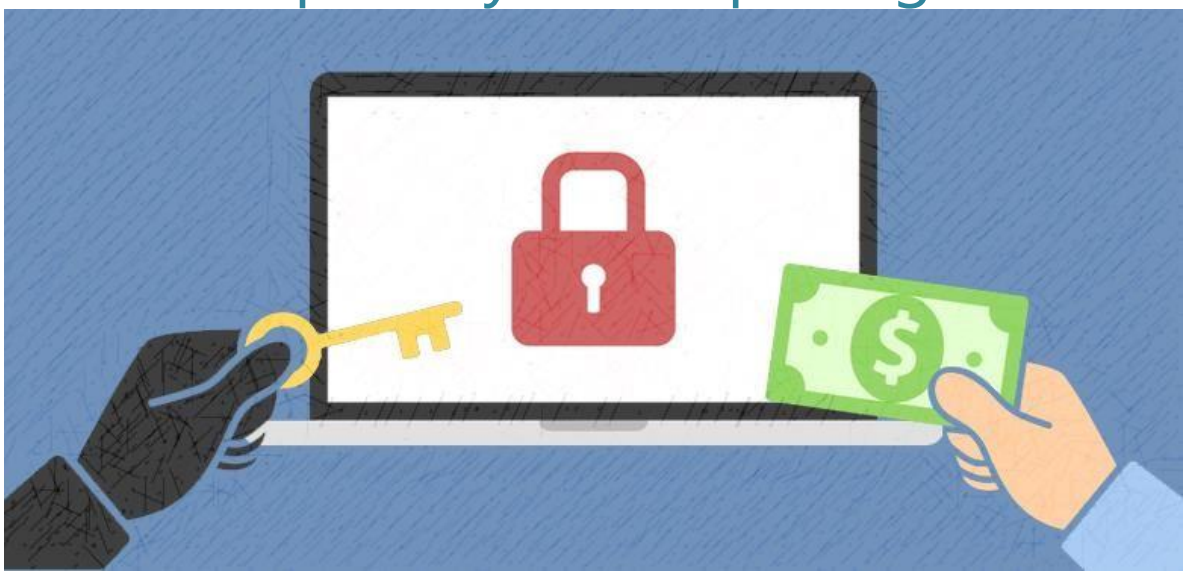
Infórmate | EDUCACIÓN SECRETARÍA DE EDUCACIÓN PÚBLICA | Instituto Politécnico Nacional "La Técnica al Servicio de la Patria"

WannaCry Ransomware
Descripción y cómo protegerse



El día de ayer hubo un ataque masivo con este Ransomware y en este hilo vamos a describir sin muchos detalles técnicos lo que se debe saber sobre este Ransomware y cómo prevenirlo.

Este Ransomware, utiliza aprovecha la Vulnerabilidad SMB de la familia de Vulnerabilidades MS17-010 con opciones de ejecución de código remoto. Esto quiere decir que para evitar específicamente este Ransomware y variantes, se debe aplicar el parche de Seguridad que corrige esta vulnerabilidad, al aplicar esta Actualización, se debe tener en cuenta el Sistema Operativo que están corrigiendo.

Es importante hacer notar que esta Vulnerabilidad, sólo puede utilizar un Exploit para obtener acceso remoto con privilegios del Sistema, lo que significa que el atacante puede obtener acceso con privilegios elevados en el Sistema, esto ocasiona que el Ransomware tiene control total de un Sistema en una red y puede extenderse a través de la misma a todos los Sistemas Windows vulnerables que no estén actualizados con el parche mencionado anteriormente.

El tamaño del archivo ransomware es de 3,4 MB (3514368 bytes).

Cómo se comporta: Desde línea de comandos, se eliminan las copias y copias de seguridad de instantáneas en los Volúmenes de los Discos Duros.
El Ransomware se escribe en una carpeta de caracteres aleatorios en la carpeta 'ProgramData con el nombre de archivo de "tasksche.exe' o en la carpeta C: \Windows\ con el nombre de archivo 'mssecsvc.exe' y 'tasksche.exe'.

Algunos Ejemplos:

C:\ProgramData\lygekvkj256\tasksche.exe
C:\ProgramData\pepauehfflzjjtl340\tasksche.exe
C:/ProgramData/utehtftufqpkr106/tasksche.exe
C:\programdata\yeznwdibwunjq522\tasksche.exe
C:/ProgramData/uvlozcijuhd698/tasksche.exe
C:/ProgramData/pjnkzipwuf715/tasksche.exe
C:/ProgramData/qjrtialad472/tasksche.exe
C:\programdata\cpmliyxlejnh908\tasksche.exe

El Ransomware otorga acceso total a todos los archivos usando el comando: Icacls. /Grant Todos:F /T /C /Q

Cómo Protegerse:

- Como mencionamos anteriormente, se recomienda actualizar el Sistema con la Acutalización MS17-101. Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017.
- Para bajar las actualizaciones localizadas para Windows Server, Windows XP, Windows 8 visitar:http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
- Las nuevas variantes del ransomware aparecen regularmente. Mantenga siempre su software de seguridad actualizado para protegerse contra ellos, es decir, su Antivirus.
- Mantenga actualizado su sistema operativo y otro software. Las actualizaciones de software incluirán con frecuencia parches para vulnerabilidades de seguridad recientemente descubiertas que podrían ser explotadas por atacantes del Ransomware.

- El correo electrónico es uno de los principales métodos de infección de Ransomwares. Tenga cuidado con los correos electrónicos inesperados o no solicitados, especialmente si contienen enlaces y/o archivos adjuntos.
- Tenga mucho cuidado con cualquier archivo adjunto de correo electrónico de Microsoft Office que le aconseje habilitar macros para ver su contenido. A menos que esté absolutamente seguro de que se trata de un correo electrónico genuino de una fuente de confianza, no habilite las macros y, en su lugar, elimine inmediatamente el correo electrónico.
- Realizar copias de seguridad de datos importantes es la forma más eficaz de combatir la infección por ransomware. Los atacantes tienen influencia sobre sus víctimas cifrando archivos valiosos y dejándolos inaccesibles. Si la víctima tiene copias de seguridad, puede restaurar sus archivos una vez que se ha limpiado la infección. Sin embargo, las organizaciones deben asegurarse de que las copias de seguridad estén debidamente protegidas o almacenadas fuera de línea para que los atacantes no puedan eliminarlas.
- El uso de servicios en la nube podría ayudar a mitigar la infección por ransomware, ya que muchos conservan versiones anteriores de archivos, lo que le permite "retroceder" a la forma no cifrada.

¿Qué hacer si estoy infectado?

Lo primero que se recomienda es NO PAGAR, ya que por un lado como estamos "negociando" con cibercriminales, nada y, nadie nos garantiza que nos darán la clave o nos descifrarán los archivos. Además, estaríamos fomentando la ciberdelincuencia y hacer crececr este tipo de amenazas.

Segundo, se recomienda ailsar el equipo de la red (si estuviese en una), aplicar los parches mencionados, conservar los archivos en copias de Seguridad, ya que es cuestión de tiempo (corto o largo) que se lanzará alguna solución para descrifrar sus archivos.

Fuente:https://answers.microsoft.com/es-es/protect/forum/protect_other-protect_scanning/wannacry-ransomware-descripci%C3%B3n-y-c%C3%B3mo/f33b380e-fbc9-4911a5f6-5251f54c74eb?auth=1