Publicado en Majadahonda el 28/06/2017

Ransomware PETYA – SOC Always On

Nuevo ataque masivo de ransomware que afecta a los ordenadores con sistemas Windows

Se ha alertado de un ataque masivo de ransomware que afecta a sistemas Windows, bloqueando el acceso a los archivos (tanto en sus discos duros como en las unidades de red a las que estén conectadas).

Se está produciendo una infección de equipos con el sistema anteriormente mencionado (Windows) en diferentes organizaciones. El malware responsable es de tipo ransomware y pertenece a la familia conocida como Petya o Petrwrap. Una vez que compromete el sistema solicita el pago de 300 dólares.

Las medidas preventivas que se recomiendan desde el Centro de Operaciones de Seguridad de Always On, empresa experta en ciberseguridad, son las siguientes:

Mantener los equipos actualizados, tanto su sistema operativo como todos los software instalados.
No abrir ficheros descargados de internet o recibidos por correo electrónico de fuentes que no son de confianza.
Realizar copias de seguridad de los ficheros.
Utilizar el principio de mínimo privilegio en todos los sistemas.
En la medida de lo posible, bloquear el tráfico de los puertos TCP 135, 445, 1024-1035.
Bloquear la ejecución de ficheros en rutas como por ejemplo %AppData% o %Temp%.
Mantenerse al tanto de las últimas informaciones que puedan publicarse sobre esta oleada.

¿Qué hacer si un euqipo ha sido afectado?
Si un equipo se ha visto afectado por el ataque de ransomware, hay que desconectarlo de la red y realizar una restauración del sistema a un punto anterior. A continuación, hay que proceder a realizar una limpieza completa del equipo con cualquier solución antivirus totalmente actualizada.
Algunos programas útiles son:

MalwareBytes
Kaspersky Security Scan

En caso de que el equipo continúe infectado se deberá realizar una reinstalación de Windows. Si el sistema operativo es Windows 8, 8.1 o 10 los pasos a seguir son: escribir en la barra de búsqueda la palabra “Restablecer” y seleccionar la opción “Restablecer este equipo”.

Si continúan los problemas, se recomienda no encender el equipo y contactar con une experto.

Consejos adicionales

Tener cuidado con cualquier archivo que envíen mediante Whatsapp.
A la hora de utilizar el teléfono móvil, no es recomendable conectarse a redes WiFi públicas sin encriptación.
No navegar por páginas de contenido sospechoso para la descarga de software.
Utilizar siempre copias de seguridad de los archivos en discos duros aislados de la red, o subirlos a plataformas en la nube por ejemplo Google Drive o Microsoft One Drive.

Datos de contacto:
Marta Ciruelos
910210150

Nota de prensa publicada en: Majadahonda

Categorías: Internacional Hardware E-Commerce Ciberseguridad