INC-01093-V0F9

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 22 DE MAYO 2020

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

REPÚBLICA DOMINICANA Con la gente y para la gente | MINISTERIO DE LA PRESIDENCIA

ALERTA DE SEGURIDAD

- **ID** INC-01093-V0F9
- **TLP** Blanco
- **Tipo de incidente Ingeniería** Social
- **Categoría** Robo de Información
- **Fecha de reporte** 21 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 DE LA ALERTA

Equipo Nacional de Respuestas a Incidentes Cibernéticos CSIRT-RD ha identificado una campaña de phishing vía correo electrónico con el asunto **"ACTUALIZAR",** que invita al usuario acceder a un enlace de actualización de los datos de su cuenta como condición para continuar utilizando el servicio.

El CSIRT-RD ha analizado el enlace en un ambiente controlado, confirmando que redirige a un portal fraudulento donde se solicita introducir las credenciales del usuario con la finalidad de capturar la información de acceso.

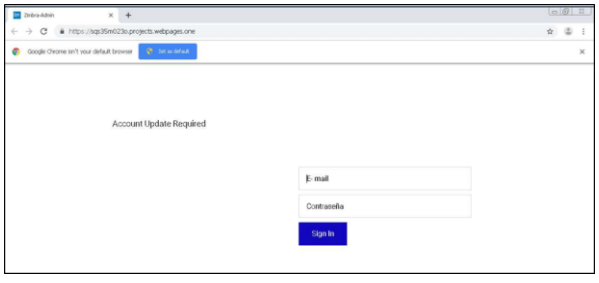
Begin forwarded message:

From: Administrador <leomil.colon@inhrr.gob.ve>
Date: May 20, 2020 at 12:49:33 AST
Subject: ACTUALIZAR

Esta es la advertencia final antes de cerrar todas las cuentas inactivas. Tenga en cuenta que no puede enviar / recibir correos electrónicos si no actualiza hoy.
Validar ahora.

--
This message has been scanned for viruses and dangerous content by
Forefront, and is believed to be clean.
Click here to report this message as spam.

La información contenida en este mensaje y/o en los archivos adjuntos es confidencial y está dirigida al uso exclusivo del emisor y/o de la persona o entidad a quien va dirigida. Si usted no es el destinatario, cualquier almacenamiento, divulgación, distribución o copia de esta información está estrictamente prohibida y sancionada por la ley. Si usted recibe este mensaje y/o archivos adjuntos por error, por favor notifique inmediatamente al remitente y borre de su sistema el mensaje y todos los archivos adjuntos. Gracias.



INDICADORES DE COMPROMISO (IoC)

Remitente
Administrador leomil[.]colon@inhrr[.]gob[.]ve

Asunto
"Fwd: ACTUALIZAR "

Conexiones IP
142[.]93[.]108[.]123
209[.]197[.]3[.]24
151[.]101[.]2[.]217
104[.]18[.]35[.]165
89[.]187[.]169[.]86

Soluciones de DNS
sqs35m023o[.]projects[.]webpages[.]one
clientservices[.]googleapis[.]com
tag[.]getdrip[.]com
micro-cdn[.]sumo[.]com

Peticiones HTTP:
Https[:]//sqs35m023o.projects.webpages.one/[Root]

Https[:]//d1zviajkun9gxg.cloudfront.net/content/layout/[sections.css]) .

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.