COMUNICADO ACERCA DEL RANSOMWARE WannaCry

CU12052017-1

COMUNICADO DEL CERT-UACh ACERCA DEL MALWARE WannaCry

Desde el viernes 12 de mayo del 2017, se está produciendo una infección masiva en computadoras y servidores a nivel mundial. Esta infección ocasiona que ciertos archivos sean cifrados, y por tanto, bloqueados para su acceso por parte del usuario. Además se solicita un pago a cambio de obtener el proceso de descifrado de los archivos. A este tipo de malware se le conoce con el nombre de "Ransomware", y en particular, el ransomware que está llevando de manera masiva esta infección es conocido como "WannaCry" y afecta a computadoras con sistemas operativos Windows de Microsoft.

CÓMO FUNCIONA "WannaCry".

Una vez que llega a instalarse este ransomware, detecta y realiza la explotación activa de una vulnerabilidad en el servicio **SMB "Server Message Block"** (ver el boletín **MS17-010** https://technet.microsoft.com/en-us/library/security/ms17-010.aspx emitido por Microsoft), luego cifra los archivos en el equipo y los de las unidades de red a las que estén conectadas, además, este malware se propaga por la red local afectando a otros sistemas Windows, por lo que toda la red corporativa puede llegar a estar comprometida.

WannaCry, además, exige el pago de un rescate de $ 300 bitcoins.

SISTEMAS AFECTADOS

Equipos con los siguientes sistemas operativos:

- Windows XP
- Windows Vista
- Windows Server 2003
- Windows Server 2008 SP2 and R2 SP1
- Windows 7
- Windows 8

- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 and R2
- Windows 10
- Windows Server 2016

CÓMO EVITAR QUE LOS EQUIPOS SEAN INFECTADOS POR WannaCry.

- Es imperativo actualizar el sistema operativo Windows de inmediato. Microsoft ha emitido actualizaciones para aquellos sistemas operativos fuera de soporte como Windows XP, Windows Server 2003 y Windows 8 a través de su Blog Oficial:

  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

- Realizar un respaldo de la información de manera inmediata.
- Contar con un software antimalware con cortafuegos integrado y activado.
- Actualizar todo el software instalado en el equipo, incluyendo navegadores, los complementos de barra de herramientas que utilice, antimalware, etc.
- No abrir enlaces de correos electrónicos, sitios web ó redes sociales (Facebook, WhatsApp, etc.) que considere sospechosos.
- Evite visitar sitios inseguros o poco confiables.
- Si recibe un email de personas conocidas con un enlace, pregúntele antes de abrir el enlace para confirmarlo. Es importante anotar que las computadoras infectadas reenvían emails aleatorios a la lista de contactos con el enlace del virus.
- Los emails fraudulentos utilizan nombres similares a servicios populares para engañar a las personas y hacer que sus equipos se infecten.
- Aislar la comunicación a los puertos 137 y 138 UDP y puertos 139 y 445 TCP en las redes de datos.
- Recuerda que el Antivirus institucional protege los equipos propiedad de la UACh. Puedes descargarlo del siguiente enlace:

  http://antivirus1.uach.mx/avi.html

QUÉ HACER EN CASO SI UN EQUIPO HA SIDO INFECTADO POR WannaCry.

- Desconectar inmediatamente el equipo de la red (desconectar el cable de red, o apagar las tarjetas de red inalámbricas).
- No realizar los pagos exigidos por el atacante, ya que no existe ninguna garantía de que los atacantes envíen la utilidad y/o contraseña de descifrado, además de que sólo incentiva su actividad y motiva a seguir distribuyendo masivamente este tipo de código dañino.
- En caso de no contar con el respaldo de sus archivos, guardar los archivos cifrados antes de llevar a cabo algún tipo de desinfección, debido a que es probable que en un futuro aparezca alguna herramienta que permita descifrar dichos archivos.
- Puedes comunicarte al CERT-UACh:

Extensiones 1722, 1769, 1780 y 1783
Teléfonos: (614) 439-18-04 y (614) 439-18-17
Correos electrónicos: yasuarez[arroba]uach.mx jrbarron[arroba]uach.mx

Enlaces de referencia y herramientas de apoyo

- Parches de actualización para sistemas operativos fuera de soporte de Microsoft:

  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

- Herramienta que el CCN-CERT (España) pone a disposición del público:

  https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4497-ccn-cert-nomorecry-tool-v-0-3-actualizada-la-vacuna-frente-a-wannacry.html

- Referencias:

  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

  https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html

  https://www.incibe.es

  http://www.cert.org.mx/boletin/

  https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/

  https://blog.kaspersky.com.mx/wannacry-estas-a-salvo/9148/