Internet y nuevas tecnologías

ROBERTO PLÁ
Coronel de Aviación
http://robertopla.net/

ANGELA MERKEL, VICTIMA DE UN TROYANO

Una muestra muy didáctica de cómo actúan los troyanos y cómo los baluartes supuestamente más seguros están expuestos a sus ataques, la hemos visto a través de una noticia difundida a mediados del mes de junio, aunque con unos titulares y una difusión muy discreta hasta el momento en que escribo esto, una semana después de los hechos. El blog 'El Hacker' -que a su vez reproduce una noticia del dominical alemán "Bild am Sonntag"- se hacía eco de que el ordenador que la canciller alemana usa en el Bundestag había sido infectado por un Troyano que fue detectado en el parlamento alemán la segunda semana de junio. El asaltante tomó el control de la cuenta de correo del ordenador y envió, con el remite de la poderosa política alemana, un mensaje convocando a una conferencia.

Muchos de los diputados que recibieron la invitación no dudaron ni por un momento de su autenticidad y aquellos que siguieron el enlace que contenía el mensaje fueron víctimas de una nueva infección. Los investigadores de seguridad declararon haber encontrado hasta quince ordenadores conectados a la red del Bundestag infectados hasta el viernes 12 de junio al mediodía, solo unos días después del suceso.

Al parecer en cinco de ellos se había producido un robo de datos, aunque desde las fuentes de la investigación no se reveló si ese robo de datos afectó también a la Canciller. Hay que tener en cuenta que en el ordenador de un parlamentario puede encontrarse información de lo más suculenta para criminales, servicios secretos, gobiernos amigos o enemigos y grupos financieros.

Es importante entender que si los ordenadores que supuestamente están más protegidos son vulnerables a este tipo de asaltos es porque la presión de la amenaza es constante y que las medidas de protección continuas y la desconfianza de cualquier mensaje o hacho sospechoso en nuestras comunicaciones, lejos de ser un rasgo paranoico, es una actitud necesaria que no solo va dirigida a proteger las fotos de nuestras vacaciones sino las direcciones de nuestros contactos, su confianza depositada en nuestro sentido común, nuestro trabajo y a veces incluso nuestro prestigio profesional y social.

http://delicious.com/rpla/raa845a

EL FALSO AVISO DE CORREOS

¿Por qué hay que ocultar siempre las direcciones en los correos que enviamos a una lista de usuarios utilizando el campo 'CCO:' del programa de correo electrónico?. Porque si no lo hacemos así, las direcciones no solo quedan visibles a todos los receptores, sino que también quedan al descubierto en todos sus servidores de correo, y un buen número de direcciones de cuentas corporativas pueden ir a parar a alguna de las listas utilizadas “por el lado oscuro” para enviar mensajes maliciosos, y está claro que no me refiero a chistes picantes o indecorosos, sino a algo bastante más desagradable.

Algo como la reciente oleada de mensajes con avisos falsos, supuestamente procedentes de Correos y que en realidad ocultaban la acción de un peligroso virus conocido como Criptolocker.

Popularizado a finales de 2013, este virus repite sus oleadas de ataques utilizando nuevas 'envolturas'. Diferentes mensajes falsos ocultan al mismo virus. La última oleada detectada son estos supuestos mensajes de Correos, escritos en un castellano incorrecto y que nos notifican que nos ha llegado un envío y que si no lo recogemos en correos, nos cobrarán una cantidad diaria. El camuflaje no es muy sofisticado, porque es fácil sospechar de un mensaje de un servicio público o compañía española que nos escribe de forma tan absurda y quien más quien menos ha recibido un aviso de correo y sabe que en caso de no recoger un envío, este simplemente es devuelto.

Sin embargo, las prisas del mundo moderno o la obcecación de un momento, nos pueden llevar a hacer 'clik' sobre el enlace que nos ofrece información o aclaraciones sobre el confuso mensaje. También podemos caer en la trampa porque en el asunto y destinatario del correo puede haber información del usuario al que va dirigido específicamente, como en nuestro caso, su empleo, destino, Ejército y nombre, lo que puede ha-

cer creer al usuario que lo recibe que es un correo legítimo.

Al seguir el enlace, disfrazado a veces como un archivo pdf, el programa que carga el virus se ejecuta en nuestro ordenador, dando inicio a un buen dolor de cabeza.

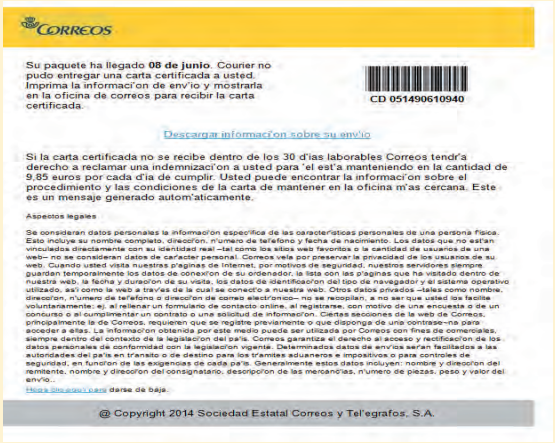
La actuación de Criptolocker consiste en cifrar nuestro disco duro. A continuación nos pide un rescate para recuperar los archivos cifrados. Si tenemos buenas costumbres como hacer una copia de seguridad diaria, lo más sencillo es limpiar el ordenador y restaurar la copia de seguridad. Pero sinceramente, ¿recuerda cuando hizo la última copia de seguridad?. Porque, aunque se borre el virus, los archivos siguen encriptados. Y por supuesto, pagar no sirve para nada.

Lo mejor es no bajar la guardia. Como la toma y el despegue en un avión, la lectura del correo es un momento crítico en el que los peligros nos acechan desde el mundo exterior a través de esa ventana que les abrimos para que entren en nuestro ordenador, nuestra red, nuestra vida.

El autor de Criptolocker es el ruso de 31 años Evgeniy Bogachev, reclamado -sin mucho éxito- por el FBI, a cambio incluso de una recompensa de tres millones de dólares. El ataque se realiza desde servidores localizables, ubicados en un país de la comunidad Europea. Y sin embargo, las garantías legales y otros enredos burocráticos impiden actuar contra la fuente de la infección.

En este estado de la cuestión, la principal recomendación es discreción y responsabilidad al custodiar y usar las direcciones de nuestros contactos. Hacer copias de seguridad frecuentes de nuestros datos vitales. Sospechar de cualquier mensaje de correo extraño, mal escrito, con noticias alarmantes y que nos invita a seguir un enlace o a abrir un archivo adjunto. Sospechar incluso si viene de un amigo o conocido y nos sugiere ver algo muy divertido o espectacular: La curiosidad mató al gato.

En los entornos corporativos, es importante dar parte de cualquier sospecha. Aquí no te revientan el coche


CORREOS

Su paquete ha llegado **08 de junio**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 051490610940

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 9,85 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Aspectos legales

Se consideran datos personales la informaci'on espec'ifica de las caracter'isticas personales de una persona f'isica. Esto incluye su nombre completo, direcci'on, n'umero de tel'efono y fecha de nacimiento. Los datos que no est'an vinculados directamente con su identidad real –tal como los sitios web favoritos o la cantidad de usuarios de una web– no se consideran datos de car'acter personal. Correos vela por preservar la privacidad de los usuarios de su web. Cuando usted visita nuestras p'aginas de Internet, por motivos de seguridad, nuestros servidores siempre guardan temporalmente los datos de conexi'on de su ordenador, la lista con las p'aginas que ha visitado dentro de nuestra web, la fecha y duraci'on de su visita, los datos de identificaci'on del tipo de navegador y el sistema operativo utilizado, as'i como la web a trav'es de la cual se conect'o a nuestra web. Otros datos privados –tales como nombre, direcci'on, n'umero de tel'efono o direcci'on de correo electr'onico– no se recopilan, a no ser que usted los facilite voluntariamente; ej. al rellenar un formulario de contacto online, al registrarse, con motivo de una encuesta o de un concurso o al cumplimentar un contrato o una solicitud de informaci'on. Ciertas secciones de la web de Correos, principalmente la de Correos, requieren que se registre previamente o que disponga de una contrase–na para acceder a ellas. La informaci'on obtenida por este medio puede ser utilizada por Correos con fines de comerciales, siempre dentro del contexto de la legislaci'on del pa'is. Correos garantiza el derecho al acceso y rectificaci'on de los datos personales de conformidad con la legislaci'on vigente. Determinados datos de env'ios ser'an facilitados a las autoridades del pa'is en tr'ansito o de destino para los tr'amites aduaneros e impositivos o para controles de seguridad, en funci'on de las exigencias de cada pa'is. Generalmente estos datos incluyen: nombre y direcci'on del remitente, nombre y direcci'on del consignatario, descripci'on de las mercanc'ias, n'umero de piezas, peso y valor del env'io.

Haga clic aqu'i para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Tel'egrafos, S.A.

al desactivar una bomba. Los compañeros que se dedican a defender la red de los asaltos de los malos, usan cada proyectil lanzado por el enemigo como fuente de información para localizarlo y obtener información de sus métodos para protegernos mejor.

http://delicious.com/rpla/raa845b

ROMBERTIK, EL MALWARE SUICIDA

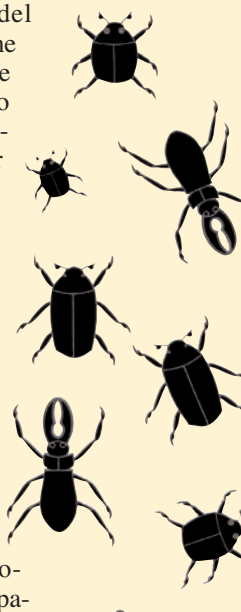
Los virus son discretos. La mayoría de este malware está diseñado para no alertar al usuario víctima de la infección. En primer lugar, la discreción permite al malware seguir infectando a otras víctimas, frecuentemente a través de los datos que encuentra en el propio sistema afectado.

En segundo lugar, actualmente, la tendencia mayoritaria en el malware no es la de realizar espectaculares acciones que obtengan repercusión para aumentar el ego de su creador, sino un puro interés crematístico. Los criminales informáticos del momento buscan información que vender o el control de un gran número de ordenadores (las redes de ordenadores 'esclavos' involuntarios o 'botnets') con los que realizar ataques de denegación de servicio, campañas de envío de spam y otras acciones por cuenta propia o con carácter mercenario para el mejor postor.

En cualquier caso, el malware, como el espía, trata de ser sigiloso para sobrevivir y continuar realizando su perversa actividad.

Hasta el momento los virus y troyanos habían recurrido a la metamorfosis para ocultarse a los programas antivirus. Incluso algunos estaban preparados para neutralizar o incluso atacar y destruir a los programas antivirus que encontrasen, pero una nueva técnica ha sido detectada en la actuación de un malware conocido como Rombertik. Este virus de tipo 'troyano' detecta los intentos de detección y rastreo de los programas antivirus y antes de ser neutralizado, destruye el disco duro en el que se aloja, intentando borrar por este método tan drástico toda huella que pueda delatar su funcionamiento.

Según han podido descubrir los analistas hasta un 97% de su código es innecesario y está destinado a ralentizar la acción de los análisis de seguridad, mientras destruye el sector de arranque del disco anfitrión e imprime mensajes mofándose de las acciones del escaneo de seguridad. Si no puede acceder al sector principal de arranque (MBR) del disco, de forma similar a como hacen los programas que 'secuestran' información, conocidos como "ramsomware", el virus Rombertik encripta los archivos del directorio principal del usuario.



Mientras no es detectado, el virus inyecta código en Explorer, Firefox, o Chrome para que le proporcionen la información que intercambia el usuario en conexiones seguras antes de ser encriptada, enviándola a través de internet al controlador remoto que explota su acción.

http://delicious.com/rpla/raa845c

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto