INC-01117-K1M6

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 31 DE JULIO 2020

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

REPÚBLICA DOMINICANA Con la gente y para la gente | MINISTERIO DE LA PRESIDENCIA

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.

ALERTA DE SEGURIDAD

- **ID** INC-01117-K1M6
- **TLP** Blanco
- **Tipo de incidente** Malware
- **Categoría** Código Malicioso
- **Fecha de incidente** 16 de julio 2020
- **Fecha de reporte** 22 de julio 2020
- **Nivel de peligrosidad** **Ambar**

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 correos electrónicos masivos con informaciones erróneas o con links para que el usuario realice acciones que tienen como principal objetivo capturar información o distribuir código malicioso en los equipos de los usuarios.

DETALLES DE LA ALERTA

A través de una notificación al correo de reportes de incidentes del Equipo Nacional de Respuestas a Incidentes Cibernéticos (CSIRT-RD), fue reportada una campaña de malware via correo electrónico con el asunto "**Aviso de entrega: factura del documento de envió**" que contiene un archivo adjunto con el nombre **"DHL-Waybill AWB#1307202000122.png.lnk".**

Se ha analizado el archivo suministrado en un ambiente controlado y se observa que al ejecutarse se realizan procesos no autorizados por el usuario con el fin de establecer un C&C sobre el dispositivo.

INDICADORES DE COMPROMISO (IoC)

Remitente
quickreport[@]bayandstreets[.]com

Asunto
Aviso de entrega: factura del documento de envió

IP Origen del Correo
192[.]236[.]192[.]135

HASH
Archivo Principal: "DHL-Waybill AWB#1307202000122.rar"
Archivo Ejecutado: " DHL-Waybill AWB#1307202000122.png.lnk "
Sha256
72644c9157922132d62ab266efa9d658eddbcddb1a5d0b46643e6b3870d9f7cb
MD5 608fb1e5d01327f20f82eb8a755ead4b

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso expuestos, indicados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces o adjuntos suministrados vía correo electrónico
3. Mantener actualizadas las plataformas y sistemas de información.
4. Realizar campañas de concientización periódica a todos los usuarios de la institución.