CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

ALERTA DE SEGURIDAD

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

Fecha de publicación: 17 de Febrero 2020

© Todos los derechos reservados

ALERTA DE SEGURIDAD

ID	INC-01020-B7W3
TLP	Blanco
Tipo de incidente	Malware
Categoría	Código Malicioso
Fecha de incidente	04 de febrero 2020
Fecha de reporte	17 de febrero 2020
Nivel de peligrosidad	**Alto**

“El presente documento es **propiedad del Centro Nacional de Ciberseguridad (CNCS)**, y fue generado mediante el análisis de varias fuentes de terceras partes y una investigación del equipo CSIRT-RD.”

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 Swift (1).xls** 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: Gomez <sonya(@)bezeqint.net>
Asunto: Pago

Conexiones IP:
50.87.150.45
104.223.170.113

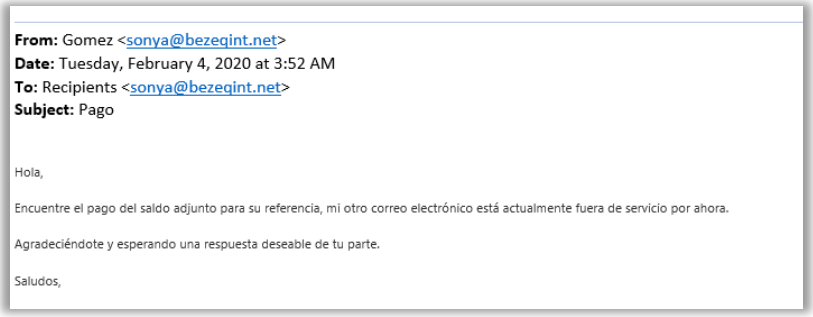
Solicitudes de Dominio DNS
ahkdev.com

HTTP/HTTPS requests URL
http(:)// 104.223.170.113 / Silkop / Panel / five / fre(.)php

Hash
Archivo Principal: "Pago Swift (1) .xls"
Gomez <sonya(@)bezeqint.net>
sha256
de4349f190f0ddd063ccbc8b7bba0d2fceb338d0becd2d67f0e81e80d3b7a51f
sha1
1e8303869cb38cabb4bea042802d8de415bde709
md5
572101b633037231e9844826037b6bff

Archivo ejecutable
C(:) \Users\admin\AppData\Local\Microsoft\Windows\Content.IE5\78RFYB7Z\build_1FB5 [1] .exe

sha256
dfb5cd72149d36c8a48a04a3d4fd7fdfb6eb0f0f45a83cacc1b2b5492ba92423


From: Gomez <sonya@bezeqint.net>
Date: Tuesday, February 4, 2020 at 3:52 AM
To: Recipients <sonya@bezeqint.net>
Subject: Pago

Hola,

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

Agradeciéndote y esperando una respuesta deseable de tu parte.

Saludos,

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.