

G-Data : B ta Bot, Le robot qui d sinstalle les antivirus.

S curit 

Post  par : JerryG

Publi e le : 10/5/2013 14:00:00

G-Data signale qu'un code malveillant pousse l'utilisateur   valider l'UAC pour infecter le syst me et d sinstaller l'antivirus pr sent. Ce nouveau bot appel  **"Beta Bot"** est r cemment entr  sur le march  parall le. Disponible pour moins de 500   , Beta Bot est un robot relativement peu cher compte tenu de sa vaste liste de fonctionnalit s.

M me si la plupart de ces caract ristiques sont assez standards (attaque DDoS, acc s   distance, captures de donn es et autres m thodes de vols d'informations) une capacit  particuli re a attir  l'attention du G Data SecurityLabs :  « D sactiver l'antivirus  » annonce la publicit  affich e sur les forums souterrains.



Une annonce suivie d'une liste de pr s de 30 programmes de s curit  cens s  tre d sactivables par Beta Bot.

Quelle est la m thode utilis e ?

Lorsqu'il est install  sur un syst me, Beta Bot cherche une solution de s curit  qu'il connaît. S il la trouve, le robot commence ses attaques en arr tant les processus, en d sactivant des cl s de registre ou en d sactivant les mises   jour automatiques. Selon le type de produit de s curit , Beta Bot tente de contourner les pare-feux en injectant certaines routines dans les programmes qui sont habituellement autoris s   passer le pare-feu, comme Internet Explorer.

Contr le d'acc s utilisateur (UAC)    contourner les permissions.

Sur les syst mes d'exploitation Windows modernes, les autorisations des utilisateurs sont r parties entre standard (faible niveau d'autorisation) et administrateur (niveau d'autorisation  lev ). Contrairement   un administrateur, un utilisateur standard ne peut pas modifier les parties critiques du syst me. La d cision d' lever le niveau de permission d'un processus est propos e   l'utilisateur par une fen tre de dialogue sp cifique. Celui-ci doit alors valider ou non cette permission. Beta Bot utilise cette boite de dialogue pour gagner des droits  lev s sur le syst me. Bien que beaucoup de codes malveillants se contentent de droits utilisateurs limit s pour attaquer le syst me, Beta Bot doit escalader les privil ges utilisateurs pour s'attaquer aux logiciels de s curit . Pour r ussir dans cette d marche, la validation de l'utilisateur est n cessaire.



Deux astuces sont utilis es par Beta Bot pour convaincre l'utilisateur de valider cette   l vation de droits.

D s que le code malveillant est ex cut  sur le syst me, il affiche une premi re fen tre dans la langue du syst me (10 langues, dont le fran ais, sont disponibles) signifiant un probl me de disque dur. Ce faux message critique joue sur la peur de perdre des donn es et invite l'utilisateur   r parer les dossiers endommag s. L'utilisateur doit choisir l'une des deux options propos es (  Restaurer les fichiers   ou   Restaurer les fichiers et r aliser une v rification de disque  ). C'est alors que le contr le d'acc s utilisateur (UAC) est lanc .

C'est   l'autre astuce de prendre le relais : Beta Bot n'est pas directement utilis  pour lancer le processus UAC. C'est le programme cmd.exe, autrement dit l'invite de commande

Windows, qui est utilis e pour d marrer le code Beta Bot. L'utilisateur est donc invit    lever les autorisations d'un programme Windows, ce qui est habituellement autoris  par la majorit  des utilisateurs.

Les solutions G-Data sont disponible chez GS2i.

[Visitez le site de GS2i](#)