G-Data : BÃªta Bot, Le robot qui dÃ©sinstalle les antivirus.
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 10/5/2013 14:00:00

G-Data signale qu'un code malveillant pousse l'utilisateur Ã valider l'UAC pour infecter le systÃ¨me et dÃ©sinstaller l'antivirus prÃ©sent. Ce nouveau bot appelÃ© "**Beta Bot**" est rÃ©cemment entrÃ© sur le marchÃ© parallÃ¨le. Disponible pour moins de 500 â¬, Beta Bot est un robot relativement peu cher compte tenu de sa vaste liste de fonctionnalitÃ©s.

MÃªme si la plupart de ces caractÃ©ristiques sont assez standards (attaque DDoS, accÃ¨s Ã distance, captures de donnÃ©es et autres mÃ©thodes de vols dâinformations) une capacitÃ© particuliÃ¨re a attirÃ© lâattention du G Data SecurityLabs : Â« DÃ©sactiver lâantivirus Â» annonce la publicitÃ© affichÃ©e sur les forums souterrains.

Une annonce suivie d'une liste de prÃ¨s de 30 programmes de sÃ©curitÃ© censÃ©s Ãªtre dÃ©sactivables par Beta Bot.

Quelle est la mÃ©thode utilisÃ©e ?

Lorsqu'il est installÃ© sur un systÃ¨me, Beta Bot cherche une solution de sÃ©curitÃ© quâil connait. Sâil la trouve, le robot commence ses attaques en arrÃªtant les processus, en dÃ©sactivant des clÃ©s de registre ou en dÃ©sactivant les mises Ã jour automatiques. Selon le type de produit de sÃ©curitÃ©, Beta Bot tente de contourner les pare-feux en injectant certaines routines dans les programmes qui sont habituellement autorisÃ©s Ã passer le pare-feu, comme Internet Explorer.

ContrÃ´le d'accÃ¨s utilisateur (UAC) â contourner les permissions.

Sur les systÃ¨mes d'exploitation Windows modernes, les autorisations des utilisateurs sont rÃ©parties entre standard (faible niveau dâautorisation) et administrateur (niveau dâautorisation Ã©levÃ©). Contrairement Ã un administrateur, un utilisateur standard ne peut pas modifier les parties critiques du systÃ¨me. La dÃ©cision dâÃ©lever le niveau de permission dâun processus est proposÃ©e Ã lâutilisateur par une fenÃªtre de dialogue spÃ©cifique. Celui-ci doit alors valider ou non cette permission. Beta Bot utilise cette boite de dialogue pour gagner des droits Ã©levÃ©s sur le systÃ¨me. Bien que beaucoup de codes malveillants se contentent de droits utilisateurs limitÃ©s pour attaquer le systÃ¨me, Beta Bot doit escalader les privilÃ¨ges utilisateurs pour sâattaquer aux logiciels de sÃ©curitÃ©. Pour rÃ©ussir dans cette dÃ©marche, la validation de lâutilisateur est nÃ©cessaire.

Deux astuces sont utilisÃ©es par Beta Bot pour convaincre lâutilisateur de valider cette Ã©lÃ©vation de droits.

DÃ¨s que le code malveillant est exÃ©cutÃ© sur le systÃ¨me, il affiche une premiÃ¨re fenÃªtre dans la langue du systÃ¨me (10 langues, dont le franÃ§ais, sont disponibles) signifiant un problÃ¨me de disque dur. Ce faux message critique joue sur la peur de perdre des donnÃ©es et invite lâutilisateur Ã rÃ©parer les dossiers endommagÃ©s. Lâutilisateur doit choisir lâune des deux options proposÃ©es (Â« Restaurer les fichiers Â» ou Â« Restaurer les fichiers et rÃ©aliser une vÃ©rification de disque Â»). Câest alors que le contrÃ´le dâaccÃ¨s utilisateur (UAC) est lancÃ©.

Câest Ã lâautre astuce de prendre le relais : Beta Bot nâest pas directement utilisÃ© pour lancer le processus UAC. Câest le programme cmd.exe, autrement dit lâinvite de commande

Windows, qui est utilisÃ©e pour dÃ©marrer le code Beta Bot. L'utilisateur est donc invitÃ© Ã Ã©lever les autorisations d'un programme Windows, ce qui est habituellement autorisÃ© par la majoritÃ© des utilisateurs.

Les solutions G-Data sont disponible chez GS2i.

Visitez le site de GS2i