CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

REPÚBLICA DIGITAL

ALERTA DE SEGURIDAD

Estafa - Correo Electrónico

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Fecha de publicación: 17 de abril 2020

ALERTA DE SEGURIDAD

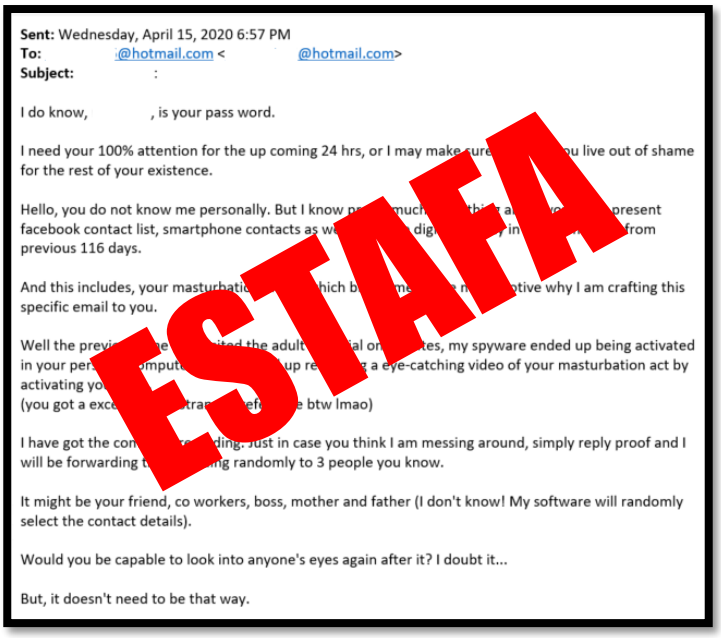
TLP	Blanco
Tipo de incidente	Ingeniería Social
Categoría	Robo de Información
Fecha de reporte	15 de abril 2020
Nivel de peligrosidad	Medio

RESUMEN EJECUTIVO

Las organizaciones están expuestas a diferentes amenazas cibernéticas como consecuencia de la utilización de páginas web, aplicaciones móviles, correos electrónicos, redes sociales, entre otras. **La mayoría de estas amenazas están siendo diseñadas para robar información personal o corporativa con el objetivo de crear ataques cibernéticos**.

DETALLES DE LA ALERTA

El CNCS ha detectado una nueva campaña de correos electrónicos fraudulentos, donde el ciberatacante extorsiona a los destinatarios revelando que posee un supuesto vídeo íntimo con contenido sexual y que tiene en su poder las credenciales del correo electrónico de la víctima. El ciberatacante amenaza con hacer pública la información si no se realiza el pago de una determinada cantidad en bitcoins, facilitando un enlace de una billetera virtual a través de la cual solicita que se realice la transferencia. **La extorsión otorga un plazo de 24 horas para realizar el pago.**



El correo electrónico fraudulento se envía desde una cuenta genérica de correo electrónico (@gmail.com, @hotmail.com). El cuerpo del mensaje, en la mayoría de los casos, está en inglés.

Con el objetivo de convencer aún más a la víctima, el atacante añade en el cuerpo del correo una contraseña vinculada a su cuenta. Esta contraseña pudo haber sido obtenida en las bases de datos recientemente filtradas en páginas y servicios de internet.

RECOMENDACIONES

1. Actualizar las contraseñas de sus cuentas de servicios por contraseñas robustas. Ej. (#*¡**” #$Ms. () =**)
2. Comprueba cada una de tus cuentas de correo electrónico y contraseñas para verificar si han sido comprometidas en las herramientas del Centro Nacional de Ciberseguridad: https://cncs.gob.do/csirt-rd/herramientas/
3. Solo introducir datos confidenciales en páginas no oficiales.
4. No realizar el pago solicitado y realizar el reporte a incidentes@csirt.gob.do