Le jeudi 20 août 2009

BitDefender découvre Win32.Induc.A, un virus menaçant les compilateurs Delphi et infectant des applications légitimes

Le virus, appelé Win32.Induc.A, se diffuse en infectant des systèmes sur lesquels le compilateur Delphi (jusqu'à la version 7.0) est installé

BitDefender® a annoncé aujourd'hui la découverte d'une menace affectant directement de nombreuses applications, parmi lesquelles TabBrowser v1.0, GreenOpen, WebMoney Keeper Classic v3.7.0.0, Tidy Favorites v4.1 et Any TV Free v2.41. Le ou les auteurs du virus sont parvenus à insérer le code du virus directement dans ces applications qui ont été distribuées déjà infectées.

Le virus, Win32.Induc.A, se diffuse en infectant des systèmes sur lequel le compilateur Delphi (jusqu'à la version 7.0) est installé. Tous les programmes qui sont compilés par la suite via le compilateur corrompu contiennent le code du virus. Bien que ce virus ne dépose aucune charge utile et ne réalise aucune action malveillante à part l'auto-réplication, le fait qu'il ait infecté des packages d'installation révèle un mode d'infection inhabituel, particulièrement efficace, qui fait craindre son utilisation à des fins malveillantes à l'avenir.

Une fois exécuté, le virus recherche certaines versions du compilateur Delphi et, s'il les trouve, crée un fichier SysConst.pas, à l'intérieur du dossier \Lib du compilateur. Il y écrit son code, puis renomme « SysConst.dcu » qu'il appelle « SysConst.bak. ». Le fichier .pas est ensuite compilé, puis supprimé. Le fichier SysConst.dcu qui en résulte est utilisé par le compilateur à chaque compilation, qui crée ainsi des exécutables infectés de façon automatique, en insérant le code malveillant à l'intérieur de SysConst.dcu.

Il est intéressant de noter que le virus n'a pas infecté que des applications légitimes : les spécialistes des Laboratoires antivirus de BitDefender ont en effet découvert que de nombreux malwares de la « famille » de Trojan.Banker avaient été infectés par Win32.Induc.A.

Détectés par BitDefender sous les noms de « Trojan.Downloader.JMGZ », « Trojan.Spy.Banker.ABWA » – « ABWC », « Trojan.Spy.Banker.ABWK » , « ABWQ », etc, ces chevaux de Troie s'attaquent à des banques locales : à la Caixa, la plus grande caisse d'épargne espagnole et à Bradesco, une grande banque du Brésil.

Il est recommandé aux développeurs Delphi de regarder si le dossier \Lib de leur compilateur contient un fichier SysConst.bak (le signe le plus évident de l'infection) et, si c'est le cas, de le renommer « SysConst.pas », en écrasant le fichier corrompu, avant de recompiler leurs applications.

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 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.