

Alerta de Seguridad de Malware: Incremento de la difusión del gusano "Stuxnet"

ZMA firma especializada en la provisión de soluciones tecnológicas para la Gestión de la Infraestructura Informática, Aplicaciones y Seguridad de la información, alerta sobre el incremento de la difusión del gusano 'Stuxnet'.

Stuxnet [1] (detectado por ESET como *Win32/Stuxnet*) es un gusano de amplia difusión que utiliza diferentes vulnerabilidades del sistema operativo Windows para propagarse entre los usuarios que no aplican las actualizaciones para dicho sistema y/o no utilizan un antivirus con capacidades de detección proactiva como ESET NOD32.

Si bien se conoce que este gusano se encontraba (secretamente) activo desde 2009, a partir de su descubrimiento en junio pasado, se ha podido comprobar su amplia repercusión política debido a que su principal objetivo es infectar infraestructuras de sistemas críticos SCADA (*Supervisory Control And Data Acquisition* - Supervisión, Control y Adquisición de Datos)[2] para robar cualquier información sensible y secreta que estos sistemas pudieran almacenar.

Esto no significa que no sea capaz de infectar sistemas hogareños y corporativos ya que, para llegar a las infraestructuras críticas, puede valerse de intentar llegar directamente a las mismas a través de técnicas de ingeniería social o bien infectar a millones de usuarios y esperar que uno de ellos tenga acceso a las organizaciones objetivo.

Para infectar estos sistemas, Stuxnet se basa en la utilización de cinco vulnerabilidades en diferentes versiones de Windows y una en Internet Explorer, cuatro de las cuales fueron del tipo *0-day*, conocidas sólo por ciertos grupos delictivos e, inicialmente, sin corrección disponible por parte del fabricante. La última de ellas ha sido corregida este mes de diciembre.

El vector de propagación inicial que utilizaba Stuxnet era a través de dispositivos removibles (USB y memorias) y para ello se aprovechaba de una vulnerabilidad existente en todas las versiones de Windows y corregida en el **Boletín MS10-046**. Esta vulnerabilidad permitía la manipulación de archivos del tipo LNK y PIF para lograr la ejecución de código arbitrario y dañino en el sistema afectado. El *exploit* es detectado por ESET como *LNK/Exploit.CVE-2010-2568 (MS10-046)*.

Posteriormente Stuxnet agregó dos nuevos vectores de propagación a través de una vulnerabilidad en todas las versiones de Windows y corregida en octubre de 2008 en los **Boletines MS08-067** (la misma de la cual se aprovecha el gusano Conficker) y **MS10-061** respectivamente. Ambas vulnerabilidades permiten la ejecución de código remoto sin autorización del usuario.

A estos vectores, luego se agregó la posibilidad de descargar y ejecutar el gusano a través de una vulnerabilidad existente en todas las versiones de Internet Explorer y corregida en enero 2010 en el **Boletín MS10-002** (el *exploit* es detectado por ESET como *JS/Exploit.CVE-2010-0249*).

Los delincuentes también comenzaron a utilizar otros fallos que permiten el escalamiento de privilegios (EoP). Uno de ellos afecta a Windows 2000 y XP y fue corregido en octubre pasado en el **Boletín MS10-073** y, el otro involucra a Windows Vista, Windows 7 y 2008 corregido en diciembre y descrito en el **Boletín MS10-092**.

Como conclusión, para evitar infecciones de Stuxnet los usuarios y administradores deben instalar todas las actualizaciones mencionadas y un antivirus con capacidades proactivas capaz de detectar la explotación de cualquiera de ellas:

- Vulnerabilidad que se aprovecha de archivos LNK y PIF - Vulnerability in Windows Shell Could Allow Remote Code Execution (**MS10-046**)
<http://www.microsoft.com/latam/technet/seguridad/boletines/2010/ms10-046.aspx>
- Vulnerabilidad que permite ejecución remota de código - Vulnerability in Print Spooler Service Could Allow Remote Code Execution (**MS10-061**)
<http://www.microsoft.com/latam/technet/seguridad/boletines/2010/ms10-061.aspx>
- Vulnerabilidad que permite ejecución remota de código - Vulnerability in Server Service Could Allow Remote Code Execution (**MS08-067**)
<http://www.microsoft.com/spain/technet/security/Bulletin/ms08-067.aspx>
- Vulnerabilidad que permite escalamiento de privilegios - Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege - Win32k.sys - (**MS10-073**)
<http://www.microsoft.com/latam/technet/seguridad/boletines/2010/ms10-073.aspx>
- Vulnerabilidad que permite escalamiento de privilegios - Vulnerability in Task Scheduler Could Allow Elevation of Privilege (**MS10-092**)
<http://www.microsoft.com/latam/technet/seguridad/boletines/2010/ms10-092.aspx>
- Vulnerabilidades que permiten ejecución de código en Internet Explorer - Cumulative Security Update for Internet Explorer (**MS02-010**)
<http://www.microsoft.com/latam/technet/seguridad/boletines/2010/ms10-002.aspx>