

Área de ciberseguridad de Monlex

Seguridad 360°

Newsletter de Ataques.

NEWSLETTER DE ATAQUES

1. Nuevo y Peligroso Ataque de Phishing “File Archiver in the
Browser”

2. La Guardia Civil alerta de una nueva estafa por WhatsApp



Certified in
Cybersecurity
An (ISC) Certification

ESPAÑA / USA / REP. DOMINICANA / MÉXICO PORTUGAL / CABO VERDE
JAMAICA / COSTA RICA / CANADA / CHIPRE / REINO UNIDO / BULGARIA
HOLANDA / ALEMANIA / MARRUECOS / TUNEZ / CROACIA / CHINA / ARUBA

Área de ciberseguridad de Monlex

Seguridad 360°

Newsletter de Ataques.

Nuevo Ataque de Phishing "File Archivers in the Browser":

Nuevo y Peligroso Ataque de Phishing "File Archiver in the Browser" Una nueva técnica de phishing denominada "file archiver in the browser" puede aprovecharse para "emular" un software compresor de archivos en un navegador web cuando la víctima visita un dominio .ZIP.

Con este ataque de phishing, se simula un software archivador de archivos (por ejemplo, WinRAR) en el navegador y se utiliza un dominio .zip para que parezca más legítimo.

En un escenario de ataque potencial, un delincuente podría recurrir a este truco para redirigir a los usuarios a una página de recolección de credenciales cuando se hace clic en un archivo "contenido" dentro del falso archivo ZIP.

Otro caso de uso es la inclusión de un archivo no ejecutable y que, cuando el usuario haga clic para iniciar la descarga, se descargue un archivo ejecutable, digamos que tenemos un archivo 'invoice.pdf'. Cuando un usuario haga clic en este archivo, iniciará la descarga de un .exe o cualquier otro archivo.



Certified in
Cybersecurity
An (ISC)² Certification

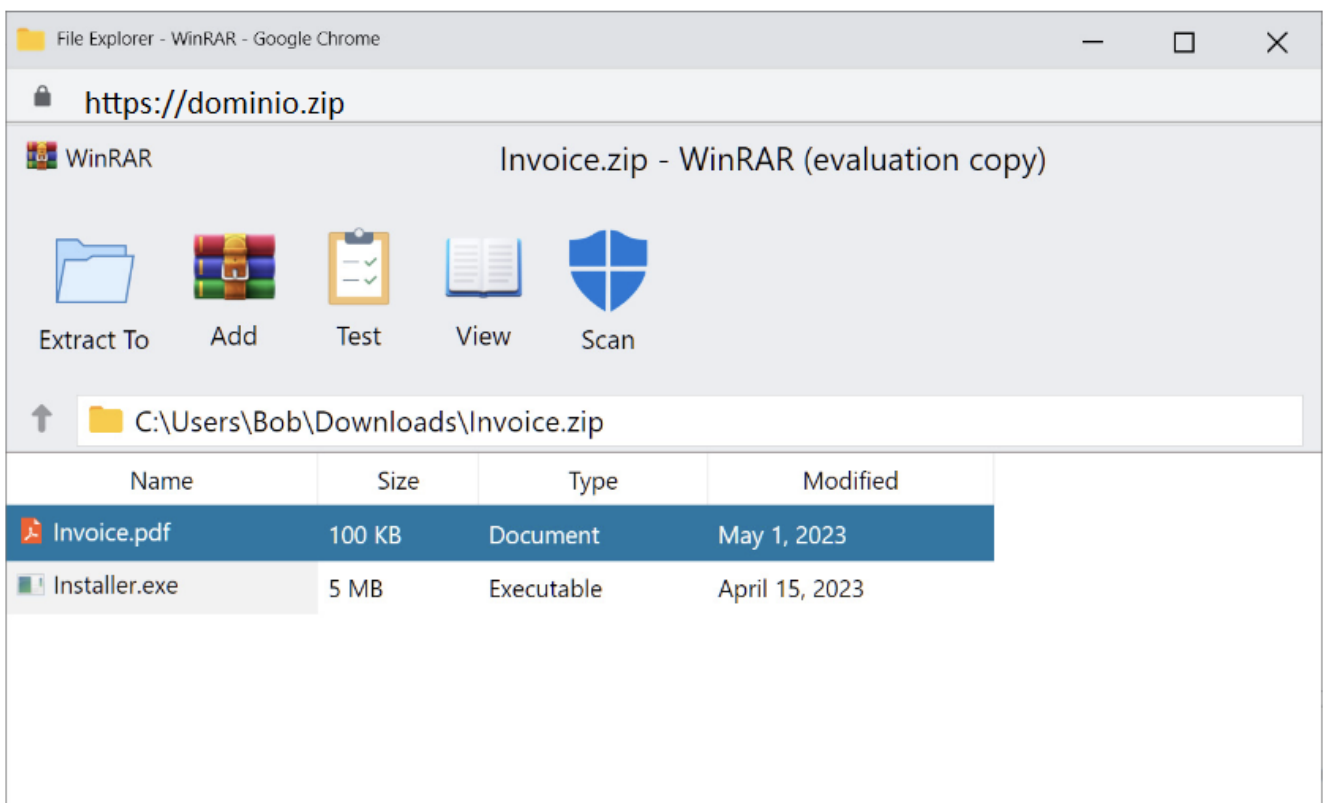
ESPAÑA / USA / REP. DOMINICANA / MÉXICO PORTUGAL / CABO VERDE
JAMAICA / COSTA RICA / CANADA / CHIPRE / REINO UNIDO / BULGARIA
HOLANDA / ALEMANIA / MARRUECOS / TUNEZ / CROACIA / CHINA / ARUBA

Área de ciberseguridad de Monlex

Seguridad 360°

Newsletter de Ataques.

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



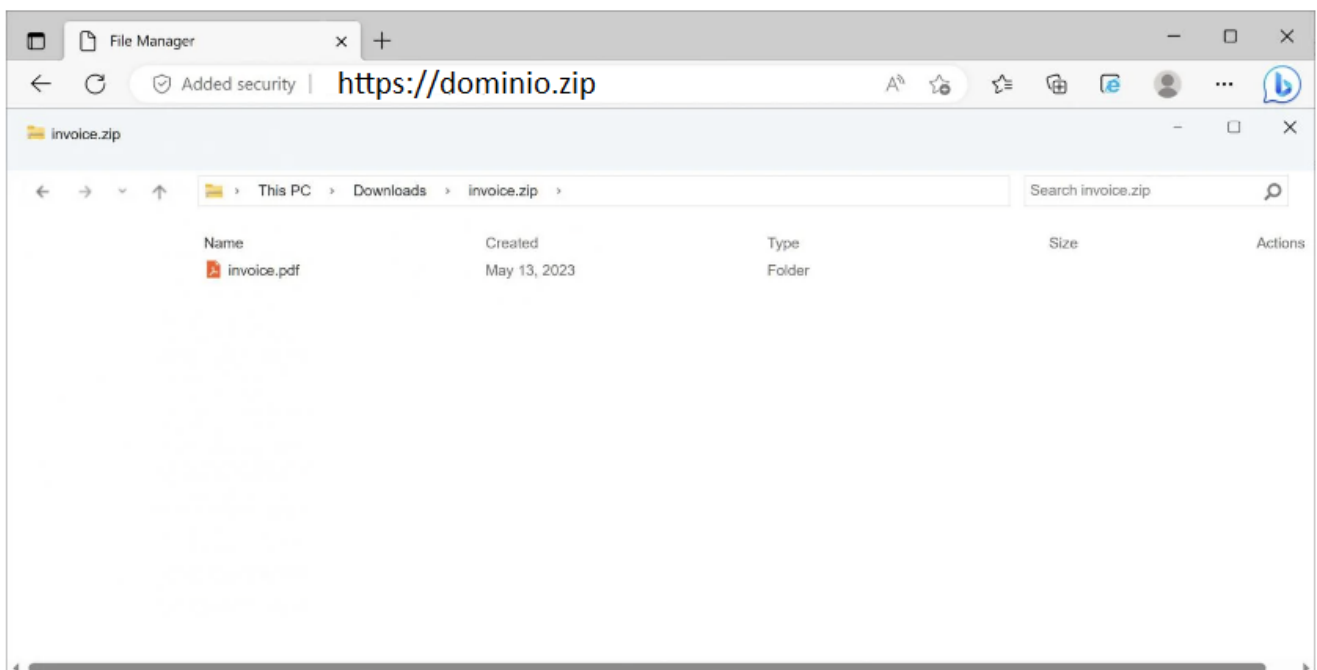
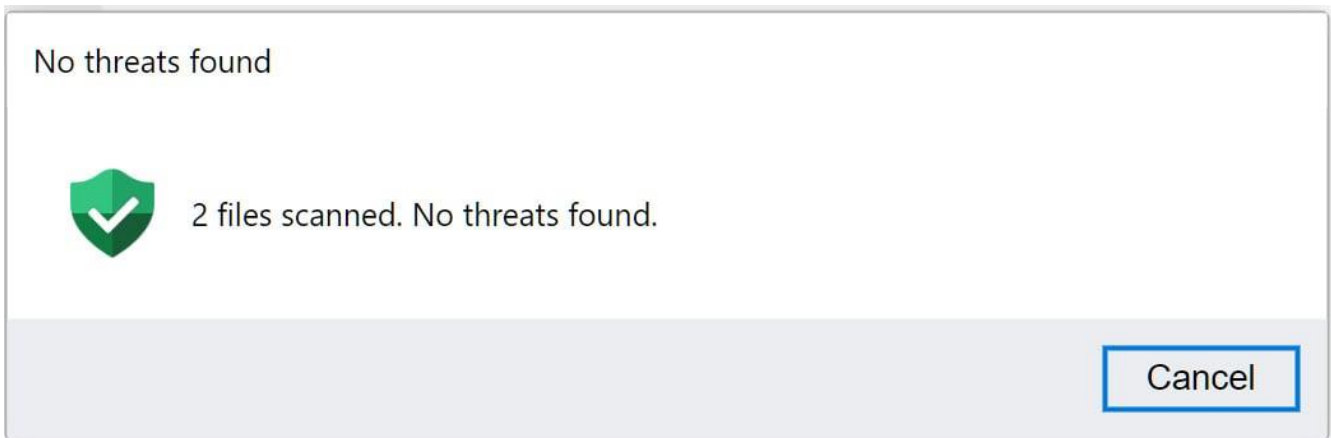
Certified in
Cybersecurity
An (ISC) Certification

ESPAÑA / USA / REP. DOMINICANA / MÉXICO PORTUGAL / CABO VERDE
JAMAICA / COSTA RICA / CANADA / CHIPRE / REINO UNIDO / BULGARIA
HOLANDA / ALEMANIA / MARRUECOS / TUNEZ / CROACIA / CHINA / ARUBA

Área de ciberseguridad de Monlex

Seguridad 360°

Newsletter de Ataques.



Certified in
Cybersecurity
An (ISC) Certification

ESPAÑA / USA / REP. DOMINICANA / MÉXICO PORTUGAL / CABO VERDE
JAMAICA / COSTA RICA / CANADA / CHIPRE / REINO UNIDO / BULGARIA
HOLANDA / ALEMANIA / MARRUECOS / TUNEZ / CROACIA / CHINA / ARUBA

Área de ciberseguridad de Monlex

Seguridad 360°

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



Certified in
Cybersecurity
An (ISC)® Certification

ESPAÑA / USA / REP. DOMINICANA / MÉXICO PORTUGAL / CABO VERDE
JAMAICA / COSTA RICA / CANADA / CHIPRE / REINO UNIDO / BULGARIA
HOLANDA / ALEMANIA / MARRUECOS / TUNEZ / CROACIA / CHINA / ARUBA