INC-01118-P5B5

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 06 DE AGOSTO 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

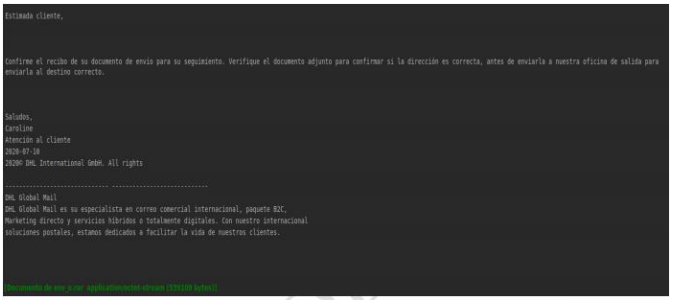
- **ID** INC-01118-P5B5
- **TLP** Blanco
- **Tipo de incidente** Malware
- **Categoría** Código Malicioso
- **Fecha de incidente** 16 de julio 2020
- **Fecha de reporte** 22 de julio 2020
- **Nivel de peligrosidad** **Ambar**

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 vía correo electrónico con el asunto **“Documento de envío (Factura, PI, Bill of Lading)”** que contiene un archivo con el nombre “**Documento de envío.rar**”



Se ha analizado el archivo suministrado en un ambiente controlado y se observa que al ejecutarse se realizan procesos no autorizados por el usuario donde se ejecuta un programa malicioso que realiza algunas conexiones con IPs de diferentes países para intentar descargar y ejecutar archivos maliciosos

INDICADORES DE COMPROMISO (IoC)

Remitentes
utilit-grade@absean[.]com
guac[@]gamaa[.]com[.]mx

Asunto
Documento de envío (Factura, PI, Bill of Lading)

Conexiones IP
192[.]129[.]188[.]197
172[.]104[.]211[.]59

HASH
Archivo Principal "Documento de envío.exe"
SHA256
25c94d3053c9cb31101390e3826902e2966efaff90a81fb3a7c5f4d18188106e
MD5 04f89d6bcacb2b20505d20ee789a9a44

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 suministrados mediante medios de mensajería instantánea.
3. Mantener actualizadas las plataformas y sistemas de información.
4. Realizar campañas de concientización periódica a todos los usuarios de la institución.