INC-01136-L3V3

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 31 DE AGOSTO 2020

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

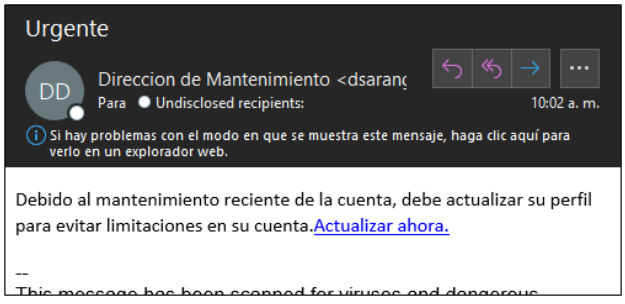
- **ID** INC-01136-L3V3
- **TLP** Blanco
- **Tipo de incidente** Ingeniería Social
- **Categoría** Robo de Información
- **Fecha de incidente** 28 de Agosto 2020
- **Fecha de reporte** 28 de Agosto 2020
- **Nivel de peligrosidad** **ALTO**

RESUMEN EJECUTIVO

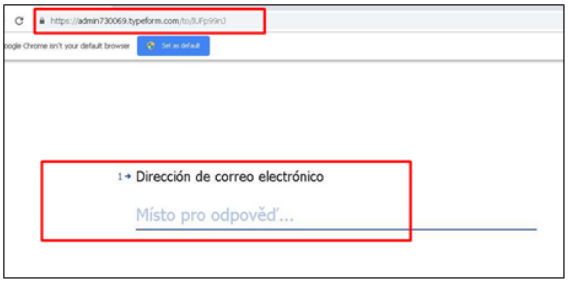
Las organizaciones están expuestas a diferentes amenazas cibernéticas como consecuencia de la utilización de páginas web, aplicaciones móviles, correo electrónico, redes sociales, entre otras. La mayoría de estas amenazas están siendo diseñadas para el robo de información personal o corporativa con el 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

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 correo electrónico con el asunto **"Urgente"** que contiene una URL haciendo referencia a realizar un proceso de actualización indicando "**Actualizar ahora**"



Se ha analizado el URL suministrado en un ambiente controlado y se observa realiza la solicitud de credenciales al usuario .



INDICADORES DE COMPROMISO (IoC)

Remitente
dsarango@eloro[.]gob[.]ec

Asunto
Urgente

Conexiones IP
107[.]23[.]29[.]155

Peticiones HTTP
https[:]//admin730069[.]typeform[.]com/to/IUFp99nJ

Solicitudes de dominio DNS
admin730069[.]typeform[.]com

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. No compartir contraseñas , usuarios ni otro tipo de credenciales en enlaces que tenga dudas de su procedencia.
5. Realizar campañas de concientización periódica a todos los usuarios de la institución.