INC-01194-W1K1

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 27 DE ENERO 2021

PRESIDENCIA DE LA REPÚBLICA DOMINICANA

MINISTERIO DE LA PRESIDENCIA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CSIRT-RD

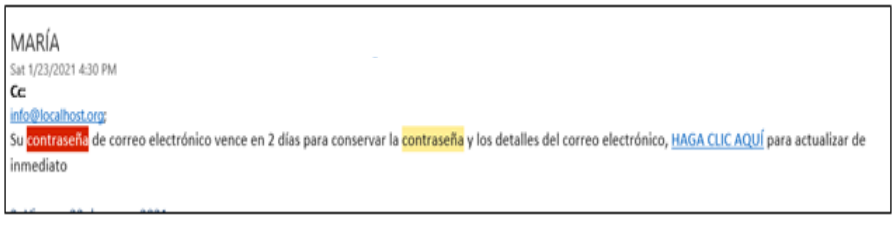
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

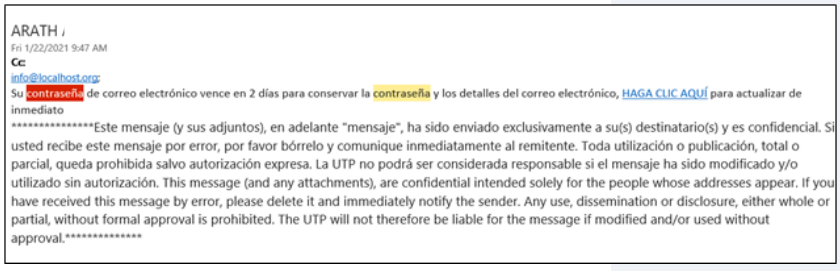
ALERTA DE SEGURIDAD

- **ID** INC-01194-W1K1
- **TLP** Blanco
- **Tipo de incidente** Ingeniería Social
- **Categoría** Robo de Información
- **Fecha de incidente** 19 de Enero 2021
- **Fecha de reporte** 26 de Enero 2021
- **Nivel de peligrosidad ALTO**

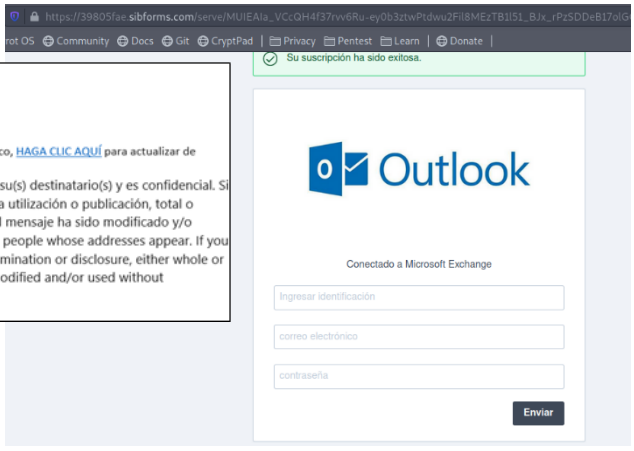
DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes CSIRT- RD ha recibido una notificación relacionada a una campaña de phishing que hace referencia a un enlace para realizar el **registro de credenciales** a los usuarios indicado que la contraseña de correo esta **próxima a vencer** y que requiere cambio.


MARÍA
Sat 1/23/2021 4:30 PM
Cc
info@localhost.org
Su contraseña de correo electrónico vence en 2 días para conservar la contraseña y los detalles del correo electrónico, HAGA CLIC AQUÍ para actualizar de inmediato



Muestra de variante del correo de suplantación de identidad.



Suplantación de portal de credenciales de Outlook para verificar y cambio de contraseña.

INDICADORES DE COMPROMISO (IoC)

Conexiones

- 104[.]18[.]174[.]7

Soluciones de Dominio DNS

- c8679251[.]sibforms[.]com
- 39805fae[.]sibforms[.]com
- f17ca927[.]sibforms[.]com

Peticiones HTTP

- https://f17ca927[.]sibforms.com/serve/MUIEAFrh8U0eVUP-zsY7FZA3Yx7rEp9xVSV-UmsHgz2zX9n4PT3kmDb-pmAWvtVv29sfU08amkyz7D496QdoOBm4wYUAsfMjK9KmThagc8uHhRSKsCQmAS98qRpDt1iLgNBrJEAwWySO_724iyAkqY7FAKUNt6XICh77nO4SXbcBIaO_bQjkU-e7H0pCgntxtiunfadBzey6iepq

- https://39805fae[.]sibforms[.]com/serve/MUIEAIa_VCcQH4f37rvv6Ru-ey0b3ztwPtdwu2Fil8MEzTB1l51_BJx_rPzSDDeB17olGG1kfD79Q5dDbcmjAvpT5mSY9MxljKcF5f38U3IONpfwWKHUT5Zu67rcliTXYj3aF6ggGVPk3KDmG-r4ih8F1NxLGTSwLBGqffdLr6HSnp-6w8pk2Qa8thLrDSweqpXTb9RjG2vZ12JE

- https://c8679251[.]sibforms[.]com/serve/MUIEABbP69ghhZbV1Ti2WfJS330e3zMO9etXG339pHQlxuLHsGeAW0j453TcK3089iQ1SywYzhlA_CbOYNm4MPFNS5jT8Gr16u2EBqD2YBgMfIEEjgR6Acrt_x3bZB-LVPE3-GHvgDNbBu58rRQYheDJjH_gGZzRR0l7v-avVZ04z1gJ9KOOZo40pnAg7ytNGl0ST0s79-J4wO0C

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 de la institución.
5. No introducir los datos personales en portales web sin antes verificar los controles de seguridad de la misma.