binauramonlex

Área de ciberseguridad de Monlex

Seguridad 360°

Newsletter de Ataques.

NEWSLETTER DE ATAQUES

1. Nuevo Ataque de Phishing Suplantando cliente en Expedia y Booking:

binauramonlex

Área de ciberseguridad de Monlex

Seguridad 360º

Newsletter de Ataques.

Nuevo Ataque de Phishing Suplantando cliente en Expedia y Booking:

Desde BinauraMonlex queremos avisar de un nuevo tipo de ataque por ingeniería social que hemos detectado y que está siendo bastante efectivo en cuanto al vector de entrada. Este ha ocurrido en un establecimiento de Cala Figuera y en otro de Alcúdia.

Os idicamos cómo lo han hecho para que podáis evitarlo.

Los delincuentes contactan a través de Booking o Expedia con el establecimiento y siguen estos pasos:

1) Mandan un correo indicando que tiene muchas alergias alimentarias y de productos de limpieza y que le gustaría mucho ir a ese establecimiento pero que no sabe si será adecuado dadas esas alergias.

2) Una vez tiene la respuesta del hotel (convencido de que tiene este problema el cliente) envía un correo con un enlace a un documento de Dropbox con contraseña:

EL ENLACE ESTÁ MODIFICADO PARA QUE NO VAYA A ESA DIRECCIÓN PERO MEJOR NO CLICKAR POR SI ACASO.

https://www.dropbox.com/s/18jf3j9ue8pjxhg/docsHOTEL.zip?dl=0

password: "cualquiera que envíen"

3) Cuando se accede a ese documento el establecimiento lo descomprime y todo parece indicar que es un PDF, pero no, es un documento de SRC(screensaver) que se ejecuta en la máquina infectándola. También puede venir en formato .exe emulando un adjunto PDF.

4) El documento aparenta tener un tamaño de 1'3GB para eludir el escaneo de los antimalware ya que estos solo escanéan hasta cierto tamaño de fichero.

binauramonlex

Área de ciberseguridad de Monlex

Seguridad 360º

Newsletter de Ataques.

Os pasamos un vídeo de cómo entraron en la cuenta de un Youtuber dedicado a la tecnología con más de 15 millones de suscriptores (en inglés) con un ataque muy similar en cuanto al tipo de acceso (el fichero src):

https://www.youtube.com/watch?v=nYdS3FIu3rI

Adjuntamos los Hashes del fichero para que vuestros equipos de IT o ciberseguridad los integren en vuestros antimalware o reglas YARA:

MD5	968026669389a833271164aebde9b947
SHA1	b3e31084c5ced79e49f96fb29c74b950ffea0702
SHA256	5a6512eaa3f1f7d339ac317a2fb03d1401e7eb2ef276e108a04382c72f8bc958
SHA512	f35daa1d7994ae3370d03ac1c48def5e1d334731d738339fa530f3ab9680fdd8998cda4cb43630bbcaa701f83e6c74d1755b9fe0a6d0cf6bc81b83bc6b99d171

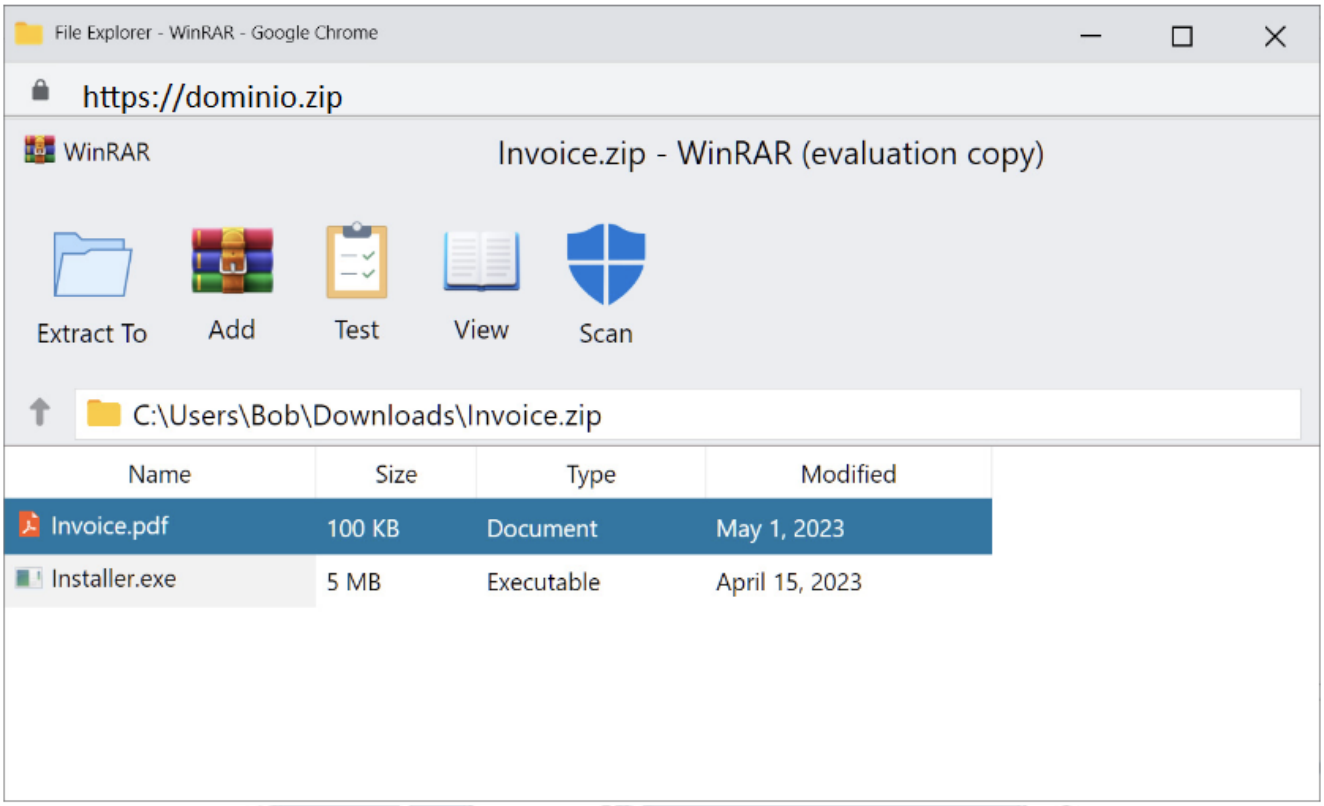
binauramonlex

Área de ciberseguridad de Monlex

Seguridad 360º

Newsletter de Ataques.

Adjuntamos capturas de pantalla de muestra de cómo podría ser un ataque de este tipo:

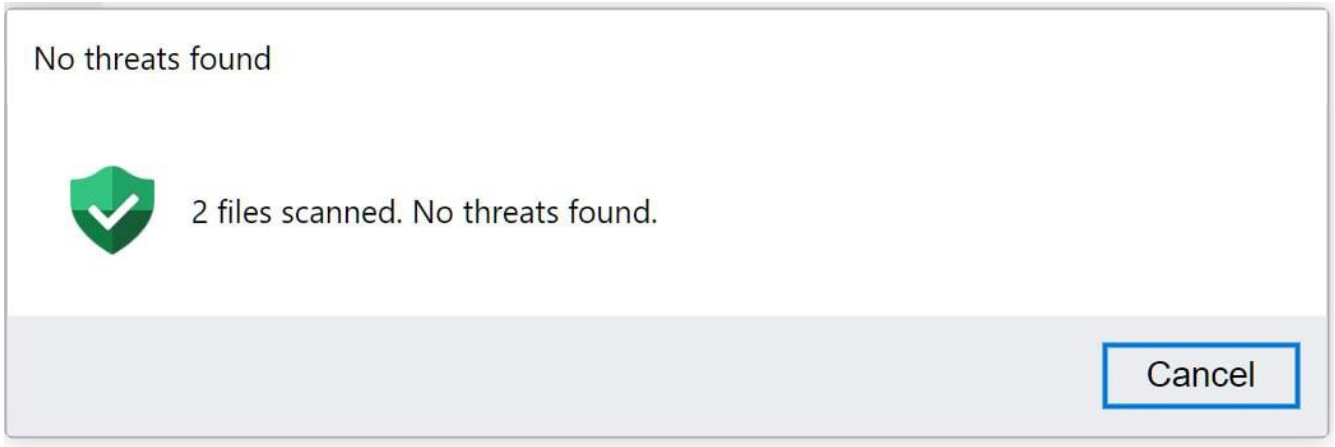


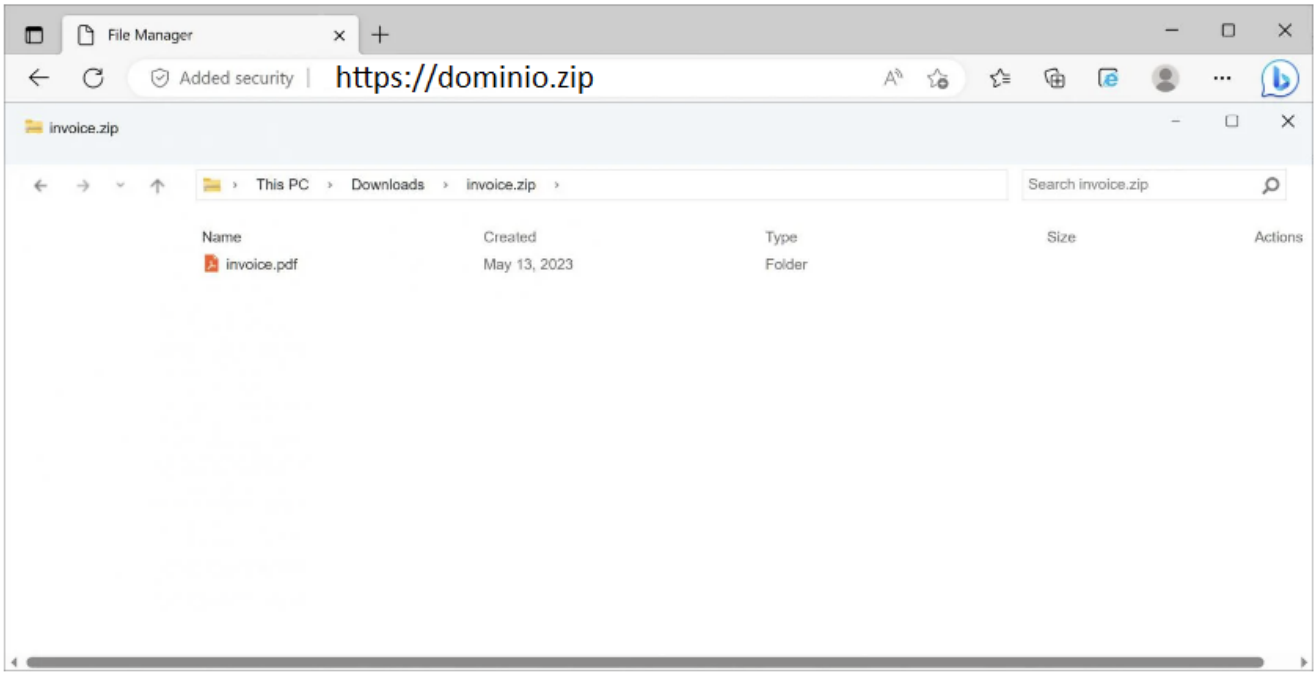
binauramonlex

Área de ciberseguridad de Monlex

Seguridad 360º

Newsletter de Ataques.





binauramonlex

Área de ciberseguridad de Monlex

Seguridad 360º

Newsletter de Ataques.

La Guardia Civil alerta de una nueva estafa por WhatsApp

Al parecer ya son muchas las víctimas que están recibiendo un mensaje de SMS en la que supuestamente "su hijo" les escribe desde un número desconocido debido a que supuestamente el suyo está roto o algo similar.

Así es como el delincuente evita que optes por llamar directamente a tu hijo para que te cuente lo ocurrido y sigas la conversación a través de WhatsApp con este "nuevo número temporal" que tiene.

Como explican, el objetivo principal es hacerse con tus datos personales, pero sí los ciberdelincuentes ven que has picado de verdad en su estafa, también irán a por tus datos bancarios diciendo que necesita dinero para solventar una urgencia.

¿Cómo evitar convertirse en víctima?

Por suerte, como decíamos antes, este tipo de estafas se basan en que el usuario pique en ellas, por lo que estas medidas de protección son fáciles de implementar.

Lo primero que hay que hacer es siempre desconfiar de remitentes desconocidos, si por la calle de repente alguien te parase y te pidiese tus datos personales diciendo que trabaja para el ayuntamiento nunca se los darías, ¿Por qué lo ibas a hacer si ocurre online?

Al tratarse de una artimaña que suplanta a tu hijo, lo mejor es que de verdad compruebes que se trata de él, para ello o bien puedes llamar al número que te ha escrito o llamar al antiguo número de tu hijo para comprobar la veracidad de la historia.

En el caso de que no te lo cojan o detectes algo extraño, lo mejor es no hacerle caso, bloquear el número y acudir a las autoridades con todas las pruebas que tengas.*

*Fuente: El Economista