Centrales eléctricas, hidráulicas, oleoductos, gasoductos y todo tipo deinfraestructuras energéticas están en el punto de mira de los hackers. Así ha quedado expuesto en las últimas ediciones de BlackHat y Def Con, las dos conferencias de ciberseguridad que han tenido lugar esta semana pasada en Las Vegas (EEUU).

En estas conferencias, las empresas -e incluso gobiernos- se ponen al día de novedades en ciberseguridad y actualizan sus sistemas de defensa gracias a la colaboración de investigadores informáticos -o 'white hackers'- que dan a conocer los últimos errores y vulnerabilidades en el sector.

Hasta ahora los objetivos más conocidos de los piratas de la Red eran teléfonos móviles y ordenadores pero, según se extrae de las dos conferencias, los hackers han ampliado su punto de mira y ya apuntan a nuevos blancos como coches controlados por control remoto, hogares inteligentes o, lo más preocupante, centrales energéticas.

Muchas de estas instalaciones se encuentran en lugares recónditos -especialmente los oleoductos- y se controlan a distancia mediante ordenadores conectados a redes con protocolos poco seguros. Su vulnerabilidad se debe a que las instalaciones «son arcaicas y fueron construidas cuando la seguridad no era una prioridad», tal y como ha declarado el investigador de la compañía de seguridad Trend Micro, Kyle Wilhoit, en la BlackHat 2013.

Ataque desde China

El investigador ha ido más allá en su discurso y, en un acto de la citada conferencia, ha revelado cómo una central hidráulica de Estados Unidos fue atacada por un grupo de hackers de origen chino que querían acceder al sistema de control de la planta. La ofensiva fue detectada en diciembre de 2012 cuando se localizó un archivo Word que escondía un archivo malicioso que quería acceder al sistema de seguridad de la planta.

Wilhoit empleó un sistema de detección de ataques denominado BeEF(Browser Exploitation Framework) que le permitió localizar el origen del ataque en China. Las características del ataque son similares al modus operandi del grupo APT1 que, según la empresa de

seguridad Mandiant, opera para el ejército chino, tal y como recoge la MIT Technologic Review.

A su vez, entre marzo y junio de este año, el investigador ha detectado un total de 74 ataques a distintas centrales repartidas por el mundo. Estas ofensivas provenían de 16 países distintos y las más potentes eran de China. «Estos ataques están ocurriendo y los ingenieros probablemente no lo saben», ha sentenciado Wilhoit a la misma fuente.

Otros objetivos: coches inteligentes

En la misma conferencia se ha expuesto el peligro que corren los coches controlados por control remoto o los polémicos drones -aviones sin piloto usados en conflictos bélicos-. En esencia, se controlan mediante ordenador y cualquiera puede acceder a su sistema para controlar volante, frenos, velocidad, bocina, indicadores… y provocar un accidente.

Un ejemplo claro es la prueba a la que se ha sometido el periodista de Forbes Andy Greenberg, que fue víctima de un hackeo voluntario al volante de un coche inteligente. Al finalizar el vídeo, el periodista declaró: «El instinto me estaba diciendo que saltara por la ventana».

Fuente: elmundo.es