Converged Day 2014
La convergencia está aquí.
Ahora es el momento.
IDG tv es

CIBERCRIMEN | NOTICIAS | 03 ABR 2014

Las 10 ciberamenazas más destacadas de 2013

Tags: Seguridad Espionaje Ciberseguridad

También te puede interesar:

- Trend Micro muestra cómo hacer frente al nuevo entorno de ciberamenazas
- El phishing encabeza la lista de ciberamenazas financieras contra los consumidores
- Las PYMES necesitan ayuda para comprender mejor las ciberamenazas
- Estados Unidos y Rusia firman un acuerdo para luchar contra las ciberamenazas

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. El ciberespionaje industrial encabeza la lista de las amenazas de 2013.

Según Entelgy, éstas son las 10 amenazas más importantes que han sacudido 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.

Eventos IDGtv

Webinars Webinar

Ver más

Movilidad Empresarial

HP EliteBook 840 G1, ultrabook de altas prestaciones para profesionales móviles

Seguridad, rendimiento y productividad son las principales características del EliteBook 840 G1, el ultrabook de HP pensado para los profesionales

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.

Imprimir ▲Subir

Compartir

Compartir 1 Compartir 10

Te recomendamos

El 23% de las empresas no cuentan con ningún plan de mitigación de DDoS

Los routers de consumo seguirán siendo una gran amenaza, aseguran los expertos

ITU impulsa la ciberseguridad

Microsoft Internet Explorer 12 soportará el protocolo de cifrado HSTS

Un 70% de las empresas españolas incumple la LOPD

recomendado por

COMENTAR

Para comentar, es necesario iniciar sesión

Login con o Crea una nueva cuenta

Se muestran 0 comentarios

Actualizar mensajes

Sin comentarios

móviles que necesitan de un ordenador portátil con altas prestaciones.

Impresión Profesional

"HP entrará en la impresión 3D con tecnología propia" Xavier Regué, HP

HP ha confirmado que tiene grandes planes en lo que respecta a la comercialización de impresoras 3D. Fue Meg Whitman, quién confirmó la intención de HP de apostar por el mercado de impresión 3D y Xavier Regué, director de categoría de impresión en HP Iberia, analiza la decisión de la firma.

ENLACE

Mejor Antivirus del 2014

Lo más visto

- Detectan un malware Android enmascarado como una app de seguridad
- ENISA explica cómo implementar informes de incidentes de seguridad en cloud
- Facebook se llena de scam
- El aumento de las amenazas choca con la falta de profesionales de seguridad TI
- Juniper garantiza la seguridad en clouds públicas y privadas con Firefly Suite
- Diego Navarrete, nuevo CEO de Panda Security
- El cibercrimen, principal amenaza para las grandes empresas
- Palo Alto refuerza su plataforma de seguridad frente a los ataques avanzados
- El nuevo smartphone Blackphone garantiza la seguridad y la privacidad
- WhatsApp, cada vez más utilizado para ataques
- Oracle lanza 144 parches de seguridad, 36 de ellos para Java
- Nueva campaña de malware en Facebook con WhatsApp como gancho

Laboratorio IDG