AMENAZAS

El top 10 de las ciberamenazas

5 de abril, 2014

Sólo en España, **INTECO**, organismo del **Ministerio de Industria, Energía y Turismo**, registró más de 54.000 ciberataques en 2013; mientras que el **CCN-CERT, del Centro Criptológico Nacional** (organismo adherido al Centro Nacional de Inteligencia) gestionó 7.260 ciberincidentes contra los sistemas de las Administraciones Públicas, empresas y organizaciones de interés estratégico nacional (energéticas, financieras, de seguridad y defensa, telecomunicaciones etc.).

Estos datos ponen de manifiesto que la ciberseguridad se ha erigido como uno de los aspectos más críticos a tener en cuenta por cualquier organización.

Entelgy, a través de **InnoTec**, empresa especializada en seguridad de la información del Grupo, ha analizado algunas de las ciberamenazas más destacadas del año 2013:

1. **Ciberespionaje industrial**: robo de información a empresas con el fin de acceder a su información más valiosa (propiedad intelectual, desarrollos tecnológicos, estrategias de actuación, bases de datos de clientes, etc.). Por ejemplo, el informe Mandiant descubrió la existencia del grupo organizado APT1 dedicado al ciberespionaje de industrias de habla inglesa claves para la economía de sus respectivos países.
2. **Ciberespionaje gubernamental**: robo de información a organismos gubernamentales como la operación “Octubre Rojo” en la que se infiltraron en las redes de comunicaciones diplomáticas, gubernamentales, de investigación científica y compañías petroquímicas de alrededor de 40 países. El objetivo era obtener información sensible y credenciales de acceso a ordenadores, dispositivos móviles y equipos de red.
3. **Ciberataques a infraestructuras críticas**, como el detectado contra Aramco, la principal compañía petrolera de Arabia Saudí, que se vio sacudida por un troyano instalado en más de 30.000 ordenadores de su red. La compañía necesitó diez días para volver a la normalidad.
4. **Cibermercenarios o grupos de hackers** con conocimientos avanzados, contratados para desarrollar ataques dirigidos contra un objetivo concreto, con el objetivo de conseguir la información deseada.
5. **Ciberdelincuencia contra servicios financieros**, y muy especialmente, los denominados troyanos bancarios, diseñados para el robo de datos de tarjetas de crédito y cada vez más, centrados en los dispositivos móviles. Por ejemplo, en la “Operación High Roller” se vieron afectadas 60 entidades financieras de todo el mundo, víctimas de un ciberataque en el que se extrajeron 60 millones de euros. El grado de sofisticación del malware indica que fue obra del crimen organizado porque la configuración del ataque requirió inversión para el desarrollo, muchas horas de trabajo y una logística muy importante.
6. **Ciberdelincuentes aislados** que venden la información obtenida al mejor postor. Un ejemplo muy sonado fue el de la cadena estadounidense de grandes almacenes Target que reconoció el robo de información de tarjetas de crédito de alrededor de 70 millones de clientes. Pocos días después, estas tarjetas estaban siendo vendidas en el mercado negro para ser clonadas y realizar compras con ellas.
7. **Ciberdelincuentes organizados o mafias** que han trasladado al mundo “virtual” sus acciones en el mundo “real”. Fraude online, clonación de tarjetas de crédito, extorsión, blanqueo de capitales, etc.
8. Infección a través de páginas web. En 2013 se detuvo al autor de Blackole, un exploit-kit (paquete que contiene programas maliciosos) que permitía explotar vulnerabilidades de webs legítimas e infectar a los usuarios que accedían a dichas páginas, millones en todo el mundo.
9. **Ciberhacktivistas**: personas o grupos que, movidos por alguna ideología, intentan socavar la estructura del oponente. El ejemplo de Anonymous es paradigmático y, en estos casos, sus ataques suelen centrarse en ataques DDoS, desfiguración de páginas web o publicación de datos comprometidos.
10. **Cibersabotaje** que busca dañar la reputación de una organización y por ende su funcionamiento. Prueba de ello es la actividad del Ejército Electrónico Sirio, que lleva meses atacando a todos aquellos que, en su opinión, propagan el odio y quieren desestabilizar la seguridad en Siria, incluidas grandes empresas periodísticas de todo el mundo. Llegaron a provocar incluso una caída de 150 puntos en el Dow Jones Industrial Average (índice bursátil de las 30 mayores empresas de la Bolsa de Estados Unidos), ante una noticia falsa de un atentado en la Casa Blanca difundido por Associated Press en Twitter.

Las ciberamenazas se han convertido en las grandes protagonistas del siglo XXI, en parte agravado por circunstancias como la dependencia de la sociedad hacia las TIC, la rentabilidad que ofrece su explotación, la facilidad y el bajo coste de las herramientas utilizadas y el reducido riesgo para el atacante.

Los ataques en la red son cada vez más graves y sus consecuencias cada vez más costosas. Las organizaciones, públicas o privadas, deben ser conscientes de cuál es la información crítica para su negocio con el objetivo de protegerla. Teniendo en cuenta, no sólo dónde se aloja dicha información, sino también, cada vez más, el modo de acceder a ella desde distintos dispositivos (PC, portátiles, Smartphone, tabletas, USB, etc.) y con diferentes herramientas (correo electrónico, servicios web, Intranet corporativa, redes sociales, etc.).

ciberamenazas ciberatacantes INTECO

ANTERIOR POST
El fin del soporte de Windows XP podría impulsar el mercado de los exploits zero Day