Ciudad de México, a 12 de abril de 2016

ALERTA PREVENTIVA CONTRA LA CIBERDELINCUENCIA No. 39

"VIRUS DE LA POLICÍA (RANSOMWARE) EN EQUIPOS TELEFÓNICOS MÓVILES ANDROID E IOS"

La Secretaría de Seguridad Pública de la Ciudad de México, 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 al incremento de denuncias a nivel nacional por ataques de una variante del código malicioso denominado "Vírus de la Policía" a teléfonos móviles, mediante el cual solicitan realizar un pago determinado para desbloquer dichos equipos; es por eso que la Policía de Ciberdelincuencia Preventiva de la Secretaría de Seguridad Pública de la Ciudad de México, realizó la siguiente "Alerta de Ciberdelincuencia" a fin de informar las medidas preventivas y de seguridad, relacionadas al denominado "**Virus de la Policía (Ransomware) en Equipos Telefónicos Móviles Android e iOS".**

Descripción:

Este virus se aloja en los equipos móviles luego de recibir y abrir correos electrónicos, mensajes o enlaces sospechosos con servicios de mensajería instantánea o al instalar aplicaciones de sitios web no oficiales e inclusive al estar navegando con el dispositivo.

Modo de operación:

El mensaje o aviso que se despliega en los equipos móviles son de supuestas corporaciones Policiales, usando escudos de la Policía Federal e incluso de Agencias de Investigación, tanto nacionales como internacionales, además se muestran datos personales del usuario, el dispostivo y de algunos contactos generando un mayor impacto y credibilidad al mensaje, dicho ransomware bloquea la pantalla del dispositivo y solicita una cantidad de dinero para su presunto desbloqueo, esto mediante la adquisición y envio de códigos de tarjetas de prepago principalmente del sistema iOS.

Recomendaciones:

- No adquiera y envie códigos de tarjetas de prepago para realizar el pago que se solicita, ¡es un fraude!.
- Utilize un software Antivirus actualizado para sus dispositivos móviles.
- Evite abrir mensajes, archivos, enlaces o acceder a ligas sospechosas que circulen a través de los sistemas de mensajería instantánea.
- No abra correos electrónicos de remitentes sospechosos o desconocidos.
- Evite descargar aplicaciones de sitios web no oficiales.
- Contacte con el área de servicio de su operadora telefónica quien le indicará cómo entrar al "modo seguro" o restaurarlo a "modo de fábrica".
- Si su dispositivo móvil es Android, el virus de la Policía se habrá instalado bajo alguna aplicación que aparentemente parece inofensiva pero esconde el virus. Para desbloquear podría intentar los siguientes pasos.
    - Compruebe si su dispositivo incluye la opción de reinicio en modo seguro (ya que no todos disponen de ella, pues depende del fabricante y la versión de Android instalada).
    - Al iniciar en modo seguro, desinstale la aplicación que muestra el falso mensaje de la policía, generalmente es la última app instalada, para ello, diríjase al Menú > Ajustes > Aplicaciones y seleccione la app maliciosa.
    - Para finalizar, reinicie el dispositivo normalmente.
- Si su Smartphone o tablet no cuenta con esta opción, deberá restaurar a la configuración de fábrica del dispositivo, tenga en cuenta que esta acción eliminará todos los datos y aplicaciones que tenga instaladas y se iniciará como cuando lo adquirió, de tal forma que si no tuviese copias de seguridad de la información almacenada (fotos, vídeos, documentos, etc.), estos se perderán.

."No se deje sorprender, ninguna institución gubernamental le requerirá pago alguno mediante la adquisición y envío de códigos de tarjetas de prepago"

Secretaría de Seguridad Pública
Policía de Ciberdelincuencia Preventiva
Twitter: @UCS_CDMX
Correo electrónico: policia.cibernetica@ssp.df.gob.mx
Teléfono 5242 5100 ext. 5086
Unidad de Atención del Secretario UCS: 5208 9898