CYBERNOTICIAS

Cyberoam

NEXXT SOLUTIONS

Avira

open source™

CONTENIDO

CREDITOS:

Revista virtual de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:
Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)
Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Revisado por:
Arturo de la Torre
adltorre@scprogress.com (+593 999025294)

Síguenos en:

www.scprogress.com www.facebook.com/SCProgress/?fref=ts @SCProgressECU

Ataques de Ingeniería Social

En la actualidad, la seguridad informática no está relacionada únicamente las seguridades tomadas en relación a los equipos y software que manejan las empresas, las mayores vulnerabilidades se encuentran en las personas que laboran en las mismas, por lo que debemos tomar mayor conocimiento y conciencia, sobre ataques que se realizan con direccionamiento hacia los seres humanos.

En la revista "Noticias de seguridad informática", se realiza un completo análisis de este tipo de ataques, con una explicación muy clara sobre sobre la manera de obtener información y aprovecharse de la misma.

"¿Cómo obtener información para el ataque de ingeniería social?

La ingeniería social es la práctica del uso de medios no técnicos, por lo general la comunicación a través del teléfono u otro medio, para atacar un objetivo. La ingeniería social no puede sonar eficaz y lo que esperamos demostrar en este artículo es que es extremadamente eficaz como método de ataque y que las empresas deben tomar esta forma de ataque tan seriamente como cualquier otro método de ataque según expertos de empresas de seguridad de la información.

Hay dos fases principales de un ataque de ingeniería social (IS). La primera fase es el reconocimiento donde se reúne información de inteligencia sobre su objetivo. Esto les ayuda a infundir confianza en su objetivo y de que la IS es quien dice ser y el objetivo se confiara en la IS. La segunda fase es la fase de ataque en el que la IS llamará al destino y comenzara el ataque.

Reconocimiento – Open Source Intelligence (OSINT)

Durante la fase de Reconocimiento, la IS reunirá toda la información sobre su objetivo como sea posible. La siguiente es una lista de algunas de las herramientas utilizadas por los expertos de empresas de seguridad de la información y hackers:

- ***Google** – Buscar en Google la empresa, buscando en el directorio de empleados, buscar en Google los nombres de los empleados.*
- ***Maltego** – Maltego se hace por Paterva y es una poderosa herramienta para recopilar, combinar y analizar OSINT sobre un objetivo.*
- ***Whois** – Whois te dirá quién es dueño de un dominio. Si una empresa está en la mira, el administrador del dominio de la empresa frecuentemente aparece con su número de teléfono o un número para el departamento de TI.*
- ***Twitter, Facebook, LinkedIn, FriendFinder** y otros sitios sociales o sitios con perfiles públicos pueden revelar una gran cantidad de conocimientos acerca de un individuo o una empresa. Los empleados de la compañía pueden revelar detalles acerca de la estructura de la empresa, horarios, nombres de compañeros, explican expertos de empresas de seguridad de la información.*
- ***Google** – Esto es lo primero que enseñan en un curso de seguridad de la información. Una característica poco conocida de imágenes de Google es la capacidad de rastrear una foto de perfil en una búsqueda de Google imágenes. Si usted puede encontrar una foto de perfil pública para un individuo, trate de rastrear en búsqueda de imágenes de Google.*
- ***PiPl.com** – Este servicio puede ser un poco atemorizante. Trate de buscar su propio nombre con o sin su ubicación. A continuación, haga clic en el resultado de que es usted. Usted se sorprenderá de la cantidad de datos manejados por pipl.com.*
- ***Shodan** – Shodan es un increíblemente potente motor de búsqueda de la red. Se va alrededor de la indexación qué los servicios que están escuchando en los puertos de red. Se puede proporcionar, por*

ejemplo, una lista de los routers Cisco de escucha en un puerto en articular de rango de direcciones IP de una empresa.

- ***TinEye** – De acuerdo a un curso de seguridad de la información es una búsqueda de la imagen inversa que también es útil para buscar fotos de perfil que coincidan con una foto existente. Revela perfiles de usuarios alrededor de la red.*
- ***Archive.org** – También se llama WayBackMachine, es una de las herramientas favoritas de empresas de seguridad de la información. Esto le permite ver las versiones anteriores de una página web, a menudo se remonta a varios años. Esto puede proporcionar nombres de los empleados anteriores que ya no están con la empresa, o la inteligencia en las actualizaciones de sitio y los cambios.*
- ***Monster.com**, **GlassDoor, Indeedy** otros sitios web relacionados con el empleo pueden proporcionar una gran cantidad de información en sus descripciones de trabajo. Usted puede aprender sobre qué hardware y software una empresa está utilizando, qué nivel de autorización de seguridad de la información mantienen los empleados y más.*

Estas son sólo algunas de las herramientas que los ingenieros sociales OSINT utilizan para recopilar datos sobre un objetivo.

Explotación – Los ataques de ingeniero social!

Aquí hay algunos de los tipos de OSINT, un ingeniero social buscará e ilustran cómo se puede utilizar la información:

- *Los nombres de los empleados: "Hola, ¿Puedo hablar con Bob Simmonds?"*
- *Sus nombres colega: "Hola Bob, esta es Mary de TI. Acabo de hablar por teléfono con Matt Smith".*
- *Lo que sus colegas están haciendo: "Matt está enfermo hoy…"*
- *Ubicación de las mesas personales: ". … Pero estoy seguro de que sabes que ya que ustedes comparten un cubículo"*
- *Los nuevos despliegues de tecnología en una empresa: "Yo quería saber cómo esa nueva estación de trabajo está trabajando para usted."*
- *¿Qué tecnología se está utilizando: "Yo sé que Windows 10 no es el favorito de todos, pero espero que la nueva versión de Office te está ayudando"*

En este punto, usted está convencido de que podría solamente estar hablando con un empleado de TI interno porque ya sabes mucho. Usted probablemente va a compartir información libremente con esta persona, según menciona un experto de seguridad de la información.

Como se ve, gastando tanto tiempo reuniendo OSINT en una empresa antes de ponerse en contacto con ellos puede hacer un ataque mucho más eficaz. Ataques de ingeniería social son muy eficaces porque los seres humanos (que somos nosotros) suelen ser el eslabón más débil y más aprovechable en una red segura. Es evidente la importancia de desarrollar políticas y procedimientos de la organización con ayuda de expertos de empresas de seguridad de la información y tomar cursos de seguridad de la información para protegerse de este tipo de ataque."

FUENTE: http://noticiasseguridad.com

4 consejos para evitar el virus ransomware

Hoy en día, escuchar hablar de virus que afectan nuestros equipos informáticos es un tema cotidiano, y la mejor solución es la instalación de antivirus óptimos que eviten por completo la infección de los mismos, y/o disminuyan significativamente el riesgo de infección.

Un virus que día a día sigue en constante crecimiento es el ransomware, que es un software malicioso que bloquea las computadoras de forma remota y encripta toda la información existente en el mismo, el virus envía a través de una ventana emergente la solicitud de un pago de un rescate para restablecer los datos, es decir, el delincuente cibernético, secuestra nuestros equipos, sin importar si son empresariales o personales para obtener dinero virtual (bitcoin) a cambio de habilitar nuevamente al equipo a su estado original.

Los ataques se originan a través de la recepción de correos electrónicos infectados, o por abrir los archivos adjuntos los mismos que también ya se encuentran infectados, se conoce que también ya se encuentran comprometidos computadores Mac.

Para ello Avira proporciona cuatro (4) consejos para evitar el ataque realizado por ransomware:

*"**1. Hacer copias de seguridad seguras y protegida.***

Es claro que una vez que haya guardado todos los datos importantes, los atacantes han perdido su influencia sobre ti. Aun así, el ransomware se está convirtiendo cada vez más sofisticado y que incluso se dirige a los archivos de copia de seguridad en unidades externas. En este caso, usted debe hacer varias copias de seguridad de servicios en la nube y el uso de unidades físicas a intervalos regulares. Además, es una buena idea hacer una copia de seguridad de archivos que queda totalmente desconectado de la red.

2. Actualizar y parchear sus sistemas

Los creadores de malware cuentan con personas que ejecutan el software obsoleto con ciertas vulnerabilidades, que pueden aprovechar para entrar en su sistema. Por esta razón, mantener su dispositivo actualizado reduce drásticamente el riesgo de tener el equipo infectado. Activar las actualizaciones automáticas, si es posible. Debido a que el malware puede ser disfrazado como una notificación de actualización de software, si no está seguro acerca de un mensaje, ir directamente al sitio web del desarrollador de software.

3. Utilice un software antivirus y un firewall

Es útil tener tanto el software anti-malware y software de un servidor de seguridad en el lugar para ayudar a identificar las amenazas o comportamiento sospechoso. Los creadores de malware se actualizan con frecuencia su trabajo con el fin de evitar la detección por lo que debe tomar medidas tanto preventivas. Si ya ha hecho clic en el malware sin realizar ninguna precaución, que sus opciones son limitadas. Obtenga una protección antivirus probado. Después de todo, hemos demostrado recientemente las reacciones de nuestros chicos de laboratorio Protección Avira obtenían de los creadores ransomware.

4. Capacitar a sí mismo y los que le rodean

Seguridad comienza entre los auriculares - para usted y para todos los que usan el ordenador. Entrenarse a sí mismo y otros para no hacer clic en enlaces o archivos adjuntos sospechosos cuestionables. Además, es importante que los administradores de sistemas limiten el acceso de los empleados a sólo algunas partes de la red que son críticos para su trabajo. Esto reduce el riesgo de tener una red infectada con ransomware.

Y nunca olvidar ...

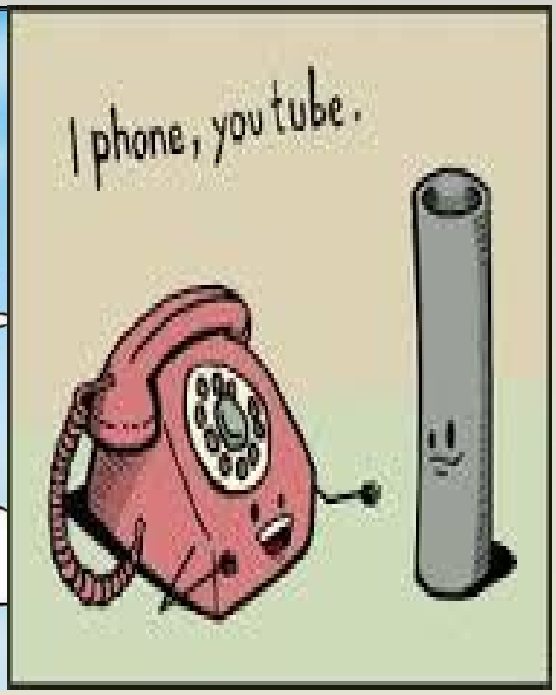
Los malos van a tratar de mantener sus archivos cifrados hasta que pague el rescate. Pero usted no debe hacer eso. Las fuerzas del orden desalientan hacer pagos de rescate, ya que sólo recompensan a los malos y les dan los recursos necesarios para realizar otros ataques. Además, el pago no es necesario ya que se recuperará los datos bloqueados.

Por lo tanto, mantener estos consejos en mente y su aplicación le ayudará a mantenerse un paso por delante de los atacantes ransomware. Hasta que salga de la guardia ...”

FUENTE: https://blog.avira.com/author/antonio-robitu/

Humor


Confirmar eliminación de archivos
¿Confirma que desea enviar "Planeta Tierra" a la Papelera de reciclaje?
Sí
No
KAPPEL

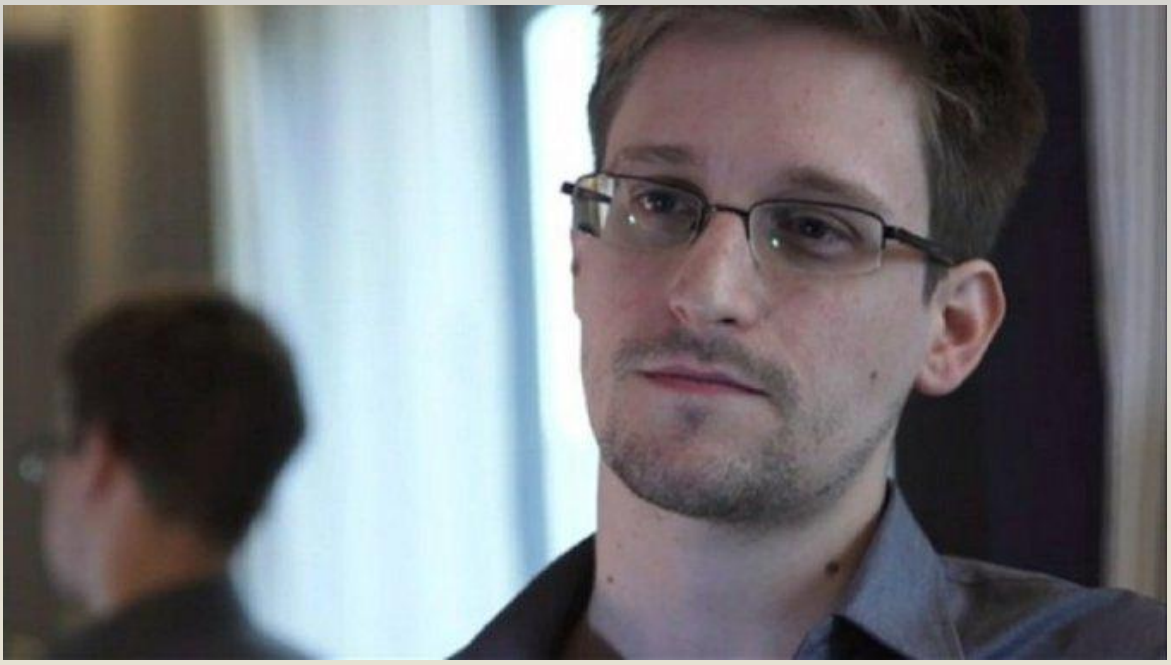

I phone, you tube.


Nuestros ordenadores están caidos, así que estamos haciendo todo en modo manual


Dame toda tu caché!!

Actualidad

Hackearon a la NSA y Snowden apuntó a Rusia



El ex analista de la Agencia Nacional de Seguridad (NSA) de Estados Unidos Edward Snowden apuntó a la posibilidad de que Rusia, país en el que está asilado, se encuentra detrás del reciente ataque al sitio web de ese organismo de espionaje.

"Las evidencias indirectas y el sentido común apuntan a que la responsabilidad es de Rusia", escribió Snowden en Twitter.

Al parecer, la web de la NSA fue atacada poco después de que el grupo Shadow Brokers anunciara que había tenido acceso al arma cibernética del colectivo Equation Group, una red de piratas informáticos supuestamente vinculado con la agencia estadounidense.

Shadow Brokers publicó en internet una parte de la información obtenida y con ello, según Snowden, demostró que dispone de los medios y programas que utiliza la NSA para espiar.

Hace tres años, el analista estadounidense reveló una trama de espionaje masivo de Estados Unidos y el Reino Unido en internet, tras lo cual se vio obligado a huir de su país y refugiarse en Rusia.

Pese a su estatus de refugiado, Snowden criticó algunas decisiones tomadas por el Kremlin, como la recién aprobada ley antiterrorista que abre la puerta al espionaje masivo de las comunicaciones es similar al que practica, según el informático, su país de origen.

Edward vive ahora en un país libre y tiene derecho de expresar cualquier opinión, lo que incluye un ámbito del que entiende muy bien", reaccionó a las últimas declaraciones de Snowden su abogado, Anatoli Kucherena.

FUENTE: www.minutouno.com

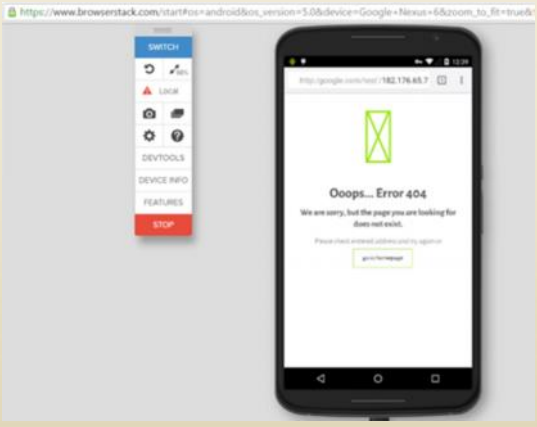
Detectan una vulnerabilidad en Chrome y Firefox que permite suplantar URLs

Que el navegador es una de las herramientas de software más utilizadas diariamente por miles de usuarios es una realidad innegable sobradamente conocida por la mayoría. Un panorama en el que, si bien contamos con múltiples opciones, Google Chrome y Mozilla Firefox cuentan con la mayor parte del pastel.

Y precisamente es de ambos de los que nos vemos obligados a hablar hoy –y no precisamente por sus cuotas de adopción como en anteriores ocasiones- sino con motivo de una vulnerabilidad que permitiría suplantar URLs en estos navegadores. Pero, ¿en qué consiste exactamente?

El investigador de seguridad Rafay Baloch que, en su blog Rafayhackingarticles ha explicado cómo opera el fallo detalladamente. Un funcionamiento muy sencillo que aprovecha un simple truco para saltarse la capa de seguridad de los citados browsers y poder suplantar una dirección aparentemente válida, por otra falsa.

En concreto, el quid de la cuestión radica en la manera en la que los navegadores gestionan las URLs que mezclan los formatos RTL (árabe) y LTR (romano). Según apunta Balock, tanto Firefox como Chrome podrían llegar a confundirse con ellos –o sea, con el orden-. Por ejemplo y para que te hagas una idea, en este último, la dirección 158.10.230.11/l/http://google.com, la convertiría en http://google.com/l/158.10.230.11.



Un bug que, de manera sencilla, podría convertirse en un arma. Es decir, los ciberdelincuentes, entre otros, tendrían la opción de generar una URL al estilo google.com/fakepath/fakepath/fakepath / … /127.0.0.1 - que dé a entender al usuario que está en un dominio de Google cuando, realmente, está accediendo a otro lugar totalmente distinto que puede comprometer su seguridad.

Para acabar, parece que el problema ya ha sido solucionado –al menos en las versiones más recientes de estos navegadores- gracias a la colaboración del citado investigador. Una detección y un informe –la vulnerabilidad se ha registrado con el código CVE-2016-5367- que le han valido la recompensa de la cifra nada desdeñable de 5.000 dólares por parte del programa de Bug Bounty de Google.

FUENTE: www.genbeta.com

Ganadores concurso SCProgress

Nuestra empresa SCProgress, organizó una encuesta con la participación de todos nuestros socios, clientes y público en general, la misma que contenía preguntas sobre nuestros productos, servicios, tecnología y seguridad informática.

El día miércoles 24 de agosto de 2016, se realizó la revisión de las encuestas recibidas y la mejor puntuada, fue la del Sr. Pedro Cazame, quien recibió una hermosa Tablet Samsung Galaxy Tab E Lite.

Así también, los señores Daniel Maldonado y Edwin Cando, fueron los ganadores de fantásticos vasos deportivos.

Felicitaciones a todos los participantes, y nuestros sinceros agradecimientos por su confianza y fidelidad, seguiremos organizando eventos en los cuales tendrán la oportunidad de ganar fabulosos premios.

Síguenos en nuestras redes sociales, a final del mes de Septiembre se entregará otra tablet de iguales características, a otro experto en nuestras líneas de productos SCProgress.

¿Seguridad informática o seguridad de la información?

En el día a día de las personas que trabajan directamente en las áreas de sistemas o Tic's, siempre pronunciamos las frases: "seguridad informática" o "seguridad de la información", que pueden escucharse iguales, pero su significado son totalmente distintos.

Debemos tener claro la diferencia entre cada una de ellas, y saber a cuál de ellas vamos a dirigir nuestro mayor esfuerzo, para proteger al activo más importante de cualquier institución o empresa.

Seguridad informática.- *"esta disciplina se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo"*. [Jeimy J. Cano, Ph.D., CFE.].

Seguridad de la información.- "es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información". [Jeimy J. Cano, Ph.D., CFE.].

Si bien existe una diferencia entre las dos, sin embargo coinciden en que se encuentran encaminadas a conseguir un objetivo común.

Seguridad Informática:	Seguridad de la Información:
• Se centra en proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización (utilizando hardware y software), y que estas sean utilizadas de la manera indicada por la Organización. • Su análisis de riesgos se centra en vulnerabilidades del hardware o software, y llevar el nivel de riesgo a nivel aceptable por la organización.	• Su propósito es proteger la información de una Organización, independientemente del lugar en que se localice: impresos en papel, en discos duros de las computadoras o incluso en la memoria de las personas que la conocen. • Tiene tres principios fundamentales: **Confidencialidad, Integridad y Disponibilidad** de la información. • Su acción cubre Análisis de Riesgos, Seguridad del Personal, Seguridad física y del entorno, Gestión de comunicaciones, Desarrollo y Mantenimiento de Sistemas, Control de Accesos, Gestión de Incidentes, y Continuidad de Negocio entre otros (de acuerdo a la ISO 27000) • Busca mantener el riesgo en la gestión de la información por debajo del nivel asumible por la propia organización

FUENTES: www.seguridadinformacioncolombia.blogspot.com, www.seguridadparatodos.es

Rincón de los Expertos

Los expertos utilizan las siguientes fuentes de información, donde podrán encontrar los últimos adelantos científicos y tecnológicos.

https://www.forrester.com/

https://451research.com/research

https://www.cepol.europa.eu/science-research/conferences/2015

Dance like no one is watching. Encrypt like everyone is.

Empresas o personas interesadas en promocionarse en nuestra revista, por favor contactarse con c.delatorre@scprogress.com

www.scprogress.com

Septiembre 2016