

INC-01110-L1X7

ALERTA DE SEGURIDAD



CSIRT-RD

Equipo Nacional de Respuestas a Incidentes
Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 06 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

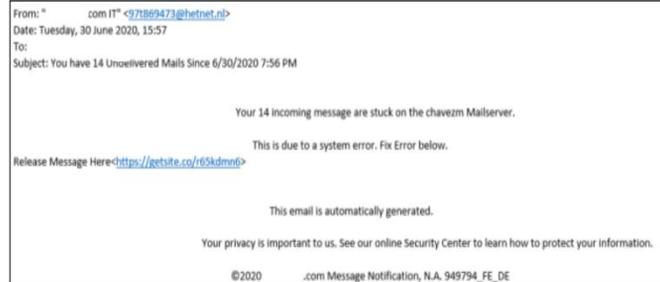
- ID INC-01110-L1X7
- TLP Blanco
- Tipo de incidente Ingeniería Social
- Categoría Robo de Información
- Fecha de incidente 30 de junio 2020
- Fecha de reporte 02 de julio 2020
- Nivel de peligrosidad **Medio**

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), se ha identificado una campaña de phishing el asunto; **“You have 14 Undelivered Mails Since 6/30/2020 7:56 PM ”** que invita al usuario acceder aun link para actualizar los datos de su cuenta para resolver supuestos problemas con su bandeja de correo.



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)

The background of this section features a large, stylized padlock icon in the center, surrounded by a circular pattern of binary code (0s and 1s). The overall color scheme is dark blue with lighter blue highlights.

Remitente 971869473[@]hetnet[.]nl	Conexiones IP 3[.]82[.]166[.]181
Asunto “You have 14 Undelivered Mails Since 6/30/2020 7:56 PM”	Peticiones HTTP https[:]//getsite[.]co/r65kdmn6

The image shows a person's hands typing on a laptop keyboard. A digital shield with a keyhole and binary code is overlaid on the right side of the image. The word 'RECOMENDACIONES' is written in large, white, bold letters across the middle of the image, underlined.

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 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.