G-Data : Les fichiers de raccourci Windows, vecteurs dâ□□infection
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 20/7/2010 0:00:00

TrÃ¨s rÃ©cemment, des rapports ont Ã©tÃ© publiÃ©s au sujet d'un nouveau genre de malware se propageant par des lecteurs amovibles comme des clÃ©s USB. Un malware exploite une nouvelle **vulnÃ©rabilitÃ© dÃ©couverte dans les fichiers de raccourci,** qui permet lâ□□exÃ©cution de code alÃ©atoire dans le systÃ¨me. Microsoft a officiellement reconnu la vulnÃ©rabilitÃ© et publiÃ© un avertissement de sÃ©curitÃ©.

Le malware, dÃ©tectÃ© par G Data comme un Win32.Worm.Stuxnet.A, est malheureusement un ver (et un rootkit) qui dispose de nombreuses ressources. Il peut se propager en utilisant une vulnÃ©rabilitÃ© 0-Day dÃ©crite ici et Ã©galement mentionnÃ©e par le CVE (Common Vulnerabilities and Exposures) comme CVE-2010-2568.

Sans antivirus, Windows (principalement, le Shell de windows) peut Ãªtre dupÃ© dans lâ□□exÃ©cution du code malveillant (un DLL) car le malware se camoufle dans un fichier de raccourci (.LNK).

Le problÃ¨me est que le Shell de Windows n'analyse pas le raccourci avant que le graphisme ne soit chargÃ©. Le code malveillant sâ□□exÃ©cute alors sans quâ□□il soit nÃ©cessaire de cliquer sur le raccourci ! Il suffit par exemple que lâ□□utilisateur ouvre le dossier contenu sur un support de stockage, pour accÃ©der Ã nâ□□importe quel fichier lÃ©gitime, pour quâ□□il affiche aussi le raccourci et soit alors infectÃ© par ce dispositif.

A noter Ã©galement que les pÃ©riphÃ©riques USB ne sont pas les seuls vecteurs potentiels : les partages rÃ©seau et les partages WebDAV peuvent Ã©galement Ãªtre employÃ©s pour

distribuer les .LNK malveillants. Des plates-formes affectÃ©es (essentiellement toutes les versions actuelles de Windows) sont mentionnÃ©es dans l'avertissement de sÃ©curitÃ©. Et il est probable quâ□□il nâ□□y ait pas de solutions pour XP SP2 et Windows 2000, qui ne sont plus supportÃ©s depuis quelques jours.

Microsoft suggÃ¨re plusieurs solutions pour limiter les risques :

â□¢ DÃ©sactiver lâ□□Autorun de Windows

â□¢ Utiliser des comptes Ã droits limitÃ©s (privilÃ©gier les comptes utilisateurs standards aux comptes administrateurs)

â□¢ Bloquer les connexions SMB sur le pare-feu pour rÃ©duire le risque de partage de fichiers.

â□¢ DÃ©sactiver l'affichage des raccourcis (**description ici**)

â□¢ DÃ©sactiver le service WebClient (**description ici**)

En termes de conclusion, G Data souhaite rappeler quâ□□il est indispensable de mettre rÃ©guliÃ¨rement Ã jour son systÃ¨me et lâ□□ensemble de ses applications. Lâ□□installation dâ□□un antivirus est aussi fortement conseillÃ©e.