La NSA y la inteligencia británica 'copiaron' a Kaspersky Lab para saber cómo burlarlo

23/06/2015

La Agencia Nacional de Seguridad (NSA) de EE.UU. y su homólogo británico, el Cuartel General de Comunicaciones del Gobierno (GCHQ), 'copiaron' a Kaspersky Lab a través de ingeniería inversa con el objetivo de evitar la detección de sus actividades por el antivirus ruso.

La agencia NSA estadounidense aunó esfuerzos con el británico GCHQ para aprender a burlar el software ruso de seguridad informática Kaspersky Lab, según ha informado este lunes 'The Intercept' que cita documentos de hace dos años filtrados por el excontratista de la NSA Edward Snowden.

Según la publicación, 23 sistemas de protección contra virus, spam o ataques de 'hackers', entre otras amenazas cibernéticas, fueron copiados de manera ilegal por los expertos de las agencias de EE.UU. y Reino Unido.

La mayoría de las empresas atacadas por la Inteligencia del 'tándem espía' anglosajón fueron productores clave de software en sus Estados, como DrWeb de Rusia, Avast de la Republica Checa o F-Secure de Finlandia. La ingeniería inversa permitía a la NSA y al GCHQ elaborar herramientas más eficaces para infiltrarse en las redes nacionales de información evitando barreras de protección.

"Los productos de seguridad personales como el software antivirus ruso Kaspersky siguen planteando retos para la capacidad de la Red Informática de Explotación del GCHQ. La ingeniería inversa es esencial para la exploración de este software con el objetivo de evitar la detección de nuestras actividades", se dice en una solicitud del GCHQ escrita en 2008. Y añade: "La examinación del Kaspersky y otros productos continúa".

La compañía rusa fundada por Yevgueni Kasperski se ha convertido en "la espina más afilada" para los piratas informáticos al servicio de Estados. En los últimos años, la compañía juega un papel clave en el descubrimiento o el análisis de programas informáticos maliciosos (Gauss, Stuxnet, Regin, Symantec) difundidos por 'hackers' vinculados con el Gobierno de EE.UU.

"Es extremadamente preocupante que las organizaciones gubernamentales apunten contra nosotros, en vez de concentrar los recursos contra adversarios legítimos, trabajando para subvertir el software diseñado para la seguridad de todos", declaró la empresa Kaspersky Lab al 'The Interceptor'. "Sin embargo, esto no es una sorpresa, pues hemos trabajado duro para proteger a nuestros usuarios de todo tipo de adversarios, y esto incluye tanto a los ciberdelincuentes comunes como a las operaciones de ciberespionaje patrocinados por un Estado o una nación", subraya.

La compañía Kaspersky, que garantiza la protección informática a más de 300 millones de usuarios en todo el mundo, insta a agencias como la NSA a trabajar junto con los diseñadores de programas de seguridad cibernética:"Nos gustaría subrayar la necesidad de que todas las empresas de seguridad trabajen como una comunidad y luchen por la privacidad del usuario, el derecho a la privacidad en Internet, para que frustren la vigilancia masiva y conviertan el mundo en un lugar más seguro".

La complicidad de la NSA con piratas cibernéticos

Por su parte el experto Enrique Rosas en declaraciones a RT opinó que uno de los "aspectos claves" de la intervención de las agencias de inteligencia estadounidenses y británicas es contener la operación de las empresas que se encuentran fuera del ámbito de su control territorial, en particular las que están basadas en Rusia.

Según Rosas, Kaspersky Lab tiene millones de usuarios en todo el mundo, y muchos de ellos son corporaciones, por lo que vulnerar sus sistemas de seguridad es obtener acceso privilegiado a los archivos de esas compañías.

Espionaje de enormes proporciones a Rusia e Irán

Por otro lado, a principios de año el gigante ruso de seguridad informática identificó a la organización de 'hackers' Equation Group, que atacó las estructuras gubernamentales, militares y comerciales de Rusia, Irán y otra treintena de países. Sus ataques también fueron coordinados principalmente desde EE.UU. y Reino Unido. Los expertos de Kaspersky Lab señalaron que "lo descubierto supera todos los ataques maliciosos hasta ahora conocidos".

Como si fuera poco, la empresa de seguridad informática aseguró que este cibergrupo secreto no podría existir sin

la ayuda de grandes recursos suministrados por un Estado. Al mismo tiempo, los expertos informáticos encontraron pistas de la vinculación de Equation Group con la NSA.

'El robo del siglo'

Kaspersky Lab también reveló el mayor robo bancario del siglo, en el que se sustrajo la exorbitante suma de un billón de dólares gracias a un masivo ataque informático a un centenar de instituciones financieras repartidas en varios países.

La compañía desveló a RT cómo se realizó este gran robo bancario utilizando correos electrónicos falsos de auténticas instituciones financieras. Posteriormente, varios medios sofisticados permitieron a los 'hackers' entender cómo trabajan los empleados de los bancos con los programas internos de los mismos para después pasar datos de un ordenador a otro y, finalmente, obtener pleno acceso a todo el sistema de un banco.

"Los métodos de ataque son de un interés especial. Representan una tendencia nueva y preocupante en el mercado del crimen cibernético, donde los ataques son cada vez más sofisticados", indicó Kaspersky.

Espionaje masivo a México y otros países

Además, el mundialmente reconocido fabricante de antivirus destapó el escándalo de espionaje que el Gobierno estadounidense llevaba realizando a México durante los últimos 19 años. El seguimiento se realizaba a través de computadoras con un 'software' espía militar de la Agencia de Seguridad Nacional instalado en el disco duro de las principales marcadas vendidas a instituciones gubernamentales, empresas de telecomunicaciones, centros científicos, entre otros, del país latinoamericano y de otras decenas de naciones más.

La NSA considera a México como un blanco importante, por ser una de las economías que más crece en el mundo, del que deseaba poseer información valiosa sobre sus futuros proyectos de infraestructura, concluyó en un informe la empresa rusa de seguridad informática.