BitDefender : Top 10 des e-menaces, le P2P vecteurs de malwares
Sécurité
Posté par : JerryG
Publiée le : 5/2/2010 0:00:00

Les plateformes de P2P principaux vecteurs de diffusion des malwares du Top 10 BitDefender des e-menaces de janvier 2010. Autorun et JavaScript sont les principaux vecteurs d'infection ce mois-ci

Le besoin constant d'interaction des utilisateurs en fait des cibles de choix pour toutes sortes de logiciels malveillants. Les principales e-menaces de ce classement mensuel sont constituées de 6 chevaux de Troie, 2 vers, 1 exploit et 1 virus que l'on trouve principalement sur des sites de torrents, « warez » et autres plateformes « peer-to-peer ».

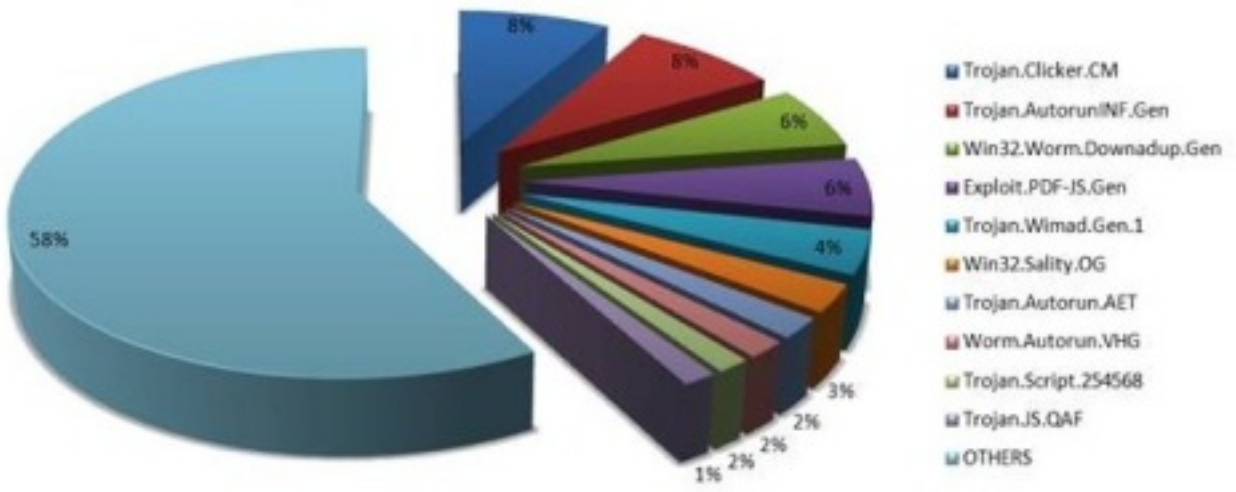
Trojan.Clicker.CM est en tête de ce classement du mois de janvier avec 8,30% de l'ensemble des ordinateurs infectés. Il provient principalement des sites de partage comme des portails de torrents, des communautés « warez » et des services proposant du contenu piraté. Ce cheval de Troie est un petit script affichant des publicités dans le navigateur des internautes. Si certaines publicités présentent des jeux gratuits en ligne, d'autres exposent les utilisateurs à de la pornographie dure ou à d'autres types de contenu inapproprié.

La deuxième place de ce classement revient à ***Trojan.AutorunInf.Gen,*** avec 8,17% des infections. Il s'agit d'un mécanisme générique de diffusion de malwares via des périphériques amovibles tels que des clés USB, des cartes mémoire ou des disques durs externes. Deux des plus célèbres familles de malwares, ***Win32.Worm.Downadup et Worm.Zimuse,*** ont également recours à cette approche pour infecter des systèmes. Il convient donc de prendre des précautions avec ces périphériques externes : s'il est vrai qu'ils permettent de transporter des données facilement, ils peuvent également endommager un ordinateur s'ils sont employés sans prendre de précaution. Les bibliothèques, les magasins et autres lieux publics d'accès à Internet sont généralement des sources d'infection notoires.

À l'origine de 6,18% des infections mondiales, Win32.Worm.Downadup.Gen occupe la troisième position du classement de ce rapport sur les e-menaces. Ce ver exploite une vulnérabilité du service serveur RPC de Microsoft Windows permettant l'exécution de code à distance (MS08-67), afin de se diffuser sur d'autres ordinateurs du réseau local. Il restreint aussi l'accès des utilisateurs à Windows Update et aux sites d'éditeurs de sécurité informatique. De nouvelles variantes installent également de faux logiciels antivirus. Ce ver, apparu il y a plus d'un an, révèle la réticence de la plupart des

utilisateurs à mettre à jour leur système d'exploitation et leur solution antimalware installée localement.

La quatrième place, correspondant à 5,76% de l'ensemble des infections, est occupée par ***Exploit.PDF-JS.Gen.*** Sous ce nom sont regroupés des fichiers PDF malformés exploitant différentes vulnérabilités détectées dans le moteur Javascript de PDF Reader, afin d'exécuter du code malveillant sur l'ordinateur de l'utilisateur. Après l'ouverture d'un fichier PDF infecté, un code Javascript spécialement conçu à cet effet entraîne le téléchargement et l'exécution à distance de codes binaires malveillants.



En cinquième position, avec 4,30 % des infections, ***Trojan.Wimad.Gen.1*** est présent principalement sur des sites Internet de torrents sous la forme d'un épisode inédit de votre série TV préférée. Ces faux fichiers vidéo peuvent se connecter à une URL spécifique et télécharger des malwares en se faisant passer pour le codec nécessaire à la lecture du fichier. Trojan.Wimad.Gen. est particulièrement actif lorsque des films de type 'blockbuster' sont attendus sur les sites de partage de fichiers.

Win32.Sality.OG, en sixième position, a entraîné 2,73% des infections. Cette e-menace malveillante est un infecteur de fichiers polymorphe qui ajoute son code crypté aux fichiers exécutables (binaires .exe et .scr). Cette famille de virus est extrêmement difficile à détecter et à supprimer car ces derniers modifient constamment leur code alors que le composant rootkit essaie de désactiver plusieurs applications antivirus installées sur le système infecté.

Trojan.Autorun.AET, un code malveillant se diffusant via les dossiers partagés de Windows et les supports de stockage amovibles, arrive en septième position avec 2,01% des infections totales. Ce cheval de Troie exploite la fonctionnalité Autorun des systèmes d'exploitation Windows antérieurs à Vista SP2 pour lancer automatiquement des applications lorsqu'un support de stockage infecté est connecté. La fonction Autorun pouvant être exploitée à des fins malveillantes, Microsoft a décidé de la désactiver dans Windows Vista SP2 et Windows 7.

Worm.Autorun.VHG est un ver de réseau/Internet qui exploite la vulnérabilité Windows MS08-067 afin de s'exécuter à distance en utilisant un package RPC (Remote Procedure Call) spécialement conçu à cet effet (une technique également utilisée par Win32.Worm.Downadup). Le ver est huitième du classement avec 1,69% de l'ensemble des infections.

Il est suivi de Trojan.Script.254568, en neuvième position avec 1,40% de l'ensemble des malwares détectés en janvier. Ce code JavaScript crypté recherche un fichier cookie nommé « CoreBeta ». Si celui-ci n'est pas présent dans l'ordinateur, il est créé et configuré pour expirer en une journée. La présence du cookie indique au cheval de Troie que le système a déjà été infecté. Si le script détecte le cookie, il injecte alors dans plusieurs pages Internet des composants cachés alors que d'autres ressources web sont piratées et conduisent vers des pages « about :blank ».

Ce top 10 s'achève avec Trojan.JS.QAF correspondant à 1,40% des infections.

Ce code Java Script « obscurci » est difficile à lire, ce qui complique sa détection. Trojan.JS.QAF crée une « IFrame » qui redirige les utilisateurs vers l'adresse : google-cn.msn.ca.shoplocal-com.[removed].ru:8080/interia.pl/interia.pl/google.com/empflix.com/debonairblog.com/.

Top 10 BitDefender des e-menaces du mois de janvier 2010 :

1 Trojan.Clicker.CM 8,30%

2 Trojan.AutorunINF.Gen 8,17%

3 Win32.Worm.Downadup.Gen 6,18%

4 Exploit.PDF-JS.Gen 5,76%

5 Trojan.Wimad.Gen.1 4,30%

6 Win32.Sality.OG 2,73%

7 Trojan.Autorun.AET 2,01%

8 Worm.Autorun.VHG 1,69%

9 Trojan.Script.254568 1,40%

10 Trojan.JS.QAF 1,40%

AUTRES 58,01%

« *Les infections des autoruns sont de plus en plus utilisées par les développeurs de codes malveillants. Les technologies de propagations s'appuient essentiellement sur les infections des autoruns des disques/clés USB et la propagation par les réseaux locaux et Internet. Tous les sites Internet sont susceptibles d'héberger des codes malveillants y compris les sites informationnels ou conventionnels, une simple navigation sur Internet peut donc être synonyme d'infection.* », déclare **Marc Blanchard**, épidémiologiste et Directeur des Laboratoires Editions Profil pour BitDefender en France.

Pour être informé des dernières e-menaces, inscrivez-vous aux **flux RSS BitDefender**