Bogotá, 27 de febrero de 2019

Phishing Davivienda

Confidencial*

Contexto de la situación

En días anteriores ColCERT emitió una alerta vía Twitter (anexo imagen), en la cual se menciona la suplantación del sitio de Davivienda.

CSIRT de Gobierno recomienda nuevamente evaluar los controles de seguridad con el fin de evitar que dicha suplantación se convierta en fraude electrónico, afectando a los funcionarios y contratistas de las entidades.

Ya se han reportado a la fecha en dos entidades del estado, donde se ha hecho efectivo el fraude a más de 50 funcionarios, realizando compras de Netflix, PayPal, pagos de servicios, compras dirigidas, etc.

El phishing aprovecha que el sitio autentica con usuario y contraseña, no utiliza doble factor de autenticación al iniciar sesión, esta se realiza a través de un software que está disponible para descargar (anexo imagen) o a través de algún parámetro habilitado por los usuarios.

Por lo general es a posterior que llega algún tipo de alerta al usuario, pero ya se ha realizado la transacción fraudulenta.

EL CCP (DIJIN) está realizando el acompañamiento a las entidades, realizando las indagaciones respectivas, así como recogiendo las denuncias para formalizar el caso.

Recomendaciones

- Reforzar los controles perimetrales.
- Verificar que el antivirus en las estaciones y su consola de administración, tengan las firmas actualizadas y estén realizando el análisis respectivo.
- Evaluar el explorador que utilizan los funcionarios, de manera que no sea vulnerable.
- Realizar recomendaciones a los funcionarios que efectúan transacciones en los equipos de la entidad.
- A través de campañas identificar usuarios que hayan sido afectados con el fin de que se realice el procedimiento para formalizar la denuncia y recolección de evidencias.

En caso de ser necesario puede comunicarse con CSIRT Gobierno por medio de los siguientes canales:

Csirtgob@mintic.gov.co

018000910742 opción 4.