CENTRO CIBERNÉTICO POLICIAL

B@CIB – 003 | Boletín de Análisis en CIBERSEGURIDAD

TROYANO FISCALÍA

En lo transcurrido de los últimos dos meses se han presentado dos ciberamenazas que se han propagado de manera indiscriminada mediante correo electrónico, a través del cual se suplanta a la Fiscalía General de la Nación constituyéndose así en una modalidad de PHISHING, engañando a las víctimas para que accedan a un enlace fraudulento.

De esta manera, al ingresar al enlace la navegación se redirige a un servidor vulnerado por el atacante, donde se descarga un troyano automáticamente. En esta ocasión un dominio colombiano, seguidamente de un dominio argentino fueron utlizados para este fin.

Alcance Internacional

Al respecto, la Organización de los Estados Américanos pone a disposición en su portal Web, diferentes guías o modelos para la atención de incidentes informaticos. En estos documentos se explica como detectar el incidente, limitar el impacto del ataque, remover la amenaza y recobrar el estado de los sistemas a una etapa normal, así como delinear y mejorar los procesos afectados.

Ref.: https://www.sites.oas.org

Características

Esta modalidad de ataque comienza con la suplantación de una entidad empleando información ilegítima en un mensaje de correo electrónico, el cual contiene embebida una URL o enlace al que debe ingresar la víctima para consultar lo que en este caso se supone es una citación por parte de la Fiscalía General de la Nación. Una vez se ingresa, se descarga un archivo con extensión *.RAR que al descomprimirse queda finalmente un archivo ejecutable, es decir un *.exe.

En consecuencia, la víctima al dar clic sobre el archivo ejecutable instala en segundo plano un troyano que realiza modificaciones en el sistema, que tienen como finalidad permitir el acceso remoto al atacante o el envío silencioso al victimario de información confidencial o restringuida de la persona afectada.

Como producto del análisis realizado por el Centro Cibertnético Policial se identificó que el nombre del archivo final o troyano es **Visualice_Denuncia_Penal5548.exe**

Este código malicioso corresponde a las siguientes firmas de verificación o HASH:

MD5 5af6140df861b2be13314c85317927a5

SHA1 ae0e4f171e856b54acf7f0ce6b6b678f7a9d5860

Icono con el que se observa el archivo malicioso en formato *.exe:

Mitigación del ataque

El Centro Cibernético Policial a través de alertas tempranas y gestión del incidente informático reportó tanto al administrador del sitio afectado en Colombia como en Argentina, logrando así evitar la propagación masiva de este troyano. No obstante, se radicó noticia criminal por la materialización de los casos donde hubo violación de datos personales para identificar a los responsables.

Por lo anterior, si a su correo electrónico llega este tipo de mensajes, absténgase de abrir cualquier archivo adjunto o ingresar a los enlaces y consulte nuestro servicio CAI VIRTUAL 24/7 (www.ccp.gov.co) para verificar y descartar cualquier tipo de contenido malicioso.