Le jeudi 5 mars 2009

L'exploitation de failles continue à dominer le Top 10 BitDefender de février

Trojan.Clicker.CM fait des ravages sur Internet pour la deuxième fois cette année

Les composants « drive-by download » (qui s'installent lors de la simple visite d'un site Internet) font partie des **dix principales E-Menaces de février** selon les Laboratoires BitDefender®. Les composants de ces Exploits sont mis bout à bout comme les maillons d'une chaîne par des créateurs de malwares. Chaque maillon représentant une nouvelle tentative de corruption de la sécurité du système d'un utilisateur par les cybercriminels.

Trojan.Clicker.CM.occupe la première place du classement pour la deuxième fois cette année, mais avec une moindre avance que le mois passé. Ce malware est un afficheur de pop-ups intempestifs devéloppé pour contourner les protections anti publicité de Norton. Il a pour objectif d'afficher un grand nombre de pop-up commerciaux qui sont intégré dans la page du navigateur Web en cours de consultation par l'utilisateur, en vue de le pousser à cliquer dessus. En cas de clic, des profits sont générés au travers des publicités fonctionnant avec un système de paiement au nombre de clics. Ce cheval de Troie utilise également plusieurs fonctions qui contournent le bloqueur de pop-ups de Norton® Internet Security.

En deuxième position se trouve un cheval de Troie plus ancien : Trojan.Wimad.Gen.1 ou Wimad, qui se fait passer pour un composant de lecteur audio/video permmetant la lecture de fichier ASF. Ce cheval de Troie est téléchargé via un autre cheval de Troie téléchargeur de fichier qui occupe la dixième place du classement.

Le virus Conficker et ses pairs sont également présents dans la liste de février, détectés de manière générique comme des virus utilisant le récent bug de l'autorun de Windows « Trojan.AutorunINF.Gen » représentant 4,17% des détections totales.

En 8ème position, Trojan.IFrame.GA est constitué d'un simple script injecté dans des pages de sites Internet corrompus qui envoie aux navigateurs un ensemble d'exploits tels que Trojan.Exploit.ANPI (en 7ème position), et qui peut diriger les systèmes vulnérables vers une page contenant Trojan.Exploit.SSX (en 5ème position).

« Cette chaîne d'infections particulière provient directement de l'analyse d'un certain nombre de sites Internet corrompus et/ou malicieux hébergés en Chine » explique Sorin Dudea, Directeur des Laboratoires de Recherche Antimalware BitDefender. *« Toutefois, ces exploits et ces téléchargeurs peuvent également apparaître dans d'autres cas d'attaques similaires »*

Trois autres téléchargeurs prennent place pour la première fois dans notre liste ce mois-ci (Trojan.Downloader.JS.Psyme.SR, Trojan.Downloader.JLPK et **Trojan.Downloader.Js.Agent.F**). Ils ont tous pour fonction de télécharger et de lancer d'autres malwares sur des ordinateurs déjà corrompus à partir de sites Internet.

TOP 10 - BitDefender des principales e-menaces de février 2009 :

Pos.	Nom	%
1.	Trojan.Clicker.CM	5.87
2.	Trojan.Wimad.Gen.1	4.39
3.	Trojan.AutorunINF.Gen	4.17
4.	Trojan.Downloader.JLPK	3.94
5.	Trojan.Exploit.SSX	3.92
6.	Trojan.Downloader.Js.Agent.F	3.9
7.	Trojan.Exploit.ANPI	3.77
8.	Trojan.IFrame.GA	2.9
9.	Trojan.Downloader.JS.Psyme.SR	2.32
10.	Trojan.Downloader.WMA.Wimad.S	2.01
	Autres malwares	62.81

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. Pour plus d'informations, visitez : www.bitdefender.fr

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 Parental Filter, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.