Insolite : Aldi Bot , le rÃ©seau zombie hard-discount
Insolite
PostÃ© par : JerryG
PubliÃ©e le : 22/9/2011 14:00:00

DÃ©cidÃ©ment, les temps sont difficiles, mÃªme pour les voyous du Net, qui seÂ mettent Ã faire **du Hard-discount en proposant des malwares Ã prix dÃ©fiants**Â toutes concurrences, cela parait insolite, mais mÃªme les vauriens des bas fondsÂ du Web ont besoin de se nourrir, alors ils proposent des "bots" Ã prix rÃ©duit etÂ cerise sur le gÃ¢teau, apportent mÃªme leur assistance aux Scripts Kiddy

Le G Data SecurityLabs a assistÃ© Ã une vente de bot particuliÃ¨re sur le marchÃ© cybercriminel. Le Bot nommÃ© Â« Aldi Â» Ã©tait vendu entre 5 et 10 â¬ par son auteur. Un bot hard-discount qui reprend une partie du code ZeuS.

L'auteur du logiciel qui a mis en vente son bot sur les rÃ©seaux cybercriminels explique qu'il aime le codage et quâ□□il ne tient pas Ã gagner beaucoup d'argent, ce qui expliquerait ce prix de commercialisation trÃ¨s bas. Une offre Ã tarif rÃ©duit qui pourrait aussi expliquer le nom du Bot, Aldi Ã©tant une chaine de magasins hard discount. Allant jusquâ□□au bout de son concept, lâ□□auteur va mÃªme jusquâ□□Ã apposer le logo de la chaine de magasins sur son logiciel.

A-t-il voulu reprendre Ã son compte lâ□□engagement Aldi (la meilleure qualitÃ© au meilleur prix) ? Possible, nÃ©anmoins lâ□□auteur du code malveillant annonce : Â« Je ne peux pas garantir que le programme que vous obtiendrez soit toujours FUD", autrement dit il n'y a aucune garantie pour les acheteurs que le code ne soit pas dÃ©tectÃ© par les solutions Antivirus. Il a raison : les solutions G Data sont par exemple capables de dÃ©tecter ce bot.

Les principales fonctions de Â«Bot Aldi Â» v1.0 sont:

â□¢ PossibilitÃ© d'effectuer des attaques DDoS

â□¢ SOCKS : le propriÃ©taire du bot peut utiliser le PC de la victime en tant que proxy

â□¢ Firefox password stealer : vol des mots de passe enregistrÃ©s dans la base de donnÃ©es de Firefox

â□¢ ExÃ©cution Ã distance de n'importe quel fichier

Une mise Ã jour v2.0 ajoute les fonctions suivantes Ã celles dÃ©jÃ disponibles :

â□¢ Pidgin password stealer : vol des mots de passe de la messagerie instantanÃ©e Pidgin

â□¢ jDownloader password stealer : vol des mots de passe du tÃ©lÃ©chargeur de lâ□□hÃ©bergeur

L'auteur a aussi postÃ© une vidÃ©o sur Youtube, qui semble montrer le Bot Â« Aldi Â» utilisÃ© dans une attaque DDoS contre **le site** de la Police fÃ©dÃ©rale allemande.

Les journaux de conversations, postÃ©s par l'auteur du code rÃ©vÃ¨le que pour ce tarif avantageux, il va mÃªme jusquâ□□Ã fournir une aide personnalisÃ©e pour l'installation et la mise en Å□uvre du bot, et cela mÃªme aux pirates dÃ©butants (appelÃ©s Â« noobs Â») qui n'ont pas la moindre idÃ©e sur la faÃ§on dâ□□utiliser ces outils malveillants ! Il va mÃªme jusquâ□□Ã utiliser un systÃ¨me de dÃ©monstration vidÃ©o pour expliquer en live Ã ses clients comment rÃ©aliser des attaques.

DerriÃ¨re lâ□□apparente lÃ©gÃ¨retÃ© de cette situation, un problÃ¨me de fond se pose. Le cÃ´tÃ© Â« amusant Â» du piratage qui conduit Ã ce type de dÃ©marche financiÃ¨rement dÃ©sintÃ©ressÃ©e attire n'importe quel internaute curieux vers le cÃ´tÃ© obscur, que ce soit pour le plaisir ou dans un but lucratif. Un Script kiddy peut ainsi acheter ce bot avec son argent de poche et sâ□□exercer Ã devenir un vrai petit cybercriminelâ□¦

Vous trouverez les solutions G-Data chez **GS2i.**