2014-01-06

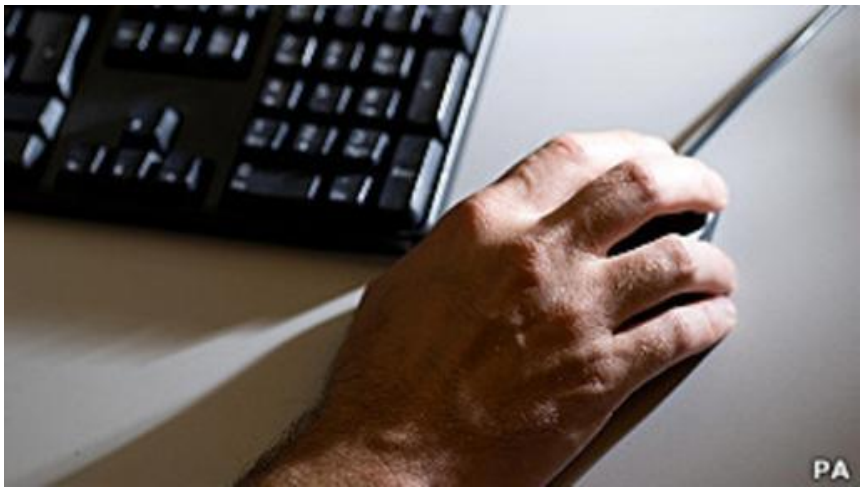
Boletín de Noticias de Seguridad Informática #20

SCProgress

www.scprogress.com

ÍNDICE

NOTICIA 1: Un malware ha infectado alrededor de 250.000 computadoras



Los investigadores aseguran que los cibercriminales atacan a internautas que navegan desde sus hogares.

Una forma virulenta de un software malicioso ha infectado alrededor de 250.000 computadoras Windows, señalaron investigadores de seguridad informática.

Cryptolocker, como se le conoce, codifica la información de los usuarios (fotos, videos, documentos) que ataca y posteriormente pide un pago para desencriptarlos, mientras corre un cronómetro.

Es una especie de operación de "rescate" contrarreloj con la que se presiona al afectado para que pague para que su información sea liberada, señaló el experto en Tecnología de BBC Mundo, David Cuen.

Analistas de Dell Secureworks señalaron que Estados Unidos y el Reino Unido han sido los países más afectados.

De acuerdo con los expertos, los cibercriminales están atacando a cibernautas caseros, después de haberse enfocado en profesionales.

La empresa ha proporcionado una lista de dominios de los que sospecha han sido usados para propagar el código, pero advirtió que más códigos se están generando cada día.

Este tipo de software malicioso ha existido desde 1989, pero este último ejemplo es particularmente problemático por la forma en que hace inaccesibles a los archivos, indicó el periodista de Tecnología de la BBC, Leo Kelion.

Fuente: http://www.bbc.co.uk

NOTICIA 2: Su tarjeta SD, un nuevo alojamiento para el malware

Fuente imagen: http://www.como-limpiar.com

Descubren un sistema para hackear los microcontroladores de las tarjetas SD, instalando un malware que intercepta los datos privados de los que las usan.

Dos investigadores de seguridad informática han encontrado una manera de hackear tarjetas SD, la forma más común de las tarjetas de memoria flash que se utilizan para almacenar datos de teléfonos móviles y cámaras digitales, y ejecutar en ellas un software que intercepta los datos de sus usuarios.

El método para instalar software malicioso en las tarjetas consiste en hackear los pequeños chips controladores de estos dispositivos de almacenamiento. Según explicaron Andrew *Bunnie* Huang y Sean *Xobs* Cross en el Chaos Computer Congress (30C3), una persona puede ejecutar el malware en la propia tarjeta de memoria. Eso es porque las tarjetas tienen pequeños microcontroladores integrados que se utilizan para supervisar los detalles del almacenamiento de datos.

Como resultado, los datos privados de las personas que usan estas tarjetas podrían quedar expuestos. "Es un escenario perfecto para un ataque man-in-the-middle (en el que el atacante puede observar e interceptar mensajes entre las dos víctimas)", dijo Huang durante la charla. "El enfoque actual del almacenamiento de memoria flash ha invitado a alguien a sentarse en medio de nuestros datos, y sólo confiamos en ellos para hacer lo que quieren hacer", continuó.

Huang y Cross creen que este tipo de ataque podría utilizarse para copiar secretamente o modificar datos confidenciales, como claves de cifrado, o para subvertir los procesos de autenticación mediante la sustitución de un archivo no autorizado para su ejecución en lugar del archivo real que fue autorizado, informa CNET.

Esta vulnerabilidad funciona, en principio, no sólo con tarjetas SD, sino también con otros dispositivos de almacenamiento basados en memoria flash, como los SSD, que se usan en lugar de los tradicionales discos duros en los ordenadores portátiles y de escritorio, y los eMMC, empleados en los teléfonos móviles. El agujero concreto hallado por Huang y Cross no se aplica a todos los dispositivos de memoria flash porque depende del microcontrolador específico usado. Sin embargo, consideran que el enfoque es generalmente eficaz, ya que todos los dispositivos flash se basan en este tipo de controladores.

Fuente: http://www.itespresso.es

NOTICIA 3: Advierten de un malware masivo que roba SMS en Android

La firma de seguridad FireEye ha advertido de un peligroso malware llamado MisoSMS que circula en la plataforma Android capaz de robar mensajes SMS y filtrarlos a ciberdelincuentes. El software proviene de China y ha sido descrito como "uno de los 'botnets' más avanzados hasta la fecha". FireEye ha informado de que se está usando en más de 60 campañas de 'spyware'.

La compañía de seguridad ha rastreado las infecciones de dispositivos Android en Corea y así ha descubierto que los atacantes se conectaban desde Corea, China y otras localizaciones para leer los SMS robados.

El equipo de investigación ha anunciado que hay un total de 64 campañas 'botnet' del 'malware' conocido como MisoSMS que utiliza más de 450 cuentas de correo electrónico maliciosas.

MisoSMS infecta los sistemas Android instalando una 'app' llamada Google Vx, que se disfraza como una aplicación de configuración nativa del teléfono para tareas administrativas. La aplicación roba los mensajes personales del usuario y los envía a los ciberdelincuentes.

Uno de los investigadores de FireEye, Vinay Pidathala, ha explicado que mientras que "algunos programas de 'malware' envían el contenido de los mensajes de los usuarios a otros números de teléfono bajo el control del atacante", MisoSMS los envía a una dirección de correo electrónico.

Pithadala ha aclarado que todas las cuentas maliciosas identificadas se han desactivado como parte de la estrategia de mitigación de las autoridades en Corea y China.

Fuente: http://www.europapress.es

NOTICIA 4: Los virus más retorcidos de 2013

Fuente imagen: http://www.audienciaelectronica.net

2013 ha confirmado una tendencia que ya se había detectado hace tiempo: hemos entrado en la era de las amenazas de seguridad informática post PC, y los virus, gusanos y *malware* pueden atacarnos ahora desde la palma de nuestra mano, es decir, desde nuestro *smartphone*. Pero hay algo que no cambia: las tretas y el ingenio de los ciberdelincuentes a la hora de engañarnos para que hagamos clic en ese enlace que tantos disgustos puede causarnos. Repasamos algunos de los virus más retorcidos de los que hemos oído hablar en este año que ya termina.

El virus de la policía

2013 fue el año en el que fue desmantelada en la Costa del Sol una célula que había logrado estafar un millón de euros al año a través de un *ramsonware* conocido como "el virus de la policía". Éste consistía en un programa informático que bloqueaba el ordenador de las víctimas acusándolas de haber consumido pornografía infantil, e instándolas a pagar una multa de cien euros para liberar su equipo. ¿Que cómo es posible que tantos ciudadanos que no tuvieran nada que ver con contenidos pedófilos *picasen*? Nos lo explicaba el analista de seguridad de Trend Micro David Sancho: por algo tan humano y básico como el sentimiento de culpa. El experto nos contó que este virus solía ser inoculado a los equipos a través de webs con contenido porno, no infantil, pero sí pornográfico, de forma que sus usuarios se veían abrumados por su propia vergüenza y preferían no decir nada.

San Valentín

Como todos los años, la festividad de los enamorados es aprovechada para infectar los equipos de muchos incautos bajo reclamos amorosos. Las redes sociales se convirtieron en 2013 en un caldo de cultivo perfecto para enlaces de supuesta descarga de tarjetas, regalos y ofertas para regalar a nuestra pareja que, en realidad, no eran más que la puerta a un ciberataque.

Un virus que se disfraza de Pony

Uno de los *malwares* que más estragos ha causado en este tercer trimestre de 2013 ha sidoPony, llamado así porque su icono es, precisamente, el del pony del juego social de Facebook Farmville. Bajo esa inocente máscara, Pony ha robado más de dos millones y medio de credenciales personales de acceso a cuentas de Gmail, Twitter, Facebook o LinkedIn.

La maratón de Boston

El *spam* suele utilizar tragedias que despiertan la conmoción colectiva como gancho, y así lo hizo este año con el atentado que tuvo lugar durante la maratón de Boston. En los días posteriores al suceso, se calculó que un 20% de los mensajes de *spam* que circulaban en la red contenían palabras clave relacionadas con estos atentados. Estos contenían enlaces a supuestas webs donde se narraban los acontecimientos, pero en realidad llevaban a los internautas a sitios capaces de robarles sus contraseñas o de monitorizar su navegación.

Lily Collins y Aquaman

La actriz británica Lily Collins y el súperheroe Aquaman han sido las dos celebridades con más enlaces maliciosos vinculados a su nombre en la red en 2013. La protagonista de *Cazadores de sombras* encabeza el ranking, elaborado este año por McAfee, de "celebridades más virulentas". En la mayoría de los casos, el *malware* estaba asociado a búsquedas como "Lily Collins descargar gratis" y "Lily Collins fotos desnuda". En cuanto a Aquaman, uno de los fundadores de la Liga de la Justicia, este súperheroe fue elegido también por la firma de seguridad informática como "el más tóxico de todos", con una probabilidad del 18,6% de llevarnos a una web peligrosa.

Fuente: http://www.ticbeat.com