2015-03-17

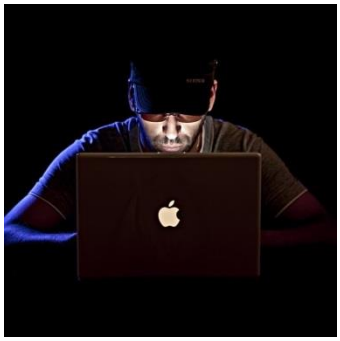
# CiberNoticias # 27


**SCProgress**

www.scprogress.com

## ÍNDICE

## Noticia # 01: La ciberseguridad, uno de los mayores retos en los próximos 10 años.



Este 14 de febrero saltaba la noticia de que una banda de piratas informáticos ha robado entre 300 y 900 millones de dólares de más de un centenar de bancos e instituciones financieras de más de 30 países del mundo. Podría tratarse de uno de los mayores robos bancarios jamás perpetrados, una especie del 'robo del siglo'.

La ciberseguridad se está convirtiendo en una prioridad de seguridad nacional para muchos países y un tema cada vez más importante en muchos foros internacionales. Así lo asegura la diplomático Alicia Moral Revilla (Valladolid, 1963), que fue nombrada embajadora en Misión Especial para la Ciberseguridad el pasado mes de octubre, en una vídeo-entrevista publicada en la web del Ministerio de Asuntos Exteriores y Cooperación.

Alicia Moral advierte de que, según muchos expertos, las amenazas y riesgos en el ciberespacio van a constituir uno de los mayores retos para la seguridad internacional en los próximos 10 años. "Estamos hablando de cibercrimen, delitos cometidos en la red: las extorsiones, las estafas, la pornografía infantil", puntualiza la embajadora especial.

**TERRORISMO EN LA RED**

Entre los delitos susceptibles de cometerse por internet figura el terrorismo. Moral explica que los grupos terroristas utilizan internet "tanto como herramienta para financiarse y captar adeptos como para cometer atentados contra por ejemplo infraestructuras críticas de un país". Y añade dos conceptos relacionados con los delitos a través de la web: "Hablamos de ciberespionaje, hablamos de ciberguerra (la capacidad de unos Estados de atacar a otros en el ciberesespacio)".

En este sentido, Moral Revilla afirma que la cooperación internacional es "fundamental". Cita como ejemplos de ciberataques el caso de Estonia en 2007, cuando el país sufrió "un ataque muy serio que lo paralizó; aunque las causas no fueron del todo claras hubo un riesgo para la seguridad internacional". Más reciente fue el hackeo a la compañía Sony Pictures en diciembre de 2014, atribuido a Corea del Norte por el estreno en EEUU de la película 'The interview'.

**COOPERACIÓN INTERNACIONAL**

"Está siendo un problema importantísimo en la agenda de muchos organismos internacionales", afirma la embajadora especial. Entre estos incluye la UE, la OSCE, la OTAN, el Consejo de Europa y la ONU. Moral afirma que España participa "activamente" en todos estos foros y promueve la cooperación internacional. También defiende la visión española de internet como un "ciberespacio abierto, libre y seguro".

La diplomático declara que aunque las tecnologías de la información y la comunicación (TIC) "sin duda" están contribuyendo al crecimiento y a la prosperidad económica, un ciberespacio abierto y sin fronteras también puede ser usado de forma "maliciosa". Esto, apunta, supone un riesgo no solo para la seguridad de los países, sino también para la economía, para las empresas y para los ciudadanos.

La embajadora para la Ciberseguridad asegura que España también está sufriendo muchos ataques "de diversa envergadura y de diversa índole". Y añade que nuestro país también "está haciendo un gran esfuezo para dotarse de capacidades institucionales y capacidades operativas". Señala que "contamos con un consejo nacional de ciberseguridad, en el que están representados todos los ministerios y organismos con competencias en este tema".

**ESTRATEGIA NACIONAL**

Además, indica que España cuenta desde 2013 con una estrategia nacional de ciberseguridad. Esta está disponible en la página web de La Moncloa. El documento se divide en 5 capítulos: El ciberespacio y su seguridad; Propósito y principios rectores de la ciberseguridad en España; Objetivos de la ciberseguridad; Líneas de acción de la ciberseguridad nacional; y la ciberseguridad en el Sistema de Seguridad Nacional.

El dossier señala varios riesgos y amenazas a la seguridad nacional: Estados extranjeros, causas técnicas, hacking, crimen organizado, terrorismo, hacktivistas, delincuencia, organizaciones terroristas, espionaje, individuos aislados, sabotaje, amenazas internas, conflictos y fenómenos naturales.



**FUENTE:** http://www.europapress.es

## Noticia # 02: Cazadores de errores: la nueva tendencia en ciberseguridad

A medida que crece el ritmo de despliegue de aplicaciones, lanzamientos de sitios web y actualizaciones de software, más empresas confían en 'hackers' para descubrir sus defectos de seguridad y así poder arreglarlos antes de que ciber delincuentes los descubran y sufran algún tipo de robo informático.

Frans Rosén es un empresario tecnológico de día y un cazador de recompensas de errores por la noche. El cofundador de Detectify, una startup de seguridad en Estocolmo, pasa las tardes recorriendo sitios web en busca de vulnerabilidades que los cibercriminales podrían encontrar. Desde que comenzó su pluriempleo en 2012, Rosén ya ha ganado 100.000 dólares por descubrir los defectos de algunas empresas. "Entre el 70 y el 80% de los errores que encuentro no son detectables por el software", afirma Rosén.

Esta práctica, aunque parezca sorprendente, no es nada nuevo. Empresas tan importantes como Google y Microsoft han ofrecido recompensas para aquellos que encuentren graves defectos en sus productos. "Cualquier empresa que está creando tecnología tendrá errores", dice Alex Rice, quien dirigió el programa de recompensas de errores de Facebook antes de fundar HackerOne en 2011. La red de hackers independientes de HackerOne abarca 150 países, según la compañía. La startup con sede en San Francisco, ha ganado más de 2 millones de dólares en recompensas de sus clientes, incluyendo Twitter.

Yahoo también ha tenido su propio programa de recompensa de errores durante años, premiando a los hackers con las tazas y camisetas de la compañía. En 2013 la compañía introdujo un "muro de la fama" virtual y premios en metálico. "Hemos creado diferentes niveles de recompensas, de 50 a 15.000 dólares, según la gravedad de la amenaza descubierta", ha explicado Ramsés Martínez, director senior de Yahoo.

Martínez decidió el año pasado externalizar este programa para HackerOne. "Realmente simplificó todo el proceso" añadió.

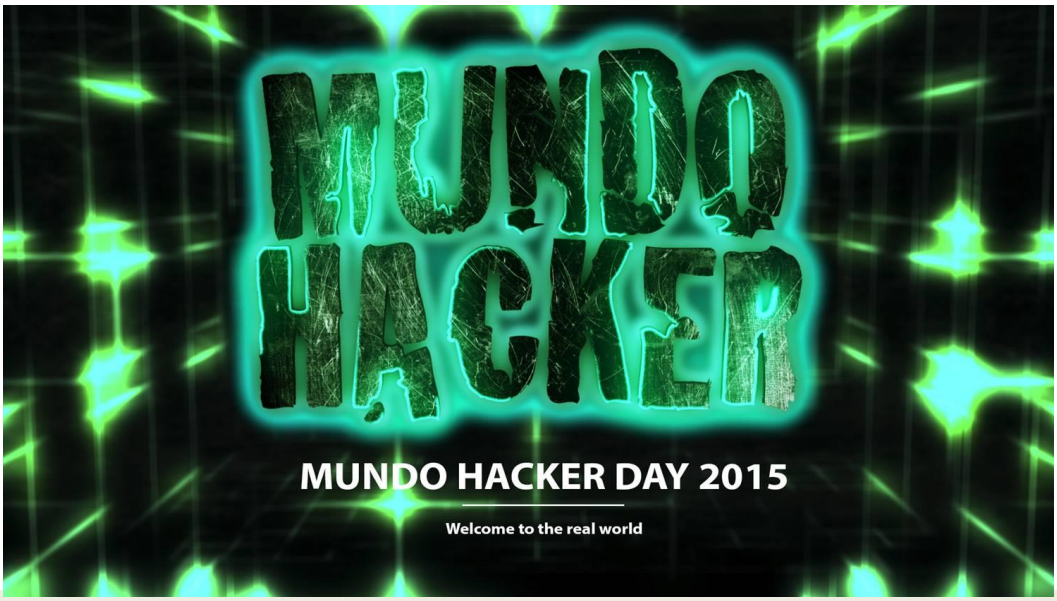
El mercado de la seguridad cibernética pasará a mover 155.700 millones de dólares en 2019, según MarketsandMarkets, una firma de consultoría.

HackerOne"es la solución perfecta en el momento adecuado", dice Bill Gurley, socio de Benchmark Capital, que el año pasado invirtió 9 millones en la empresa. HackerOne compite con otras empresas nuevas en este sector como, Bugcrowd, SYNACK y Crowdcurity.

Según señala Bloomberg, mientras que sus listas de clientes están llenas de empresas de tecnología, HackerOne también está persiguiendo a clientes dentro de las industrias de la salud, banca, comercio minorista y telecomunicaciones

**FUENTE:** http://www.dirigentesdigital.com

## Noticia # 03: Concentración de hackers y expertos en ciberseguridad




Mundo Hacker Day 2015, uno de los mayores eventos de ciberseguridad en España, tendrá lugar los días 28 y 29 de abril en Madrid. En esta concentración se reunirán más de 1500 expertos internacionales, empresas y profesionales del sector para dar a conocer los actuales problemas de seguridad de nuestro país, las nuevas amenazas que afectan a la industria y cómo protegerse de los peligros de la red.

Según Antonio Ramos, hacker y presentador del evento, "aún seguimos viendo cómo existen muchas empresas que no invierten lo necesario en seguridad porque sólo contemplan esta partida como un gasto. Sin embargo, las pérdidas que una brecha de seguridad ocasiona a una organización pueden acabar con ella".

Por lo visto, España no es todavía un país consciente de los peligros que contiene la red pero va llegando la hora de que todas las empresas tomen conciencia y apuesten por un sistema de seguridad en la red mucho más rígido. El Mundo Hacker Day 2015 no solo pretende concienciar sino también saber el estado de seguridad en nuestro país y sobre todo las amenazas que se pueden encontrar en un futuro, informaciones esenciales a la hora de dibujar y establecer un plan de seguridad efectivo en una empresa.

Cómo saber a lo que nos enfrentaremos podría suponer la clave de la ciberseguridad. Mundo Hacker Day 2015 ofrece una serie de charlas en las que se incluyen: generar inteligencia OSINT con Whatsapp, predicción de delitos con Big Data o identificar individuos en un honeypot wifi.

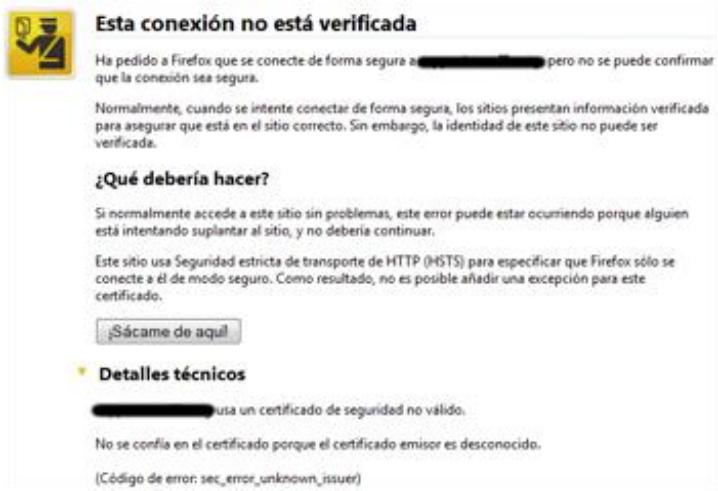
Desde expertos en desarrollo de virus informáticos a especialistas en inseguridad de redes wifi, el evento incluirá más charlas aún por confirmar que vendrán acompañadas de demos técnicas de seguridad informática, *hacking* y mesas redondas. El primer día de charlas girará en torno a la industria del *Open Source*, y el segundo día sobre tendencias en ciberseguridad. Una cita obligada a empresarios que aún no han invertido en ciberseguridad en su empresa, aunque también para todas aquellas personas que estén interesadas en el mundo de la seguridad en la red.

Mundo Hacker Day 2014 contó con más de 750 conexiones en *streaming* y más de 500 asistentes entre los que se encontraron perfiles muy variados, desde estudiantes de ingeniería informática hasta CIOs o CSOs. Como podéis comprobar la puerta está abierta a todo el mundo, no desaprovechéis la oportunidad si os interesa, la ciberseguridad nos concierne a todos.



**FUENTE:** http://es.ign.com

## Cybertruco : Resetear certificados almacenados en Firefox




A medida que vamos usando nuestro navegador**,** en este se van almacenando decenas de certificados de diferentes webs. Puede llegar un momento en el que por seguridad o debido a una manipulación incorrecta de los mismos necesitemos resetear los certificados almacenados en nuestro Administrador de Certificados. En este Cybertruco vamos a ver cómo.

Hoy en día, cuando afortunadamente la mayoría de navegadores comprueban los certificados de las diferentes páginas web, la pantalla de alerta por conexión no verificada es bien conocida por todos. En determinadas ocasiones hacemos caso del aviso y dejamos de navegar por esa página pero otras tantas vamos confirmando excepciones de seguridad y poco a poco la base de datos de certificados de nuestro navegador va creciendo. En este caso simplemente por seguridad es bueno resetear de vez en cuando nuestro Administrador de Certificados.

Otro escenario en el cual nos podemos encontrar es de necesidad de resetearlo, debido a una manipulación incorrecta de los certificados. Ponemos un ejemplo muy claro y reciente. En el post que comentábamos sobre Lenovo y Superfish, recomendábamos eliminar del Administrador de Certificados un posible certificado de Superfish. Nos podemos encontrar en el caso de entrar a revisarlo y encontrar o no este certificado, pero por un exceso de celo empezar a eliminar otros certificados sin saber muy bien a que se refieren simplemente por no sonarnos; pensando que esta sería una buena manera de hacer limpieza.

En este caso es posible que creemos un buen problema y que nuestro navegador nos empiece a bloquear el acceso a cualquier página HTTPS, recibiendo el mensaje "No se confía en el certificado porque el certificado emisor es desconocido**"** y siendo imposible añadir una excepción de seguridad a través de esa misma pantalla. Existe la opción de añadir un certificado a mano a través del Administrador de Certificados, ya sea importándolo o añadiendo una excepción especificando la URL, pero este método en muchas ocasiones no funciona.

En estos dos y en otros casos vamos a ver cómo podemos resetear nuestro Administrador de Certificados de una manera sencilla:

-Accedemos a la carpeta de perfiles de Firefox en nuestro ordenador (dependiendo del sistema operativo que tengamos su ubicación puede variar)

-Borramos o renombramos el fichero cert8.db, para eliminar los certificados que se han ido almacenando al navegar por sitios seguros

.-Borramos o renombramos el fichero cert_override.txt, para eliminar todas las excepciones que hayamos podido forzar.

Reiniciamos nuestro navegador y ya dispondremos de un Administrador de Certificados limpio para seguir navegando de manera mucho más segura.



**FUENTE:** http://cyberseguridad.net