El CNI investiga ataques informáticos del Ejército chino a militares españoles. Han utilizado 'archivos señuelo' similares a los detectados en Estados Unidos

21 de febrero del 2013 EL CONFIDENCIAL DIGITAL

Algunos organismos sensibles del Estado, sobretodo altos estamentos militares, han sufrido ataques similares a los que se han detectado en Estados Unidos y cuya presunta autoría se ha centrado en el Ejército chino. Expertos del CCN reconocen las mismas técnicas en 'asaltos' registrados en España.

El Confidencial Digital informaba el pasado mes de diciembre del **aumento de ataques** a altos funcionarios del Estado **registrados en 2012**. Un año en el que el **Centro Criptológico Nacional,** encargado de la seguridad del Estado ante el ciberespionaje, detectó un centenar de asaltos e **intrusiones "críticas**" en los sistemas informáticos de **Zarzuela**, **La Moncloa** o en **Defensa** y otros ámbitos militares.

Las **investigaciones** de algunos de estos ataques, según ha sabido ***ECD***, **apuntan a China**. Tal y como explican las fuentes consultadas "las intrusiones detectadas en ámbitos militares y diplomáticos **comparten muchas características** con los que se describen en el informe que se acaba de publicar en Estados Unidos".

Hacen referencia a las conclusiones de una investigación realizada por la empresa de ciberseguridad **Mandiant**, determinando que ciertas infraestructuras informáticas sensibles de Estados Unidos **lleva años siendo atacadas por IPs –**identidad digital**-** pertenecientes a una **unidad**

especial del Ejército chino denominada 61398, localizada en un edificio público de Pekín. El Gobierno de China niega cualquier implicación.

Los mismos archivos

Los ataques se producían a través de **'troyanos'** y **'spyware'**, herramientas que infectan un ordenador o un teléfono Smartphone y que otorgan su control al pirata informático, **posibilitando el robo de archivos.** Se suelen trasferir a través de archivos adjuntos en correos electrónicos.

Tanto en los casos registrados en Estados Unidos como en algunos que se investigan en España, los **nombres de los archivos del informe coinciden** con los hallados en ataques a militares y diplomáticos españoles.

Son habitualmente archivos con cierto '**gancho' para militares** y diplomáticos, como '**North Korea Launch'** (Lanzamiento de Corea del Norte), '**China Sea Security'** (seguridad marítima china) o **'ChinaUSAviationSymposium'**(simposio sobre la aviación china y estadounidense) o '**CloseCombatManual'** (Manual de Combate Cercano). Todos llegaban con la apariencia de informe o documento gráfico de actualidad.

Saltaba la protección antivirus

En ocasiones, tal y como explican las fuentes de la seguridad del Estado consultadas, el antivirus del ordenador conseguía detectar el ataque, pero poco a poco "se iban mejorando los sistemas de camuflaje y el **virus era capaz de saltarse la protección**" aseguran.

Algunos de los ataques fueron descubiertos en **fase de infección**, por lo que se investiga **cuánta información** y **de qué tipo** pudo ser sustraída.