CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

ALERTA DE SEGURIDAD

INC-01065-R0T7

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

Fecha de publicación: 15 de abril 2020

ALERTA DE SEGURIDAD

ID	INC-01065-R0T7
TLP	Blanco
Tipo de incidente	Malware
Categoría	Código Malicioso
Fecha de incidente	10 de abril 2020
Fecha de reporte	14 de abril 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 **DHL EXPRESS** con el asunto: **FW: DHL Shipment Notification for,** el cual contiene un archivo malicioso adjunto con el nombre **Receipt Address Confirmation (Please Sign)_Pdf.html** 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 descargan un programa malicioso que infecta el equipo.

INDICADORES DE COMPROMISO (IoC)

Asunto:
" DHL Shipment Notification"

Conexiones IP:
142[.]11[.]195[.]232

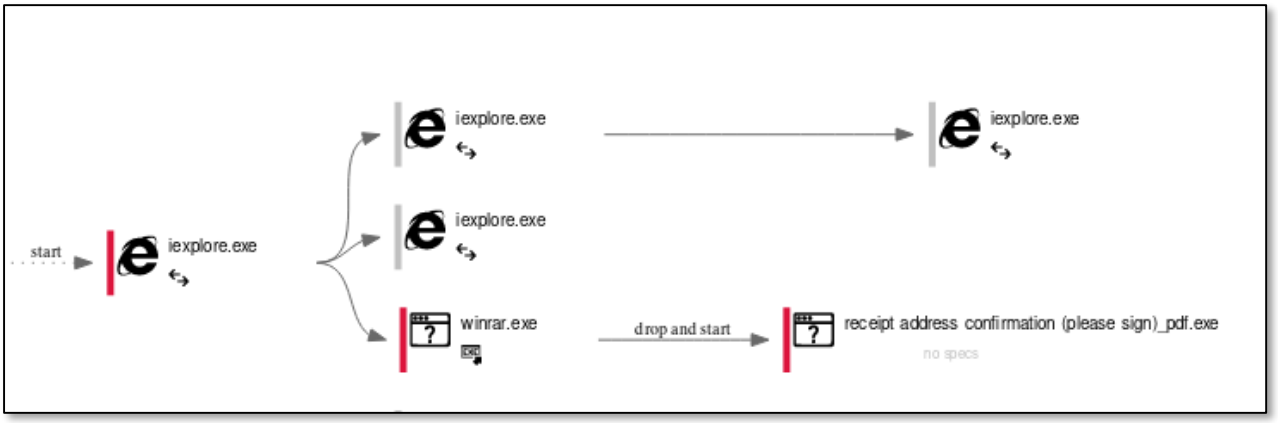
Peticiones HTTP:
http[:]//dhlexpress[.]duckdns[.]org/orders/SKMBT_C3641903 1917150[.]Pdf[.]zip

Solicitud de dominio DNS
dhlexpress[.]duckdns[.]org

Hash

Archivo Principal: " Main object- "SKMBT_C36419031917150[.]Pdf[.]html"
SHA1: C217D1531C064F8099105A245C6D3D8AB0B9A136
MD5: B0BC85ACAF28E0D92B15655E63BBE906

Archivo secundario:
C:\Users\admin\AppData\Local\Temp\Rar$EXa1632.38377 \Receipt Address Confirmation (Please Sign)_Pdf.exe
SHA256
ee26aa2c63784f39472fbcdda797249384d2f5b15b10d37bd a7da95b5c53c435



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 carga mediante API			Instalación de certificado root		Consulta de Registro				
	Ejecución de usuario			Modificación de registro						

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.