CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

ALERTA DE SEGURIDAD

INC-01022-L9X9

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Fecha de publicación: 19 de Febrero 2020

ALERTA DE SEGURIDAD

ID	INC-01022-L9X9
TLP	Blanco
Tipo de incidente	Malware
Categoría	Código Malicioso
Fecha de incidente	03 de febrero 2020
Fecha de reporte	19 de febrero 2020
Nivel de peligrosidad	**Alto**

RESUMEN EJECUTIVO

Las organizaciones están expuestas a diferentes amenazas cibernéticas como consecuencia de la utilización de páginas web, aplicaciones móviles, correo electrónico, redes sociales, entre otras. **La mayoría de estas amenazas están siendo diseñadas para el robo de información personal o corporativa con el objetivo de crear ataques cibernéticos**. Dentro de los métodos comúnmente utilizados se encuentran el uso de malware o programa de código malicioso que tienen como objetivo dañar los sistemas de información, causar un mal funcionamiento o robar datos, ejecutando acciones no deseadas ni detectadas por los usuarios en el sistema.

DETALLES DEL INCIDENTE

A través de una notificación al correo de reportes de incidentes del Equipo Nacional de Respuestas a Incidentes Cibernéticos (CSIRT-RD), se ha identificado una campaña de malware vía correo electrónico que contiene un archivo malicioso adjunto con el nombre **PrÃ³xima reuniÃ³n de finanzas.doc** que invita al usuario abrir el documento.

Se ha analizado el archivo en un ambiente controlado y se observa que al ejecutarse se realizan procesos no visibles por el usuario que descarga un programa malicioso para infectar el equipo.

INDICADORES DE COMPROMISO (IoC)

Remitente: ventas1sancristobal[@]torresbatiz[.]com

Asunto: Todos deben asistir a la reunión de mañana

Conexiones IP:

45[.]122[.]220[.]220
189[.]235[.]233[.]119
42[.]115[.]22[.]145
145[.]14[.]144[.]244

HTTP/HTTPS requests URL

http[:]//khomaynhomnhua[.]vn/dup-installer/tyl31xi-nmfh-643542/
http[:]//42[.]115[.]22[.]145/hlBQN9
http[:]//189[.]235[.]233[.]119/FbXd34FmBkN

Hash

Archivo Principal: PrÃ³xima reuniÃ³n de finanzas.doc

sha256

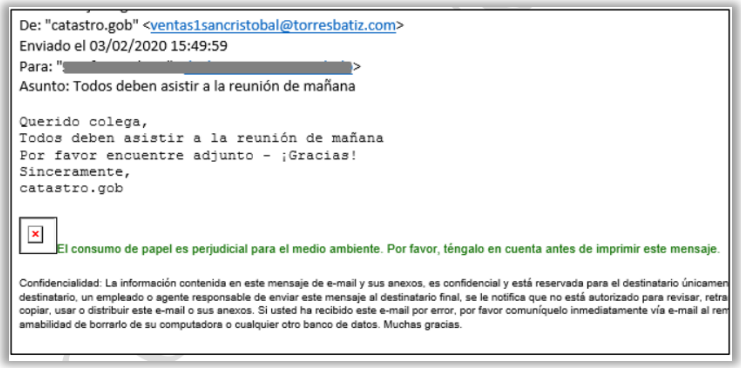
9A01FF3D7DFA98E7792784AC96B282570DAEE69E7ED72F2A722E16983B50408D

Archivo ejecutable

C:\Users\admin\633.exe

sha256

D1F4EB095A541ECFE4AE5692A8FABA8FE32F04898B10384F77B0A0F0761D380E



De: "catastro.gob" <ventas1sancristobal@torresbatiz.com>
Enviado el 03/02/2020 15:49:59
Para: "[redacted]"
Asunto: Todos deben asistir a la reunión de mañana

Querido colega,
Todos deben asistir a la reunión de mañana
Por favor encuentre adjunto - ¡Gracias!
Sinceramente,
catastro.gob

El consumo de papel es perjudicial para el medio ambiente. Por favor, téngalo en cuenta antes de imprimir este mensaje.

Confidencialidad: La información contenida en este mensaje de e-mail y sus anexos, es confidencial y está reservada para el destinatario únicamen destinatario, un empleado o agente responsable de enviar este mensaje al destinatario final, se le notifica que no está autorizado para revisar, retra copiar, usar o distribuir este e-mail o sus anexos. Si usted ha recibido este e-mail por error, por favor comuníquelo inmediatamente vía e-mail al rem amabilidad de borrarlo de su computadora o cualquier otro banco de datos. Muchas gracias.

RECOMENDACIONES

1. Bloquear los indicadores de compromiso expuestos.
2. Mantener actualizadas las plataformas y sistemas de información.
3. Realizar campañas de concientización periódica a los usuarios de la institución.