ransomware
LockBit Black

Se ha detectado en nuestra plataforma de correo UPTC, una campaña de correos fraudulentos de tipo phishing, que, a través de un adjunto, pretenden instalar un ransomware LockBit Black capaz de cifrar los archivos contenidos en el dispositivo.

El ransomware es un malware que cifra y mantiene secuestrado o bloqueado los datos de un dispositivo, la tendencia de uso de esta práctica malintencionada incrementa al mismo tiempo que crece las transacciones en criptomonedas. Por otra parte, los correos de nuestro dominio son usados como trampolín para que un ciberdelincuente invada a otras instituciones con prácticas ilícitas.

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones

Denuncie a soporte.seguridad@uptc.edu.co cualquier correo que no ha solicitado o mensaje que lo involucre en una actividad que no tenga conocimiento, cualquier campaña publicitaria en la que no pueda confirmar su procedencia, recuerde que en avisos y enlaces que se cliquean inocentemente puede existir la descarga e instalación de un malware.

Los mensajes recibidos pueden provenir de correos de su propia lista de contactos denunciando, alertando, invitando a contestar o descargar un archivo con formato pdf u ofimático que se presume inofensivo, pero en realidad realizan la descarga de un fichero comprimido que contiene un programa malicioso que se ejecuta autónomamente en segundo plano e imperceptiblemente para él usuario.

Generalmente esos mensajes están acompañados de técnicas phishing que pretenden engañar o persuadir al usuario para la descargar del software dañino, en muchos de los casos provienen de dominios de uso general como Gmail, Hotmail, Outlook etc, que los hace reconocibles para dudar de ellos.

Nuestro dominio @uptc.edu.co posee el licenciamiento y certificación que lo posiciona en niveles de confianza transaccional óptimo para que los destinatarios tengan la credibilidad suficiente para aceptarnos, para que otros dominios no nos bloqueen, ni nos coloquen en listas negras.

Por lo anterior algunos de nuestros correos han sido usurpados o hackeados por terceros para ser usados como medio de envió y reenvió de mensajes no solicitados tipo SPAM como notas o comunicaciones que buscan engañar a sus destinatarios; el ejercicio ocurre cuando es lanzando contenidos a listas donde el remitente es nuestro correo y la respuesta a los mismos son re direccionadas a un buzón desconocido. Por lo general la emisión de esos mensajes son malintencionados y están encaminados en la búsqueda de una consignación monetaria en donde nos podemos ver envueltos.

Nos podemos dar cuenta que nuestro correo está siendo **usado por un tercero cuando**:

- En la bandeja de envió vemos mensajes que **no hemos emitido conscientemente**.
- Cuando al enviar un mensaje nuestro destinatario lo percibe **con un nombre distinto o alterado**
- Cuando recibimos mensajes por no entrega a un **destinatario que no conocemos**.

Este problema sucede por tener contraseñas no seguras **Cómo actuar ante este incidente**

Para corregir siga los siguientes pasos:

1. Cambie la contraseña de acceso al correo institucional por autoservicio que lo encuentra en la parte final de la página de acceso al correo en el portal de la institución o en el siguiente link:

https://apps1.uptc.edu.co/Autoservicios/#/dashboard/main

2. Después del cambio de credenciales de acceso por favor **ingresar a configuración** que es el icono que encuentra en la parte superior derecha en forma de piñón en medio del icono de interrogación y el icono de acceso a los aplicativos de google conformado por un cuadrado por 9 puntos; seguidamente ingrese a ver todos los ajustes

3. En la ventana que se abre encontrará un menú horizontal con las palabras General, Etiquetas, Recibidos, Cuentas, Filtros y direcciones bloqueadas .... ingrese o haga click sobre **Cuentas**

4. De arriba hacia abajo encontrará **enviar como**: allí puede estar la afectación a nuestro correo es donde el software malicioso o malware realizó el cambio y puede restablecerlo haciendo click en el vínculo **editar datos**

5. Al ingresar por editar datos, se abre una ventana amarilla donde puede reestablecer el nombre del correo y borrar o quitar el direccionamiento a otro correo que muy seguramente no es conocido.

6. En la ventana con el menú horizontal con las palabras General, Etiquetas, Recibidos, Cuentas, Filtros y direcciones bloqueadas, Reenvío y correo POP/IMAP .... ingrese o haga click sobre **Reenvío y correo POP/IMAP**

7. En el apartado **reenvió** no debe existir ninguna cuenta debe estar deshabilitado y en el caso de que exista una cuenta debe de eliminarla o quitarla dentro del mismo combox.

8. En el caso de que se encuentre habilitado el pop **debe inhabilitarlo** también

9. Corra o **ejecute un antivirus y/o antimalware capaz de identificar gusanos informáticos, spoofing** que presuntamente es el responsable de la afectación, haga este punto en todos los equipos incluyendo los móviles en donde aperturo la cuenta institucional.

Con efecto de seguimiento y prevención **informe a DTIC-UPTC** de lo sucedido con el objeto de tomar las medidas pertinentes desde el área de seguridad de la información y correo electrónico, recuerde que el uso del correo institucional es de su responsabilidad

Próxima temática Creación de contraseñas seguras