BitDefender, La protection contre le backdoor Yonsole corrompant le MBR
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 24/6/2010 15:00:00

BitDefender a publiÃ© des signatures et un **outil de dÃ©sinfection gratuit** afin de protÃ©ger ses utilisateurs **contre un nouveau backdoor** Ã©crasant la zone dâ□□amorÃ§age du disque dur local, et empÃªchant ainsi Windows de dÃ©marrer.

Cette menace peut empÃªcher les systÃ¨mes dâ□□exploitation de dÃ©marrer

DÃ©tectÃ©e par BitDefender sous le nom de **Backdoor.Yonsol**e, cette e-menace a Ã©tÃ© dÃ©couverte samedi 19 juin. Elle est livrÃ©e avec plusieurs applications, dont lâ□□une se fait passer pour une Â« mise Ã jour critique de MicrosoftÂ® WindowsÂ® Â». Des analyses prÃ©liminaires ont rÃ©vÃ©lÃ© la prÃ©sence de deux variantes (A et B) ayant la mÃªme fonctionnalitÃ©, mais qui infectent diffÃ©remment les services Windows.

AprÃ¨s avoir infectÃ© le systÃ¨me hÃ´te, le malware installe et enregistre un service backdoor permettant Ã un attaquant distant dâ□□Ã©mettre des commandes, ainsi que dâ□□initier une session Bureau Ã Distance. Lâ□□une des commandes prises en charge permet dâ□□Ã©craser la zone dâ□□amorÃ§age (MBR) du disque dur, un comportement caractÃ©ristique des cÃ©lÃ¨bres vers de la famille Zimuse.

Nous recommandons vivement aux utilisateurs craignant que leurs systÃ¨mes nâ□□aient Ã©tÃ© corrompus dâ□□exÃ©cuter lâ□□outil de dÃ©sinfection disponible sur Malware City. Si le MBR nâ□□a pas encore Ã©tÃ© Ã©crasÃ©, lâ□□outil de dÃ©sinfection nettoiera le systÃ¨me et lancera un redÃ©marrage. BitDefender a mis Ã jour ses signatures afin de bloquer et de supprimer les deux variantes de Backdoor.Yonsole dÃ¨s samedi ; les utilisateurs de BitDefender sont donc protÃ©gÃ©s contre cette e-menace.

Pour plus dâ□□informations sur Backdoor.Yonsole et sur lâ□□outil de dÃ©sinfection gratuit, consulter le site de Malware City.

Pour plus dâ□□informations concernant les produits BitDefender.