FACUA.org - Internacional - 26 de noviembre de 2014

Descubierto un sofisticado 'malware' que desde 2008 espía a gobiernos y clientes de grandes empresas

La empresa de tecnología de protección informática Symantec Corp. ha descubierto un sofisticado software malicioso conocido como Regin, que ha sido utilizado desde el 2008 para espiar a gobiernos, institutos de investigación, compañías privadas y clientes de grandes empresas.

Se trata de una pieza compleja de software malicioso del tipo *backdoor* cuya estructura muestra un grado de competencia técnica que no es muy común, según explica la compañía en su web. Este programa permite, ente otras cosas, personalizar una amplia gama de capacidades en función del objetivo ya que ofrece a sus controladores un marco de gran alcance para la vigilancia de masas.

Los expertos de la empresa fabricante de los productos antivirus Norton han señalado que es probable que su desarrollo durara meses, e incluso años. Sus capacidades y el nivel de recursos hacen pensar que es una de las principales herramientas de ciberespionaje utilizadas por los propios países.

Este malware estuvo funcionando entre 2008 y 2011, aunque tras ser desactivado volvió a aparecer una nueva versión del mismo programa el pasado año. Los objetivos que persigue este software malicioso incluyen empresas privadas, entidades gubernamentales e institutos de investigación.

Regin es una amenaza de múltiples etapas y cada una está oculta y cifrada, excepto la primera. Cada etapa individual proporciona poca información sobre el paquete completo. Sólo mediante la adquisición de las cinco etapas es posible analizar y comprender la amenaza, han apuntado desde la compañía.

Symantec ha averiguado que *"el malware usa varias características invisibles e incluso cuando su presencia es detectada, es muy difícil determinar qué está haciendo. Muchos componentes de Regin siguen sin ser descubiertos y podrían existir funcionalidades y versiones adicionales"*.

Telecomunicaciones, energía, aerolíneas, hotelería e investigación

La investigación también ha concluido que los objetivos eran más los clientes de compañías, en lugar de las compañías en sí. Cerca de un veintiocho por ciento de los blancos estaban en el sector de telecomunicaciones, mientras que hubo otras víctimas en firmas de energía, aerolíneas, hotelería e investigación.

Casi la mitad de todas las infecciones ocurrieron en direcciones de proveedores de servicios de internet, según el informe difundido por la empresa con sede en Mountain View.

La compañía californiana ha destacado que Rusia y Arabia Saudi representan cerca de la mitad de las infecciones confirmadas de Regin. Otros países afectados por esta amenaza han sido México, Irlanda, India, Irán, Afganistán, Bélgica, Austria y Pakistán.