CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

ALERTA DE SEGURIDAD

INC-01041-K9L8

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

Fecha de publicación: 06 de marzo 2020

ALERTA DE SEGURIDAD

ID	INC-01041-K9L8
TLP	Blanco
Tipo de incidente	Malware
Categoría	Código Malicioso
Fecha de incidente	05 de marzo 2020
Fecha de reporte	05 de marzo 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 **pago.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: Garcia <c[.]garcia[@]faroproducts[.]com>

Asunto: Pago

Conexiones IP:

198[.]58[.]120[.]47
104[.]223[.]170[.]113[:]80
37[.]221[.]193[.]103
62[.]122[.]170[.]168
195[.]201[.]28[.]161

Soluciones de DNS

sercon[.]com[.]mx 198[.]58[.]120[.]47[:]443
www[.]ckav[.]ru
ns3[.]salenames[.]ru,
ns4[.]salenames[.]ru
void[.]blackhole[.]mx

Peticiones HTTP

http[:]//104[.]223[.]170[.]113/rithy/Panel/five/fre[.]php

Hash

Archivo Principal: " pago.doc "

SHA1 71B3412724D7DA2D69A6D0A50CAAFF671889339C

MD5 A304F3197481A533A93F945C6A6BD2B0

Archivo secundario: " tnex.exe "

SHA1 3DE29FC808A6AB9B72DB975DA4F90FD48222339C

MD5 7B5DBC773351A48CF50A807EA9D7D118


From: Garcia <c.garcia@faroproducts.com>
Date: March 5, 2020 at 11:33:35 AST
Subject: Pago

Buenos Dias,

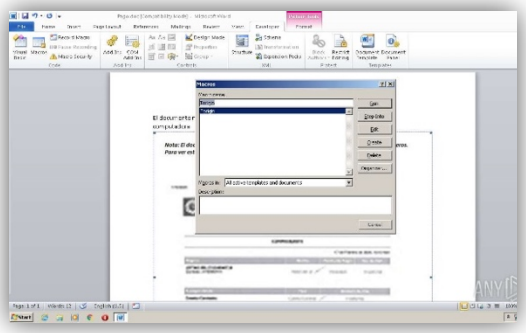
Mi nombre es García del departamento de cuentas,

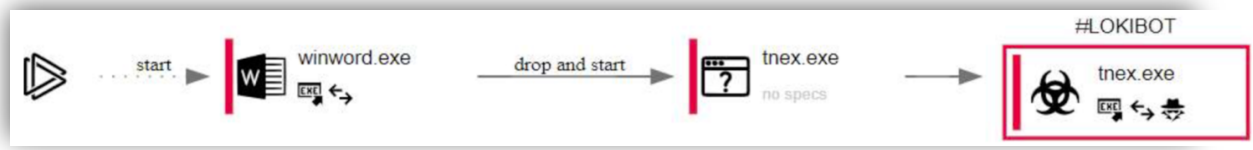
Encuentre el pago adjunto para su referencia, mi otro correo electrónico está actualmente fuera de servicio por ahora.

Este pago es por los productos y materiales que pedimos

Agradeciéndote y esperando una respuesta deseable de tu parte.

Saludos





Mitre ATT&CK, Técnicas de detección

Acceso Inicial	Ejecución	Persistencia	Escala de privilegios	Evasión de defense	Acceso de credenciales	Descubrimiento	Movimiento Lateral	Colección
	Ejecución de servicio	Hooking	Hooking	Modificar registro	Hooking	Aplicación Windows Discovery		Recolección de correo electrónico.
		Inicio de Aplicaciones office	Proceso de inyección	Proceso de inyección				

RECOMENDACIONES

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso expuestos, indicados en este documento.
2. Mantener actualizadas las plataformas y sistemas de información.
3. Realizar campañas de concientización periódica a todos los usuarios de la institución.