CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

ALERTA DE SEGURIDAD

INC-01078-Q7G6

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Fecha de publicación: 13 de mayo 2020

ALERTA DE SEGURIDAD

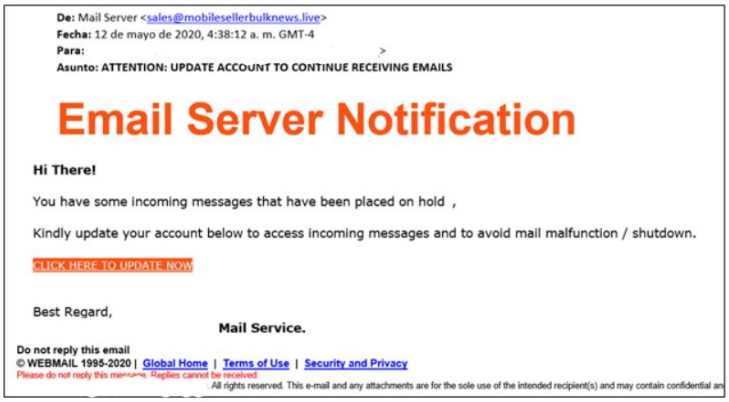
ID	INC-01078-Q7G6
TLP	Blanco
Tipo de incidente	Ingenieria Social
Categoría	Robo de Información
Fecha de incidente	12 de mayo 2020
Fecha de reporte	13 de mayo 2020
Nivel de peligrosidad	**Alto**

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 DEL INCIDENTE

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 vía correo electrónico con el asunto; **FW: ATTENTION: UPDATE ACCOUNT TO CONTINUE RECEIVING EMAILS** que invita al usuario acceder a un link para actualizar los datos de su cuenta y poder continuar utilizando el servicio.



De: Mail Server <sales@mobilesellerbulknews.live>
Fecha: 12 de mayo de 2020, 4:38:12 a. m. GMT-4
Para: >
Asunto: ATTENTION: UPDATE ACCOUNT TO CONTINUE RECEIVING EMAILS

Email Server Notification

Hi There!

You have some incoming messages that have been placed on hold ,

Kindly update your account below to access incoming messages and to avoid mail malfunction / shutdown.

CLICK HERE TO UPDATE NOW

Best Regard,

Mail Service.

Do not reply this email
© WEBMAIL 1995-2020 | Global Home | Terms of Use | Security and Privacy
Please do not reply this message. Replies cannot be received
All rights reserved. This e-mail and any attachments are for the sole use of the intended recipient(s) and may contain confidential an

Se ha analizado el link 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:
sales@mobilesellerbulknews.live

Asunto:
“ATTENTION: UPDATE ACCOUNT TO CONTINUE RECEIVING EMAILS”

Conexiones IP:
172[.]217[.]219[.]95

Soluciones de DNS
firebasestorage.googleapis.com

Peticiones HTTP:
https[:]//firebasestorage.googleapis.com/[v0]/b/pacel-225bf.appspot[.com]/o/BN298%2Fwebauth.htm?alt=media&token=80c71aaf-00b3-43c2-a937-17fbcda83d70#xxxxxxx.

RECOMENDACIONES

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