Irán sufre un ataque informático contra sus instalaciones nucleares

El potente virus Stuxnet afecta ya a unos 30.000 ordenadores en el país

ÁNGELES ESPINOSA - Teherán - 28/09/2010

Irán asegura que sus instalaciones nucleares están a salvo, pero ha reconocido que Stuxnet ha afectado al menos 30.000 ordenadores dentro de su territorio y continúa propagándose. Aunque el nombre suene a videojuego, se trata de algo mucho más peligroso: el primer *gusano* informático que ataca plantas industriales.

Irán asegura que sus instalaciones nucleares están a salvo, pero ha reconocido que Stuxnet ha afectado al menos 30.000 ordenadores dentro de su territorio y continúa propagándose. Aunque el nombre suene a videojuego, se trata de algo mucho más peligroso: el primer *gusano* informático que ataca plantas industriales. Y haciendo realidad lo que hasta ahora pertenecía al mundo de la ciencia-ficción, algunos expertos advierten de su capacidad para hacer estallar la instalación infectada. "Es parte de la ciberguerra de Occidente contra Irán", ha denunciado Mahmud Liayí, un alto cargo del Ministerio de Industria.

"Los ataques continúan y se están propagando nuevas versiones de ese *gusano",* informó ayer Hamid Alipour, director adjunto de IRITCo, uno de los principales proveedores de Internet de Irán, citado por la agencia Irna. Stuxnet salió a la luz el pasado junio cuando una compañía de seguridad informática de Bielorrusia, VirusBlokAda, lo descubrió en unos ordenadores pertenecientes a un cliente en Irán. Entonces los expertos creyeron que se trataba de un programa malicioso diseñado para robar procesos de fabricación o bocetos de productos. Sin embargo, desde que la semana pasada se conocieron nuevos detalles sobre su estructura y sus capacidades, la posibilidad de que hubiera sido creado para sabotear el programa nuclear iraní ha extendido el interés fuera de los circuitos especializados.

"Habíamos previsto eliminarlo en dos meses, pero no es estable y desde que comenzamos las operaciones de limpieza han aparecido tres nuevas versiones", añadió Alipour. Sus palabras indican que, a pesar de las declaraciones de otros responsables iraníes asegurando que Stuxnet no ha causado daños graves a los sistemas industriales de su país, el *gusano* aún no está bajo control y sigue produciendo quebraderos de cabeza.

El vicepresidente de la Organización de la Energía Atómica encargado de asuntos de seguridad, Asghar Zarean, afirmó el domingo que el *gusano* no había alcanzado ninguna de las plantas nucleares ni su *software*. Sin embargo, el jefe de la central atómica de Bushehr, Mahmud Jafarí, admitió que estaban tratando de eliminarlo de "varios ordenadores de empleados". Serían algunos de los al menos 30.000 contaminados que reconoció Liayí, el secretario del Consejo de Tecnología de la Información en el Ministerio de Industria, para quien estamos ante un caso de ciberguerra.

No es paranoia. Por un lado, Irán es el país que más ataques ha sufrido (un 60% del total). Por otro, la complejidad del programa es tal que los especialistas en seguridad informática que lo han examinado están convencidos de que no puede ser obra de un mero pirata informático. La mayoría opina que hay un Estado detrás y que es el primer ejemplo de guerra cibernética. Algunos analistas han apuntado a EE UU e Israel como posibles implicados en un proyecto de esa envergadura.

Además, el diario *The New York Times* reveló el año pasado que el presidente George W. Bush había autorizado durante su mandato -concluyó en enero de 2009- nuevos esfuerzos, incluidos algunos de carácter experimental, para dañar los sistemas eléctricos, informáticos y otras redes del programa nuclear iraní. Estados Unidos y sus aliados sospechan que ese programa persigue objetivos militares. Teherán, que rechaza las acusaciones, persiste en su empeño.

Según los especialistas, Stuxnet se dirige a un programa concreto de la marca Siemens que se utiliza en el control de oleoductos, plataformas petroleras, centrales eléctricas y otras instalaciones industriales, con el objetivo de sabotearlos. Eso ha llevado a especular que una vez dentro de una planta, por ejemplo Natanz, podría reprogramar las centrifugadoras para hacerlas fallar sin que se detectara. El último informe de los inspectores de la ONU, el pasado septiembre, refleja un nuevo descenso en esos aparatos operativos de 4.592 a 3.772. Los inspectores no aclaran, sin embargo, si esa tendencia, que se prolonga desde el año pasado, se debe a las sanciones internacionales, el pobre diseño de las máquinas o el sabotaje.

Ralph Langner, un investigador alemán de seguridad informática citado en la revista digital *Wired,* va más allá en su *blog* (http://www.langner.com/en/index.htm) y califica Stuxnet de "un arma de un solo tiro". En su opinión, tras los procesos que desencadena ese *gusano* se puede "esperar que algo estalle" y especula con la posibilidad de que el ataque ya se haya producido.