RANSOMWARE

NOTI 309 – Marzo de 2021

Clases de Ransomware detectadas en Colombia:

- Ransomware de cifrado.
- Lock Screen Ransomware.
- Master Boot Record (MBR) Ransomware.
- Ransomware de cifrado de servidores web.
- Ransomware de dispositivos móviles

Imagen tomada de: Informe de Tendencias Cibercrimen Colombia 2019-2020

Debido al incremento de los casos de Ransomware, hemos decidido dedicar un pequeño espacio para hablar sobre este tema tan importante.

El Ransomware es un ciberdelito que viene en crecimiento en nuestro país. De acuerdo al informe de Tendencias Cibercrimen Colombia 2019-2020, Colombia es el país de América Latina que ha recibido más ataques de este tipo en el último año; siendo las PYMES el blanco preferido debido a sus bajos niveles de seguridad.

Pero, ¿en qué consiste? Consiste en el secuestro de información para pedir un rescate, el cual se exige en criptomonedas. Sin embargo, el pago no garantiza que la información sea devuelta o liberada, por lo que una de las recomendaciones es no pagar el rescate.

En Colombia, se han detectado cinco tipos de Ransomware pero hay dos que se presentan con mayor frecuencia:

- Ransomware de Cifrado: cifra archivos personales, documentos, archivos multimedia, etc.

- Lock Screen Ransomware: Bloque la pantalla del PC, inhabilitando cualquier acción, mostrando un mensaje donde se solicita el pago.

Los asuntos de correos electrónicos más utilizados por los cibercriminales son: embargos judiciales, citaciones judiciales, comparendos, reporte a centrales de riesgos y alarmas de transferencias no consentidas.

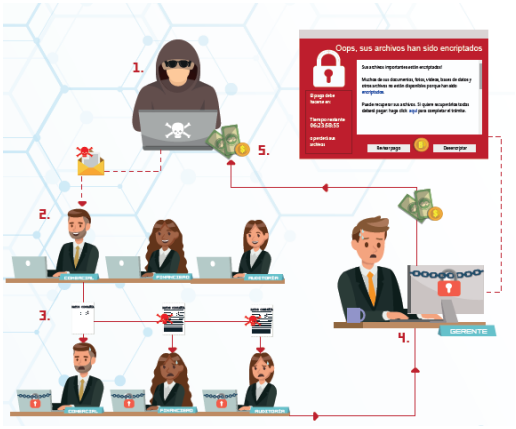

Imagen tomada de: Informe de Tendencias Cibercrimen Colombia 2019-2020

Por: Laura Castrillón, Directora Administrativa, ASR S.A.S.

Medellín, Colombia
+57 4 266 33 64
asr@asr.com.co
http://www.asr.com.co/

Generalmente, los cibercriminales envían correos electrónicos con asuntos alarmantes que generan pánico en el destinario y lo llevan a abrir archivos adjuntos o a hacer clic en enlaces, que descargan algún Malware, afectando al equipo de cómputo, a la red y al servidor.

Como habíamos mencionando en nuestros Notis 257 y 279, es importante revisar varios aspectos antes de abrir algún archivo adjunto o hacer clic en algún enlace, entre los cuales están:

- El nombre del remitente, ya que el nombre de una entidad pública, por ejemplo, puede pasar de Ministerio de Transporte a Ministerio de Tránsito.
- Verificar la dirección de correo electrónico, ya que ésta puede ser cambiada en una simple letra, siendo minombre@minombre.com a minombre@mjnombre.com.
- Revise la ortografía, ya que un correo con múltiples faltas de ortografía tiene altas probabilidades de ser un correo malicioso.

Si ya es víctima de este tipo de Ciberdelito, el Centro Cibernético Policial tiene, en su página web, una enlace que lo llevará al portal NO MORE RANSOMWARE donde se podrán encontrar algunas claves para desbloquear la información, de acuerdo al tipo de Ransomware. No están todas pero alguna podría serle de utilidad.

Recuerde tener back ups de la información y establecer mecanismos perimetrales de protección (Antivirus, antimalware y anti-pishing).

En la próxima entrega, continuaremos con el tema del Perfil del Defraudador.

asr@asr.com.co