CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

ALERTA DE SEGURIDAD

INC-01077-P1C3

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

Fecha de publicación: 13 de mayo 2020

ALERTA DE SEGURIDAD

ID	INC-01077-P1C3
TLP	Blanco
Tipo de incidente	Malware
Categoría	Código Malicioso
Fecha de incidente	11 de mayo 2020
Fecha de reporte	13 de mayo 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 distribuidos por correo electrónico 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 phishing vía correo electrónico suplantando la identidad de la empresa **SICOVEL** con el asunto: **Pago,** el cual contiene un archivo malicioso adjunto con el nombre **Pago.xls,** he 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 descargan un programa malicioso conocido ***Macro[.]Trojan-Downloader[.]Agent[.]HQ*** e infecta el equipo.

INDICADORES DE COMPROMISO (IoC)

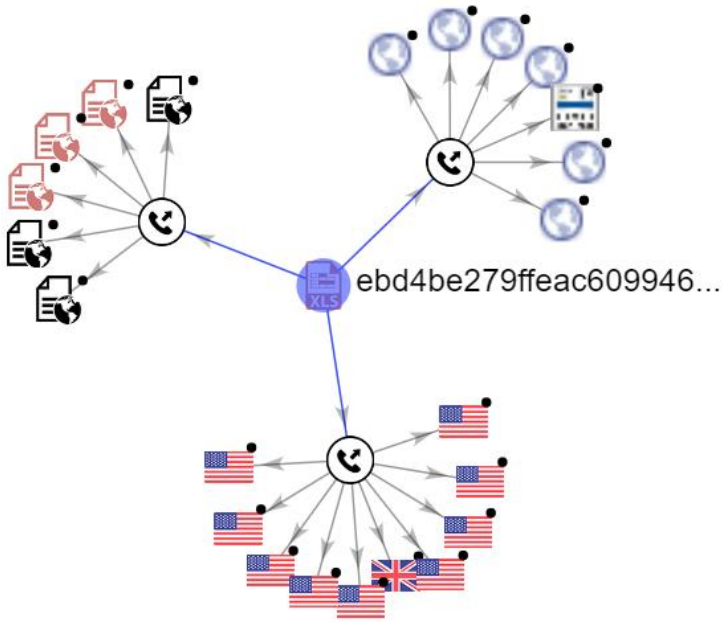
Asunto:
" Pago"

Conexiones IP:
157[.]52[.]211[.]247
192[.]35[.]177[.]64
45[.]14[.]112[.]101
107[.]180[.]41[.]145

Peticiones HTTP:
https[:]//nilemixitupd[.]biz[.]pl/SILVER/COJHJHHGHVCDKNJKJ[.]exe
http[:]//157[.]52[.]211[.]247/arinate/Panel/five/fre[.]php

Solicitud de dominio DNS
protestlabsmovings.es
nilemixitupd.biz.pl
sicovel[.]mx

Hash
Archivo Ejecutado " jjrr.exe "
SHA1: 552c271a2f3457ea137cc52d669b2ff0b256741b
MD5: 58a8b51e7c69f75f563747eae7bc12fb



Mitre ATT&CK, Técnicas de detección

Acceso Inicial	Ejecución	Persistencia	Escala de privilegios	Evasión de defensa	Acceso de credenciales	Descubrimiento	Movimiento Lateral	Colección	Ex filtración	C&C
	Ejecución de servicio	Incorporación	Incorporación	Inyección del proceso	Incorporación	Descubrimiento aplicación windows				
	Ejecución de usuario	Inicio de aplicación de office	Inyección del proceso							

RECOMENDACIONES

1. Recomendamos realizar un análisis exhaustivo con un antimalware o antivirus ante la amenaza de un malware para identificar y contener la amenaza.
2. Se recomienda hacer uso de las buenas prácticas de higiene digital y mantener actualizados los sistemas con su última versión estable.
3. Mantener la consola de antivirus actualizada y licenciado.
4. Evaluar el bloqueo preventivo de los indicadores de compromisos y mantener actualizadas todas las plataformas tecnológicas.
5. Realizar concientización permanente a la comunidad extendida, colaboradores y cadena de suministro, (proveedores) para evitar que sean víctimas de estas amenazas cibernéticas.