TENDENCIAS

Así pueden los ‘hackers’ apagarte la luz o desviar un bus

El Ciudadano · 19 de abril de 2017

De la mano del desarrollo tecnológico han venido también crecientes peligros digitales. Ahora los ‘hackers’ pueden apoderarse no solo de computadoras sino también del control infraestructuras enteras y hasta privarle de la luz y el transporte. ¿Pero cómo?

Así pueden los 'hackers' apagarle la luz o desviarle su autobús

pexels.com / RT

Síguenos en Facebook

El mundo sigue desarrollando nuevas tecnologías y **junto a las nuevas oportunidades que se abren también aumenta el número de potenciales vulnerabilidades**. Los 'hackeos' actuales pueden estar dirigidos no solo a un computador sino también a infraestructuras enteras.

Desde los años 1980 libros y películas de ciencia ficción nos alertan sobre las amenazas relacionadas con la computarización. Este proceso abre nuevas oportunidades para realizar ataques cibernéticos. Al tiempo que aumenta el número de ámbitos e instalaciones donde se aplican nuevas herramientas se abren puertas nuevas para los 'hackers'.

Actualmente muchas instalaciones industriales utilizan la herramienta llamada SCADA (Supervisión, Control y Adquisición de Datos): un sistema que utiliza las tecnologías de comunicación para automatizar los procesos de monitoreo y control de las obras que se realizan dentro de la instalación.

A pesar de su utilidad, el sistema muestra **una serie de vulnerabilidades críticas**: según la investigación de un equipo de científicos del Departamento de Lenguajes y Ciencias de la Computación de la Universidad de Málaga (España), la conexión del SCADA con otros sistemas lo hace más vulnerable frente a ataques, hecho que genera nuevos problemas de seguridad.

Asimismo, los científicos aseguran que **los ataques tanto internos como externos pueden ser realizados contra cualquier parte del sistema**. En el primer caso se trata de errores cometidos por los operadores del sistema y en el segundo de 'hackeos'. Según recuerdan, la base de datos CERT ha identificado unas 2.500 vulnerabilidades.

El acceso remoto al SCADA permitió a unos 'hackers' realizar un ataque contra Ucrania que provocó un corte de electricidad en toda la región de Ivano-Frankivsk en diciembre de 2015, señala el portal Wired.

Los 'hackers' también pueden causar un apagón total de un distrito entero, alerta Vasilios Hioureas, experto de la compañía de seguridad informática Kaspersky Lab, y Thomas Kinsey, de la empresa Exigent Systems. Y el método es similar a lo que nos muestran los videojuegos Watch Dogs: **un ataque de estas características podría ser realizado a través de un aparato de aire acondicionado**.

Los especialistas matizan que las instalaciones regionales de electricidad emiten señales de por la radiofrecuencia que se amplifican a través de repetidores instalados en distintas zonas de la ciudad para apagar los acondicionadores de aire.

Pero los sistemas que Hioureas y Kinsey han analizado no usan ningún tipo de protección, hecho que tiene como resultado que «cualquier persona con 50 dólares puede generar una señal que puede sobrepasar a un repetidor; y cualquiera con 150 dólares podría generarla a través de un amplificador y presuntamente afectar a un distrito entero».

El acceso remoto hace vulnerables no solo grandes instalaciones sino dispositivos mucho más pequeños. Por ejemplo, bombillas inteligentes que pueden manejarse desde el móvil, dispositivo con el que soñaría el agente 007, protagonista de los libros de Ian Fleming que recurría a una gran variedad de artefactos futuristas en sus aventuras.

El experto de la Universidad Dalhousie (Canadá) Colin O'Flynn

y otros compañeros investigadores israelíes han llevado a cabo una investigación que mostró que las bombillas inteligentes LED manifiestan vulnerabilidades frente a posibles infiltraciones. O lo que es lo mismo, el control de la iluminación de una habitación normal podría caer en manos de los 'hackers', advierte CBC News.

O'Flynn y sus colegas aseguran que **es posible programar una bombilla de tal manera que le permita apagar otras que estén situadas en áreas cercanas** y el virus puede tener un alcance de entre 30 y 400 metros.

Los expertos también aseguran que una fuente de la vulnerabilidad de varios dispositivos reside en el concepto llamado 'Internet de las cosas', o sea la interconexión digital de varios objetos cotidianos, por ejemplo cámaras de seguridad o termostatos. «Es posible que a través de una bombilla inteligente se pueda obtener acceso a un termostato Wi-Fi, y a través de este a alguna otra red», concluye O'Flynn.

Varios sistemas de transporte también manifiestan vulnerabilidades frente a los 'hackeos'. Según Serguéi Gordéichik y Aleksandr Timorin, miembros del grupo de investigadores de la seguridad cibernética SCADA StrangeLove, resulta «completamente fácil» 'hackear' la infraestructura ferroviaria.

Además, aseguran que el uso de computadores en lugar de los sistemas de control manual puede provocar que, por ejemplo, un tren sea 'hackeado' y descarrile o colisione con otro.

De hecho, ya se ha perpetrado un ataque cibernético contra el sistema de ferrocarriles ligeros de San Francisco (EE.UU.). El incidente se produjo el noviembre pasado, cuando **se interrumpió el funcionamiento del sistema interno de computadores de la Agencia Municipal de transporte** de la ciudad y en las pantallas de las máquinas expendedoras de los pasajes apareció el mensaje «fuera de servicio», recuerda el diario 'USA Today'.

Los autores de aquel ataque pidieron un rescate, «un método muy oportunista y motivador de ataques», según Kevin Albano, miembro del equipo de especialistas en seguridad IBM X-Force. «Una vez infectado su blanco, los 'hackers' pueden ajustar el precio si captan en su red un blanco que valga más», añade.

Uno de los más destacados casos de uso de herramientas para 'hackeos' se produjo en Irán, cuando el desarrollo del programa nuclear fue postergado por un ataque sufrido con el 'gusano' Stuxnet. Según estima el diario 'The New York Times', este virus afectó casi a a una quinta parte de todos los centrifugadores nucleares iraníes.

El mismo medio describe el Stuxnet como «el arma cibernética más sofisticada» y explica su funcionamiento: un elemento del virus **garantizó la pérdida de control de los centrifugadores mientras el segundo mostró a los operadores del sistema señales normales**, como si todo funcionara sin problema alguno. Otra vez, se trata de algo que solo habíamos vimos en las películas sobre espías.

Pexels.com

No obstante, el experto independiente en seguridad informática y una de las primeras personas que lograron descodificar Stuxnet, Ralph Langner, aseguró al periódico estadounidense que «cualquier persona que mire [el 'gusano'] detenidamente puede construir algo semejante». El mismo especialista opina que el uso de ese virus dio comienzo a una nueva forma de guerra industrial.

La empresa especializada en seguridad Checkpoint ha creado una lista con **los mayores objetivos para los 'hackers' en 2017** en la que se incluyen dispositivos móviles, el 'Internet de las cosas' y el modelo de uso de los equipos informáticos conocido como 'la nube', recuerda el portal OneMagazine.

La conclusión es que no existe ningún método que prevenga todo tipo de ataques cibernéticos a todos estos sistemas.

vía: RT

Fuente: El Ciudadano