2013-07-25

CiberNoticias # 11

SCProgress

www.scprogress.com

ÍNDICE

Noticia # 01: Casi 500 millones de celulares en peligro de ser atacados por piratas informáticos.

Miles de teléfonos están en problemas.

Nohl dijo que, de acuerdo a su estimación más conservadora, al menos 500 millones de teléfonos están vulnerables a los ataques y agregó que ese número podría crecer si otros investigadores comienzan a revisar el tema y hallan otros modos de explotar la misma clase de vulnerabilidad.

Boston (Reuters). Un grupo de Naciones Unidas que asesora a los países sobre seguridad informática planea enviar una alerta sobre vulnerabilidades significativas en tecnología de teléfonos móviles que podría permitir a piratas informáticos atacar remotamente a al menos 500 millones de unidades.

La falla, descubierta por una empresa alemana, permite a los piratas obtener control en forma remota y también clonar ciertas tarjetas SIM de teléfonos móviles. Así, se podrían usar tarjetas SIM comprometidas para cometer crímenes financieros o realizar espionaje electrónico, según Security Research Labs de Berlín, que describirá las vulnerabilidades en la conferencia sobre pirateo informático Black Hat que comenzará en Las Vegas el 31 de julio.

La Unión Internacional de Telecomunicaciones (ITU, por su sigla en inglés) de la ONU, con sede en Ginebra y que revisó la investigación, la describió como "enormemente significativa" e indicó que notificará a reguladores y otras agencias gubernamentales en casi 200 países sobre la amenaza potencial y también a cientos de compañías de telefonía móvil, académicos y otros expertos de la industria.

La ITU estima que actualmente funcionan alrededor de 6.000 millones de teléfonos móviles en todo el mundo. La entidad planea trabajar con la industria para identificar cómo proteger a dispositivos vulnerables de ataques, sostuvo Touré.

Fuente: el comercio

Noticia # 02: Avira Free Antivirus se actualiza y es compatible con Windows 8.

Avira fue fundada hace 27 años, cuenta con más de 100 millones de consumidores y pequeñas empresas confían en la experiencia en seguridad de Avira.

Avira Free Antivirus se actualiza y es compatible con Windows 8

Uno de los mejores Antivirus para los sistemas operativos Windows de Microsoft, se llama Avira Free Antivirus. El mismo es gratuito, y ahora se ha actualizado a la versión 13.0.0.3884. Avira Free Antivirus, antes conocido como AntiVir Personal, es el antivirus gratuito de Avira. Bajo su paraguas, tu PC está a salvo contra todo tipo de virus, spyware y rootkits. Avira Free Antivirus 2013 se destaca por su gran eficacia y velocidad.

El consumo de recursos es bajo, incluso durante los escaneos, y la tasa de detección de malware es de las mejores. La configuración admite dos modalidades, Principiante y Experto. La segunda muestra todas las opciones de configuración de Avira Free Antivirus, que son lo suficientemente abundantes. Rápido y letal contra los virus, y por fin traducido al español, es completamente gratuito.

Fuente: avira.com

Noticia # 03: Las “criptofiestas” están en boga.

Desde que estalló el escándalo en torno a programas de espionaje masivo como PRISM y Tempora, en Alemania crece la demanda por información sobre cómo proteger la esfera privada del Estado y los vigilantes globales.

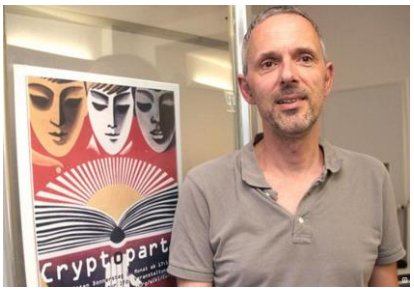
Las “criptofiestas” se celebran con cada vez mayor frecuencia en Alemania. Se trata de reuniones informales organizadas para que uno o más expertos informáticos les enseñen a los interesados cómo proteger efectivamente el contenido de sus correos electrónicos. De ahí el nombre que se le ha dado a estos eventos privados; “criptofiesta” alude al arte de encriptar, que consiste en convertir un texto normal en un texto codificado para que sólo las personas con claves de acceso al mismo puedan leerlo.

La idea proviene de Australia, en donde se decretó una ley que atribuía funciones de vigilancia a los proveedores de Internet. De eso hace ya un año. Cuando la normativa entró en vigencia, un usuario de Twitter escribió un mensaje en el que preguntaba si había especialistas dispuestos a explicarle a él y a otras personas como blindarse contra esta forma de control estatal. La noticia circuló velozmente en todo el mundo porque la propuesta incluía el incentivo de intercambiar conocimientos en una atmósfera relajada y divertida.

Desde que estalló el escándalo en torno a programas de espionaje masivo como PRISM y Tempora, en Alemania crece la demanda por información sobre cómo proteger la esfera privada del Estado y los vigilantes globales. Jürgen Fricke, especialista en seguridad informática, solía ofrecer cursos breves sobre la materia a tres o cinco personas. Ahora, cuando recibe a un grupo en su oficina –que tiene capacidad para veinte personas– no cabe un alma más. El partido alemán Los Piratas intentó instrumentalizar el fenómeno políticamente… en vano.

Fuente: www.dw.de

La protección de datos nos interesa a todos.



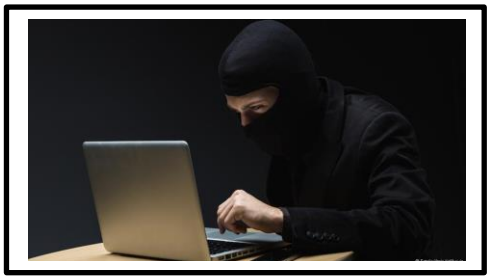
Los organizadores independientes de "criptofiestas" no respondieron al llamado de Los Piratas. "El de las 'criptofiestas' es un movimiento internacional que no comulga con las visiones de un solo partido. Todos los partidos democráticos tienen que ocuparse del tema de la protección de datos; este asunto no le pertenece a un solo grupo político", comentó Jochim Selzer en entrevista con DW. Selzer es matemático, administrador de sistemas informáticos y organizador de "criptofiestas" en Colonia y en Bonn.

Fricke se ha tomado este fenómeno muy en serio. "Nuestra meta es conseguir que, de aquí a dos o tres años, diez millones de personas en Alemania sepan cómo encriptar sus documentos", sostiene el experto. Ojalá el empresariado germano fuera tan optimista. Aunque el tópico de la protección de datos es de vital importancia para sus compañías, la infraestructura informática de las mismas suele ser su talón de Aquiles. "La seguridad informática de las empresas en Alemania es pésima; va desde 'deficiente' hasta 'inservible' ", comenta Mark Semmler, otro conocedor de la materia.

Por otro lado, las "criptofiestas" y otras estrategias similares sólo resuelven el problema de la protección de datos hasta cierto punto. Las técnicas para encriptar pueden contribuir a codificar los contenidos de los correos electrónicos, pero "metadatos" como la fecha y hora en que se produjeron los e-mails siguen estando visibles para todo el que quiera leer esa información. De ahí que los organizadores de las "criptofiestas" no se cansen de advertir: "Todos los días protagonizamos un striptease masivo; da igual que lo queramos o no".

Fuente: www.dw.de

Noticia # 04: Darknet: la red oculta en Internet.



El espionaje de datos por parte de servicios secretos, como en el caso de la NSA, de EE. UU., no representa el fin de la criminalidad en Internet. Ahora, los delincuentes de la red usan la "Darknet".

Mientras políticos y expertos hablan de la "autopista de datos" en Internet, los delincuentes parecen estar usando un atajo, es decir, la red oculta dentro de la red, la "Darknet". Para ingresar a ella no solo es necesario ser un experto en nuevas tecnologías, sino que también se deben explorar de manera autónoma los caminos a seguir, ya que en Darknet no existen máquinas buscadoras como Google, sino solo una especie de catálogo en el que tampoco están registradas todas las páginas.

Fuente: www.dw.de

Darknet: descentralizada y anónima

En Darknet el intercambio de información es casi imposible de rastrear.

Las dos grandes diferencias entre Internet y Darknet es que ésta última funciona de manera descentralizada y su uso es totalmente anónimo. Es decir que ambas redes poseen estructuras muy distintas. Internet está organizado, en gran parte, de manera centralizada. Quien usa Facebook, por ejemplo, se registra en el sistema y deja en esa plataforma sus datos, fotos y textos. Otro usuario de Internet que quiera ver esa información también debe registrarse en Facebook e ingresar a su cuenta. Es decir que la clave es el servidor de Facebook, ya que allí se almacenan todos los datos de los usuarios. Desde el punto de vista de la protección de datos, esa es la característica más vulnerable de la red: quien tenga acceso a los servidores de Facebook, de Google o de otra gran plataforma puede también acceder a los datos de los usuarios. Y eso es, según Edward Snowden, justamente lo que hizo el servicio secreto estadounidense NSA.

La Darknet, por el contrario, funciona sin esa estructura central. Cada computadora es, al mismo tiempo, un servidor que solo guarda una parte de las informaciones necesarias y, además, de manera codificada. También la transmisión de datos entre las terminales conectadas a Darknet se realiza en forma anónima, de modo tal que el observador –y también los servicios de inteligencia- captan los datos, pero no les sirven de nada.

Fuente: www.dw.de

Tampoco los metadatos revelan información.

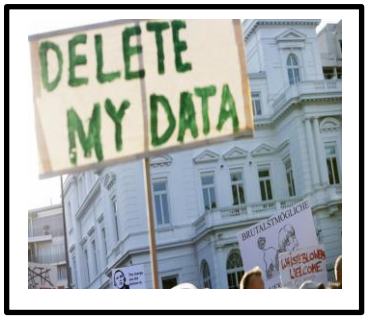
Además, los creadores de Darknet idearon otro truco para garantizar el anonimato en la red. Los metadatos tampoco pueden ser utilizados por intrusos. En ellos se registra la dirección de la computadora receptora y la de la emisora. De ese modo, quien captura información de Internet puede reconocer qué tipo de datos se transmiten de ordenador a ordenador. Y aún si los datos están codificados es posible averiguar qué computadoras están en contacto una con la otra, así como la magnitud del intercambio de datos, es decir, que hay mucho margen para el espionaje. En Darknet, cada paquete de datos se envía a través de tres computadoras elegidas al azar. En cada etapa, el paquete de datos recibe otro nombre emisor, y, al final del trayecto, no es posible averiguar desde qué computadora fueron enviados. Una desventaja: la Darknet es más lenta que Internet.

Regreso a los métodos tradicionales de investigación.

Para los servicios de inteligencia y la Policía hay pocas posibilidades de seguirles los pasos a los usuarios de Darknet. Localizar informaciones y analizarlas no sirve de nada en la "red oscura". En lugar de eso, la Policía trata de rastrear a narcotraficantes, por ejemplo, de otro modo. Los investigadores se hacen pasar por compradores, siguiendo las huellas de los paquetes del envío, o intenta establecer un lazo de confianza con los traficantes, para sacarlos del anonimato solicitando una entrega personal de la mercadería en lugar de usar la vía postal.

Fuente: www.dw.de

La favorita de opositores y delincuentes



Protestas contra el almacenamiento de datos en Internet.

Darknet hizo posible que se estableciera una red paralela que parece atraer, sobre todo, a la escena de los ciber delincuentes. Se crearon mercados como "Silk Road" o "Black Market Reloaded", en los que se ofrecen armas, drogas y servicios, además de la programación de virus a pedido. El pago se realiza en forma totalmente anónima, para lo cual se usa la moneda de Internet: el Bitcoin. El intercambio de datos es anónimo, y la moneda virtual se puede cambiar legalmente en dinero. También los opositores a ciertos gobiernos prefieren usar la Darknet. A través del programa "Tor", que se puede bajar de Internet, cualquiera puede acceder a la red detrás de la red. También Edward Snowden se comunicó con reporteros del periódico británico The Guardian a través de Darknet.

Fuente: www.dw.de