Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

# ¿De qué nos podemos fiar...? (142 lectures)

Per **LauraCeldranS**, ***LauraCS*** (http://laura.celdran.name)

Creado el 17/01/2006 10:57 modificado el 17/01/2006 10:59

> *Tal día como hoy en Hispasec se comenta ...*
>
> Históricamente se han considerado archivos potencialmente peligrosos para Microsoft Windows los que poseían las muchas extensiones de aplicaciones ejecutables que existen. En su código es posible ocultar cualquier acción dañina para el sistema, y puede ser disimulada y pasar desapercibida par el usuario. EXE, VBS, PIF, SRC, VBS, BAT y un largo etcétera, son extensiones de las que hemos aprendido a desconfiar hace tiempo. Desde hace poco, sin embargo, se pueden unir al conjunto de sospechosas muchas otras que se han considerado desde siempre confiables.
>
> Pero lo más agrabante es que no sólo los usuarios de Microsoft deben preocuparse
>
> *¿De qué nos podemos fiar...?*[1]

De un tiempo a esta parte, se ha popularizado el uso de archivos con extensiones históricamente confiables con la finalidad de difundir código malicioso. El ejemplo más claro y conocido ha ocurrido con la vulnerabilidad de procesamiento de **WMF** (Windows Meta File) que permitía la ejecución de código arbitrario en el sistema con la simple visualización de una imagen. Este fallo ha permitido la dispersión de virus ocultos bajo aparentemente inofensivas imágenes con formatos **JPG o GIF** gracias a exploits muy potentes y sofisticados.

El mismo día 1 de enero de 2006 **VirusTotal** detectaba un fichero que fue enviado de forma masiva por correo electrónico y que simulaba una felicitación para el nuevo año. El archivo adjunto, una imagen en formato JPG, "HappyNewYear.jpg", comprometía el sistema con tan sólo visualizarla. A partir de ahí, se han recibido en VirusTotal más de diez variantes de malware con extensión JPG que aprovechaban la vulnerabilidad y algunas variantes con extensión GIF. Debido a la popularidad y facilidad para aprovecharse de esta vulnerabilidad, la previsión es que vayan en aumento.

**No sólo los usuarios de Microsoft deben preocuparse** por estas extensiones. En enero se han encontrado varias vulnerabilidades en Apple QuickTime que pueden se aprovechadas por atacantes para ejecutar código a través de formatos aparentemente inofensivos. Imágenes con formato QTIF, TGA, TIFF y GIF especialmente manipuladas y visualizadas con Apple **QuickTime Player versión 7.0.3 y anteriores (para Mac OS X y Windows)** permiten la ejecución de código en el sistema de la víctima.

Igualmente este mes, se ha identificado una vulnerabilidad en **BlackBerry Enterprise Server** (conocido servidor de comunicaciones inalámbricas) que puede ser aprovechada por atacantes remotos para ejecutar código arbitrario a través de un archivo PNG (Portable Network Graphics) especialmente manipulado y enviado como adjunto.

Por si fuese poco, cuando ya creíamos enterrados a los virus de macro que se extendían a través de documentos elaborados con la suite Microsoft Office y este formato se consideraba relativamente seguro, aparece un nuevo **fallo de denegación de servicio en Microsoft Excel** que se rumorea (aún está por confirmar) que puede llevar a la ejecución de código arbitrario con la simple visualización en Microsoft Office de una hoja de cálculo en este formato.

*Tras leer cosas como estas yo me planteo la siguiente cuestión ... si casi cualquier formato en cualquier momento de la historia ha sido o va a ser utilizado para explotar cierta vulnerabilidad, ¿llegará un momento que seamos unos paranoicos incapaces de abrir si quiera un correo que nos envíe nuestro propio jefe?.*

Lo que si que está claro es que yo no me ponía en el pellejo de cualquier administrador de correo de una compañía grande al que le exijan confirmar la seguridad del servicio... De todos modos Suerte a los administradores de correo.

---

**Lista de enlaces de este artículo:**

1. http://laura.celdran.name

---

E-mail del autor: laura _ARROBA_ laura.celdran.name
**Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=2270**