Pánico en EEUU ¿Quién hackeó la NSA?

DAVID BOLLERO :: 22/08/2016

Que se haya hackeado la NSA no es nuevo, que se sepa, sí. Con este tuit, Edward Snowden abría el camino a una serie de reflexiones en esta red social sobre un hackeo de la agencia de espionaje estadounidense por parte de un grupo bautizado como Shadow Brokers (nombre extraído del video juego Mass Effect).

El ataque en concreto se habría dirigido contra una sección de la NSA llamada Equation Group que, en opinión de expertos en seguridad como el fabricante Kaspersky, es la responsable del malware Stuxnet –que tumbó las centrifugadoras de uranio de Irán- o Flame. Lo curioso de esta acción es que, en realidad, se ejecutó en 2013 y no ha sido hasta esta semana cuando se ha hecho público a través de twitter y tumblr.

Al parecer, Shadow Brokers habría conseguido hacerse con una serie de ficheros, de muestras de código con las que la NSA desarrolla malware para romper la seguridad de otros países como Rusia, China o Irán… y tendría intención de subastarlos al mejor postor por un millón de bitcoins (alrededor de 550 millones de euros). Casi al mismo tiempo, WikiLeaks anunciaría que en breve publicará también archivos varios de este agencia de seguridad.

Entre los ficheros que ha adelantado Shadow Brokers -alrededor de un 40% del total- se ofrecerían detalles de cómo romper la seguridad de los cortafuegos de fabricantes como Fortinet, Cisco, Juniper o TopSec… algo así como un toolkit anti-firewalls. La página oficial en las que volcó este adelanto ya no está disponible, pero los ficheros campan a sus anchas clonados por toda la Red.

Mientras algunos apuntan a que la autoría de los ataques proviene del propio Snowden, él es más partidario de mirar hacia Rusia. En esa línea, cuando en 2013 Snowden pasó a ser un prófugo de la justicia de EEUU, la NSA movió de servidores todo el código al que su ex empleado hubiera podido tener acceso, incluso, dejando fuera de servicio esas máquinas. ¿Qué pasó? Aún no se sabe con certeza, aunque para calmar las aguas hay analistas que señalan que más que la NSA haya sido hackeada, la información procedería de un sistema comprometido que contendría esta brecha.

Sea como fuere, la brecha de seguridad, a las puertas de las Presidenciales de noviembre, ha extendido la intranquilidad en la Administración estadounidense. Esta brecha podría ser un recado según el propio Snowden: alguien tiene pruebas para demostrar la responsabilidad de EEUU detrás de los ataques cometidos empleando este malware.

kaostica

---

https://www.lahaine.org/mm_ss_mundo.php/panico-en-eeuu-iquien-hackeo