<< NOTICIAS DE SEGURIDAD INFORMÁTICA >>

www.scprogress.com

Nueva formas de hacer dinero ilegal: RansomWare

Todo comenzó hace casi 15 años (1989) con un paquete que era distribuido por correo postal a las empresas farmacéuticas. El paquete contenía un disquete con un programa (con supuesta información del SIDA) que evaluaba ciertas condiciones y cuando se daban las mismas, procedía a cifrar el disco rígido y presentaba una "factura" a la víctima para recuperar la clave de cifrado. El programa en cuestión se llamó AIDS.

Más tarde, en 1996, los hermanos Young (Adam y Moti) desarrollaron un concepto teórico en donde un virus utilizaba criptografía pública para cifrar información del usuario.

El estudio de esta nueva modalidad de virus fue bautizado como Criptovirología y desde entonces ha sido una disciplina únicamente utilizada en laboratorios.

Como se sabe, todo concepto puede ser usado para hacer daño, y en este caso se ha aprovechado parte del mismo, pero agregando un condimento de extorsión puramente económico, objetivo último de los nuevos desarrolladores de malware.

Así, el término sajón "Ransom" se define como la exigencia de pago por la restitución de la libertad de alguien o de un objeto, lo que en castellano se traduciría como "secuestro".

Si a esto agregamos la palabra software obtenemos RansomWare, definido como el secuestro de archivos a cambio de un “rescate”.

Esta nueva modalidad de virus ha visto la luz en mayo de 2005 con "PGPCoder", y regresado con el recientemente descubierto "CryZip". La modalidad de trabajo es la siguiente: el código malicioso infecta la computadora del usuario por los medios normalmente utilizados por cualquier malware y procede a cifrar los documentos que encuentre (generalmente de ofimática), eliminando la información original y dejando un archivo de texto con las instrucciones para recuperarlos.

En los casos mencionados el rescate ha sido el depósito de dinero en una cuenta determinada por el creador del código malicioso. Luego que el dinero es depositado, se le entrega al usuario la clave para descifrar los archivos.

Hasta ahora, y por ser los primeros especimenes "menos desarrollados", los métodos de cifrado han sido sencillos y fácilmente reversibles, lo que permite a los especialistas conocer la clave y evitar que los usuarios pierdan dinero.

Además, el modo de utilización de cuentas bancarias aún no se ha perfeccionado, lo que permite rastrearlas en forma relativamente sencilla.

Es fácil imaginarse que cuando estos métodos se perfeccionen ocurrirá lo inevitable: las técnicas de cifrado utilizadas se aproximarán al modelo de Young, utilizando criptografía simétrica fuerte, o incluso criptografía asimétrica, lo que imposibilitará el descifrado de los archivos.

Sería bueno preguntarse: ¿hay remedio a este nuevo tipo de ataques? La respuesta es que sí, a los actuales ataques sencillos sin criptografía avanzada, pero como ya he dicho es inevitable que este sistema de

secuestro se perfeccione y tienda a la Criptovirología y Kleptografía.

Cuando esto suceda la respuesta a la pregunta planteada será un rotundo NO y entonces sólo tendremos dos caminos posibles: realizar copias de seguridad de nuestra información en forma periódica, y contar con una defensa preactiva para nuestros sistemas, que nos proteja en todo momento de amenazas conocidas y desconocidas.

NOTA: La criptografía simétrica utiliza una clave que es la que permite cifrar y descifrar los archivos.
La criptografía pública o asimétrica hace uso de dos claves: una pública y otra privada.
La información cifrada con una es descifrada con la otra. En nuestro caso la información del usuario sería cifrada con clave pública del creador del virus y solo sería descifrada con la privada, que solo él tiene y entregaría a quien pague el rescate.

EVENTO:

Los días 7 y 8 de Junio se desarrollara el ***4ª Congreso Internacional en Sistemas e Informática*** en la **Escuela Politécnica del Ejército,** sede Sangolquí.

En este evento se trataran las últimas tendencias en desarrollo de software, seguridades informáticas y tecnologías de redes de computadoras.

Para mayor información escriba a:

fgalarraga@espe.edu.ec , gnacato@espe.edu.ec , adelatorre@espe.edu.ec

Telf: (593-2) 2338831 ext 2621

NOTA DEL EDITOR

En el mundo contemporáneo, la implementación de sistemas que prevengan a los usuarios contra los efectos negativos de virus y spam a través del correo electrónico es una necesidad impostergable, ya que la caber-delincuencia cada vez encuentra otras formas de afectar a los intereses de los usuarios de tecnología. Es responsabilidad de cada Proveedor de Servicios de Internet buscar la mejor forma de proteger a sus clientes contra el fraude informático.

Atentamente

Arturo de la Torre

Venta y distribución de Sistemas
Antivirus y Antispam
Servidores HP e Intel
Equipos de Comunicaciones
Consultorias - eLearning

Oficina
Teléfonos: 2900 916 ; 09 6004105; 09 6105959
vscp@scprogress.com , vscp@rdyec.net
Quito – Ecuador

Si el contenido de este mensaje no es de su interés, lamentamos que le haya llegado: mil disculpas. Para no volver a recibir esta información responda a este e-mail e incluya en el asunto la palabra.
"UNSUSCRIBE"
De acuerdo a la Ley de Comercio Electrónico del Ecuador y su Reglamento publicado en el Registro Oficial 735 de 31 de diciembre de 2002, Decreto No.3496, Artículo 22.- Envío de mensajes de datos no solicitados, usted puede pedir el cese del envío de información en cualquier momento, siendo nuestra obligación legal cesar los envíos ante su solicitud. Todo mensaje electrónico que cuente con la opción de de-suscripción no se considera SPAM