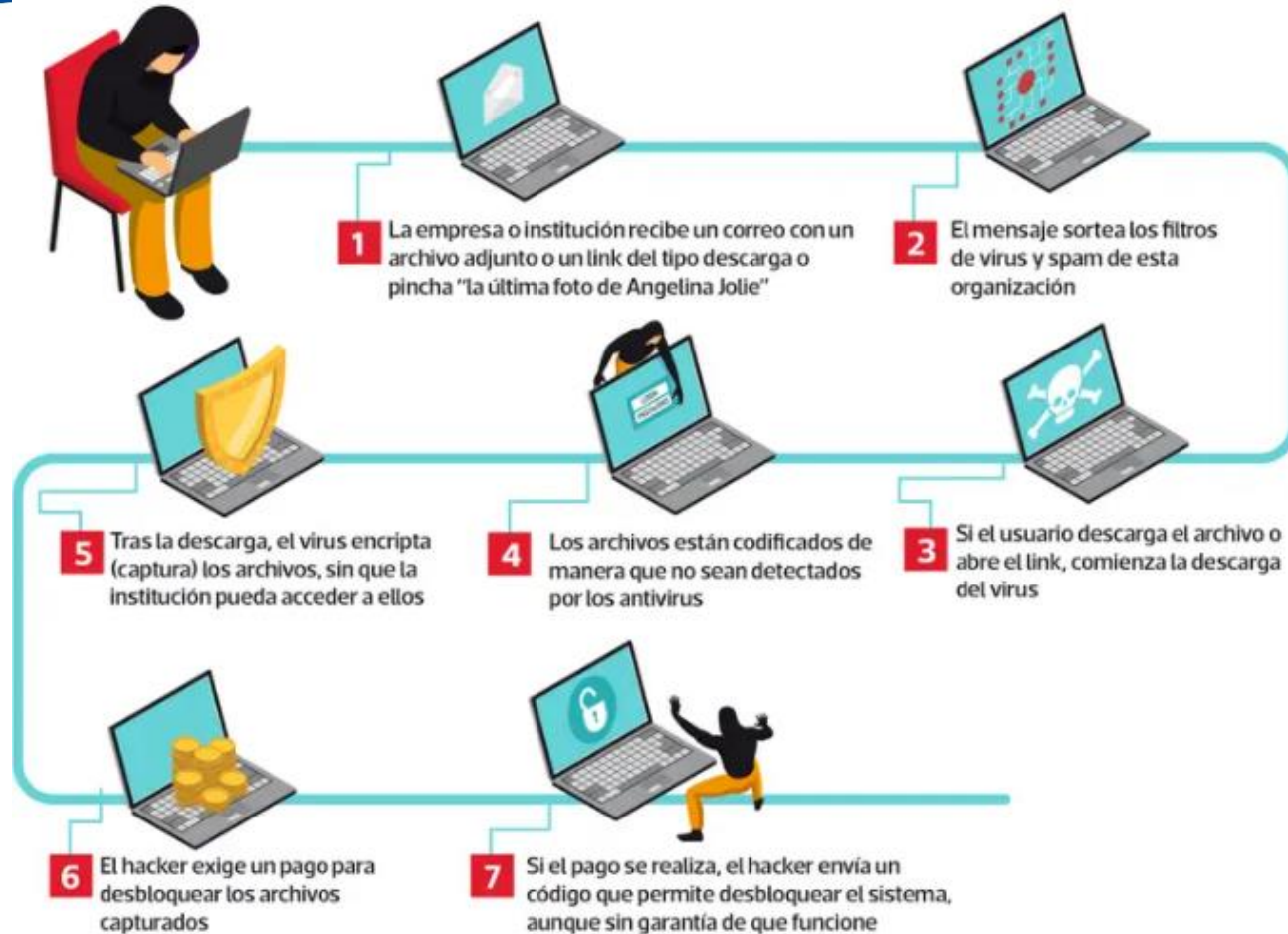


BOLETÍN DE NOTICIAS Y NOVEDADES DE

SEGURIDAD INFORMÁTICA

Conozca como funciona el código malicioso de mayor crecimiento en el mundo “RANSOMWARE”



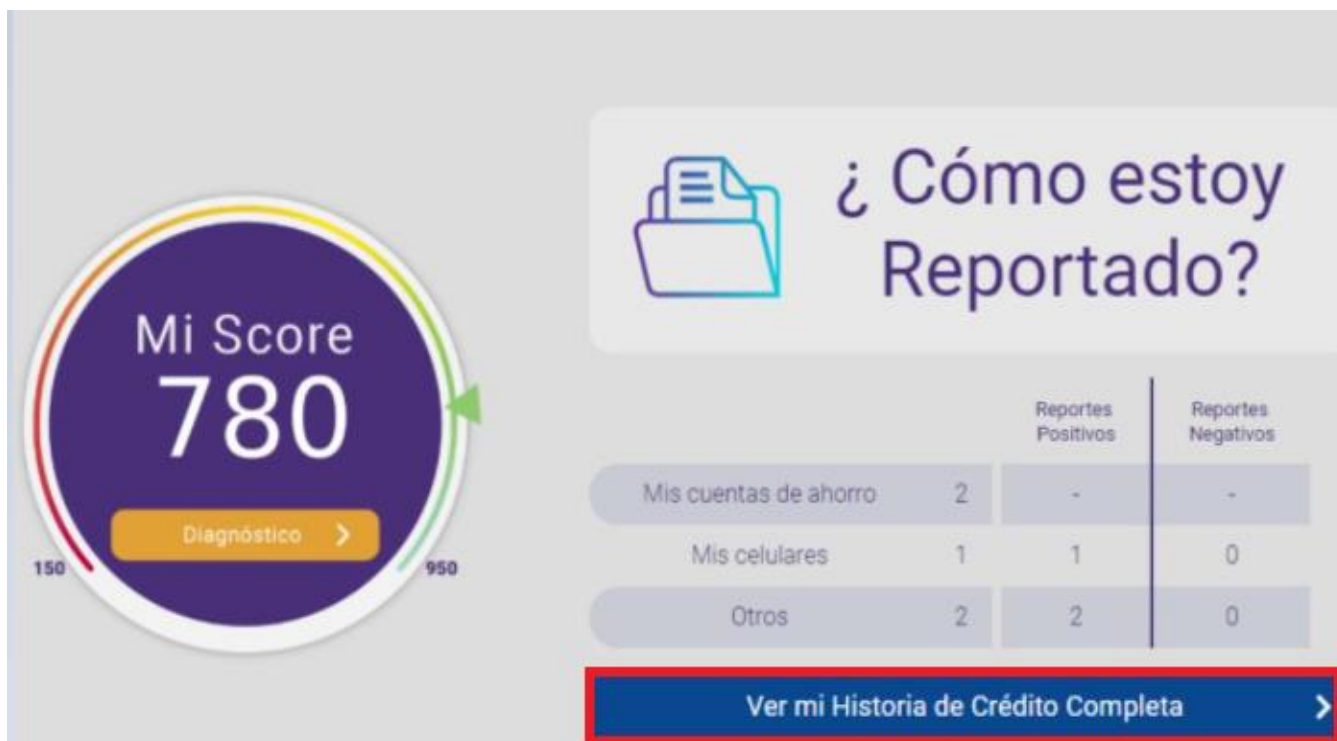
El Ransomware es un tipo de ataque cibernético cuya función es ingresar a una red de equipos y cifrar la información que hay en ella para luego pedir un rescate por su liberación.

El ataque parece ser muy sofisticado, pero su mecanismo es bastante burdo. Se calcula que el 56% de los ataques llegan a través de un correo electrónico, ya sea con un archivo descargable y ejecutable (del tipo “ve la última foto de Angelina Jolie”) o bien un link a un sitio (“pincha aquí para obtener dinero gratis”) desde el cual se descarga el programa malicioso.



BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA

¡ALERTA! ESTAFA USANDO EL NOMBRE DE DATACRÉDITO



Tomado de: <https://www.valoraanalitik.com/>

A través de comunicado Data Crédito Experian informa sobre correos electrónicos falsos que personas inescrupulosas están utilizando con su marca sin autorización alguna para enviar links a través de mensajes que direccionan a un sitio de descarga de una aplicación ejecutable en dispositivos Android”.

La recomendación es no abrir links donde informan tiempo de mora o estado de la obligación reportada, ya que desde Data Crédito Experian no se envía ese tipo de links. Para cualquier inquietud ingresen directamente a nuestra página oficial www.datacredito.com, www.midatacredito.com o www.datacreditoempresas.com”

BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA



¡ALERTA! CAMPAÑA PHISHIN CIRCULANDO EN A RED

De: Bancolombia <iegrupo@vps-139996.iegrupo.co>
Fecha: lun., 16 sep. 2021, 08:46 p. m.
Para: xxxxxxxx@hotmail.com
Asunto: Servicio de Alertas y Notificaciones Bancolombia

Notificación
Informativa

Bancolombia te informa BLOQUEO de T.Deb y/o T.Cred el 08/09/2021. Actívala realizando un proceso de verificación de titularidad en el siguiente enlace:

<https://www.grupobancolombia.com.co>

Este es una notificación automática

Bancolombia

Si tiene alguna inquietud puede contactarnos en nuestras líneas de atención telefónica:

Bogotá (571) 513 0000, Medellín (574) 513 0000,
 Cali (572) 554 0000, Esmeraldas (577) 581 8888, Buenaventura
 (571) 297 2222, Cartagena (573) 522 4400,
 Radio del grupo 01800081234G
 Sede principal Cra. 45 No. 20-59 Torre
 Flama, Medellín - Colombia

Cancelar suscripción

El sistema le pedirá ingresar a su cuenta de Bancolombia donde le sugiere ingresar su clave y contraseña, luego le solicita actualizar sus datos personales, de esta manera obtienen toda su información.

Por medio de un correo Phishing suplantando el sitio oficial de la entidad BANCOLOMBIA, varios ciudadanos han sido engañados al ingresar sus datos personales, robando cuentas bancarias y sus credenciales. Verifique siempre el remitente; es de notar que el correo remitente es iegrupo@vps-139996.iegrupo.co y el dominio real de la página de BANCOLOMBIA es www.grupobancolombia.com, recuerden tener precaución con este tipo de mensajes, bloquear remitente y eliminar.

Tomado de: <https://cc-csirt.policia.gov.co/>



**Universidad
de Santander**
Personería Jur. 810 de 12/03/96 Min.Educación **UDES**



BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA

!ALERTA! CAMPAÑA PHISHIN CIRCULANDO EN A RED

De: Notificación Ach <notificacionesach@hotmail.com>

Enviado: lunes, 06 de Septiembre de 2021 3:23 p. m.

Asunto: Transacción de Pago Pse.



¡Hola!

Gracias por utilizar los servicios de PSE. los siguientes son los datos de tu transacción:

Estado de la Transacción: Aprobada

CUS: 1053440068

Empresa: Portal Zona Pagos

Descripción: CUOTA DE ADMINISTRACION

Valor de la Transacción: \$ 586.813

Fecha de Transacción: 26/08/2021



Notificación de Pago Pse...

2 KB



TransaccionesACH



@ACH_Informa

Tomado de: <https://cc-csirt.policia.gov.co/>

Falso correo electrónico está siendo enviado a través de la red, con un comunicado sobre supuesta notificación realizada por parte de ACH, el remitente emplea una cuenta de correo Hotmail (notificacionesach@hotmail.com), el cual contiene un enlace que descarga un archivo adjunto, y al extraer su contenido se observa un archivo con muestras maliciosas, esto pone en riesgo la seguridad de su información personal tanto en los dispositivos móviles como los de escritorio. Recuerden tener precaución con este tipo de mensajes, bloquear remitente y eliminar.



**Universidad
de Santander**

Personería Jur. 810 de 12/03/96 Min.Educación **UDES**



BOLETÍN DE NOTICIAS Y NOVEDADES DE SEGURIDAD INFORMÁTICA

!ALERTA! CAMPAÑA PHISHIN CIRCULANDO EN A RED

De: <jeromanja@hotmail.com>

Enviado el: martes, 31 de agosto de 2021 16:00 p.m.

Asunto: BOLETA DE CITACION DE JUZGADO SEGUNDO PROMISCO DE FAMILIA

CITACIÓN Y EMPLAZAMIENTO

EL JUZGADO SEGUNDO PROMISCO DE FAMILIA, EN CUMPLIMIENTO A LO ORDENADO EN EL ARTÍCULO 102 DE LA LEY 1098 DE 2006, cita por medio el presente suscrito, por línea materna y paterna y demás personas con interés legal de su familia, Sírvese comparecer el requerimiento Judicial dentro de los cinco (5) días siguientes al envío de la presente comunicación, a diligencia de notificación personal, ingresando de manera inmediata al archivo para la información adecuada del motivo de la citación.

Por motivos de seguridad el archivo se encuentra protegido con un PIN de cuatro dígitos para visualizar la información requerida deberá diligenciar la siguiente CLAVE: 2021

De no ingresar al archivo se entenderá surtida la notificación, motivo por el cual el juzgado tomará medidas pertinentes en cuanto a su ausencia en concordancia con el artículo 102 Código de la Infancia y la Adolescencia y artículo 293 del Código General del Proceso

Boleta de Citación Juzgado 02.pdf
442 KB

Boleta de citación.r21
MD5:be0cd64278bc6cd9c7c7b32f0c78e20c
SHA1:931b3139830e5485f198bb72ecba50475e4c8df2

Se encuentra circulando falso correo electrónico a través de la red, comunicando una supuesta notificación realizada por parte del juzgado segundo, la cual utiliza de remitente una cuenta de correo Hotmail (jeromanja@hotmail.com), que contiene un enlace que descarga un archivo comprimido, y al extraer su contenido nos muestra dos archivos con muestras maliciosas, esto pone en riesgo la seguridad de su información personal tanto en los dispositivos móviles como los de escritorio. Recuerden tener precaución con este tipo de mensajes, bloquear remitente y eliminar.

Tomado de: <https://cc-csirt.policia.gov.co/>



**Universidad
de Santander**

Personería Jur. 810 de 12/03/96 Min.Educación **UDES**