INC-01113-B5D4

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 07 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

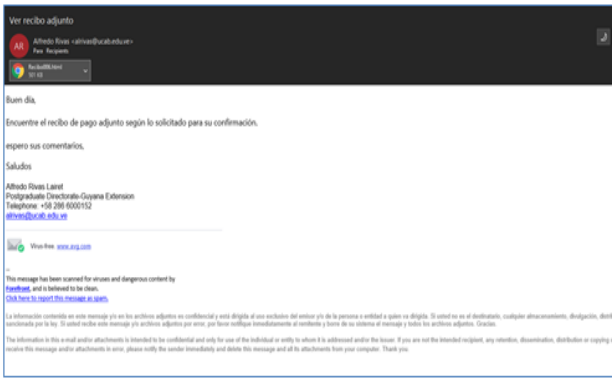
- **ID** INC-01113-B5D4
- **TLP** Blanco
- **Tipo de incidente** Ingeniería Social
- **Categoría** Robo de Información
- **Fecha de incidente** 07 de julio 2020
- **Fecha de reporte** 07 de julio 2020
- **Nivel de peligrosidad** **Medio**

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), se ha identificado una campaña de phishing con el asunto; **“Ver recibo adjunto”** que invita al usuario acceder aun link en un HTML adjunto para ver el recibo solicitado.



Se ha analizado el enlace suministrado en un ambiente controlado y se observa que redirige a un portal donde se solicita introducir las credencias con el fin de capturar la información.

INDICADORES DE COMPROMISO (IoC)

Remitente
alrivas[@] ucab[.]edu[.]ve

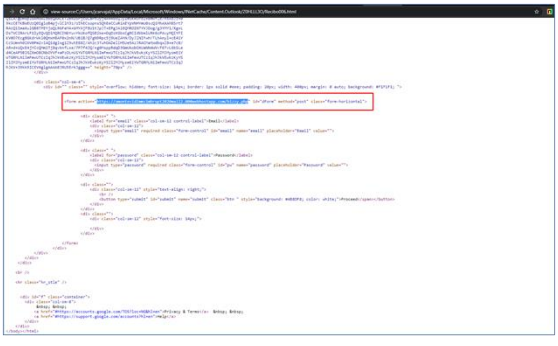
Asunto
“Ver recibo adjunto”

URL
omontevidimmzimbrupt2020mail2[.]000
webhostapp[.]com

Conexiones IP
145[.]14[.]145[.]232
145[.]14[.]145[.]36
210[.]209[.]11[.]142
200[.]2[.]15[.]150
145[.]14[.]145[.]65

Peticiones DNS
omontevidimmzimbrupt2020mail2[.]000webhostapp[.]com
network[.]com[.]tw
ucab[.]edu[.]ve

Pagina HTML que es enviada como adjunto al correo.



Ruta URL con método POST que envía las credenciales a una página de terceros.

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 adjuntos 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.