CIRCULAR 04

1002.01-TD-005

Manizales, 31 de Mayo de 2021

PARA: Comunidad Universitaria

ASUNTO: Alerta de Malware circulando en la red

La Oficina de Sistemas se permite informar a toda la Comunidad Universitaria que Desde el grupo de respuesta a incidentes de seguridad informática CSIRT de la Policía Nacional de Colombia se detecta una alerta el día 30 de mayo del 2021 a las 11:47 PM, la cual consiste en un falso correo electrónico que está circulando a través de la red.

En este correo se informa de una supuesta notificación realizada por parte de la Fiscalía General de la Nación, la cual utiliza de remitente una cuenta de correo Hotmail "fiscaliageneralcuentadecobro4@hotmail.com" el cual tiene como asunto "IMPORTANTE BOLETA FISCAL No 004741", en este correo se adjunta la supuesta citación en un archivo comprimido denominado como "PROCESO JUDICIAL EN SU CONTRA.tbz" el cual dentro de este se encuentra el archivo "PROCESO JUDICIAL EN SU CONTRA.vbs" que contiene muestras maliciosas.

De acuerdo a los análisis que se realizaron en los Antivirus de las empresas de seguridad MicroWorld-eScan, FireEye y AegisLab se tuvo como resultado archivos con contenido malicioso catalogados como VB:Trojan.Downloader.JVDR y Trojan.Script.Generic.4!c.

Los programas clasificados como Trojan-Downloader descargan e instalan nuevas versiones de programas maliciosos como troyanos en las computadoras de las víctimas. Una vez descargados, estos programas se ejecutan automáticamente cuando se inicia el sistema operativo.

Los scripts se pueden escribir en una gran cantidad de lenguajes de programación y se pueden usar para realizar una amplia variedad de acciones, lo que los convierte en herramientas versátiles para el atacante. En el caso del Trojan.Script.Generic.4!c, es un script que se utiliza para generar archivos de secuencias de comandos que incluyen código malicioso que son detectados como troyanos.

De: FISCALIA GENERAL <fiscaliageneralcuentadecobro4@hotmail.com>
Enviado: domingo, 30 de mayo de 2021 11:47 p. m.
Asunto: IMPORTANTE BOLETA CITA FISCAL No 004741

Fiscalía General de la Nación

Asunto: IMPORTANTE BOLETA CITA FISCAL No 004741

Bogotá - Cundinamarca 04 de Mayo de 2021

Numero de proceso. 0091-002018-0917764

El presente es el requerimiento enviado a declarar por el proceso 0091-002018-0917764 con fecha de inicio 27 de junio de 2021.

Respectivamente anexamos su boleta de citación (No 004741) a la Fiscalía 07 con motivos de declaraciones donde se detalla lugar fecha y hora de esta misma y así mismo toda la información necesaria para usted.

Este archivo está protegido por su seguridad.

LA CONTRASEÑA CORRESPONDIENTE A SU PROCESO ES [123]

Atentamente,
Fiscalía General de la Nación Sede 07
Diagonal. 22B # 52- 01 (Ciudad Salitre)
+57 57(1)570 20 00 -57(1)414 90 00
Abierto · Atendemos hasta 5: PM

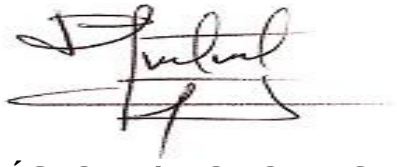
Ciudad Bogotá – Colombia

Antivirus	Signature
MicroWorld-eScan	VB:Trojan.Downloader.JVDR
FireEye	VB:Trojan.Downloader.JVDR
AegisLab	Trojan.Script.Generic.4!c

Recomendaciones

- Nunca haga clic en enlaces dentro de un correo electrónico desconocido y siempre ignore los que le soliciten estas acciones.
- No responda mensajes que le soliciten información personal o financiera.
- Use programas que verifiquen automáticamente si una URL es legítima antes de que se acceda al sitio web.
- Identifique los correos que le son enviados por remitentes desconocidos, en los cuales le solicitan información personal y financiera.

Atentamente,



HÉCTOR FABIO TORRES MARTÍNEZ
Coordinador De Grupo Oficina De Sistemas