Ciudad de México, a 12 de mayo de 2017.

ALERTA PREVENTIVA CONTRA LA CIBERDELINCUENCIA No. 48

“Ransomware WannaCry”

La Secretaría de Seguridad Pública de la CDMX, de conformidad con las atribuciones que tiene conferidas en los artículos 3°, fracciones I, IV y V de su Ley Orgánica, 1, fracción II, y 15, fracciones I y II de la Ley que Regula el Uso de Tecnología para la Seguridad Pública del Distrito Federal, así como en los artículos 3 y 14, fracción IV de su Reglamento Interior de la Secretaría, relativas a realizar en el ámbito territorial y material del Distrito Federal las acciones dirigidas a salvaguardar la integridad y patrimonio de las personas, prevenir la comisión de delitos e infracciones a las disposiciones gubernativas y de policía, así como preservar las libertades, el orden y la paz públicos.

Situación:
Derivado de labores de monitoreo en redes sociales e internet, la Policía de Ciberdelincuencia Preventiva de la Secretaría de Seguridad Pública de la Ciudad de México, se ha detectado un virus informático, del tipo ransomware, (virus que encripta archivos y solicita dinero para tener acceso nuevamente a la información) que ataca a ciertas computadoras que tengan instalado cualquier versión del sistema operativo Windows (fabricado por la empresa Microsoft) y no hayan instalado todas las actualizaciones de seguridad que publica el fabricante.

Descripción:
La propagación se puede llevar a cabo de las siguientes maneras:

Método 1. Al recibir un correo electrónico, con una liga hacia un sitio web, en dicha página se descarga un archivo en la PC, detecta si no se tiene instaladas todas las actualizaciones de seguridad del sistema operativo Windows, en caso de que exista esa vulnerabilidad, se instala e inicia el proceso de encriptación de ciertos archivos. Aparece una pantalla, donde se indica que es necesario pagar por la llave para poder tener acceso nuevamente a los archivos encriptados.
Método 2. Accesar a un servidor (que previamente ya fue infectado por el ransomware) y producto del acceso a este equipo, el archivo de instalación se copia a la PC e inicia el proceso de infección.
Método 3. En ambientes donde estén presentes más de dos PCs con conexión de red entre ellas, si al menos una PC se contamina, es muy probable que sean contaminadas el resto de PCs.

Recomendaciones:

- Verificar que la PC que utilice con sistema operativo Windows, se encuentre actualizada en sus boletines de seguridad (Windows Update).
- Considere que existen ciertas versiones de Windows que ya no cuentan con soporte por parte del fabricante.
- Confirmar que tenga instalado el boletín de seguridad de Microsoft MS17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)
- Verificar que su software de antivirus se encuentre funcionando y actualizado.
- Solicite al ingeniero de soporte técnico, desactive los servicios del sistema operativo de su PC, que usted no utilice.
- En caso de requerir mayor información para la instalación de boletines de seguridad para Windows, contacte al fabricante de hardware de su PC, o al ingeniero de soporte técnico de su confianza.
- También puede contactar el fabricante de su software antivirus.

“Verifique que tenga actualizado los boletines de seguridad de su PC y el software antivirus”

Secretaría de Seguridad Pública
Policía de Ciberdelincuencia Preventiva
Twitter: @UCS_CDMX
Hashtag #CibernéticaCDMX
Correo electrónico: policia.cibernetica@ssp.cdmx.gob.mx
Teléfono 5242 5100 ext. 5086