2014-02-17

CiberNoticias # 23

SCProgress

www.scprogress.com

ÍNDICE

Noticia # 01: **Aumenta la compra de extensiones de Chrome para introducir malware en los equipos.**

Muchas veces las funciones que posee un navegador son limitadas, y se desea disponer de otras que mejoren la experiencia del usuario. Por este motivo aparecieron las extensiones para los navegadores web, sin embargo, el uso que se pretende dar hoy en día a estas, por ejemplo en Google Chrome, es para controlar la navegación del usuario y ofrecerle privacidad e infectar el equipo con malware.

Hackers y campañias de publicidad se encuentran inmersas en esta nueva tendencia que ya comienza a tener sus frutos.

Los frutos siempre han sido bien vistos en Internet para tratar de generar dinero gracias a la audiencia de un sitio web. Sin embargo, lo que se pretende con la compra de estas extensiones es forzar al usuario que visite un sitio web manipulando su navegación.

Algo similar sucede con los hackers, que invierten una gran cantidad de dinero en la compra de extensiones que poseen una gran cartera de clientes y utilizan esta o bien para redirigir al usuario hacia páginas web infectadas con malware o bien provocar la instalación de malware en el equipo del usuario

De forma directa, sirviendo al hacker de puente para poder acceder al equipo del usuario.

El gigante de Internet se ha tomado la justicia por su cuenta y ha comenzado a hacer una selección de aquellas extensiones que son de confianza para los usuarios, eliminando todas aquellas cuya actividad sea sospechosa o no esté del todo clara.

Durante el mes de enero se ha podido ver como hackers han llegado a pagar altas sumas de dinero por una extensión que posee una cartera con 30.000 clientes.

Fuente: www.redeszone.net

Noticia # 02: **Almacenamiento en la nube: ¿cifrado en cliente o cifrado en servidor?**

El almacenamiento en la nube es una realidad indiscutible. Servicios como Dropbox, SkyDrive o Google Drive son ya herramientas básicas para millones de personas en todo el mundo, que confían sus archivos y mucho más a estas empresas por la comodidad que ello supone. El fenómeno es tal, de hecho, que la oferta de soluciones Open Source independientes es igualmente surtida, por lo que nos encontramos con diferentes formas de hacer las cosas en cuanto a cifrado se refiere.

La sincronización de archivos entre diferentes dispositivos es sin duda una de las grandes bazas de este modelo. Pero, en cualquier caso, los archivos que salen de un equipo deben estar protegidos, y para eso se utiliza el cifrado, tanto del contenido como en la transferencia de éste. Por lo general, eso sí, el cifrado que se realiza una vez el archivo ha llegado al servidor.

Cifrado en servidor

Cifrado en servidor o cifrado del lado del servidor es el método que utilizan la mayoría de servicios de almacenamiento de archivos en la nube. Esto quiere decir que los archivos llegan al servidor sin cifrar, y allí son cifrados, normalmente, con la contraseña del usuario (por lo tanto, conviene tener contraseñas seguras).

El nivel de este método es perfectamente aceptable, siempre que la transferencia de los archivos se haga a través de una conexión segura (HTTP / SSL), claro está, debido a que los archivos viajan de un equipo al servidor sin cifrar. Pero no hay de qué preocuparse ç: los sitios web de estos servicios y las aplicaciones para PC o móvil fuerzan la conexión segura.

Fuente: Net-Security

Cifrado en cliente

Cifrado en cliente o cifrado del lado del cliente consiste en cifrar los archivos antes de que salgan del equipo, por lo general también, con la contraseña del usuario. Asimismo, lo ideal en este caso, aunque no todas las aplicaciones lo cumplen, es que la contraseña nunca salga del cliente. O dicho de otro modo: los responsables del servicio solo almacenan y sincronizan datos cifrados, cuyo contenido no pueden descifrar.

El cifrado en cliente tiene varias ventajas para las dos partes:

- Para el usuario es más privado, pues solo en su equipo permanecen sus archivos descifrados.
- Cualquier robo de datos en el servidor o durante la transferencia del archivo solo obtendrá archivos cifrados.
- El servicio "se lava las manos" de los contenidos que aloje el usuario, porque de hecho no tiene acceso a ellos.

El cifrado en cliente, no obstante, tiene una particularidad capital: el usuario perderá el acceso a su información si pierde su contraseña, ya que ésta solo se guarda en el cliente.

Dos ejemplos de servicios con cifrado en cliente son SpiderOak y Wuala.

Fuente: muyseguridad.net

Noticia # 03: **Mantener Windows XP a partir de abril, todo un reto.**

Microsoft continúa recomendando la migración desde Windows XP ante el peligro de mantener el sistema operativo cuando el 8 de abril de 2014, finalice su soporte técnico y sus múltiples vulnerabilidades no tengan respuestas a base de actualizaciones de software de Windows Update o nuevos controladores.

Especialmente grave es la situación en empresas donde Windows XP aún mantiene una gran cuota de mercado. Un sistema exitoso pero que cuenta con doce años a sus espaldas, que por arquitectura no es posible mejorar o cuya tasa de infección por malware es seis veces superior a la hallada en Windows 8, Vista o Windows 7.

Una situación que se agravará más allá de abril de 2014 y distintos informes destacan que la muerte de XP será una oportunidad para le cibercrimen, ya que los creadores de malware están retrasando la publicación de vulnerabilidades zero day para las que no se conoce solución, a la espera que Microsoft deje de publicar actualizaciones y puedan obtener mayores beneficios de los correspondientes exploits.

Así las cosas, actualizar a Windows 7 u 8, a una distribución GNU/Linux o aprovechar unaserie de medidas de seguridad como las que nos porponen de seguridad como las que nos proponen desde MuyComputer.

Fuente: muyseguridad.net

Algunas de ellas son:

- Instalar una aplicación tipo sandbox para ejecutar de forma segura las aplicaciones y prevenir la infección de ordenadores.

- Utilizar una aplicación de mitigación de exploits para evitar que se exploten vulnerabilidades de seguridad en el software.

- Utilizar un cortafuegos para controlas las conexiones de red.

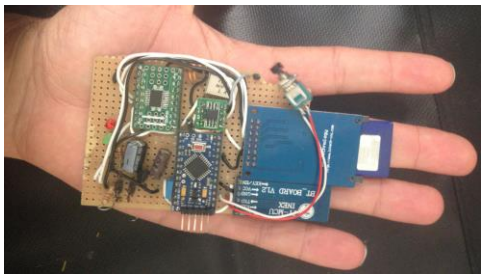
- Instalación de antivirus.

- Mantener actualizas o eliminar si no usamos aplicaciones Java, Flash o el Reader de Adobe, método de entrada predilecto para inyección de la mayoría de malware mundial. También navegadores, cliente de correo o en general, todas las aplicaciones.

- Instalar las extensiones de seguridad que ofrecen los principales navegadores web.

Fuente: muyseguridad.net

Noticia # 04: **Crean un dispositivo para hackear un coche en solo cinco minutos.**



En los últimos meses, ante la cada vez mayor presencia de elementos tecnológicos conectados en los coches nuevos, son muchos ya los que han comenzado a mostrar su preocupación acerca del potencial peligro que supone para los conductores el riesgo de que su vehículo sea hackeado. Ahora, dos investigadores españoles les han dado la razón.

Javier Vázquez-Vidal y Alberto García han desarrollado el denominado CAN Hacking Tool (CHT), un dispositivo que se instala en los coches y que permite controlarlos a través de Bluetooth en menos de cinco minutos. Después, "podríamos esperar un minuto o un año y luego activarlo para hacer cualquier cosa para lo que lo hayamos programado", explica Vázquez-Vidal, quien trabaja como asesor de seguridad de información y tecnología en Alemania, en na entrevista a Forbes.

Pero ambos investigadores quieren ir más allá. Conscientes de que el Bluetooth limita a unos cuantos metros el control del vehículo, García y Vázquez-Vidal están trabajando en un modelo que funcione a través del sistema de radio GSM –el antiguo sistema 2G de cobertura para móviles-, de cara a la presentación del CHT en la conferencia Black Hat que tendrá lugar en Singapur el próximo mes.

Fuente: El Economista

Urgencia por establecer protocolos de seguridad

Una vez conectado el gadget al CAN Bus (el sistema destinado a controlar el motor e interconectar las unidades de control electrónico) del vehículo que se va a hackear, es posible tener accesoal control de la alarma, las ventanillas, las luces, el sistema de frenado y el volante a través de un ordenador. “Un coche es una mini red y, por ahora, no hay ningún tipo de seguridad implementado”, declara Alberto García.

De esta forma, el dispositivo desarrollado por estos dos investigadores españoles vuelve a incidir sobre las carencias de seguridad que presentan los vehículos a medida que avanza la tecnología conectada a la red, poniendo de relieve una vez más la urgencia de que se apruebe una regulación al respecto que garantice la integridad del vehículo y de sus ocupantes frente a este tipo de amenazas.

Fuente: El Economista

Noticia # 05: **Un ataque DDos masivo afecta a plataformas de monederos y de intercambio de bitcóin.**

Según informó el gerente de seguridad de la plataforma, Andreas Antonopoulos, el ataque distribuido de denegación de servicio (DDoS, por sus siglas en inglés) no puede afectar los fondos de los usuarios. Sin embargo, impide el funcionamiento ordinario del servicio.

El ataque DDoS consiste en que una red de los llamados 'bots', es decir, unos programas informáticos que imitan a los seres humanos, realizan un gran número de transacciones malformadas con monederos de bitcoines, provocando confusión y finalmente la falta de servicio.

Sin embargo, Antonopoulos indicó que Blockchain.info no ha sido tan afectado por el ataque como varias plataformas de intercambio de la moneda virtual, cuyos sistemas internos de contabilidad se desincronizaron por la gran cantidad de transacciones.

Los propietarios de bitcoines y las plataformas de intercambio han sufrido varios problemas últimamente. La semana pasada Apple Store eliminó la aplicación de Blockchain, que era la única aplicación que permitía a los usuarios de iOS realizar pagos con bitcoines.

Poco después Mt.Gox, una de las mayores plataformas de intercambio de la moneda virtual, frenó las operaciones de retirada de bitcoines debido al número rampante de estas operaciones. La decisión llevó a la caída inmediata del precio de la moneda virtual, que en los últimos meses ha llegado a ser de más de mil dólares por bitcóin.

El precio actual del bitcóin se sitúa en los 571 dólares por unidad, según Mt.Gox.

Fuente: http://actualidad.rt.com/