Personal de F-Secure descubrió tras años de investigación un virus que ataca principalmente a empresas industriales del sector energético, al controlar de manera remota los servidores.

La compañía de seguridad informática expuso que el virus denominado Havex es una herramienta de control remoto genérica (RAT, por sus siglas en inglés).

Este penetra el servidor con un troyano capaz de infectar los sistemas de control industrial de Scada (supervisión, control y adquisición de datos), con capacidad de desactivar presas hidroeléctricas, sobrecargar las centrales nucleares e incluso apagar la red eléctrica de un país con solo pulsar un botón.

Según un comunicado de la firma, los expertos consideran que Havex tiene un específicointerés en sistemas de control industrial y utiliza un innovador enfoque de caballo de troya para comprometer a las víctimas.

El equipo de F-Secure realizó un análisis en el que descubrió que los ciberdelincuentes además de usar los métodos de infección tradicionales, como los “exploits” y correos electrónicos de “spam”, también utilizan uno nuevo eficaz para difundir Havex RAT y llevar a cabo espionaje.

‘Recientemente se ha utilizado para llevar a cabo espionaje industrial contra una serie de empresas en Europa que utilizan o desarrollan programas y maquinaria industrial’, refiere el comunicado.

Este método consiste en hackear los sitios web de compañías de software y buscan aplicaciones legales vulnerables en las que instalan el troyano; el usuario, al aceptar la descarga del archivo denominado mbcheck.dll, realmente está aceptando el virus RAT.

Advierte que una vez instalado el malware, los atacantes usan el servidor de control para el troyano que da instrucciones a los ordenadores infectados de que descarguen y ejecuten otros componentes del software infectado.

La mayoría de las empresas que fueron víctimas de los ataques se encuentran en Europa, aunque también existiría al menos una ubicada en California, añade la empresa de seguridad en línea de Finlandia.

Fuente: yucatan