UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS	**BOLETÍN DE SEGURIDAD 2018-01** **RED DE DATOS UDNET** **ALERTA SOBRE CORREOS MALICIOSOS**	RED DE DATOS UDNET
	Fecha: 10-08-2018 | **Versión: 1**	

RESUMEN:

Esta alerta y solicitud se hace a causa de la filtración de mensajes de correo electrónico maliciosos que buscan aprovechar algunas vulnerabilidades en diferentes programas y sistemas operativos, en especial Windows. Puede comprometer la seguridad de la información alojada en los equipos de cómputo donde sean abiertos, así como otros equipos en la red, permitiendo robar, alterar o borrar la información que haya sido comprometida.

¿QUÉ ES UN CORREO MALICIOSO?:

Es un tipo de mensaje de correo electrónico que tienen fines maliciosos, tiene apariencia de ser un correo de una fuente confiable pero realmente no lo es. Puede incluir archivos adjuntos que al abrirlos ejecutan un malware (programa informático malintencionado) que infecta el equipo de cómputo con el fin de robar credenciales bancarias, robar, alterar, borrar o secuestrar la información alojada en los equipos de cómputo, entre otros. Básicamente si un usuario abre un correo electrónico de este tipo es posible que su información o parte de la misma sea comprometida o que termine siendo víctima de una extorsión por internet.

¿CÓMO SE PROPAGA?:

Existen diferentes tácticas usadas para la difusión de correos maliciosos, unas de ellas son:

1. Mensajes que piden actualizar los datos de una cuenta bancaria, de correo o página WEB e incluyen un enlace que dirige a una página WEB fraudulenta para que el usuario ingrese la información solicitada y de esta forma robarla. A continuación se presenta un ejemplo:

   De: Patrik Hansson <patrik.hansson@abf.se> **-> el dominio "abf.se" es sospechoso**
   Enviado el: jueves, 26 de julio de 2018 11:38 a.m.
   Para: undisclosed-recipients: **-> no se identifica que el mensaje es para alguien específico**
   Asunto: Universidad Distrital Francisco José de Caldas

   Estimado usuario de cuenta,

   Estamos cerrando nuestro correo web actual para crear espacio para 2018 Web Access con una gran definición visual y espacio. Este servicio crea más espacio y fácil acceso al correo electrónico. Actualice su cuenta haciendo clic en el enlace a continuación y complete la información para la Activación.

   HAGA CLIC AQUÍ **-> contiene enlaces a páginas WEB fraudulentas**

   Siga el procedimiento y complete la información haciendo clic en Iniciar sesión. Se creará un nuevo espacio dentro de las 48 horas. **-> solicita información confidencial (credenciales de acceso)**

   Gracias por entender,

   Equipo de ayuda. **-> La firma es sospechosa al no contener información del remitente.**

2. Mensajes de cobros de multas que parecen ser de entidades o empresas confiables, incluyen una clave para abrir el archivo que está adjunto al correo electrónico e intimidan con consecuencias si no realiza un pago:

De: Registraduria Nacional del Estado Civil [mailto:notificacionprocesos@registraduria.gov.co]
-> el dominio de la Registraduría aparenta confiabilidad
Enviado el: martes, 17 de julio de 2018 03:50 p.m.
Para: Undisclosed-Recipients: ***-> no se identifica que el mensaje es para alguien específico***

Asunto: Usted tendrá que pagar una multa de 10 salarios mínimos mensuales legales vigentes porque no asistió a cumplir con sus deberes con el cargo como Jurado votación
Importancia: Alta

Bogotá 17 de Julio

Registraduría Nacional del estado Civil: SEGUNDA NOTIFICACION

Señor ciudadano, teniendo en cuenta las votaciones realizadas el 27 de mayo de 2018, y según el informe presentado por el delegado de la registraduría encargado del punto de votación en cual usted fue asignado y avisado con 3 meses de anticipación, usted no asistió a cumplir con sus deberes con el cargo como JURADO DE VOTACION.

El artículo 105 del Código Electoral establece que el cargo de jurado de votación es de "forzosa aceptación" y el incumplimiento de esas obligaciones puede acarrear sanciones de hasta 20 años de inhabilidad para ejercer cargos públicos.

Si no es un servidor público, tendrá que pagar una multa de hasta de 10 salarios mínimos mensuales legales vigentes.

Según lo anterior Hemos adjuntado detalles de descargos legales y circular de citación.
-> Informa que tiene un archivo adjunto, en este caso un fichero comprimido que contiene malware.
Todo documento adjunto personal es adjuntado con una clave
-> Informa la clave para descomprimir el fichero adjunto que contiene malware.
la clave del documento adjunto es : 20180709registraduria421e68dd993c4a8bb9e3d5e6c066946r

¿CUALES SON LOS SISTEMAS Y VERSIONES AFECTADOS?:

En especial cualquier versión de los sistemas operativos Microsoft Windows, programas como Microsoft Office, Adobe Acrobat, Reproductores multimedia, entre otros. Sin embargo, la Red de Datos UDNET ha detectado malware en equipos con otros sistemas operativos por lo cual se sugiere ser cauteloso sin importar la plataforma que se use.

¿QUÉ DEBO HACER COMO USUARIO?:

1. No confíe en correos electrónicos sospechosos, no acceda a vínculos de páginas WEB o archivos adjuntos que estén incluidos en ellos y no responda nunca a estos mensajes.

2. Si recibe un mensaje de alguna entidad bancaria o ente gubernamental, no acceda a vínculos que se encuentre en el mensaje ya lo pueden redirigir a páginas web fraudulentas para robar sus credenciales de acceso. Si requiere ingresar a un portal web de entidad bancaria digite la dirección URL directamente en el navegador web.

3. Notifique a la Red de Datos UDNET reenviando el correo sospechoso a servidores@udistrital.edu.co, el área de Plataformas Computacionales analizará el mensaje y tomará las acciones necesarias para mitigar los riesgos informáticos implicados.

4. Nunca comparta información personal ni financiera solicitada a través de correos electrónicos, llamadas telefónicas, mensajes de texto o redes sociales.

5. Tenga cuidado con los sitios web que visite, desconfíe de los dominios que no conozca.

6. Si requiere descargar software asegurese que sea de sitios que conozca y considere confiables, en caso de no conocer o desconfiar de la página de donde está descargando el software consulte con el área de soporte de su facultad o sede para obtener asesoría en el proceso.

7. No descargue contenido multimedia por redes de intercambio tales como ares u otro gestor de descargas.

8. Evite conectar dispositivos extraíbles que desconozca su procedencia como dispositivos USB.

9. Tenga una copia de seguridad (backup) de su información.

10. Haga las actualizaciones de su sistema operativo. Para que estas sean efectivas su software debe ser legal. Consulte con el área de soporte de su facultad o sede para verificar este procedimiento.

11. Mantenga su software de seguridad (antivirus) activado y actualizado. Consulte con el área de soporte de su facultad o sede para verificar este procedimiento.

Atentamente,

Ing. Hernán Darío Orjuela Morales.
Ingeniero Servidores Red UDNET.
servidores@udistrital.edu.co