INC-01132-ZOT5

# ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 26 DE AGOSTO 2020



PRESIDENCIA DE LA REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS




# ALERTA DE SEGURIDAD

- **ID** INC-01132-Z0T5
- **TLP** Blanco
- **Tipo de incidente** Ingeniería Social
- **Categoría** Robo de Información
- **Fecha de incidente** 25 de Agosto 2020
- **Fecha de reporte** 26 de Agosto 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 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 phishing vía correo electrónico con el asunto **"Pago"** que contiene un archivo con el nombre "**CALENDARIO DE PAGO.xls**"


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)

**Remitente**
scan@cavaillon[.]com

**Asunto**
Pago

**Conexiones IP**
162[.]159[.]137[.]232

**Solicitudes de Dominio (DNS)**
Nilemixitupd[.]biz[.]pl

**Peticiones HTTP**
http[:]//nilemixitupd[.]biz[.]pl/bkvktnhsyrfvhilmjnbvcudkjuhbkjbnmcophtivopmnvifij/ZgkwTYu
http[:]//nilemixitupd[.]biz[.]pl/ughbdhbfygolijkngjfhuhpkliOlpekmvnhyetgfne/UjfnOlJHKJFHhfijkfjbdeyv[.]exe

**HASH**
Archivo Principal "CALENDARIO DE PAGO.xls"
**MD5** 2604d59a74c1ef0828761e8a09d28c02

Archivo Ejecutado "rghxbko.exe"
**MD5** 8ac467c488227a3bd2b639c84f914cfc


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