Publicado en San Sebastián de los Reyes el 16/05/2017

El malware que afectó a Telefónica podría infectar a más ordenadores

Cualquier ordenador con sistema operativo Windows que no haya sido parcheado con la actualización de Microsoft MS17-010 podría ser víctima del ataque

Telefónica, entre otras compañías, sufrió un ciberaque global el pasado viernes.
El malware WannaCry, un virus que bloquea el acceso a los archivos del ordenador, está detrás de este ciberataque.

El pasado viernes se alertó de un ataque masivo de ransomware que afecta a los sistemas Windows y que bloquea al usuario el acceso a los archivos que tiene almacenados (tanto en sus discos duros como en las unidades de red a las que estén conectadas).

El punto más crítico de este ciberataque viene provocado por la explotación de la vulnerabilidad descrita en el boletín MS17-010 utilizando EternalBlue/DoublePulsar, que puede infectar al resto de sistemas Windows conectados a esa misma red y que no estén debidamente actualizados.

"La infección de un solo equipo puede llegar a comprometer a toda la red corporativa", afirma Iván Stojanovic, experto en Ciberseguridad de Always On. "Cualquier sistema operativo Windows que no haya sido parcheado con la actualización de Microsoft MS17-010 podría ser víctima del ataque."

La compañía experta en Ciberseguridad y que cuenta con un SoC propio para dar solución en estos casos, explica que hacer para proteger los equipos:

Mantener el sistema operativo actualizado y no usar versiones sin soporte oficial.
Configurar una copia de seguridad automática de los archivos.
No abrir enlaces ni archivos sospechosos, especialmente si llegan por correo electrónico o redes sociales.
Desconfiar de los archivos .exe.
Permitir que el antivirus de Microsoft haga su trabajo y descargar algún programa antimalware reputado complementario para detener el virus antes de que se active.
Descargar la herramienta facilitada por el CCN-CERT NoMoreCry e instalarla.
Instalar un antivirus de confianza y mantenerlo actualizado.

Si el equipo se ha visto afectado por el virus, desconectarlo de forma inmediata de la red, evitando que se propague por el resto de equipos conectados. Formatear el equipo, realizar la restauración del sistema a una versión anterior y proceder a realizar una limpieza completa del equipo con una solución antivirus totalmente actualizada.

Si el equipo continúa infectado, realizar una reinstalación de Windows. Si el sistema operativo es Windows 8 , 8.1 o 10, escribir en la barra de búsqueda la palabra 'Restablecer' y seleccionar la opción 'Restablecer este equipo'.

"Las actualizaciones de sofware y aplicaciones son fundamentales para prevenir que un virus o malware afecte un equipo, pero en muchos casos no es posible evitar este tipo de ataques, por lo que es prioritario tener una copia de seguridad actualizada", puntualiza Stojanovic. "En cualquier caso, para prevenir este tipo de ataques, no se deben ejecutar archivos de origen sospechoso ni navegar por páginas desconocidas para la descarga de software", aconseja Iván.

Para descargar el parche correspondiente al sistema operativo usado pinchar aquí.

Datos de contacto:
Marta Ciruelos
Expertos en Ciberseguridad
911728574

Nota de prensa publicada en: San Sebastián de los Reyes

Categorías: Hardware Software Ciberseguridad