



INC-01135-C7P5

# ALERTA DE SEGURIDAD



**CSIRT-RD**

Equipo Nacional de Respuestas a Incidentes  
Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 31 DE AGOSTO 2020

© Todos los derechos reservados





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-01135-C7P5
- TLP Blanco
- Tipo de incidente Ingeniería Social
- Categoría Robo de Información
- Fecha de incidente 26 de Agosto 2020
- Fecha de reporte 26 de Agosto 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), fue reportada una campaña de phishing vía mensajes de WhatsApp relacionado al programa **QUÉDATE EN CASA** que contiene una URL haciendo referencia a realizar un proceso de registro de datos para recibir el beneficio.



Se ha analizado el enlace en un ambiente controlado y se observa que al acceder se solicita que el usuario ingrese información en un formulario webs capturando información de país, nombre, edad y teléfono con fines de recolectar esta información personal.

## INDICADORES DE COMPROMISO (IoC)

**Remitente**  
Mediante mensaje de WhatsApp

**Conexiones IP**  
50[.]31[.]188[.]30

**Asunto**  
Ayuda quedate en casa

**DNS Request**  
<https://ayudaquedateencasa.org>



# RECOMENDACIONES

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.