BitDefender : Des posts de keyloggers sur des pages Web
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 17/6/2010 0:00:00

De nombreux **posts de keyloggers** se sont accumulÃ©s sur Pastebin.com faisant craindre des **attaques massives de keyloggers**

Comme si le nombre dâ□□entrÃ©es postÃ©es par les keyloggers (programme agissant Ã l'insu de l'utilisateur et enregistrant toutes les frappes de clavier) sur Pastebin nâ□□Ã©tait pas suffisant, leur contenu a Ã©galement de quoi inquiÃ©ter : au lieu du code open-source attendu, on y trouve des mots de passe Facebook ou de Messagerie InstantanÃ©e, ainsi que des informations dÃ©taillÃ©es sur lâ□□historique de navigation des utilisateurs peu mÃ©fiants.

La quantitÃ© de donnÃ©es exposÃ©es est suffisante pour Ã©liminer lâ□□hypothÃ¨se dâ□□une mise en ligne manuelle. Une observation plus attentive rÃ©vÃ¨le quâ□□il sâ□□agit dâ□□une infection massive de keyloggers

Pourquoi utiliser Pastebin.com comme rÃ©fÃ©rentiel de logs ?

En gÃ©nÃ©ral, les keyloggers ont recours Ã des approches de transfert classiques et envoient les paquets de donnÃ©es via des e-mail ou FTP, ce qui augmente considÃ©rablement les risques que les autoritÃ©s dÃ©couvrent lâ□□identitÃ© de lâ□□attaquant.

De plus, lâ□□approche par e-mail est extrÃªmement peu discrÃ¨te : il est facile pour un administrateur systÃ¨me de dÃ©tecter le trafic, sans parler du fait que les logiciels antimalwares informent gÃ©nÃ©ralement les utilisateurs quâ□□un e-mail quitte leur systÃ¨me. Dâ□□autres fois, les ports de messagerie (en gÃ©nÃ©ral les ports 25, 465 et 578) sont sÃ©curisÃ©s ou bloquÃ©s, ce qui empÃªche la transmission des donnÃ©es du keylogger.

Câ□□est pourquoi ce keylogger emploie des tactiques Â« personnalisÃ©es Â» telles que le dÃ©pÃ´t des donnÃ©es sur un emplacement web. Disons que Pastebin Ã©vite dâ□□Ãªtre bloquÃ© par un pare-feu, de laisser des traces, nâ□□indique pas lâ□□adresse IP dâ□□origine et permet donc de protÃ©ger lâ□□identitÃ© de lâ□□attaquant.

Pastebin est une Ã©norme plateforme collaborative hÃ©bergeant des millions de lignes de code publiÃ©es au format texte. Contrairement aux forums ou aux rÃ©seaux sociaux, le texte publiÃ© ne

sera probablement pas vu par dâ□□autres utilisateurs, Ã moins quâ□□ils ne le recherchent. Mais en faisant une recherche ciblÃ©e, lâ□□attaquant obtiendra assurÃ©ment les logs pertinents dans la fenÃªtre du navigateur.

Ainsi, les victimes se font voler leurs identifiants et mots de passe via le keylogger, mais les donnÃ©es recueillies sont Ã©galement accessibles Ã dâ□□autres internautes. Et pour couronner le tout, tout ce qui a Ã©tÃ© postÃ© reste accessible pour toujours, mÃªme si les pages en question sont supprimÃ©es (câ□□est lâ□□inconvÃ©nient de la mise en cache des donnÃ©es), de sorte que des personnes mal intentionnÃ©es peuvent rÃ©cupÃ©rer ces informations Ã tout moment, et les utiliser de nouveau.

Lâ□□observation des forums Â« underground Â» utilisÃ©s par les crÃ©ateurs de malwares rÃ©vÃ¨le une grande quantitÃ© de code source pouvant Ãªtre intÃ©grÃ© dans ces nouveaux types de keyloggers. Cela rend cette situation bien plus inquiÃ©tante quâ□□une mini-Ã©pidÃ©mie provoquÃ©e par lâ□□apparition dâ□□un seul malware et marque le dÃ©but dâ□□une nouvelle vague dâ□□exploitation de services publics et rÃ©putÃ©s, comme cela sâ□□est produit avec les botnets contrÃ´lÃ©s sur Twitter.

Informations complÃ©mentaires

Il semble que lâ□□un des keyloggers utilisant Pastebin afin de prÃ©server son anonymat, soit en circulation depuis suffisamment de temps pour Ãªtre Ã lâ□□origine de la plupart des posts. DÃ©tectÃ© par BitDefender sous le nom de Trojan.Keylogger.PBin.A, ce keylogger est une

application console et utilise lâ□□interface de programmation Pastebin pour envoyer les frappes de clavier interceptÃ©es Ã intervalles alÃ©atoires.

Pour plus dâ□□informations concernant les produits BitDefender, vous pouvez consulter : BitDefender.fr.