



INC-01115-S9N9

ALERTA DE SEGURIDAD



CSIRT-RD

Equipo Nacional de Respuestas a Incidentes
Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 21 DE JULIO 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

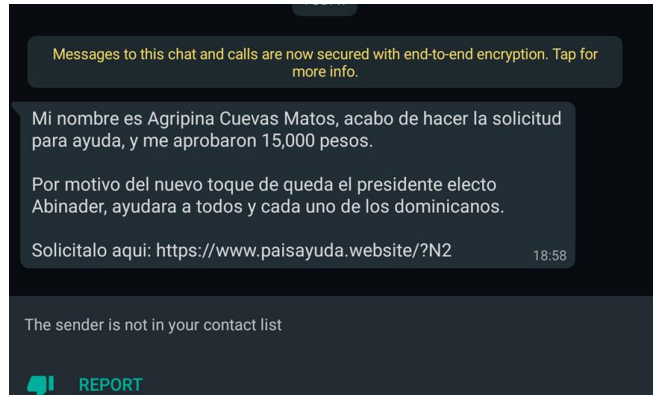
- ID INC-01115-S9N9
- TLP Blanco
- Tipo de incidente Ingeniería Social
- Categoría Robo de Información
- Fecha de incidente 21 de julio 2020
- Fecha de reporte 21 de julio 2020
- Nivel de peligrosidad **Ambar**

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.

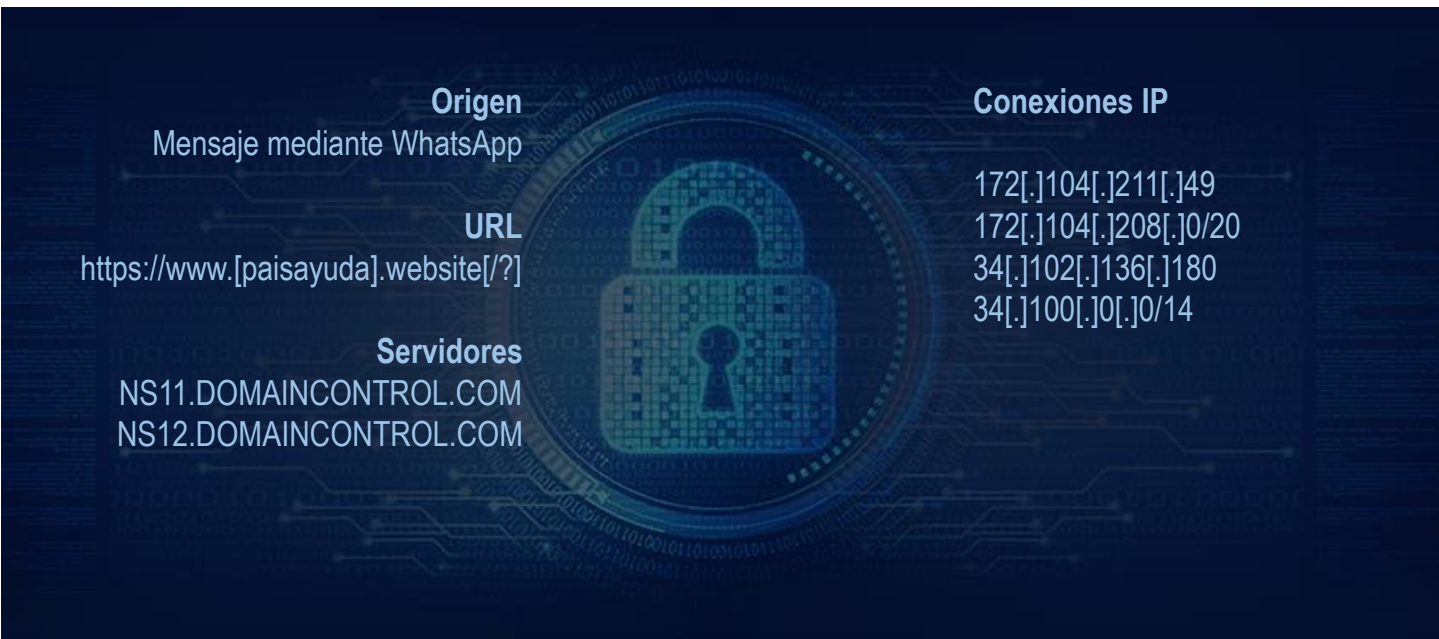
DETALLES DE LA ALERTA

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 relacionada a una **solicitud de ayuda económica debido al nuevo toque de queda** mediante whatsapp.



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

INDICADORES DE COMPROMISO (IoC)



Origen Mensaje mediante WhatsApp	Conexiones IP 172[.]104[.]211[.]49 172[.]104[.]208[.]10/20 34[.]102[.]136[.]180 34[.]100[.]0[.]10/14
URL https://www.[paisayuda].website/[?]	
Servidores NS11.DOMAINCONTROL.COM NS12.DOMAINCONTROL.COM	



Página HTML que es enviada mediante el link del mensaje..



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 instantánea.
3. Mantener actualizadas las plataformas y sistemas de información.
4. Realizar campañas de concientización periódica a todos los usuarios de la institución.