INC-01143-B4R2

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 18 DE SEPTIEMBRE 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

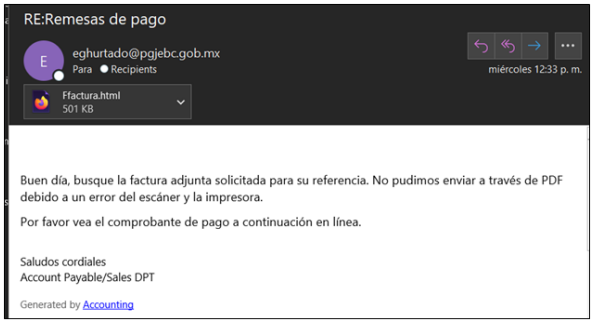
- **ID** INC-01143-B4R2
- **TLP** Blanco
- **Tipo de incidente** Ingeniería Social
- **Categoría** Robo de Información
- **Fecha de incidente** 16 de Septiembre 2020
- **Fecha de reporte** 17 de Septiembre 2020
- **Nivel de peligrosidad** ALTO

RESUMEN EJECUTIVO

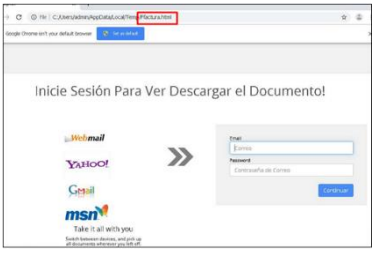
Las organizaciones están expuestas a diferentes amenazas cibernéticas como consecuencia de la utilización de páginas web, aplicaciones móviles, correo electrónico, redes sociales, entre otras. La mayoría de estas amenazas están siendo diseñadas para el robo de información personal o corporativa con el 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 **“RE:Remesas de pago ”** que contiene un archivo con el nombre “**Ffactura.html**”



Se ha analizado el archivo suministrado en un ambiente controlado y se observa que al ejecutarse se abren el navegador donde se muestra un formulario para hacer login y capturar las credenciales del usuario.



INDICADORES DE COMPROMISO (IoC)

Remitente
Eghurtado[@]pgjebc[.]gob[.]mex

Asunto
RE:Remesas de pago

Conexiones IP
145[.]14[.]145[.]248

Peticiones HTTP
https[:]//webbscurelogn2020com[.]000webhostapp[.]com

HASH Archivo
sha1:
0e3aded1a926b27606ff03dec655d559aae774cd
md5:
6eb4afd6a31114a3b99e012f64880ee5

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.