Departamento de Seguridad Informática MINSAP

Abril 2017

Volumen 1, nº 1

Boletín de Seguridad Informática

Contenido:

Puntos de interés especial:

-Copiar nuestros archivos a otro medio extraíble, recurrir a un servicio FTP o un servidor NAS puede ser algunos gestos que mejoran sin lugar a dudas el resultado final.

-Descargar archivos de Internet es una acción que hay que realizar con cierta prudencia. .

-La firma digital en documentos se utiliza para: Poder verificar la autoría del archivo (autenticación), verificar que el documento no ha sido modificado (integridad) y adjudicar la autoría innegable del archivo (no repudio).

Tan importante es hacer copias de seguridad como dónde almacenarlas

Poco a poco los usuarios se mentalizan de que resulta importante realizar copias de seguridad de la información almacenada en dispositivos de forma periódica. Esto es lo único que puede permitir la recuperación de información ante un fallo hardware o la presencia de un virus informático. Sin embargo, **¿es recomendable almacenar estas copias de seguridad en el propio equipo?**

No vamos a dejar escapar la oportunidad para contestar en primer lugar a la pregunta: No. Realizar una copia de seguridad de forma manual o ayudándonos de un programa y almacenar el archivo generado en el propio equipo no sirve para nada. No queremos ser tan radicales, pero sí es cierto que la práctica deja de ser eficaz.

Copiar nuestros archivos a otro medio extraíble, recurrir a un servicio FTP o un servidor NAS puede ser algunos gestos que mejoran sin lugar a dudas el resultado final.

A continuación, os ofrecemos los motivos para no dejar las copias de seguridad realizadas en el propio equipo.

Fallo de un componente hardware.

No importa que hablemos de un SDD o de un HDD, ambos son sensibles sufrir fallos, de ahí que sea muy importante extraer la información de forma periódica o redundarla recurriendo a algún RAID, aunque este método no es inmune a los virus informáticos.

Presencia de virus informáticos.

Además del problema comentado con anterioridad, no hay que olvidarse de las amenazas software. Los virus informáticos son un problema en la actualidad para copias de seguridad. Los conocidos como *ransomware* no solo se centran en cifrar la información, también buscan carpetas en las que puedan encontrar copias de seguridad y proceden a su cifrado o borrado.

Tal y como puede observarse, en caso de infección *malware* poco se puede hacer si nos encontramos ante un software de esta familia.

Disponibilidad limitada.

Sobre todo, si hablamos de equipos de sobremesa. A donde queremos llegar es que, en el caso de necesitar la información en otro lugar, deberíamos cargar con la torre. Sin embargo, en un servicio FTP, NAS, disco duro externo o memoria USB dispondremos de un acceso mucho más fácil y desde cualquier lugar y momento.

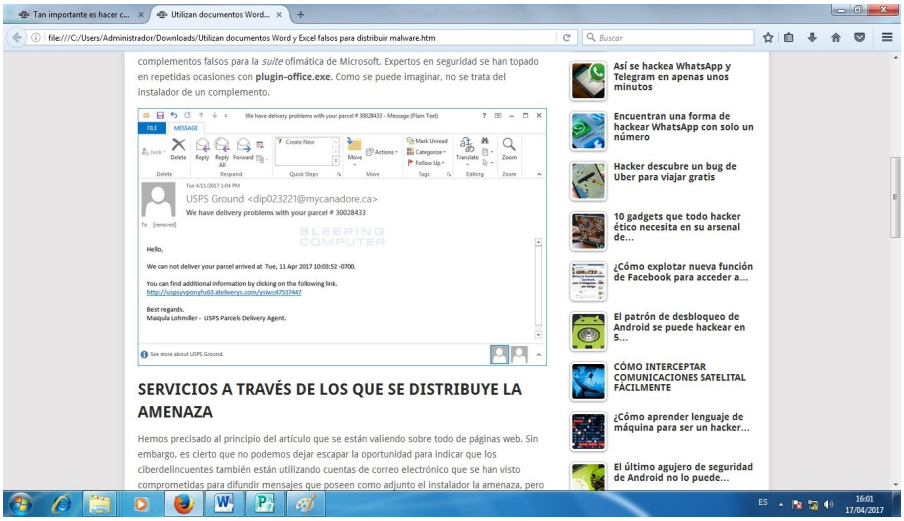
Copias de seguridad: Sí, pero tampoco en la nube.

Hay que tener en cuenta de qué estamos hablando. En muchos casos, la información puede ser importante, y almacenarla en un servicio de terceros nos obliga a depender de su seguridad. Ya hemos comprobado en el pasado que no son infalibles y que en cualquier momento se pueden ver sorprendidos por hackers. Por este motivo, desde RedesZone os animamos a que como medio de almacenamiento de las copias de seguridad se utilicen dispositivos NAS o bien memorias USB o discos duros externos con la información cifrada, ya que en caso de pérdida no se podrá acceder a la información.

Samba o FTP tal vez sean los mejores servicios. También es cierto que cada vez son más los fabricantes que optan por incluir un software que te permite almacenar tus archivos en una nube creada por ti mismo en tu hogar.

Las formas de almacenamiento son varias, ahora solo falta que cada uno escoja la que más se adapte a sus necesidades.

Utilizan documentos Word y Excel falsos para distribuir malware



Descargar archivos de Internet es una acción que hay que realizar con cierta prudencia. Los ciberdelincuentes se aprovechan del desconocimiento y confianza ciega que muestran los usuarios para distribuir *malware*. Podría decirse que esto es lo que está sucediendo en la actualidad. Se están valiendo de documentos Word y Excel falsos para que los usuarios descarguen un nuevo *ransomware*.

Aunque no se trata de una amenaza nueva, sí es cierto que se trata de una evolución de CryptoMix. Ha tenido bastante protagonismo en los últimos meses y parece bastante evidente que la publicación de variantes es una forma que posee los ciberdelincuentes para alargar la vida de esta amenaza informática. Mole es el nombre de la amenaza que nos ocupa.

Tal y como hemos comentado al comienzo, los ciberdelincuentes están utilizando documentos falsos de Word y Excel para distribuir la amenaza. O lo que es lo mismo, el usuario cree que está descargando un .docx o .xls. Sin embargo, el archivo final posee una extensión .exe. Es decir, el instalador del *ransomware* que hemos citado con anterioridad.

Es necesario mencionar que además de esta forma de distribución también están recurriendo a complementos falsos para la *suite* ofimática de Microsoft. Expertos en seguridad se han topado en repetidas ocasiones con **plugin-office.exe**. Como se puede imaginar, no se trata del instalador de un complemento.

Servicios a través de los que se distribuye la amenaza.

Hemos precisado al principio del artículo que se están valiendo sobre todo de páginas web. Sin embargo, es cierto que no podemos dejar escapar la oportunidad para indicar que los ciberdelincuentes también están utilizando cuentas de correo electrónico que se han visto comprometidas para difundir mensajes que poseen como adjunto el instalador la amenaza, pero siempre haciendo mención a documentos de la *suite* de ofimática de los de Redmond o instaladores de complementos.

Funcionamiento de Mole.

Cuando el usuario realiza la apertura del archivo aparece a simple vista un

texto genérico. En este mensaje el usuario solo posee la opción "OK". En realidad, se trata de un mensaje de UAC enmascarado. Pulsando en el único botón existente el usuario otorga al instalador permisos de administrador.

Esto desencadenará la ejecución del archivo **C:\Windows\SysWOW64 \wbem\WMIC.exe**. Este hará uso del archivo que anteriormente se ha descargado el usuario.

Posteriormente, el usuario visualizará un mensaje de UAC para otorgar permisos de cambios en el equipo al ejecutable citado con anterioridad. En la mayoría de los casos el usuario no se lo pensará dos veces y pulsará en la opción "Sí".

Pulsado este botón, el *ransomware* comenzará con su actividad con privilegios de administrador.

Consecuencias para el usuario y su equipo.

Aunque no lo hemos mencionado aún, indicar que esta amenaza afecta a equipos Windows con versión 7 o superiores.

Una vez ejecutado, en primer lugar genera un ID que identificará al equipo infectado, enviado al servidor de control remoto de forma instantánea. Una vez hecho esto, comienza el cifrado de los archivos existentes en el equipo utilizando el algoritmo RSA de 1024 bits.

Si tienes copias de seguridad en el equipo no servirán de nada.

El problema de esta amenaza es que no solo limita la actividad al cifrado de los archivos. Posteriormente se centrará en desactivar procesos del sistema relacionados con mecanismos de seguridad, haciendo gala de los permisos de administrador de los que disfruta.

Una vez hecho esto pasará a centrarse sobre todo en detectar copias de seguridad y puntos de restauración y proceder a su eliminación y cifrado, haciendo inútil cualquier intento por parte del usuario de recuperar el acceso a la información. Muchos expertos en seguridad, a la vista de las consecuencias recomiendan realizar una instalación limpia del equipo Windows.

Herramientas para firma digital de archivos.

La firma digital en documentos se utiliza para: Poder verificar la autoría del archivo (autenticación), verificar que el documento no ha sido modificado (integridad) y adjudicar la autoría innegable del archivo (no repudio). En este post trata sobre unas herramientas para firma digital, algunas muy sencillas y otras que pueden funcionar como servidor para arquitectura en red. Estas herramientas son: XolidoSign, eParapher, SimpleAuthority y SignServer.

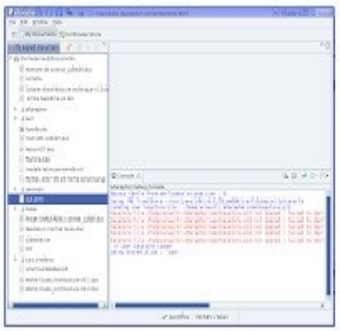
XolidoSign una herramienta de firmas digitales en documentos con DNI electrónico o con un certificado digital. Entre las características de XolidoSign destaca:

- Soporta muchos tipos de certificado digital.
- Permite firmar cualquier documento o archivo sin límite de tamaño: PDF, Excel, Word, Powerpoint, archivos txt, html, php, bases de datos, imágenes, diseños vectoriales, archivos 3D, vídeos, planos, música…
- Soporta firma PDF integrada o externa. Permite hacer visible o invisible el campo de firma en el propio documento PDF.
- Permite la firma de múltiples documentos y archivos de una sola vez. Robusto y sencillo.
- Comprueba la validez del certificado electrónico y el estado de revocación con la entidad emisora.
- Puede firmar con sello de tiempo integrado o realizar sello temporal independiente de los documentos o archivos.
- Añadiendo el sellado temporal al documento, archivo o firma, se puede garantizar su existencia en un momento determinado. XolidoSign permite utilizar cualquier servidor de sellado de tiempo.

Es una herramienta gratuita disponible solo bajo la plataforma Windows.

Más información o descarga: https://www.xolido.com/lang/xolidosign/

eParapher una herramienta que soporta casi todo tipo de archivos. Esta herramienta firma y convierte el archivo a tres posible estándares: Pdf, PDF/A, CMS y XML. Entre sus características destaca:



- Conversión y firma rápida de cualquier archivo de texto, imagen y archivos de Office u OpenOffice.
- Permite crear, suprimir, importar y exportar certificados y llaves privadas.
- Soporta los archivos de almacenamiento de llaves: PKCS#12, JKS, JCEKS y BKS.
- Permite utilizar certificados de Windows y SmartCards.

eParapher está disponible para las plataformas: Windows, MacOSX y Linux.

Más información y descarga de eParapher:
http://maven.eparapher.com/index.html

SimpleAuthority una autoridad de certificación (CA). Genera las claves y los certificados proporcionando identidades digitales criptográficas para usuarios de tu sistema. SimpleAuthority esta diseñada para ser fácil de utilizar y no requiere una base de datos externa ni componentes adicionales.

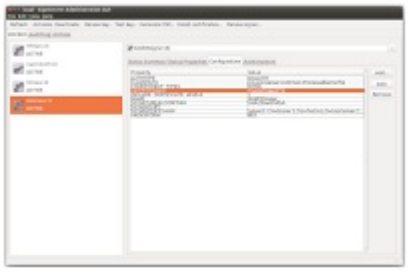
SimpleAuthority se puede utilizar para generar certificados digitales para: firma digital y el cifrado del email, acceso a través de de VPN, proporcionar un alto nivel de seguridad en la autentificación de usuarios en el sistema operativo, cliente SSL para autentificar un usuario en un servidor Web.

Esta CA esta disponible para las plataformas Windows y Macintosh. Es una herramienta muy útil para aumentar la seguridad de la información en redes pequeñas en la plataforma Windows en las que no se emplea un dominio y se opera en grupo de trabajo.

Más información y descarga de SimpleAuthority:
http://simpleauthority.com

SignServer es una herramienta bajo licencia LGPL v2.1 para firmar digitalmente documentos y código, manteniendo las claves de firma en un almacenamiento seguro, sin perjudicar los flujos de trabajo, haciéndolos seguros y auditables. SignServer es una aplicación servidor que atiende llamadas de otros sistemas. Es flexible y se puede personalizar a las necesidades específicas. Posee plugins para diferentes tipos de firma. Las claves de firma se mantienen seguras en el lado del servidor y los usuarios se autentican para realizar firmas en línea.

Entre sus características destaca:



- Autoridad de firma digital de tiempo compatible con RFC 3161 y MS Authenticode.
- Firmas para diferentes documentos: PDF, XML, ODF, OOXML, MRTD (ePassport), XadES-BES y XadES-T.
- Contiene firmas de propósito general.
- Validadores para documentos: XML, XadES-BES y XadES-T.
- Marco de servicio de validación de certificados, para validar certificados que utilizan CRL u OCSP.
- EPassport: firmante de MRTD conforme a la OACI
- Permites tener claves de firma gestionadas en almacenes de llaves o módulos de seguridad de hardware PKCS # 11.
- Gestión centralizada de los firmantes, control de acceso y auditoria.
- Posee claves de firma individuales para cada usuario o una clave central para la organización.
- La interfaz gráfica de usuario o las API de integración, garantizan la integración en el flujo de trabajo.
- Múltiples interfaces de administración.
- Firma de documentos individuales o por lotes.
- Desarrollado para trabajar en cluster permitiendo una alta disponibilidad y máxima confiabilidad.
- Soporte para CRL y OCSP.
- Permite escribir sus propios plugins de firma y validación.

SignServer es una aplicación que realiza operaciones criptográficas para otras aplicaciones. Está destinado a ser utilizado en entornos en los que se supone que las claves están protegidas en hardware, pero no es posible conectar dicho hardware a aplicaciones empresariales existentes o donde las operaciones se consideran más sensibles para que el hardware tenga que protegerse con más cuidado. Otro uso es proporcionar un método simplificado para proporcionar firmas en diferentes aplicaciones administradas desde una ubicación de la empresa. Ha sido diseñado para alta disponibilidad y puede trabajar en cluster para una máxima fiabilidad.

SignServer viene con un Time-Stamp compatible con RFC 3161/5816 que atiende peticiones a través de HTTP o HTTPS autenticado por el cliente. Un firmante MRTD (documento de viaje de lectura mecánica, es decir, pasaporte electrónico). Un firmante de PDF que añade automáticamente una firma a un documento PDF cargado, un firmante de ODF que agrega automáticamente una firma a un documento de ODF

cargado, un OOXML Signer que agrega automáticamente la firma a un documento OOXML cargado y un servicio de validación utilizado para buscar la validación de un documento firmado.

Las firmas digitales centralizadas en un servidor proporcionan el máximo control y seguridad, permitiendo que los usuarios y aplicaciones firmen convenientemente documentos y código. De esta forma se obtiene la mayor seguridad mientras se ahorra tiempo y costos. En lugar de administrar pequeñas aplicaciones de firma digital, donde cada equipo tiene su propia solución, el uso de una solución de firma centralizada simplifica la administración, mejora la seguridad y reduce los costos. Un servidor de firma digital permite cubrir los aspectos de: cumplimiento de políticas y auditorias, protección de claves de firma y es mas fácil de controlar.

Chrome, Firefox y Opera vulnerables a un ataque Phishing indetectable.

Los navegadores web son las aplicaciones más vulnerables a todo tipo de ataques informáticos ya que son las aplicaciones que tienen contacto directo tanto con los servidores remotos como con el usuario.

Por ello, los desarrolladores de estos navegadores, como Google, Mozilla u Opera, entre otros, deben asegurarse de actualizar periódicamente los navegadores para evitar que existan fallos que puedan poner en peligro a los usuarios, aunque estos fallos no siempre se encuentran en los propios navegadores, sino que dependen de la ingeniería social de los piratas informáticos.

Un experto de seguridad chino ha detectado un nuevo ataque de phishing indetectable que engaña a los usuarios para hacerse con sus datos haciéndose pasar por páginas web como Apple, Google y eBay, entre otras.

Este tipo de ataque informático es una variante moderna de los “IDN homograph attacks“, una serie de ataques phishing detectados en 2001 que **utilizan caracteres diferentes**, pero que se visualizan iguales (como la O latina y la O cirílica) para engañar a los usuarios y hacerles pensar que están en una web cuando en realidad están visitando otra.

Un ejemplo de este tipo de ataque es utilizar la URL “**xn-80ak6aa92e.com**” que, al visualizarla en el navegador, se muestra como “**apple.com**“, tal como podemos ver en la siguiente web de prueba copiando la URL y pegándola en nuestro navegador: https://www.apple.com/.

Como podemos ver, es prácticamente imposible diferenciar esta URL de la dirección original de Apple -> https://www.apple.com/.

Además, ambas **utilizan un certificado HTTPS válido**, aunque Apple confía en Symantec como emisor del certificado, mientras que la web de prueba depende de Comodo como emisor, aunque, si nos fijamos en los detalles del mismo, podremos ver para qué web ha sido generado en realidad.

La versión más temprana del desarrollo de Google Chrome 59 ya incorpora un parche para solucionar este problema de seguridad, aunque todo apunta a que llegue de manera definitiva a todos los usuarios con el lanzamiento de **Google Chrome 58**, la nueva versión del navegador prevista para este mismo mes.

Mozilla, por el momento, se encuentra estudiando una solución a este fallo, aunque podemos mitigarla manualmente cambiando el valor de “**network.IDN_show_punycode**” por **“true”** dentro de del menú de configuración avanzada “about:config” del navegador.

Internet Explorer, Microsoft Edge y Vivaldi no son vulnerables.

Mientras que Google Chrome, Mozilla Firefox y Opera son algunos de los navegadores web vulnerables, otros navegadores, como Internet Explorer, Microsoft Edge y Vivaldi, entre otros, están protegidos de esta vulnerabilidad ya que no muestran estos caracteres como sus rivales.

Por ello, si intentamos abrir la web de prueba que hemos citado anteriormente en un navegador no afectado por este fallo podemos ver cómo en la barra de direcciones nos aparece la URL con sus caracteres reales, lo que ya nos lleva a sospechar de ella, aunque tenga un certificado HTTPS.

Como podemos ver, cada vez los ataques informáticos y de phishing son más complejos y complicados de detectar, aunque, si tenemos un navegador web moderno y actualizado, probablemente reduzcamos la probabilidad de terminar siendo víctimas de los piratas informáticos