Uroburos, le rootkit russe qui espionne les entreprises

Le gouvernement Russe est-il à l'origine d'une nouvelle attaque, non pas de la Crimée, mais numérique cette fois ? G Data, éditeur allemand de solutions de sécurité, met en avant Uroburos (du nom d'un serpent se mordant la queue dans la mythologie grecque), un rootkit conçu pour viser les grands réseaux, les espionner, et en prendre le contrôle.

D'après G Data, Uroburos est un rootkit, c'est-à-dire un logiciel capable de créer un accès (ou backdoor) au système dans lequel il est implanté, et ce, en totale discrétion. Le rootkit en question se limite à deux fichiers. Le premier est un pilote permettant son fonctionnement sur tout terminal disposant d'un système d'exploitation Microsoft en 32 ou 64 bits, et l'autre est un fichier système chiffré, explique *ITespresso.fr*.

Le code d'Uroburos est considéré comme «*hautement dangereux*» par G Data car il a la particularité de disposer d'une structure modulaire adaptée à distance par les hackers en fonction de leurs besoins. Un rootkit sur mesure selon la cible, en quelque sorte. Et ce ne sont par les particuliers mais bien les réseaux des multinationales, administrations étatiques, et services de renseignement, etc., qui seraient visés.

Depuis 2011

Uroburos, qui fonctionne en point à point, est d'ailleurs capable de se dupliquer en contaminant tous les terminaux en transitant sur le réseau infecté. La méthode d'infection n'est cependant pas détaillée par l'éditeur de solutions de sécurité. Techniques de hameçonnage (phishing) ou de drive by download (infection malware en consultant une page Web) sont évoquées.

D'après G Data, le code de cette cybermenace est bien trop complexe et efficace pour qu'il s'agisse de l'œuvre d'un ou plusieurs hackers indépendants. Le coût d'une telle action indiquerait plutôt un pilotage d'Etat. Les soupçons se portent sur la Russie. Car Uroburos est conçu pour vérifier la présence du programme Agent.BTZ du nom d'une menace associée à une cyberattaque russe à l'encontre des Etats-Unis en 2008 et ne pas s'activer si tel est le cas. Autre indice : les développeurs du rootkit utilisent le Russe, selon G Data. Le plus inquiétant est qu'Uroburos sévirait depuis 2011, en toute discrétion jusqu'à présent.

Crédit image : bloomua – Shutterstock.com

Lire également
5 questions pour mieux comprendre le malware The Mask
La sécurité absorbe 17% des budgets de la DSI
Un ver informatique cible les routeurs Linksys
Le français Snecma fait les frais d'une vulnérabilité d'Internet Explorer