INC-01162-N9M7

ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 11 DE NOVIEMBRE 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-01162-N9M7
- **TLP** Blanco
- **Tipo de incidente** Ingeniería Social
- **Categoría** Robo de Información
- **Fecha de incidente** 11 de Noviembre 2020
- **Fecha de reporte** 11 de Noviembre 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 Equipo Nacional de Respuestas a Incidentes Cibernéticos (CSIRT-RD), fue reportado un portal que suplanta un servicio de verificación de pagos del Banco Central de la Republica Dominicana.

Dentro del portal se encuentran los logos de la mayoría de los bancos locales , donde le indica al usuario que seleccione la plataforma a utilizar.

Para el robo de credenciales se le solicita al usuario desde el portal web **https[:]//certifiquesupagod[.]com/login[.]html** que ingrese sus credenciales de usuario y contraseña

INDICADORES DE COMPROMISO (IoC)

Conexiones IP
148[.]66[.]138[.]126

Peticiones HTTP
https[:]//certifiquesupagod[.]com

Soluciones de Dominio DNS
certifiquesupagod[.]com

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.