type et la version du navigateur, ainsi que la localisation.

© 2012 Bitdefender

7. Win32.Ramnit.L – 2,68 % (nouveau / nouveau)

Win32.Ramnit.L est un infecteur de fichiers qui ajoute son code malveillant à des fichiers possédant des extensions particulières. Pour se lancer, il injecte également son code dans certains processus, particulièrement dans le navigateur par défaut. Après avoir infecté l'ordinateur, Win32.Ramnit.L contacte son serveur de commande et de contrôle et attend les instructions. Entre autres choses, Ramnit peut voler les autorisations de connexion FTP, ainsi que les cookies de navigation.

8. Win32.Virtob – 2,28 % (-0,12 / -1)

Le 3ème infecteur de fichiers du classement est Win32.Virtob, un type de malware qui s'attache également à des fichiers scr et exe sur le PC de la victime. Ecrit en langage assembleur, le virus est optimisé au niveau de la rapidité et de la discrétion. Il accorde une attention extrême aux fichiers qu'il infecte et, pour éviter que le système ne tombe en panne et le supprime, il n'infecte pas les fichiers systèmes. Les principales spécialités de Virtob comprennent le vol de fichiers et de cookies, la collecte d'autorisations de connexion de tous les comptes authentifiés sur le système.

9. Script.SWF.Cxx – 2,14 % (nouveau/ nouveau)

Neuvième dans le classement du rapport, Script.SWF.Cxx est une détection qui intercepte une partie du code ActionScript utilisé dans une attaque visant des personnels de l'armée américaine. Cette partie de code était empaquetée dans un document Word prétendument secret concernant la situation en Iran, au sujet du pétrole et du nucléaire. Après Exploit.CplLnk, Script.SWF.Cxx a été le deuxième type de malware utilisé pour collecter des renseignements militaires.

10. Win32.Sality.OG – 1,74 % (-0,66/ -2)

Win32.Sality.OG arrive dernier de la liste du Top 10 du malware du premier semestre 2012. Cette variante du virus Sality possède toutes les caractéristiques de Win32.Sality.3, mais utilise un algorithme de cryptage plus ancien et moins sophistiqué pour protéger son code contre l'analyse et la détection. Le virus a reculé de deux rangs depuis la seconde moitié de 2011.

© 2012 Bitdefender

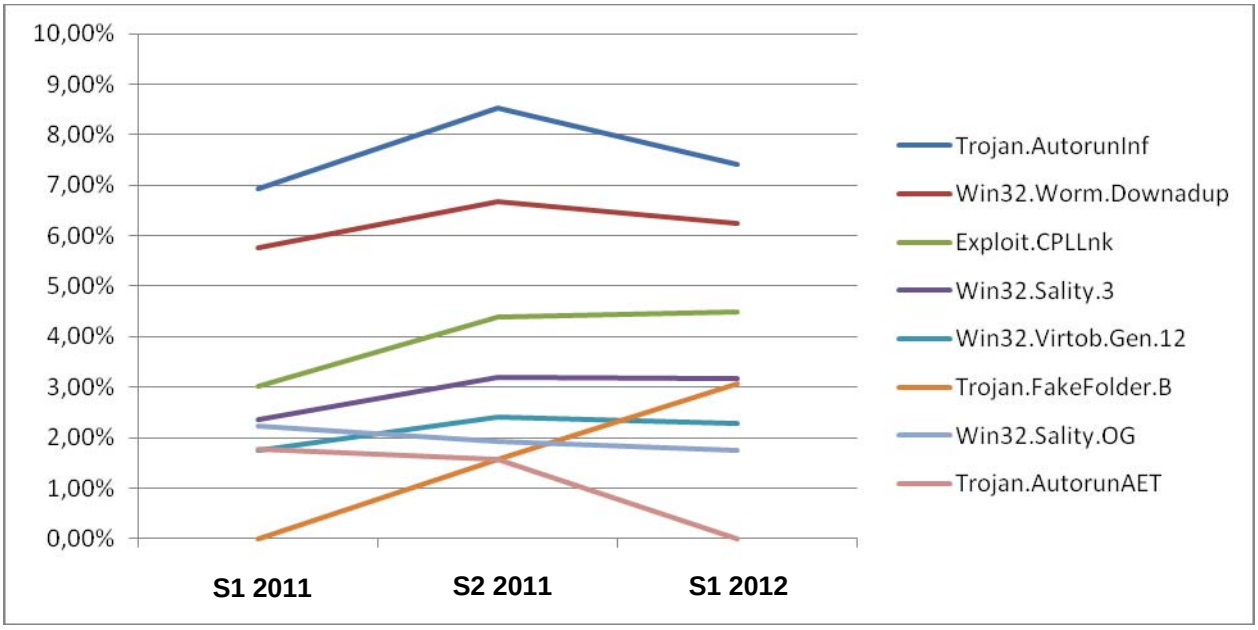


Figure 2 - Evolution des malwares aux 1er et 2nd semestres 2011 et au 1er semestre 2012.

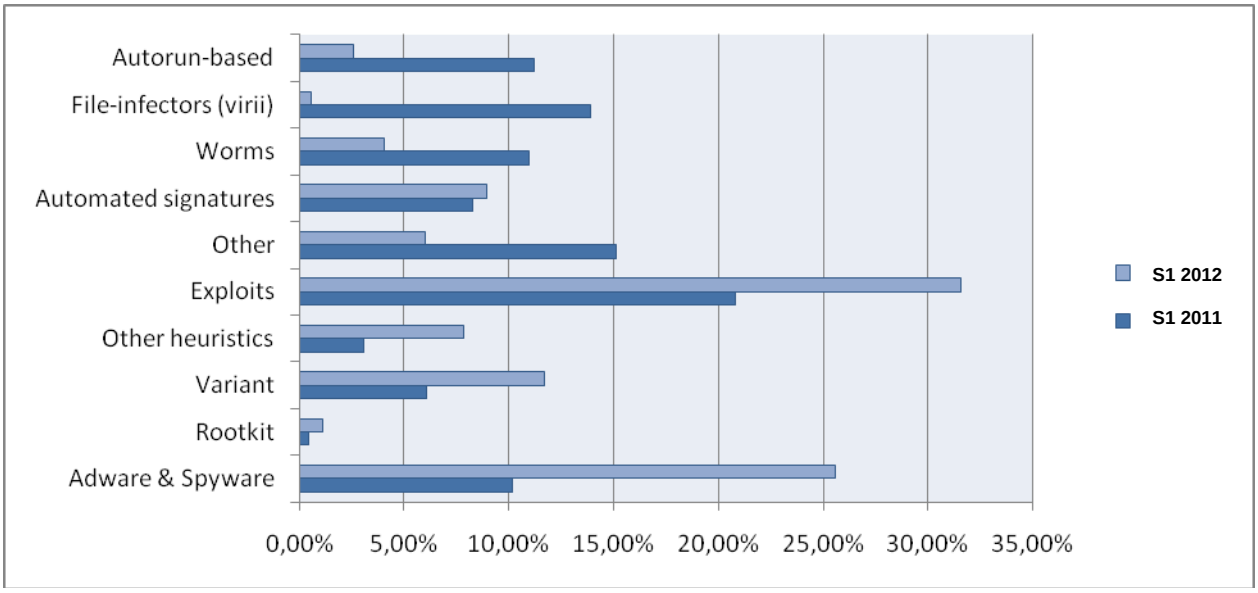


Figure 3 - Analyse des malwares du 1er semestre 2012 – Les exploits sont le vecteur privilégié des infections.

L'utilisation d'exploits de logiciels via Internet sont désormais le mode de distribution le plus répandu des malwares – une conséquence directe de la généralisation de l'usage d'Internet dans le monde et de la liberté d'accès à des « packs d'exploits » zero-day. Parmi les applications les plus vulnérables, on trouve Adobe Reader dans ses versions antérieures à 9.04, Java Runtime Environment version 7 et antérieures, ainsi que le plugin Adobe Flash.

© 2012 Bitdefender

Menaces sur les réseaux sociaux

Quelle que soit leur nature, les réseaux sociaux ont un grand nombre d'utilisateurs partageant librement des informations sur eux-mêmes, leur travail et/ou leurs amis. Les 900 millions d'utilisateurs de Facebook ont été exposés ce premier semestre à une multitude d'escroqueries, allant du classique « votre Facebook d'une autre couleur » jusqu'à des arnaques plus récentes promettant la suppression de la fonction Journal (Timeline).

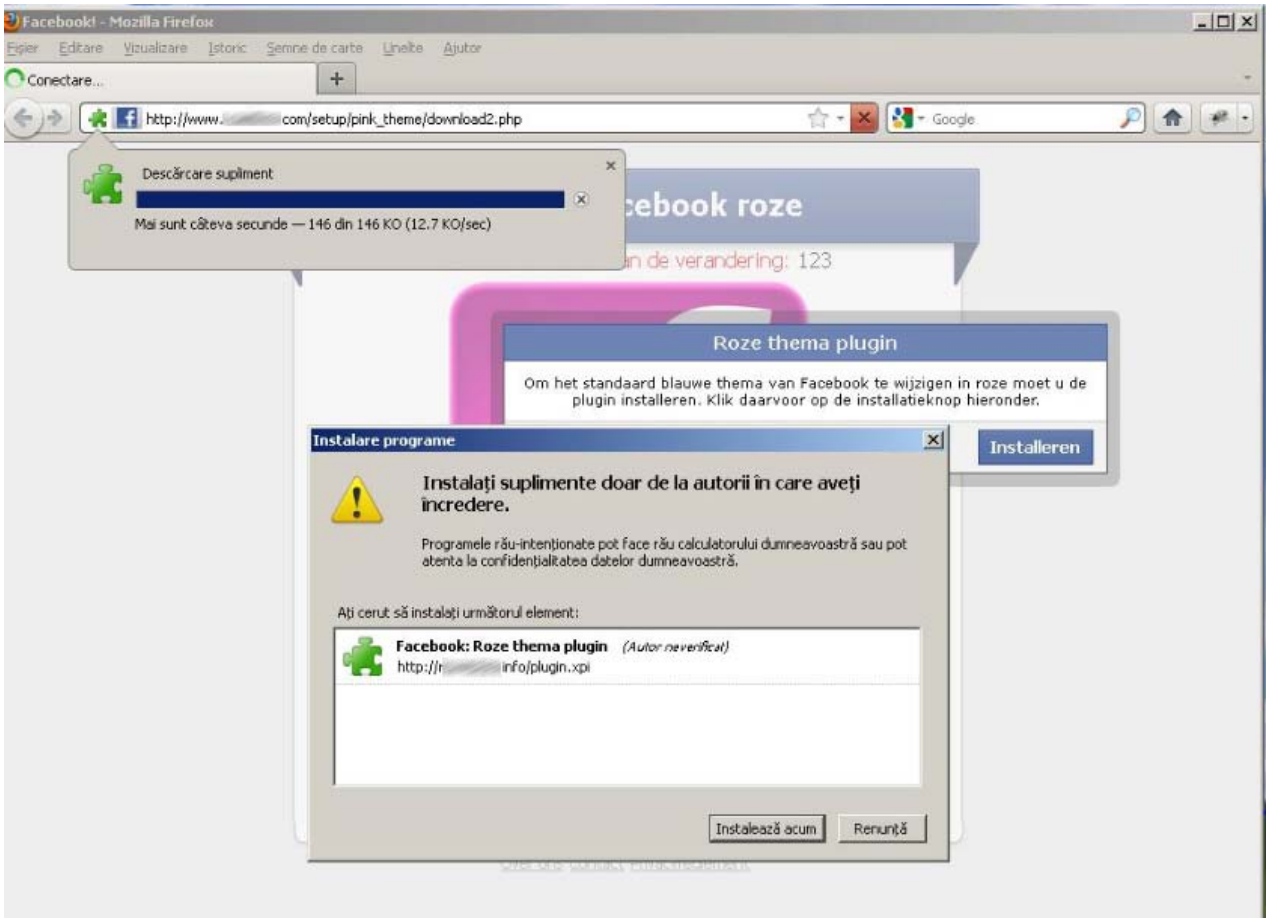


Figure 4 - Le modificateur de thème Facebook délivre des add-ons malveillants aux utilisateurs de Chrome et de Firefox.

Cette campagne s'adresse aux utilisateurs qui souhaiteraient passer du bleu standard à une autre couleur (rose ou vert par exemple). Cette arnaque très répandue consiste à demander à l'utilisateur de télécharger et d'ouvrir un fichier à partir d'un emplacement extérieur au réseau social. Le fichier se révèle être un add-on pour Firefox ou Chrome, qui va modifier le site Facebook en manipulant le fichier CSS, mais va également effectuer des redirections vers des pages d'enquêtes ou des services SMS surtaxés, comme des horoscopes ou des sonneries.

© 2012 Bitdefender

Les fausses applications Facebook développées et hébergées par des tiers s'en sont également pris aux données des utilisateurs. Cette application spécifique, découverte à la mi-mai, a pris pour cible les utilisateurs d'appareils portables. L'application, surnommée « Girlfriend Checklist » (Liste de copines) surveille le trafic des mobiles et redirige les utilisateurs vers des jeux Android qu'ils sont invités à installer. Pour assurer sa diffusion, l'application demande une autorisation de tagging de telle sorte que les « candidats potentiels » puissent être mis au courant de l'existence de cette application.

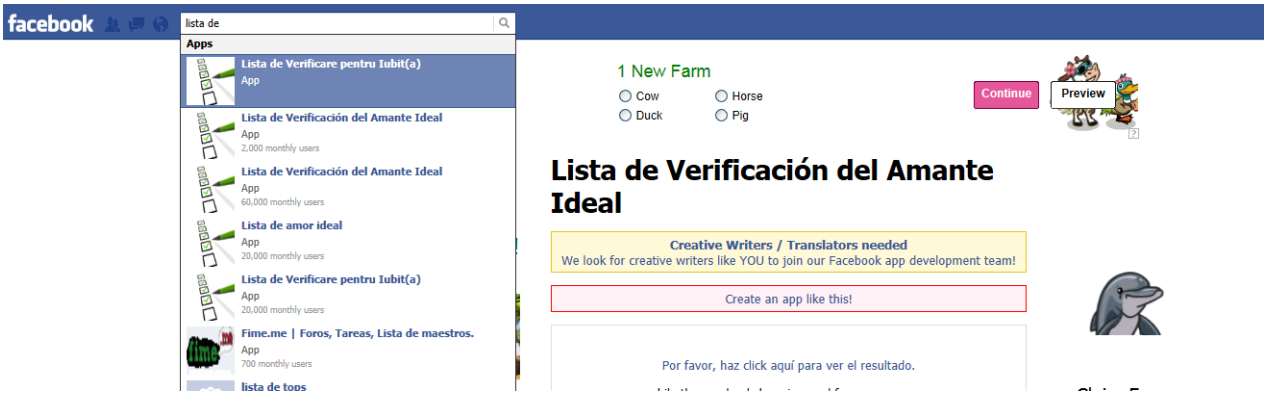
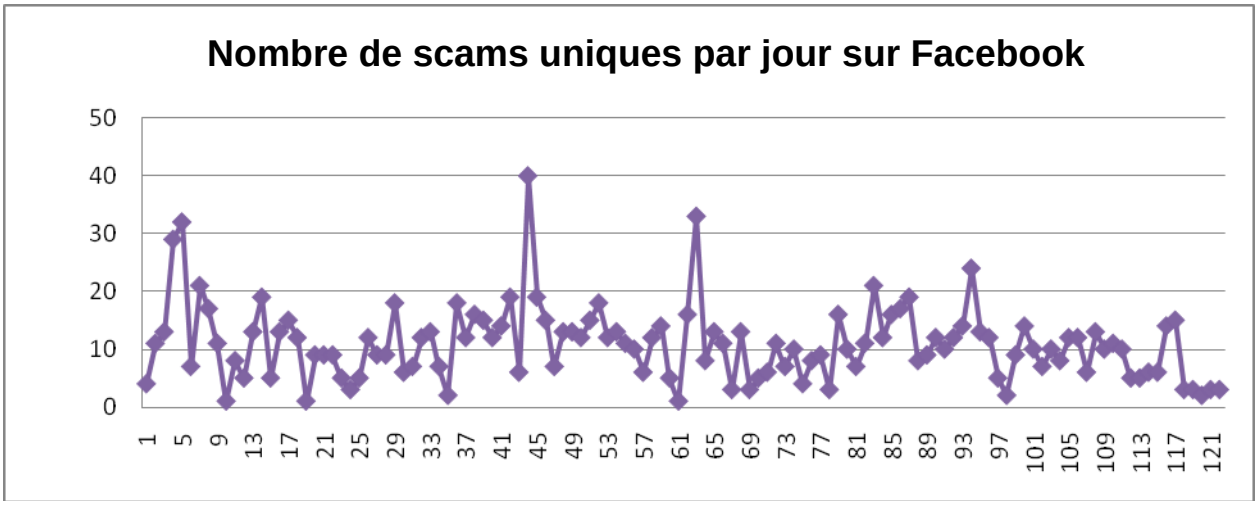


Figure 5 - Fausses applications Facebook redirigeant le trafic des mobiles Android.

Entre janvier et juillet 2012, Bitdefender a identifié en moyenne 7,3 nouvelles arnaques par jour, comme le montre le graphique ci-dessous. Ces arnaques ont atteint plus du quart d'un million d'utilisateurs. Etant donné l'étroitesse de la période de diffusion, on peut facilement en conclure que ces utilisateurs ont été touchés en un jour ou deux après l'émergence de cette arnaque.



Bien qu'étant le réseau social le plus fréquenté, Facebook n'a pas été le seul à être visé au premier semestre 2012. Tandis que Pinterest commence à gagner du terrain, de nombreux outils de subversion sont déjà disponibles sur des forums clandestins.

© 2012 Bitdefender

Certains outils installent d'invisibles boutons « Suivre » sur des pages Web tierces, d'autres utilisent une approche plus radicale de socialisation. L'un de ces outils multi-fonctions est PinPal Bot, une application qui permet la création de multiples comptes Pinterest, servant à envoyer du spam aux autres utilisateurs, pour vendre des produits en affiliation sous les abords légitimes.

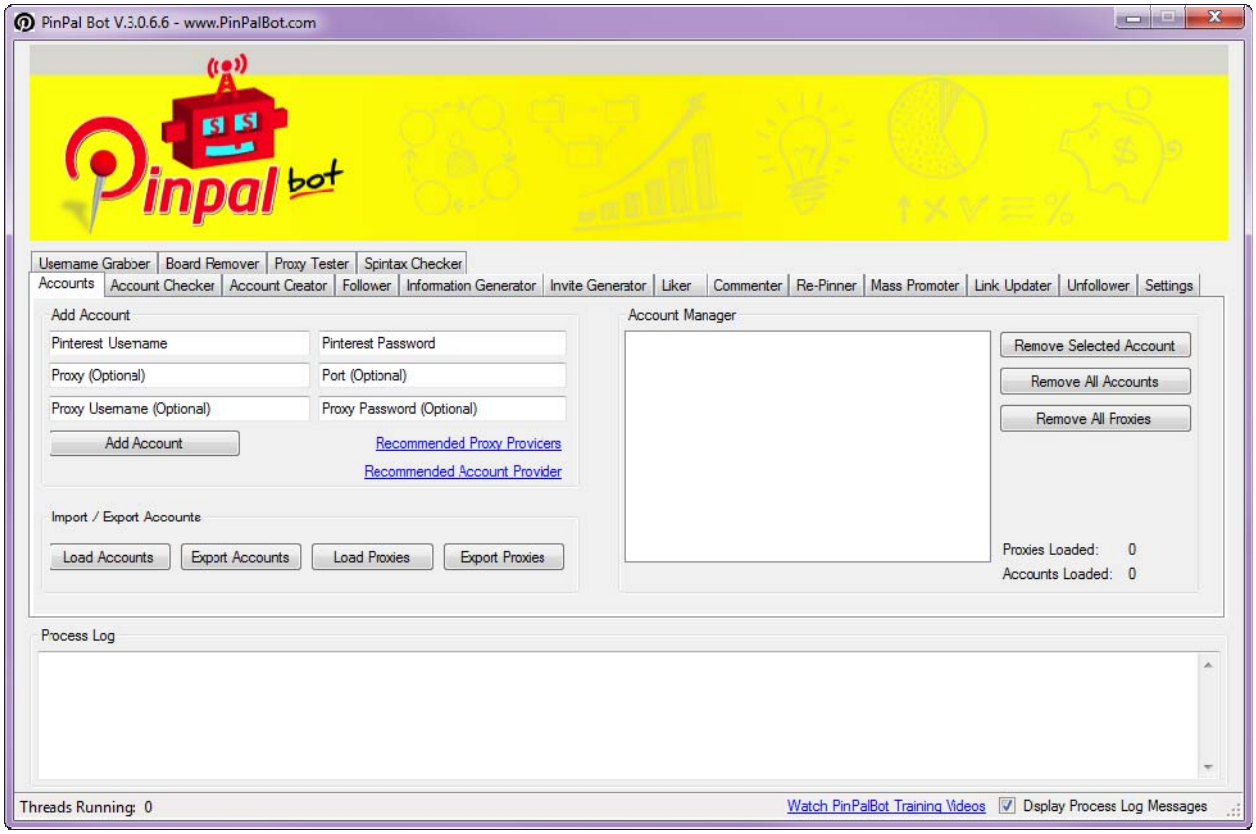


Figure 6 - PinPal Bot, un outil polyvalent d'abus.

© 2012 Bitdefender

Analyse des menaces de spam

Le spam a continué de diminuer au cours des six premiers mois de 2012, ne représentant plus que 70 % de la totalité des emails expédiés dans le monde. Par comparaison avec le semestre précédent, les Laboratoires antispam de Bitdefender ont enregistré une baisse de volume d'environ 5 %. Ceci semble lié à l'arrêt de petits botnets, et aussi à la migration des spammers vers les réseaux sociaux où ils peuvent cibler plus facilement leurs victimes.

Si la plupart du spam était en anglais jusqu'à la première moitié de 2011 pour atteindre le public le plus vaste, les spams « régionaux » visant spécifiquement certains pays, ont augmenté au cours du premier semestre 2012. L'une des vagues de ces spams consiste par exemple en une offre d'emploi rédigée en huit langues.

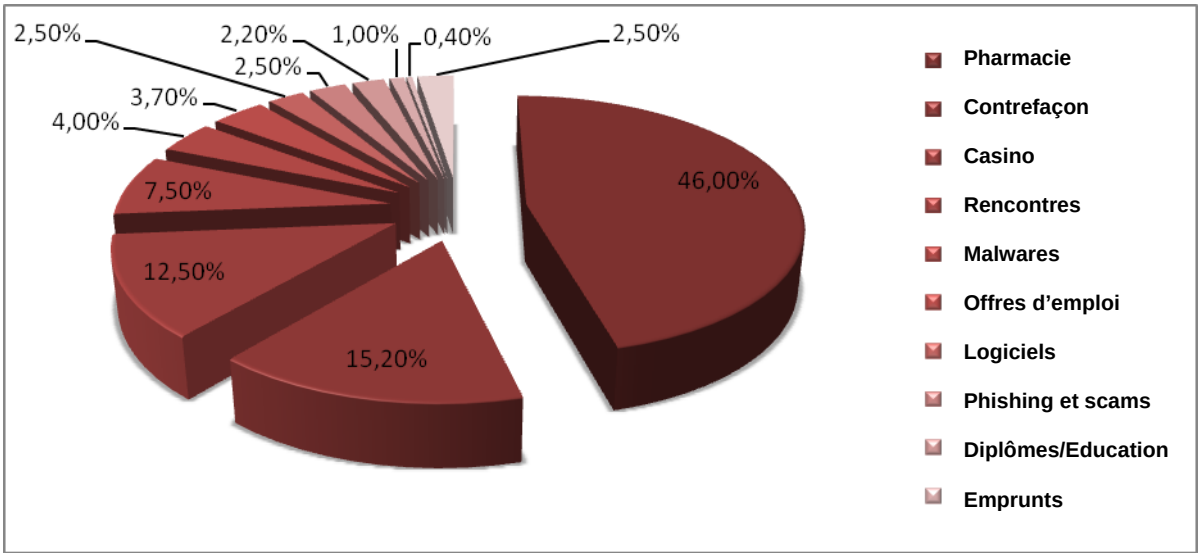


Figure 7 - Répartition du spam par catégories.

Le spam pharmaceutique est encore une fois la niche la plus occupée par les spammers, avec environ 46 messages de spam sur cent proposant une vaste gamme de produits, allant des médicaments sur ordonnance, aux stimulants sexuels de 'Canadian Pharmacy', en passant par les pilules amaigrissantes dont la FDA (aux Etats-Unis) n'a pas autorisé la vente au grand public. Les campagnes de spams médicaux ont pris de multiples aspects, depuis des messages complexes illustrés à ceux d'une seule ligne comportant des liens.

© 2012 Bitdefender

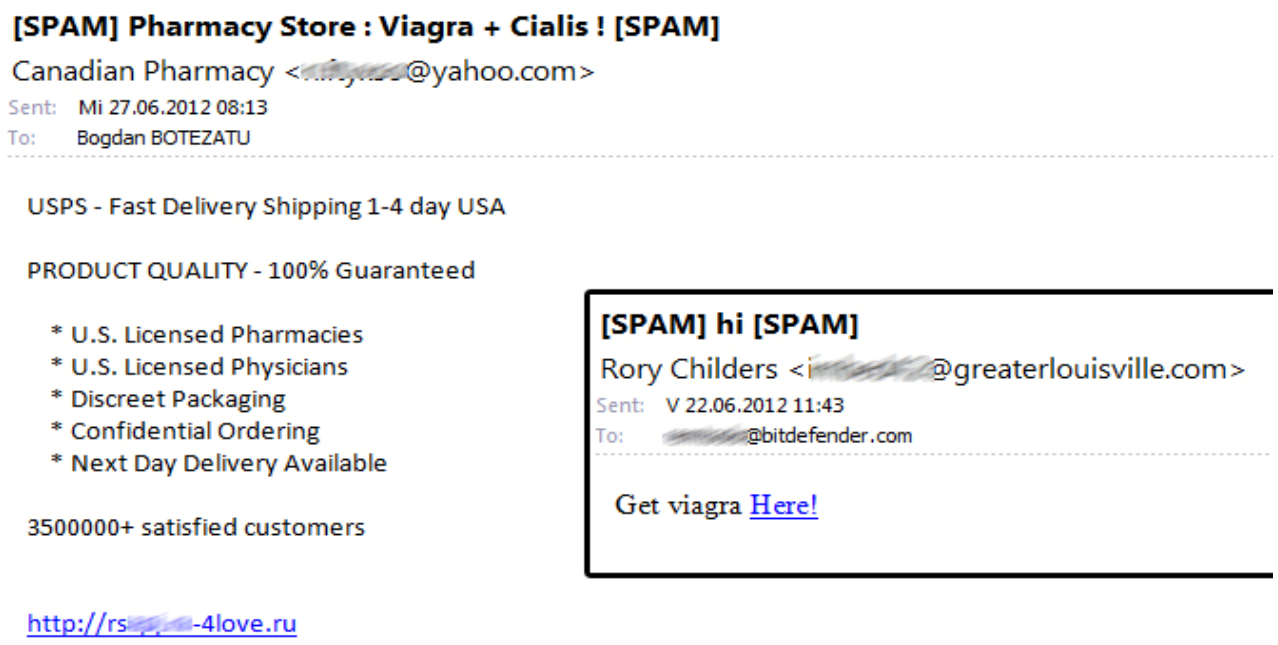


Figure 8 - Modèle de spam de Canadian Pharmacy.

Le nombre de messages de spam comportant des pièces jointes malveillantes a également augmenté au cours de la première moitié de 2012, passant de 2,5 % au deuxième semestre 2011 à 4 %. Les plus importantes campagnes de spam avec des malwares embarqués comportaient le bot Zeus, des téléchargeurs génériques et d'autres éléments de malwares plus anciens.

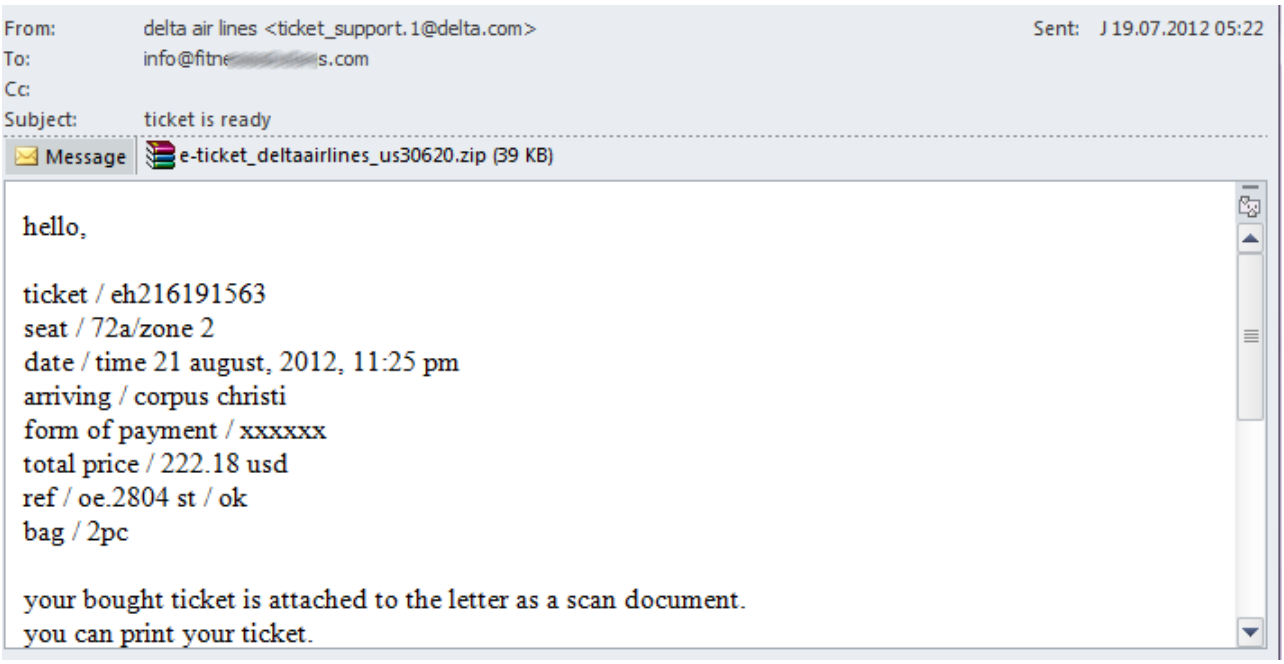


Figure 9 - Message de spam de confirmation de réservation de billet contenant Zeus.

© 2012 Bitdefender

Les spams d'offres d'emploi sont montés en flèche au cours des six derniers mois. Même si le nombre de messages a légèrement diminué (de 4 % au deuxième semestre 2011 à 3,7 % au deuxième semestre 2012), les vagues de spam se sont diversifiées et sont devenues plus attrayantes pour les internautes. Les emplois les plus souvent proposés sont ceux qui permettent un travail à distance, ou une présence à temps partiel, ainsi que des offres régionales. Les vagues de spam identifiées au cours du premier semestre 2012 sont hautement ciblées et souvent traduites dans la langue natale de la victime. Bien que ces offres d'emploi puissent sembler intéressantes, particulièrement dans un contexte de crise de l'emploi, il s'agit de véritables escroqueries. Il est demandé à la victime de payer des « frais de dossier RH », ou de fournir des informations personnelles à des fins d'usurpation d'identité, ou, le plus souvent, pour transférer de l'argent ou des biens volés par des cybercriminels.

Les arnaques liées aux FAI ont aussi sensiblement augmenté, les pirates se faisant passer pour des entreprises légitimes pour tromper les utilisateurs.

SFR Votre facture neufbox et fixe

Votre référence client : 1-39K0Q0M

Carrément vous.

Cher client,

Ce mail vous est envoyé en dernier avis, après plusieurs tentatives infructueuses de vous joindre sur Votre numéro personnel.

En effet le 11/07/2012 une erreur s'est produit lors des prélèvements de la mensualité effectué sur votre Compte ce dernier était doublement débiter de la somme de cinquante-neuf quatre vingt 59.80 € (29.90*2) .

Pour une régularisation immédiate de votre situation, et le remboursement de la somme débitée vous Devez remplir instamment le formulaire ci-dessous.

Https:// [illegible]

Merci pour votre compréhension. dés réception de votre fiche nous vous contacterons sur le numéro que vous aller fournir. toute oubli, lors de la saisie des informations demandées aura pour conséquence le rejet automatique de votre formulaire et le non remboursement de la somme 58,80 Euro.

Notre service décline toute responsabilité juridique à défaut d' une réponse immédiate de votre part et aucune réclamation ne sera acceptée.

Urgent

Dominique REMOND
Directeur Service Client

Le Service Client SFR
www.sfr.fr

Figure 10 – Arnaque mail qui usurpe l'identité d'un FAI.

© 2012 Bitdefender

Une autre vague de spam importante et inhabituelle, qui a circulé en 2012, a été l'invasion de messages [sans sujet] envoyés à travers les infrastructures de Yahoo! par les utilisateurs d'ordinateurs dont les comptes avaient été compromis. Le message d'une ligne comprenait un lien vers un site corrompu (généralement une installation Wordpress vulnérable). Le lien conduisait l'utilisateur vers des publicités de Canadian Pharmacy après une série de redirections du navigateur.

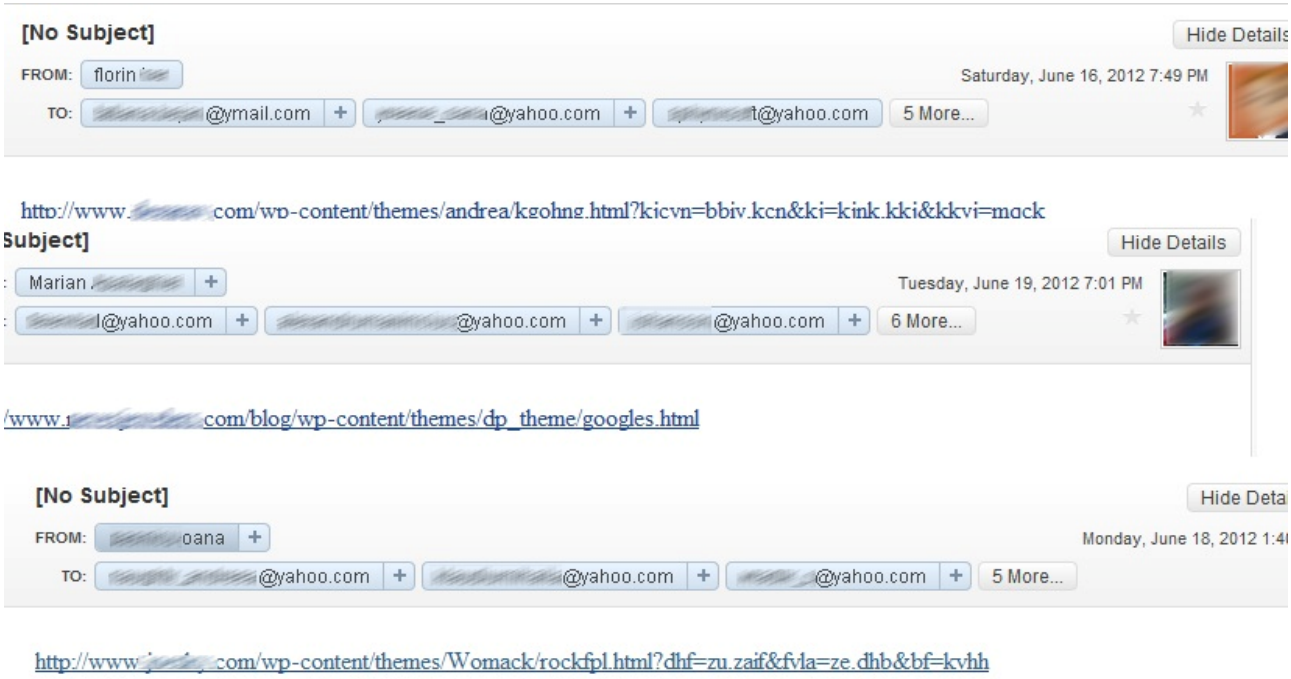


Figure 11 - La vague de spam [sans objet] se répand comme une traînée de poudre.

© 2012 Bitdefender

Phishing et usurpation d'identité

Au cours des six premiers mois de 2012, les phishers ont été plus actifs que pendant la seconde moitié de 2011, leur production passant de 1,5 % de tous les messages spams envoyés dans le monde à un pourcentage estimé à 2,5%. Plus de la moitié (51 %) de toutes les pages de phishing du monde entier étaient hébergées sur des serveurs ou des botnets (zombies) à haut débit aux Etats-Unis. D'autres pays « accueillants » pour le phishing sont l'Allemagne (5,5 %), le Royaume-Uni (4,5 %) et le Canada (4,2 %).

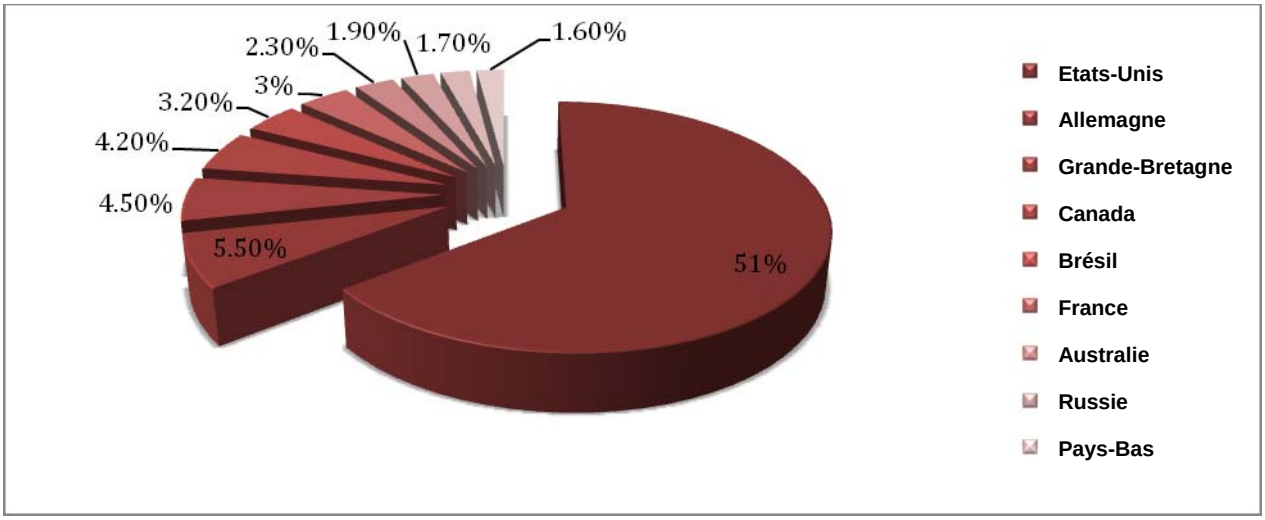


Figure 12 - Top 10 des pays hébergeant des pages de phishing au 1er semestre 2012.

Les organismes financiers ont été une fois encore les institutions les plus ciblées par les e-mails de phishing. Les systèmes de paiement en ligne, comme PayPal et Western Union, ont également été visés par de multiples attaques issues de - kits de campagne phishing - « à faire soit même ».

© 2012 Bitdefender

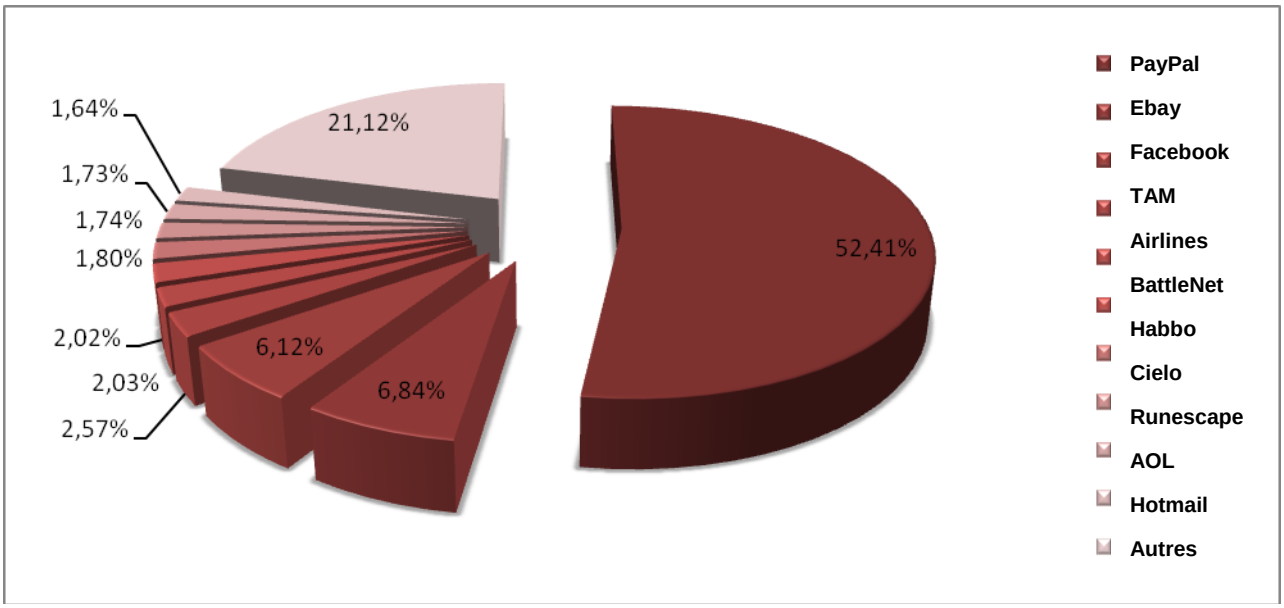
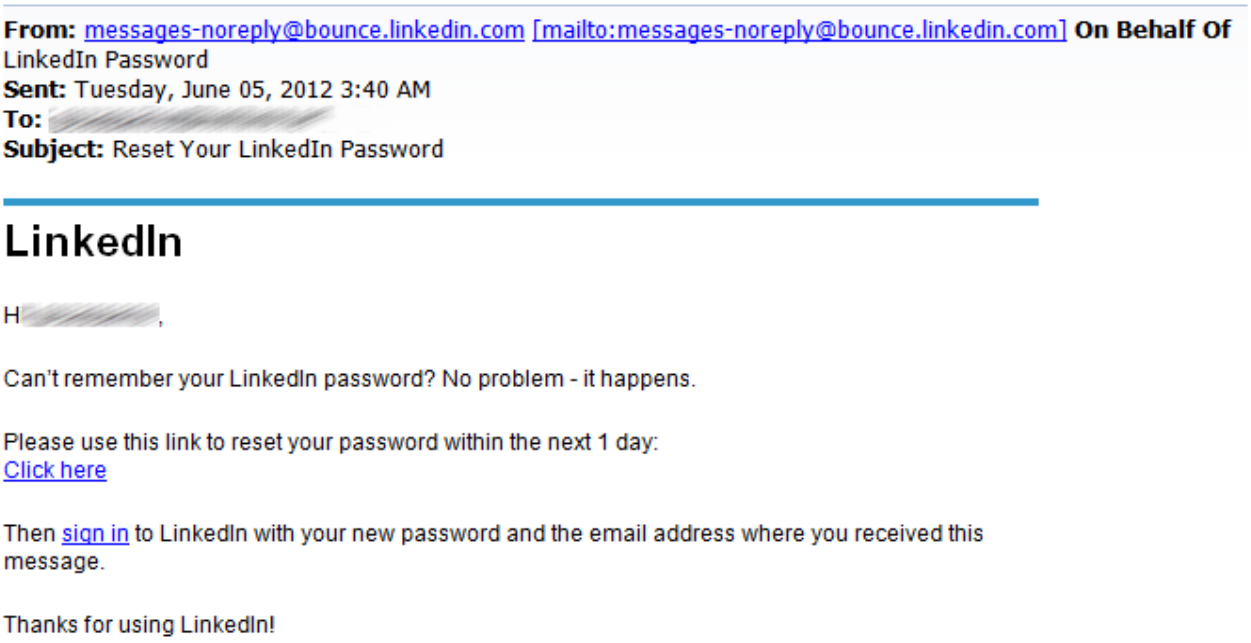


Figure 13 - Top 10 des marques visées par le phishing au 1er semestre 2012.

Figure 14 - Page de phishing PayPal.

Les attaques de phishing ciblées sont en hausse au cours de la première moitié de 2012. Les internautes ont été particulièrement atteints par le phishing consécutif aux fuites de données chez LinkedIn, eHarmony et LastFM. Même lorsque le réseau social professionnel avait expressément signalé aux utilisateurs concernés qu'il n'enverrait pas de notifications de changement de mot de passe, de nombreuses vagues de spam ont déferlées à la suite des fuites dans la base de données.

© 2012 Bitdefender



From: messages-noreply@bounce.linkedin.com [mailto:messages-noreply@bounce.linkedin.com] **On Behalf Of** LinkedIn Password
Sent: Tuesday, June 05, 2012 3:40 AM
To:
Subject: Reset Your LinkedIn Password

LinkedIn

H,

Can't remember your LinkedIn password? No problem - it happens.

Please use this link to reset your password within the next 1 day:
Click here

Then sign in to LinkedIn with your new password and the email address where you received this message.

Thanks for using LinkedIn!

Figure 15 – De prétendue demande de changement de mot de passe par LinkedIn.

Si les internautes peuvent perdre de l'argent à cause du phishing, les entreprises et les gouvernements doivent se préparer au pire : brèches de sécurité dévastatrices, perte de données sensibles, et même des fuites de renseignements militaires. Ce fut le cas mi-mars, lors d'attaques hautement ciblées en provenance de Chine contre des fonctionnaires de l'armée américaine.

© 2012 Bitdefender

Le paysage Android

Au cours des six derniers mois, nous avons enregistré une augmentation alarmante d' **Android.Adware.Mulad.A**, qui est en fait un adware injecté dans d'autres applications. Nous pourrions assister à un nouveau moyen pour les développeurs de logiciels malveillants de générer des gains semi-légitimes.
Après avoir injecté un code adware dans des applications légitimes, ces applications sont téléchargées sur des marchés tiers. Bien qu'ils ne soient pas malveillants par nature, l'affichage de ces pubs agaçantes peut gâcher le plaisir de l'utilisateur notamment lorsque l'on joue.

Bien que nous n'ayons pas fait figurer **Android.Adware.Mulad.A** dans notre Top 10 des malwares pour le premier semestre, nous devons signaler que 25,94 % de toutes les applications analysées témoignaient de la présence de ce type d'adware. Une application sur quatre possédant Mulad, on peut aisément penser qu'au moins l'une d'entre elles se trouve installé sur votre appareil.

Sans avoir enregistré l'arrivée de graves menaces ces six derniers mois, nous avons quand même constaté une augmentation des malwares ayant trait aux vols de données, au « rootage », et une tendance générale à un comportement similaire à celui des malware visant les PC. Nous avons également observé deux exemples de la manière dont les malwares pour Android utilisent les plateformes de microblogging comme Twitter pour masquer les noms de domaines C&C.

Les codeurs de malwares semblent s'intéresser à la mise en place de botnets par l'intermédiaire d'applications malveillantes, une tactique d'autant plus claire que la part de marché des smartphones est en augmentation constante. Il ne manque que le support Ipv6 par les FAI, afin que les botnets de smartphones constituent le moyen les plus puissant pouvant être utilisés pour des attaques de type Déni de Service (DDoS).

L'évolution des malwares pour appareils Android met en relief le fait que les codeurs passent de plus en plus de temps à développer des applications indésirables. Cette tendance va probablement s'amplifier puisque ce type d'appareils est et sera utilisé pour réaliser des opérations bancaires en ligne, des paiements sans contact et d'autres actions impliquant les informations personnelles ou confidentielles de l'utilisateur.

Le nombre de portables en circulation atteignant presque le milliard, ils deviennent une cible d'autant plus intéressante que la majorité des utilisateurs choisissent désormais des abonnements comprenant une connexion à Internet. Dans la mesure où les tâches à la fois personnelles et professionnelles sont gérées

© 2012 Bitdefender

par des appareils identiques fonctionnant sous Android, les malwares qui leur sont destinés vont probablement grimper en flèche dans un proche avenir.

Les vedettes du premier semestre

Un exemple intéressant est la découverte récente d'un spyware Android qui se dissimule des utilisateurs, puis tente d'établir une connexion Wi-Fi pour récolter des informations sur les bornes Wi-Fi proches. Ces informations, ainsi que l'opérateur et les coordonnées GPS, sont envoyés à un domaine contrôlé par l'attaquant. Les renseignements peuvent être utilisés pour planifier des attaques sur des réseaux ou d'autres opérations malveillantes.

Un bot SMS se diffusant par l'intermédiaire de pièces jointes à des courriers s'est fait remarquer en composant des numéros surtaxés à l'insu des utilisateurs. Le domaine caché de commande et de contrôle de Twitter a aussi reçu les identifiants des bots pour que les attaquants puissent suivre de près le nombre d'appareils infectés. Le malware reçoit des instructions d'accepter des paramètres comme le numéro de téléphone, le contenu du message, et le nombre de fois que le SMS devra être envoyé.

Cet exemple montre que la dissimulation du nom du domaine au moyen de plateformes de microblogging est dérivée du malware pour PC. Cette technique sera probablement utilisée dans d'autres attaques car les codeurs de malwares ont besoin d'effacer leurs traces.

Ice Cream Sandwich, également connu sous le nom d'Android 4.0.4, a été la cible d'une application de type proof-of-concept qui pouvait permettre aux attaquants de « rooter » un périphérique au moyen d'une simple application, sans nécessiter un redémarrage. Cette stratégie d'attaque a été illustrée grâce à un exemple de détournement de clic ('clickjacking') permettant aux attaquants de contrôler le comportement des applications. Sans même avoir besoin d'un échantillon de malware pour ce type d'attaque, la démonstration constitue une preuve suffisante pour prévoir que des méthodes nouvelles et sophistiquées sont susceptibles d'être développées pour cibler les utilisateurs d'Android.

© 2012 Bitdefender

Top 10 des menaces Android au 1er semestre 2012

Notre rapport du premier semestre sur les malwares Android portait principalement sur les exploits et les chevaux de Troie – rien d'extraordinaire à cela. Les malwares utilisent généralement des exploits pour avoir un accès privilégié aux ressources des appareils. Les appareils « rootés » rendent la tâche plus facile aux pirates pour développer des chevaux de Troie et autres attaques.

Le fait de « rooter » volontairement un appareil Android est risqué et ouvre la porte à de nombreuses menaces. Le nombre d'exploits détectés reflète donc le choix personnel des utilisateurs lorsqu'ils choisissent l'option de « rootage » de leur appareil.

Les pourcentages calculés ci-dessous ne comprennent pas les échantillons d'**Android.Adware.Mulad.A**, parce qu'ils sont considérés comme étant de type adware et non de type malware.

Top des malwares Android de janvier à juillet 2012		
01.	ANDROID.TROJAN.FAKEDOC.A	21,83 %
02.	ANDROID.EXPLOIT.RATC.A	13,53 %
03.	ANDROID.EXPLOIT.GINGERBREAK.A	7,73 %
04.	ANDROID.EXPLOIT.EXPLOID.B	5,64 %
05.	ANDROID.HACKTOOL.FACENIFF.A	3,46 %
06.	ANDROID.EXPLOIT.ASROOT.B	2,00 %
07.	ANDROID.EXPLOIT.ASROOT.A	1,95 %
08.	ANDROID.TROJAN.FAKEDOC.B	1,81 %
09.	ANDROID.ADWARE.WALLAP.A	1,80 %
10.	ANDROID.HACKTOOL.DROIDSHEEP.A	1,76 %
11.	AUTRES	38,5 %

1. Android.Trojan.FakeDoc.A

Nous avons déjà fait la connaissance de ce cheval de Troie, embarqué dans « Battery Doctor », une application Android supposée optimiser la durée de la batterie de l'utilisateur. Avant l'installation, l'application réclame l'accès au compte Gmail de l'utilisateur, ce qui lui permettra de transmettre secrètement l'emplacement, les courriers et les identifiants à un serveur contrôlé par le pirate, toutes les quatre heures. L'utilisateur est également bombardé de pubs via des pop-up. Représentant 21,83 % de l'ensemble des infections, ce cheval de Troie est classé en tête de notre rapport du premier semestre sur les malwares Android.

2. Android.Exploit.RATC.A

Plus connu sous le nom de « Rage Against the Cage », il est utilisé pour « rooter » les appareils Android pour que les utilisateurs puissent avoir un accès privilégié à certaines des ressources de l'appareil. Le revers

© 2012 Bitdefender

de la médaille est que, si l'appareil « rooté » est infecté par un malware, ce dernier peut disposer d'un niveau de privilège élevé pour accéder aux mêmes ressources. Le système d'exploitation des appareils Android « rootés » est vulnérable aux attaques des applications malveillantes. En seconde position, avec un taux d'infection de 13,53 %, cet exploit est encore celui qui est le plus utilisé pour le « rootage ».

3. Android.Exploit.GingerBreak.A

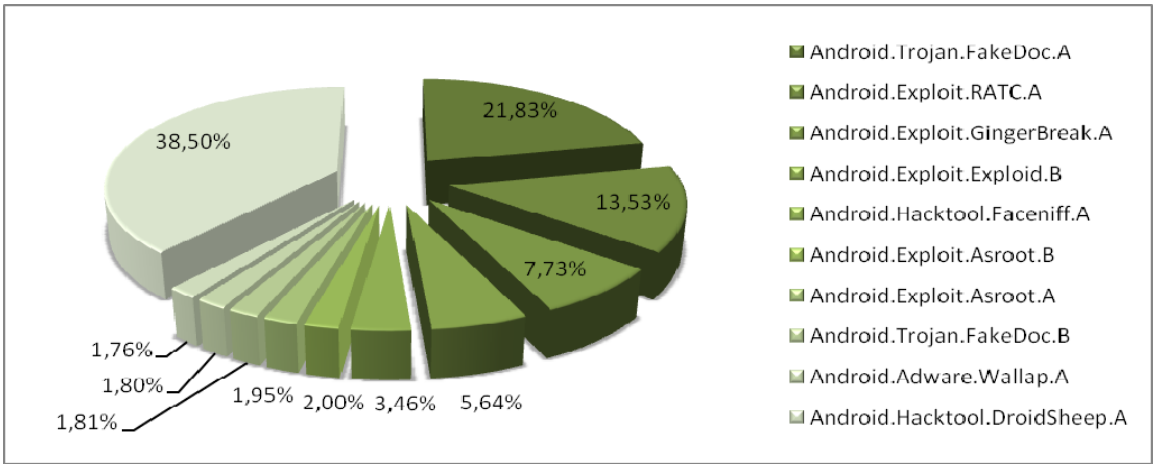
Les appareils Android utilisant Gingerbread (connu aussi sous le nom Android 2.3.3) sont souvent « rootés » en utilisant cet exploit et les utilisateurs ne réalisent pas que le malware contient souvent un code venant de cet exploit en particulier. La plupart des chevaux de Troie embarqués avec des applications légitimes utilisent le code de l'exploit pour accéder à des ressources. Bien qu'il ne compte que pour 7,73 % de la totalité des infections, il prouve qu'un grand nombre des appareils Android tournant sous Gingerbread sont encore « rootés » par les utilisateurs.

4. Android.Exploit.Exploid.B

C'est le troisième type d'exploit pour le « rootage » des appareils Android. Son code est également utilisé par différentes familles de malwares qui essaient de « rooter » des appareils à l'insu de l'utilisateur pour tenter d'outrepasser les sécurités d'Android. 5,64 % de l'ensemble des infections ont été provoquées par cet exploit, classé quatrième dans notre rapport du premier semestre.

5. Android.Hacktool.Faceniff.A

Principalement utilisé pour intercepter le trafic Wi-Fi, cet outil Android permet aux attaquants de tracker les noms d'utilisateurs et mots de passe de services populaires comme Twitter, Facebook ou d'autres plateformes de réseaux sociaux. Cet outil de piratage peut être particulièrement utile à ceux qui pratiquent l'usurpation d'identité par l'intermédiaire des réseaux sociaux. Son taux infectieux de 3,46 % place ce malware en cinquième position dans notre classement.



© 2012 Bitdefender

6. Android.Exploit.Asroot.B

Voici encore un exploit utilisé pour « rooter » les appareils Andoid grâce à un bug du noyau (kernel bug) activé par une macro. C'est un élément de code assez répandu que les malwares utilisent pour obtenir un accès privilégié à un appareil. Avec un taux d'infection global de 2 %, l'exploit joue encore un rôle important dans l'expansion des malwares.

7. Android.Exploit.Asroot.A

Tout comme Android.Explot.Asroot.B, cette nouvelle variante du même exploit se comporte presque de la même manière, permettant aux malwares Android d'accéder aux ressources auxquelles ils n'auraient pas accès en temps normal. Ce type de code malveillant est généralement embarqué avec des applications tierces et peut comporter des charges utiles diverses.

8. Android.Trojan.FakeDoc.B

Ce cheval de Troie n'est qu'une variante de Android.Trojan.FakeDoc.A. La seule différence entre les deux se situe dans les applications dans lesquelles ils sont embarqués. Il est logique que les pirates injectent du code malveillant dans les applications les plus populaires pour donner un impact maximum à leurs attaques. Bien que leur taux d'infection soit inférieur à celui d'Android.Trojan.FakeDoc.A, de seulement 1,81 %, il est peu probable q ue cette famille de chevaux de Troie disparaisse complètement.

9. Android.Adware.Wallap.A

Un autre adware, qui paraît être injecté dans des applications légitimes et distribué par l'intermédiaire de marketplace tiers, semble être destiné à générer des revenus. Nous avons constaté une augmentation alarmante de ces applications infectées avec ce type de code, comme Android.Adware.Mulad.A l'a démontré. Même si Android.Adware.Wallap.A n'est responsable que de 1,80 % du taux global des infections, il pourrait gagner du terrain.

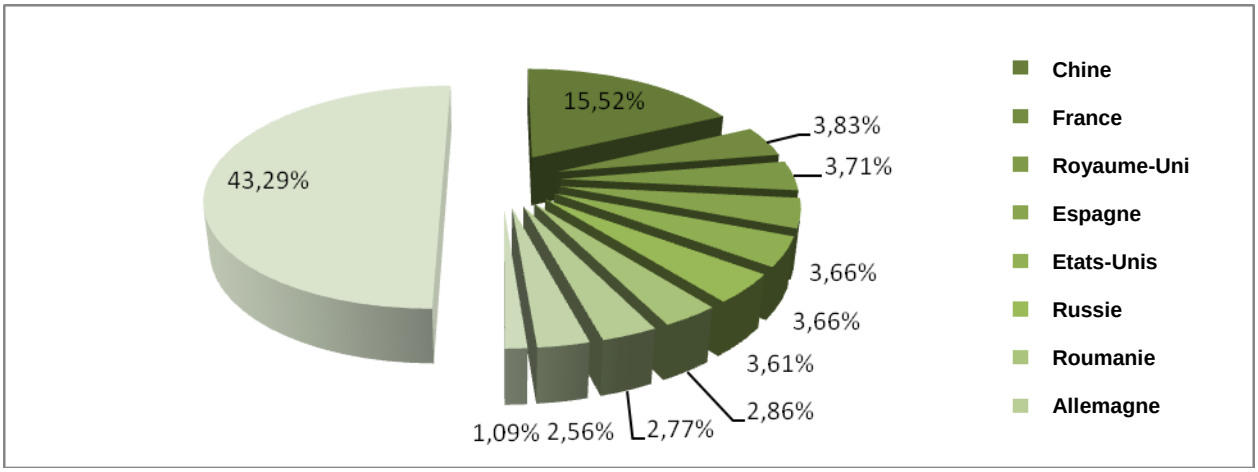
10. Android.Hacktool.DroidSheep.A

Classé au dixième rang de notre tableau de toutes les infections enregistrées, cet outil de piratage est principalement utilisé pour pirater des comptes personnels en contrefaisant des réseaux Wi-Fi publics et en recueillant les noms d'utilisateur et les mots de passe des personnes connectées. Avec un taux d'infection de 1,76 %, il apporte la preuve que l'usurpation d'identité et le piratage de comptes restent dominant sur les appareils tournant sous Android.

© 2012 Bitdefender

Top 10 des pays touchés par les malwares Android

Bien que les malwares Android ne soit généralement pas propres à un pays, à part les chevaux de Troie de SMS surtaxés, le rapport sur le premier semestre fait apparaître que la plupart des pays enregistrent à peu près les mêmes pourcentages d'infection. En dehors de la Chine, qui bat des records avec un taux de 15,52 %, la France et le Royaume-Uni sont presque au coude à coude avec des taux d'infection respectifs de 3,83 et 3,71 %.



L'Espagne et les Etats-Unis ont le même taux d'infection de 3,66 %, suivis de près par la Russie, en sixième position avec un taux de 3,61 %. Ces cinq derniers pays semblent générer un intérêt comparable chez tous les pirates. Les différences de pourcentage ne sont pas très significatives, ce qui laisse penser que les malwares ne sont pas reliés aux situations géographiques, aux populations et aux cultures.

La Roumanie occupe le septième rang avec un taux d'infection de 2,86 %, suivie par l'Allemagne et l'Inde avec des taux respectifs de 2,77 et 2,26 %. La Malaisie arrive dixième, avec un taux d'infection de 1,09 %.

© 2012 Bitdefender

Prévisions

Le développement croissant des malwares va se poursuivre au cours de la seconde moitié de 2012. Nous nous attendons à voir le nombre d'applications malveillantes bondir de 65,5 à 76 millions, car les cybercriminels conçoivent de nouvelles méthodes de dissimulation et de distribution des e-menaces.

Les exploits visant des logiciels très répandus vont également continuer de jouer un rôle clé dans les tentatives de piratage des ordinateurs des utilisateurs. Certains de ces exploits vont s'attaquer à certains systèmes d'exploitation, mais d'autres vont probablement exécuter des charges utiles spécifiques en fonction du système d'exploitation installé localement.

La sortie de Windows® 8 en octobre va probablement aussi poser de nouveaux défis aux utilisateurs, à domicile comme dans l'entreprise. Si l'on se réfère à l'expérience vécue avec Windows Vista® et Windows® 7, les premiers exploits vont sans doute apparaître peu de temps après la sortie de Windows® 8.

Les entreprises vont également être confrontées de manière croissante aux risques pour la sécurité que pose la tendance de plus en plus courante chez les dirigeants au niveau mondial, d'apporter leur propre matériel au bureau. Dans la mesure où ces appareils qui servent à stocker des données professionnelles sensibles ne sont pas gérés par le service informatique de l'entreprise, la probabilité de pertes de données par vol ou perte de ces appareils est en augmentation.

A mesure que sa popularité va croissante, la plateforme Android va subir un feu nourri d'attaques dans les six prochains mois, ceci d'autant plus que son type de distribution facilite la diffusion de malwares à partir d'applications repackagées, notamment dans des pays où il n'existe pas de Store officiel, comme en Chine par exemple.

© 2012 Bitdefender