GS2I / G Data : Uroburos, un logiciel espion d'origine russe
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 4/3/2014 11:30:00

GS2i est une sociÃ©tÃ© FranÃ§aise de Service et de Distribution de produits et logiciels informatiques, nous informe que G-Data vient de dÃ©couvrir Uroburos, un logiciel espion d'origine russe, un code malveillant dont le design et le niveau de complexitÃ© laissent Ã penser quâ□□il est probablement lâ□□Å□uvre de services secrets.

Le rootkit appelÃ© Uroburos travaille en autonomie dans les rÃ©seaux infectÃ©s. Selon G Data un tel programme nâ□□est rÃ©alisable quâ□□avec un important investissement humain. Plusieurs dÃ©tails techniques, tels que le nom des fichiers, le cryptage, ou encore le comportement du programme, montrent quâ□□Uroburos provient dâ□□une source russe, la mÃªme que celle ayant menÃ© une cyberattaque contre les USA en 2008 avec le programme Â« Agent.BTZ Â».

Decription d'Uroburos

Uroburos est un rootkit qui comporte deux fichiers, un pilote et un fichier systÃ¨me cryptÃ©. Avec lâ□□aide de ce programme malveillant, le cybercriminel prend le contrÃ´le du PC infectÃ©.

Il exÃ©cute alors nâ□□importe quel programme et dissimule son activitÃ©. Uroburos est en outre capable de voler des donnÃ©es et dâ□□interrompre le trafic de donnÃ©es sur le rÃ©seau.

GrÃ¢ce Ã sa structure modulaire, le cybercriminel peut dÃ©velopper le programme pour dâ□□autres utilitÃ©s. G Data classe ce rootkit dans un haut niveau de dangerositÃ© compte tenu de sa flexibilitÃ© et de sa modularitÃ©.

Une complexitÃ© technique Å□uvre des services secrets

La complexitÃ© et le design dâ□□Uroburos induisent un dÃ©veloppement sophistiquÃ© et coÃ»teux. Selon G Data, ses auteurs ne sont pas des cybercriminels, mais plus probablement des services secrets.
Uroburos est dimensionnÃ© pour les grands rÃ©seaux tels que les administrations et les grandes entreprises.

Le programme malveillant se diffuse de faÃ§on autonome et travaille en mode point Ã point. Les ordinateurs infectÃ©s communiquent ensemble via un rÃ©seau fermÃ©. Le code nâ□□a ainsi besoin que dâ□□un seul ordinateur connectÃ© Ã Internet pour se rÃ©pandre dans le rÃ©seau.

Les documents et autres donnÃ©es prÃ©sents sur les ordinateurs infectÃ©s sont transmis sur des serveurs distants. Uroburos infecte les systÃ¨mes Microsoft 32 bits et 64 bits.

Russie vs Ã□tats unis ?

Des dÃ©tails techniques (le nom des fichiers, le cryptage, le comportement du programme) indiquent que les attaquants ayant ciblÃ© les Ã□tats-Unis en 2008 avec le programme malveillant Â« Agent.BTZ Â» ne sont pas Ã©trangers Ã cette nouvelle attaque.

En effet, Uroburos vÃ©rifie si lâ□□Agent.BTZ est dÃ©jÃ installÃ© sur le systÃ¨me, et dans ce cas ne sâ□□active pas.

Â

Autre indice : les dÃ©veloppeurs des deux programmes malveillants utilisent la langue russe. Le fonctionnement dâ□□Uroburos montre enfin que le particulier nâ□□est pas la cible de lâ□□attaque.

Les efforts investis impliquent des cibles telles que les multinationales, les administrations Ã©tatiques, les services de renseignements, ou dâ□□autres grandes organisations.

Un code actif depuis plus de trois ans

Le rootkit Uroburos est un programme malveillant trÃ¨s avancÃ© et ancien. Le plus ancien pilote dÃ©tectÃ© par lâ□□analyse a Ã©tÃ© compilÃ© en 2011.

Un vecteur dâ□□infection qui reste Ã dÃ©finir

Ã lâheure actuelle, les moyens utilisÃ©s par les attaquants pour infecter leurs cibles avec Uroburos ne sont pas dÃ©finis. De nombreuses mÃ©thodes restent possibles, telles que lâhameÃ§onnage, lâinfection dite Â« Drive-by-download Â» ou encore lâattaque par ingÃ©nierie sociale.

Que signifie Uroburos?

Le programme malveillant a Ã©tÃ© baptisÃ© Â« Uroburos Â» par G Data car ce nom est inscrit Ã plusieurs endroits dans les fichiers de pilote du code malveillant - Urobur()sGotyOu#. Dans la mythologie grecque, Uroburos est le symbole dâun serpent ou un dragon qui se mord la queue.

Lâanalyse complÃ¨te dâUroburos est disponible.

Â