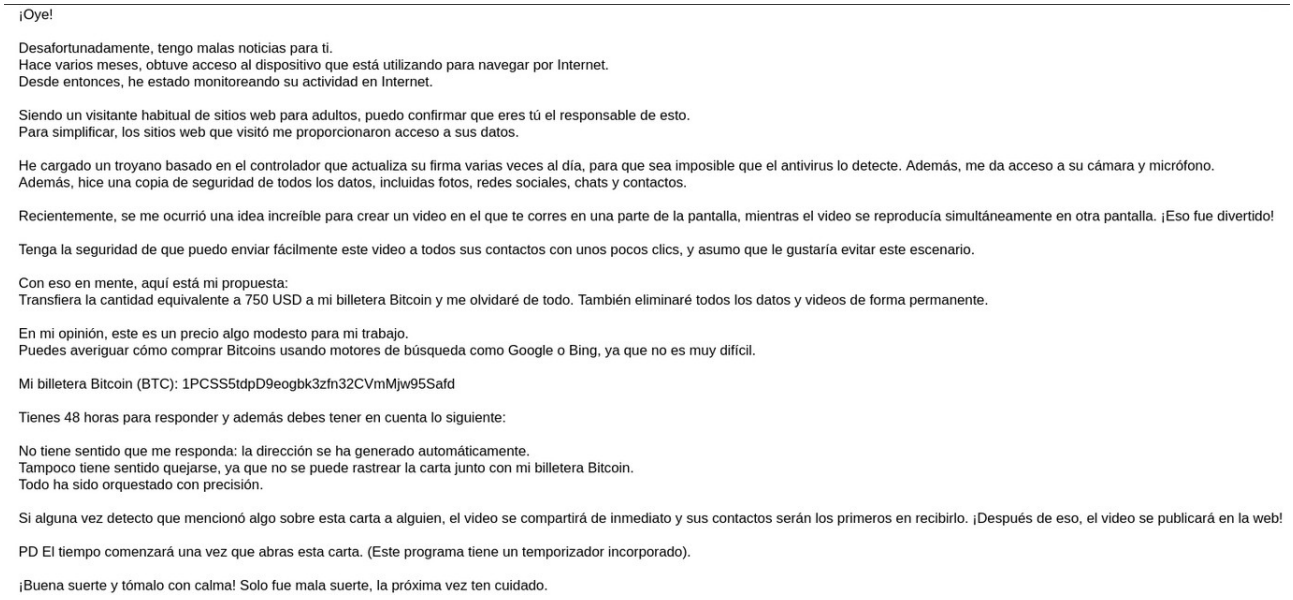
Extorsión



¡Oye!

Desafortunadamente, tengo malas noticias para ti.
Hace varios meses, obtuve acceso al dispositivo que está utilizando para navegar por Internet.
Desde entonces, he estado monitoreando su actividad en Internet.

Siendo un visitante habitual de sitios web para adultos, puedo confirmar que eres tú el responsable de esto.
Para simplificar, los sitios web que visitó me proporcionaron acceso a sus datos.

He cargado un troyano basado en el controlador que actualiza su firma varias veces al día, para que sea imposible que el antivirus lo detecte. Además, me da acceso a su cámara y micrófono.
Además, hice una copia de seguridad de todos los datos, incluidas fotos, redes sociales, chats y contactos.

Recientemente, se me ocurrió una idea increíble para crear un video en el que te corres en una parte de la pantalla, mientras el video se reproducía simultáneamente en otra pantalla. ¡Eso fue divertido!

Tenga la seguridad de que puedo enviar fácilmente este video a todos sus contactos con unos pocos clics, y asumo que le gustaría evitar este escenario.

Con eso en mente, aquí está mi propuesta:
Transfiera la cantidad equivalente a 750 USD a mi billetera Bitcoin y me olvidaré de todo. También eliminaré todos los datos y videos de forma permanente.

En mi opinión, este es un precio algo modesto para mi trabajo.
Puedes averiguar cómo comprar Bitcoins usando motores de búsqueda como Google o Bing, ya que no es muy difícil.

Mi billetera Bitcoin (BTC): 1PCSS5tdpD9eogbk3zfn32CVmMjw95Safd

Tienes 48 horas para responder y además debes tener en cuenta lo siguiente:

No tiene sentido que me responda: la dirección se ha generado automáticamente.
Tampoco tiene sentido quejarse, ya que no se puede rastrear la carta junto con mi billetera Bitcoin.
Todo ha sido orquestado con precisión.

Si alguna vez detecto que mencionó algo sobre esta carta a alguien, el video se compartirá de inmediato y sus contactos serán los primeros en recibirlo. ¡Después de eso, el video se publicará en la web!

PD El tiempo comenzará una vez que abras esta carta. (Este programa tiene un temporizador incorporado).

¡Buena suerte y tómalo con calma! Solo fue mala suerte, la próxima vez ten cuidado.

La imagen muestra un ejemplo de correo electrónico utilizado en campañas de extorsión digital. En este tipo de mensajes, el atacante afirma haber obtenido acceso al dispositivo de la víctima, asegura haber recopilado información personal y amenaza con difundir supuestos contenidos privados si no se realiza un pago, generalmente en criptomonedas.
Estos correos suelen utilizar un lenguaje intimidatorio, plazos urgentes y afirmaciones técnicas falsas para generar miedo y presionar a la persona destinataria. En la mayoría de los casos, no existe ningún acceso real al dispositivo ni material comprometedor: se trata de un engaño masivo basado en la manipulación psicológica.
Ante mensajes de este tipo, se recomienda no responder, no realizar pagos y reportar el correo como fraude o spam a protege@unq.edu.ar