Le mercredi 2 septembre 2009

Les vers continuent à dominer le Top 10 BitDefender des e-menaces au mois d'août avec Trojan.Clicker.CM en première position

Trojan.Clicker.CM, en tête de ce classement, est de plus en plus présent sur les sites Internet de « warez » (portails de téléchargement hébergeant des cracks et des générateurs de clés pour les applications commerciales).

En deuxième position, **Trojan.AutorunINF.Gen** représente environ 10% de l'ensemble des infections. La fonctionnalité Autorun de Windows est utilisée par de nombreuses familles de malwares qui se propagent ainsi via des supports amovibles.

Trojan.Wimad.Gen.1 occupe la troisième position du classement du mois d'août avec 6% de l'ensemble des infections. Ce cheval de Troie affecte les fichiers ASF, qui ont la capacité de télécharger automatiquement des codecs vidéo appropriés s'ils sont absents du système. Les créateurs de malwares modifient généralement ces fichiers afin qu'ils téléchargent à la place un fichier binaire malveillant.

Plus de 8 mois après son entrée dans le Top 10 BitDefender des e-menaces, **Win32.Worm.Downadup** occupe la quatrième position avec 4% de l'ensemble des machines infectées. Aussi connu sous les noms de **Conficker** ou **Kido**, le ver bloque l'accès à des sites Internet de sécurité informatique.

En cinquième position ce mois-ci, **Win32.Sality.OG** est un infecteur de fichiers polymorphe qui ajoute son code crypté à des fichiers exécutables (binaires .exe et .scr). Afin de ne pas se faire remarquer, il déploie un rootkit sur la machine infectée et tente de supprimer les applications antivirus installées en local.

La sixième place est occupée par **Win32.Induc.A**, un malware moins courant, infectant des applications créées avec les versions Delphi 4 à 7 de Borland (maintenant Embarcadero). Le virus n'infecte pas de fichier binaire, mais modifie le fichier SYSCONST.PAS et y injecte son code malveillant avant de le recompiler. Toutes les applications créées avec le compilateur corrompu sont infectées par le virus. Win32.Induc.A n'a pas de charge utile malveillante, mais sa progression rapide dans le Top 10 montre que peu de développeurs Delphi ont conscience de sa propagation.

Trojan.Autorun.AET, en septième position, est un malware qui se diffuse via les dossiers partagés de Windows et via des médias amovibles (supports NAS ou disques connectés). Ce cheval de Troie exploite la fonctionnalité Autorun des systèmes d'exploitation Windows pour s'exécuter automatiquement lorsqu'un dispositif infecté est connecté.

En huitième position dans ce classement mensuel des e-menaces, **Trojan.JS.PYV** est un script malveillant affectant les utilisateurs consultant des sites Internet malveillants ou des sites Internet légitimes compromis par des attaquants.

En neuvième position se trouve Win32.Virtob.Gen, un infecteur de fichiers écrit en langage assembleur. Ce malware se camoufle en utilisant des process de Windows pour se lancer. L'attaque s'effectue en temps réel en mémoire et est détectée immédiatement par BitDefender Active Virus Control. Ce procédé ne compromet pas les fichiers système, il les utilise.

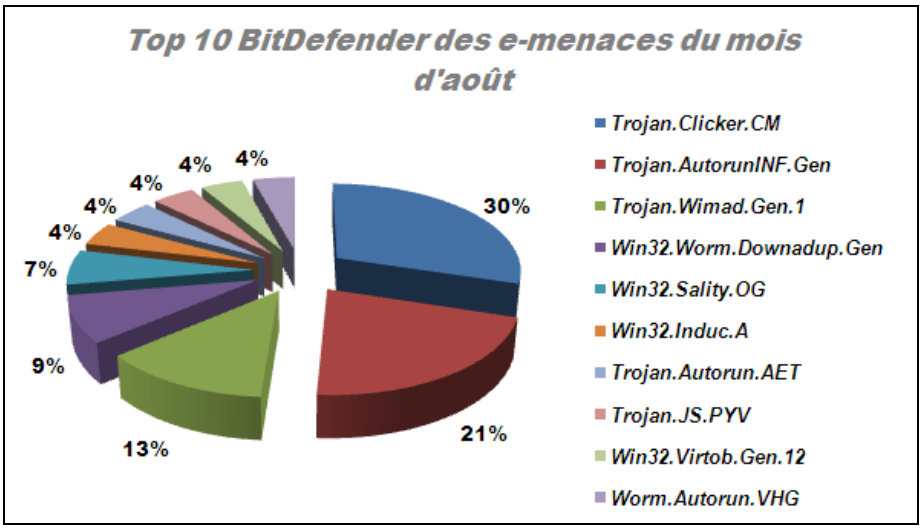
Enfin, **Worm.Autorun.VHG,** est un ver de réseau/Internet qui exploite la vulnérabilité Windows MS08-067 afin de s'exécuter à distance en utilisant un package RPC (Remote Procedure Call, appel de procédure à distance) spécialement conçu à cet effet (une technique également utilisée par Win32.Worm.Downadup). La présence de ce ver dans le classement de BitDefender confirme que les utilisateurs ne prennent pas en compte les alertes de sécurité de Microsoft et ne déploient pas les

patchs de sécurité.

Marc Blanchard, Epidémiologiste, Directeur des Laboratoires Editions Profil / BitDefender en France ajoute au sujet de l'infection par Win32.Induc.OG qui corrompt les applications créées avec Delphi : « Cette méthode d'infection apparue en 1997 et touchant les compilateurs Java de l'époque refait son apparition avec les compilateurs Delphi. Le concept est d'infecter les compilateurs eux-mêmes avant que les programmes soient compilés, ce qui permet de générer automatiquement une faille dans chaque programme compilé avec ce compilateur compromis ».

Top 10 BitDefender des e-menaces du mois d'août :

Position	Nom	%
1.	Trojan.Clicker.CM	14
2.	Trojan.AutorunINF.Gen	10
3.	Trojan.Wimad.Gen.1	6
4.	Win32.Worm.Downadup.Gen	4
5.	Win32.Sality.OG	3
6.	Win32.Induc.A	2
7.	Trojan.Autorun.AET	2
8.	Trojan.JS.PYV	2
9.	Win32.Virtob.Gen.12	2
10.	Worm.Autorun.VHG	2



À propos de BitDefender®

*BitDefender est la société créatrice de l'une des gammes de **solutions de sécurité** la plus complète et la plus certifiée au niveau international reconnues comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les **solutions de sécurité** BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont*

disponibles via le ***Centre de presse****. Retrouvez également sur le site* ***www.malwarecity.fr*** *les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.*

À propos des Editions Profil

Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et de contrôle parental Parental Filter 2, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.