



Snowden afirma que la NSA hackeó al mayor fabricante de tarjetas SIM del mundo

Masterhacks - Después de todas las revelaciones del antiguo miembro de la NSA, Edward Snowden, acerca de los programas que intentarían atentar contra la privacidad de las personas, sale a la luz una nueva revelación bastante impactante, pues según lo revela The Intercept, la NSA y sus aliados hackearon a Gemalto, el mayor fabricante de tarjetas SIM del mundo.

Este ataque se llevó a cabo en 2010 con el despliegue del equipo Mobile Handset Exploitation Team, con miembros de la NSA y su equivalente británico, el Cuartel de Comunicaciones del Gobierno.

Aunque el nombre de Gemalto no resulte tan conocido, basta con decir que es una copañía situada en Amsterdam que fabrica tarjetas SIM para más de 450 proveedores de telecomunicaciones en todo el mundo, por lo que se habla de un hackeo de tarjetas SIM a nivel global, siendo una gran infracción contra la privacidad de los usuarios.

Según el documento que se filtró, las llaves de encriptación robadas en el hackeo de las tarjetas SIM permite a las agencias de inteligencia monitorizar las comunicaciones vía móvil sin necesidad de contar con los permisos de los proveedores de telecomunicaciones, todo esto sin dejar rastro.

Cabe mencionar que no fue hasta que The Intercept dio a conocer el documento, Gemalto comenzó a investigar acerca del ataque, puesto que no tenían conocimiento sobre ello, y hasta ahora, no han podido encontrar ningún rastro del ataque.

Por si fuera poco, el documento también expresa que las agencias de inteligencia tuvieron acceso a cuentas de correo y de Facebook de proveedores de telecomunicaciones y fabricantes de tarjetas SIm para encontrar a personas con acceso a los servidores centrales de Gemalto y poder conseguir las llaves de encriptación, por lo que se suma otro delito más.

Se trata de una maniobra más que pone en duda la confiabilidad a las agencias de inteligencia del gobierno, que ellos mismos afirman, garantizar la seguridad a los ciudadanos, aunque esto lleve a atentar contra su propia privacidad.