2015-02-28

CyberNoticias # 003

SCProgress

www.scprogress.com

ÍNDICE

Noticia # 01: EEUU CREÓ UNA NUEVA AGENCIA DE SEGURIDAD INFORMÁTICA.

La preocupación del presidente estadounidense, Barack Obama, respecto a la vulnerabilidad informática y posibles ataques en la red por parte de hackers y terroristas es de vieja data. Desde los atentados del 11 de septiembre de 2001 hasta los recientes atentados cibernéticos a Sony Pictures y el Comando de Defensa de ese país, la Casa Blanca busca intensificar las medidas de prevención de acceso a información secreta del estado.

Por tal motivo, se inauguró una nueva agencia de seguridad informática que fue denominada Integración de Inteligencia contra la Amenaza Cibernértica (CTIIC, en sus siglas en inglés) que tendrá como principal tarea evitar que terceros accedan a información confidencial del Gobierno y detectar a los atacantes.

La asesora de seguridad nacional y para la lucha antiterrorista del presidente Barack Obama, Lisa Monaco, advirtió que las amenazas cibernéticas contra EEUU son cada vez más "diversas, sofisticadas y peligrosas". Y explicó que la CTIIC no recolectará inteligencia, sino que integrará y analizará la recopilada por otras agencias gubernamentales para detectar amenazas cibernéticas y prevenir ataques que pongan en riesgo al país. "En los últimos años, las ciberamenazas contra EEUU incrementaron "en frecuencia, escala, sofisticación y gravedad del impacto", subrayó Monaco, quien nombró a Rusia, China, Irán y Corea del Norte entre los países con "capacidad" para ejecutar ataques en la red. "Lo más preocupante, quizá, es la naturaleza cada vez más destructiva y maligna de los ataques cibernéticos", sostuvo. Ataques como el sufrido a finales del año pasado por la compañía Sony Pictures "se convertirán en norma si no actuamos rápido", advirtió la asesora de Obama. El Gobierno atribuyó a Corea del Norte ese ciberataque, supuestamente cometido en represalia por la película "The Interview", una comedia que se burla del líder de ese país, Kin Jong-un. En referencia a eso, Monaco dijo que ese ataque marcó "un punto de inflexión" por el robo de millones de datos y porque se trató de un intento de "coerción" por parte de Pyongyang.

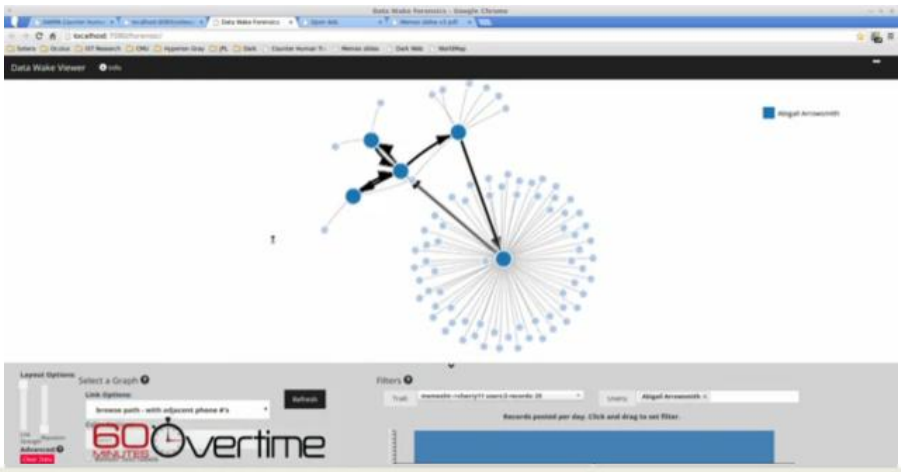
Fuente: http://www.infobae.com/2015/02/11/1626130-eeuu-creo-una-nueva-agencia-seguridad-informatica

Noticia # 02: **SON VULNERABLES EL 63% DE LAS APLICACIONES DE CITAS PARA ANDROID.**

Investigadores de IBM analizaron las 41 aplicaciones de citas más populares para el sistema operativo móvil Android y concluyeron que más del 60% de ellas tienen problemas de seguridad que oscilan entre intermedios y severos.
IBM no reveló los nombres de las apps con problemas, pero sí informó de la situación a las compañías que las desarrollaron. Según un informe elaborado en 2013 por el Pew Research Center, unos 31 millones de norteamericanos utilizaron sitios web o aplicaciones de citas.
"Muchos usuarios usan y se fían de sus móviles para distintas aplicaciones. Esa confianza permite a los piratas informáticos explotar puntos débiles, como las que encontramos en estas aplicaciones de citas", explicó en un comunicado Caleb Brown, vicepresidente de IBM Security. Brown animó a los usuarios a ser cuidadosos y no revelar demasiada información confidencial en esos sitios. El estudio de IBM reveló que muchas de estas aplicaciones de citas tienen acceso a características adicionales en dispositivos móviles, como cámara, micrófono, almacenamiento, ubicación GPS e información sobre facturación de billetera móvil que, sumado a las vulnerabilidades, puede convertirlos en blanco de piratas.
IBM también halló que casi el 50% de las organizaciones analizadas tienen por lo menos una de estas populares aplicaciones de citas instaladas en dispositivos móviles utilizados para acceder a información de la empresa. IBM recomendó a los que utilicen ese tipo de aplicaciones el usar contraseñas únicas que no utilicen en otras páginas, actualizar sus aplicaciones y utilizar conexiones seguras a internet.

Fuente: http://www.infobae.com/2015/02/12/1626434-son-vulnerables-el-63-las-aplicaciones-citas-android

Noticia # 03: MEMEX: BUSCADOR EN LA DEEP WEB



Hace un año, DARPA (Defense Advance Research Projects Agency) anunció MEMEX, un proyecto para crear un nuevo motor de búsqueda que pueda encontrar cosas en la Deep web que no esten indexadas por ningún otro buscadores comercial.

El proyecto, denominado Memex Deep Web Search Engine, está en camino, y por primera vez el domingo 8 de febrero del 2015 por la noche el "motor de búsqueda de lucha contra el crimen" entró en acción. La Agencia del Pentágono dio una vista previa sobre el software al programa 60 Minutos. El inventor de Memex, Chris White, explicó cómo funciona este nuevo motor de búsqueda y cómo podría revolucionar las investigaciones de la ley. "El internet es mucho más grande de lo que la gente piensa: según algunas estimaciones Google, Microsoft Bing y Yahoo! sólo dan acceso a alrededor del 5% del contenido en la Web. Eso deja mucho espacio para malos actores que operan libremente en las sombras".

Memex está siendo probado en estado Beta por las oficinas de distrito, una agencia del orden público y una organización no gubernamental. El siguiente nivel de la prueba se hará por un amplio grupo de beta-testers en unas semanas. Uno de los principales objetivos de esta ronda es poner a prueba nuevas capacidades de búsqueda de imágenes, que puedan analizarse fotos incluso cuando existan solo porciones o estén ofuscadas. Otro objetivo es probar las interfaces de usuario y experimentar con arquitecturas que evalúan datos sensibles.

Fuente: http://seguinfo.blogspot.com/2015/02/memex-buscador-en-la-deep-web.html

Noticia # 04: **NSA DEFIENDE LAS PUERTAS TRASERAS EN EMPRESAS TECNOLÓGICAS.**

El director de la Agencia de Seguridad Nacional estadounidense, Mike Rogers y el jefe del Comando Cibernético del país, defendieron el uso de puertas traseras en productos y servicios tecnológicos ante una audiencia de criptógrafos, oficiales de las compañías de alta tecnología y medios en una conferencia en la New America Foundation in Washington.

La NSA trata de calmar las preocupantes informaciones que hace tiempo llegan de sus actividades. Una estrategia defensiva ante las opiniones que claman frenar lo que para muchos son violaciones de libertades fundamentales. Rogers aseguró que las puertas traseras en productos y servicios tecnológicos no serían perjudiciales para la privacidad, no comprometerían los estándares de cifrado y no arruinarían los mercados internacionales para las empresas de Estados Unidos. ???

El jefe de los espías reconoció que la infiltración del gobierno (como en los discos duros) podría suponer una publicidad negativa pero sugirió que la mayor amenaza estaba en los ataques cibernéticos. A pesar de los escándalos que se ciernen sobre su organización, Rogers reclamó un marco legal más amplio que permita realizar sus actividades "legalmente". A este respecto comentó que la Casa Blanca está tratando de llegar a un acuerdo con empresas como Apple, Google o Yahoo! para establecer este marco.

Van a tener trabajo las grandes tecnológicas para desprenderse de las denuncias de connivencia con las agencias de espionaje que está sembrando una gran desconfianza en el sector.

Fuente: http://muyseguridad.net/2015/02/27/puertas-traseras

Noticia # 05: G DATA ANALIZA EL SPYWARE BABAR.

G DATA Security Labs ha estado investigando una muestra de un sofisticado spyware que graba y transfiere pulsaciones de teclado, datos del portapapeles, capturas de pantalla y conversaciones de audio apodado Babar. Babar fue mencionado por primera vez en unos documentos del servicio de inteligencia canadiense CSEC (Communication Security Establishment Canada) filtrados por Snowden y que mencionaban dicho malware dentro de la «operación Snowglobe». El primero que se hizo eco de estos documentos fue el periódico francés Le Monde hace casi un año. Los expertos de G DATA han publicado los primeros detalles técnicos así como un exhaustivo análisis de Babar realizado junto a otras agencias de seguridad internacionales. En opinión de los expertos, desarrollar un spyware como el mencionado requiere grandes inversiones en infraestructuras y personal muy cualificado. Por su parte, los servicios de inteligencia canadienses apuntaban al origen francés de la amenaza. Las soluciones de G DATA detectan y bloquean este software malicioso.

«Babar solo puede haber sido creado por desarrolladores muy preparados y con conocimientos técnicos muy elevados», explica Eddy Willems, responsable de ciber seguridad de G DATA. "Está específicamente diseñado para robar los datos sensibles en redes empresariales, organismos públicos, instituciones de investigación... Es capaz incluso de grabar conversaciones vía Skype y podría haber sido utilizado en ataques dirigidos a individuos específicos. Una distribución masiva del malware, sin embargo, parece poco probable», concluye Willems.

Fuente: https://mx.gdatasoftware.com/prensa/notas-de-prensa/news-details/article/g-data-analiza-el-spyware-babar