Aprende a identificar el malware al navegar en internet

Publicado el El Informatico - 2 de enero de 2021 -

Las mascarillas pueden protegernos contra los virus biológicos, pero no son efectivas contra virus informáticos. (Imagen de uso libre bajo licencia Pixabay)

Si eres de esos usuarios que reciben malware frecuentemente y desconoce cómo, o simplemente tienes miedo y quieres aprender como evitar ser objeto de un ataque, en éste artículo explicaré algunos de los métodos más comunes que utilizan los estafadores para infectar tu equipo, o incluso sacarte dinero si caes en la trampa. Son métodos bastante sencillos de identificar si prestas atención a lo que haces en internet y, con el tiempo, llegarás a aprender a identificarlas de forma inmediata.

La mayoría de los ejemplos aquí detallados son **ataques reales** que he encontrado tras navegar durante un tiempo por numerosas páginas de descarga de "dudosa legalidad", así que podrás ver algunas de las técnicas reales que utilizan los atacantes para infectarte o hacerse con tus datos.

> **AVISO:** En éste artículo se detallan prácticas que no son seguras de forma intencionada, y en un entorno controlado, a modo de demostración. **NO**

> REALICES ÉSTAS PRÁCTICAS EN TU EQUIPO. Se trata de que aprendas a identificar cualquier amenaza potencial para evitar ser objeto de ataques.

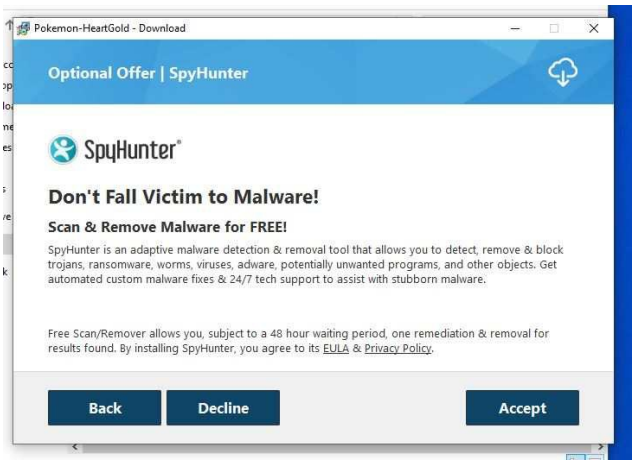
Instaladores con Adware

Este tipo de malware es frecuente en páginas de descargas, sobre todo en páginas con torrents para descargar contenido protegido por derechos de autor o de descarga directa. Pero también se da bastante a menudo en algunos sitios de descargas legales.

Suelen ser sitios donde descargas un instalador para algún tipo de software, que posteriormente te brinda descargas adicionales de software, normalmente comercial, como antivirus, productos de mantenimiento, barras de navegador, etc. El truco está en que la compañía que te brinda la descarga se lucra mediante éstas descargas adicionales. Pero es peligroso, ya que muchos de éstos programas pueden realizar actividades no deseadas en tu ordenador, aparte de instalar software que generalmente no deseas.

¿Búscas un ROM de un juego? ¡Toma ejecutable!

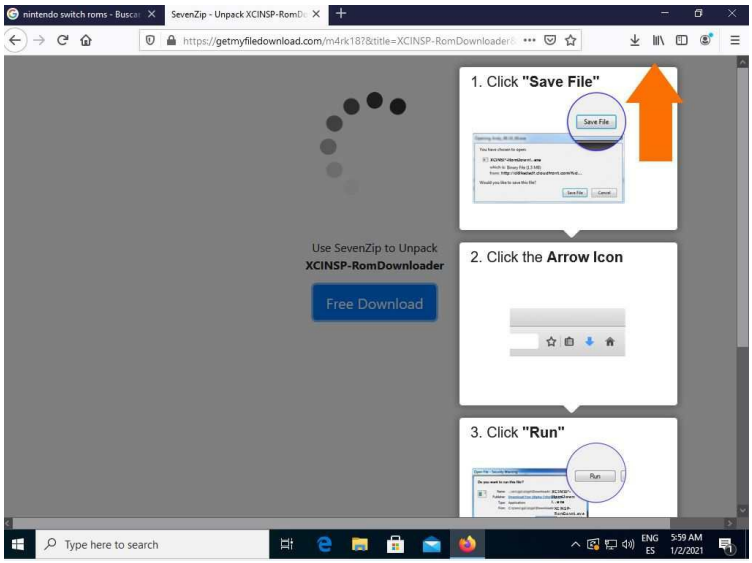
Normalmente la página te ofrecerá descargar un archivo ejecutable mientras intentas descargar algún otro tipo de archivo, sea un juego, una imagen, un archivo de audio, etc. En medio de la “instalación”, que generalmente se trata de descargar el software que originalmente estuvieses intentando descargar, te ofrecerá algún tipo de “oferta” adiccional.



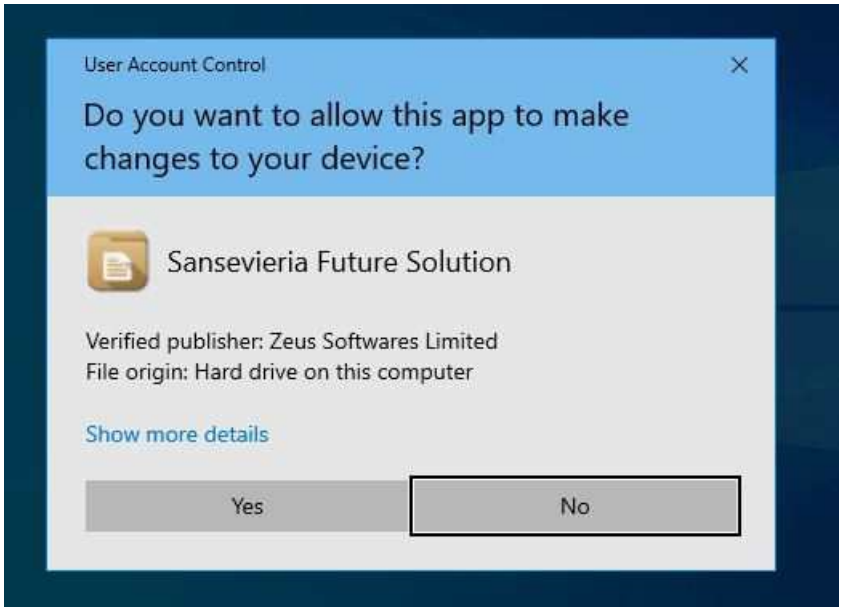
Normalmente éste tipo de instaladores te permiten no descargar éste software rechazando la oferta, pulsando algún botón como *skip*, *decline*, etc. Pero hay que tener cuidado porque algunos también hacen trampa y te hacen clickar alguna casilla adicional. Muchos usuarios suelen pulsar sobre "*siguiente*" o "*aceptar*" sin pararse a leer en lo que les ofrece el instalador, con lo que es muy fácil caer en la trampa.

"Sigue los pasos indicados para continuar"

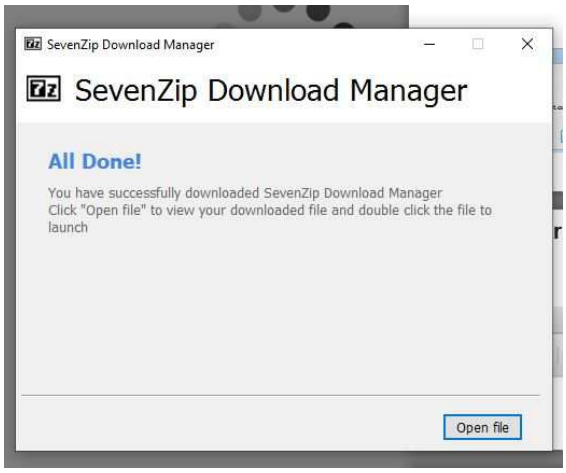
¡Ojo con ésta estafa! Es también bastante común en páginas de descargas. Éstas páginas nos brindan enlaces a páginas donde se nos pide que sigamos unos pasos determinados para obtener la descarga que, aun de cumplirlos, nunca obtendremos. Normalmente suelen pedirnos que abramos un ejecutable con malware, **pero en ocasiones nos piden que aceptemos algún tipo de confirmación en nuestro equipo**. Por ejemplo, las notificaciones en el navegador. O incluso que realicemos algún tipo de encuesta (*survey*). O una combinación de los anteriores.

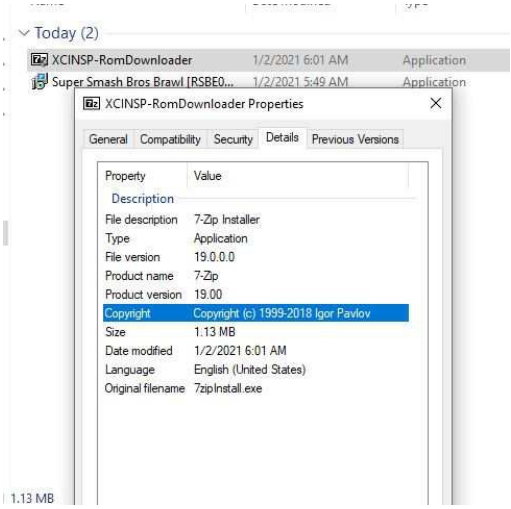


En éste ejemplo, la página indica que guardes y ejecutes el archivo indicado, que se trata de un ejecutable (.exe). Si lo abres, el ejecutable no tiene absolutamente nada que ver con lo que se indica en la página, evidentemente.

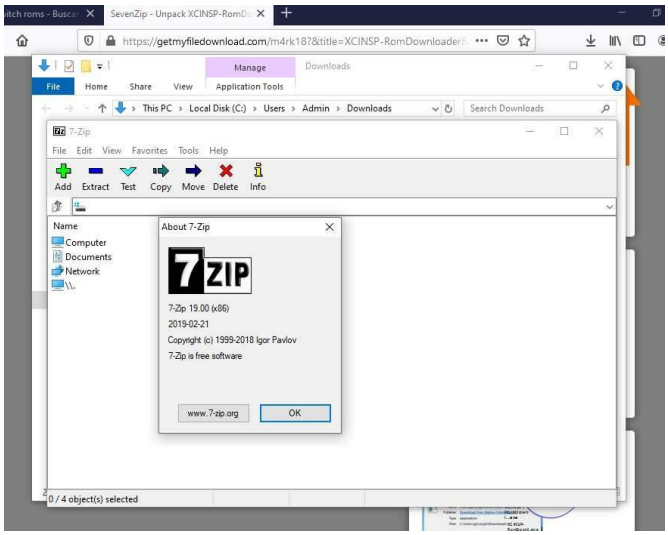


Entre otras cosas menos deseables, lo que hace el “instalador” es descargar una versión no oficial de 7zip, que es un programa gratuito y libre de compresión y descompresión de archivos.

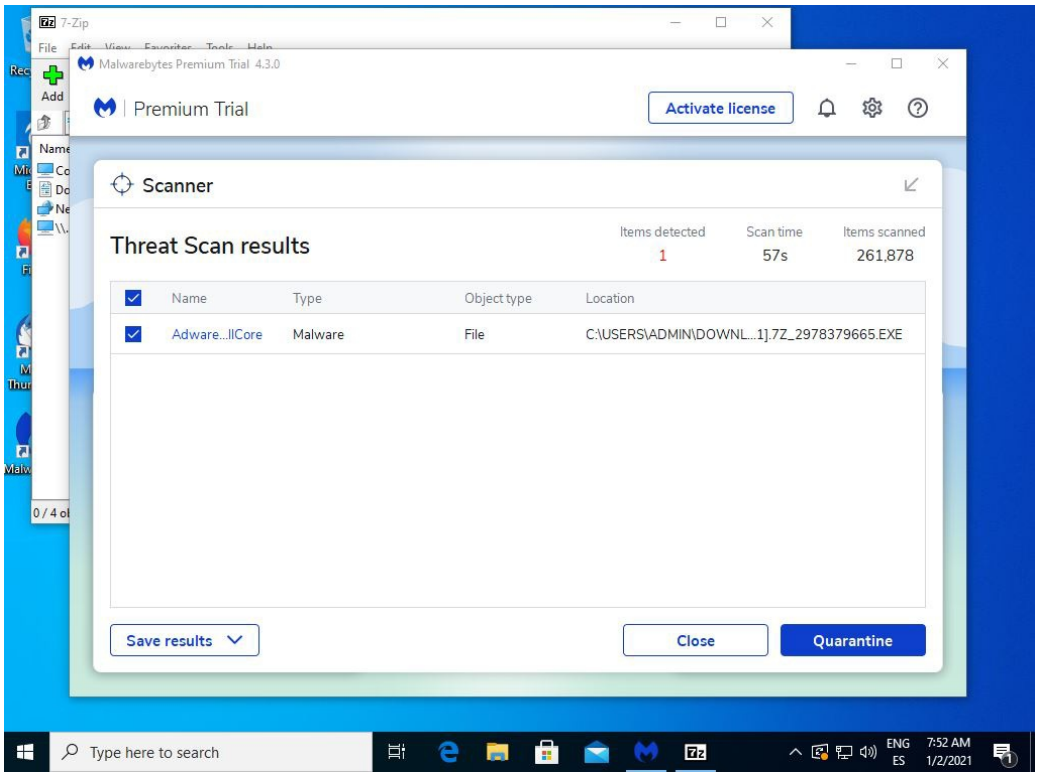




No sólo es una simple descarga infectada con malware, sino que además no lo instala. Aunque al menos se trata de la última versión... (Eso sí, de 32 bits).



7zip se puede descargar de forma gratuita y sin malware de la página oficial 7-zip.org. Con lo cual no sólo ésta descarga no tiene nada que ver con lo que buscábamos, sino que no ofrece nada de interés y, lo que es peor, ha instalado de forma silenciosa malware en nuestro equipo. Tras un escaneo del sistema con MalwareBytes, y como era de esperar, ocurre esto:

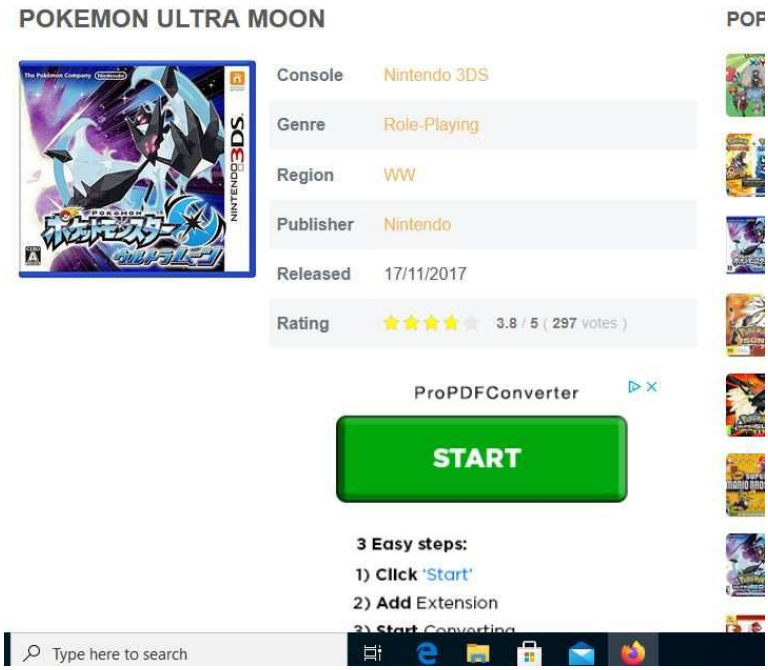


Nuestra copia de 7zip está infectada con un adware.

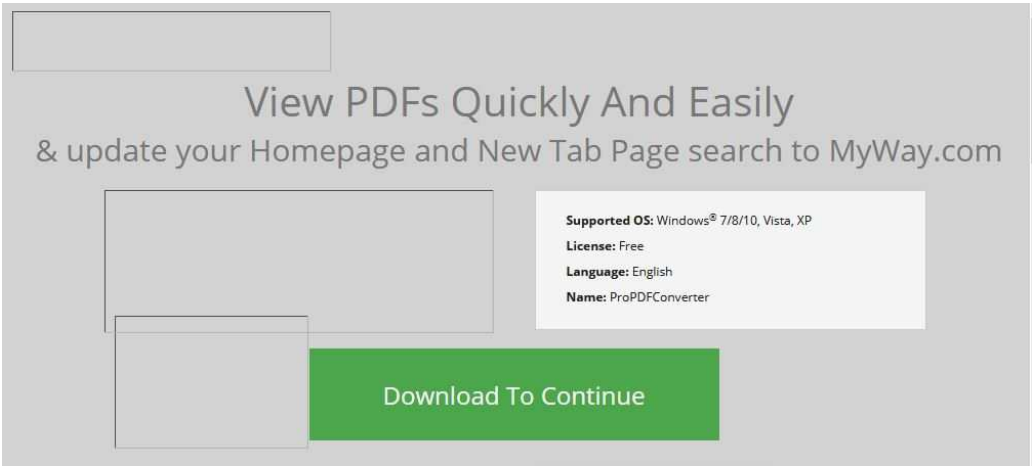
> NO TE LA JUEGUES. No acudas a sitios con descargas ilegales y compra siempre los juegos de las tiendas oficiales. Tu bolsillo puede resentirse, pero merece la pena más que arriesgarte a estropear tu sistema, pudiendo llegar a perder tus archivos.

Anuncios engañosos

Si entras en una página de descargas sin algún tipo de adblocker, probablemente verás en tu navegador una buena ristra de *banners* con anuncios. Algunos de los cuáles pueden simular ser botones de descarga, lo cuál puede ser muy confuso.



Estos botones suelen llevar a otra página donde se descargará algo que no tiene que ver con lo que estás intentando descargar, probablemente adware o algún otro tipo de malware similar al caso anterior.

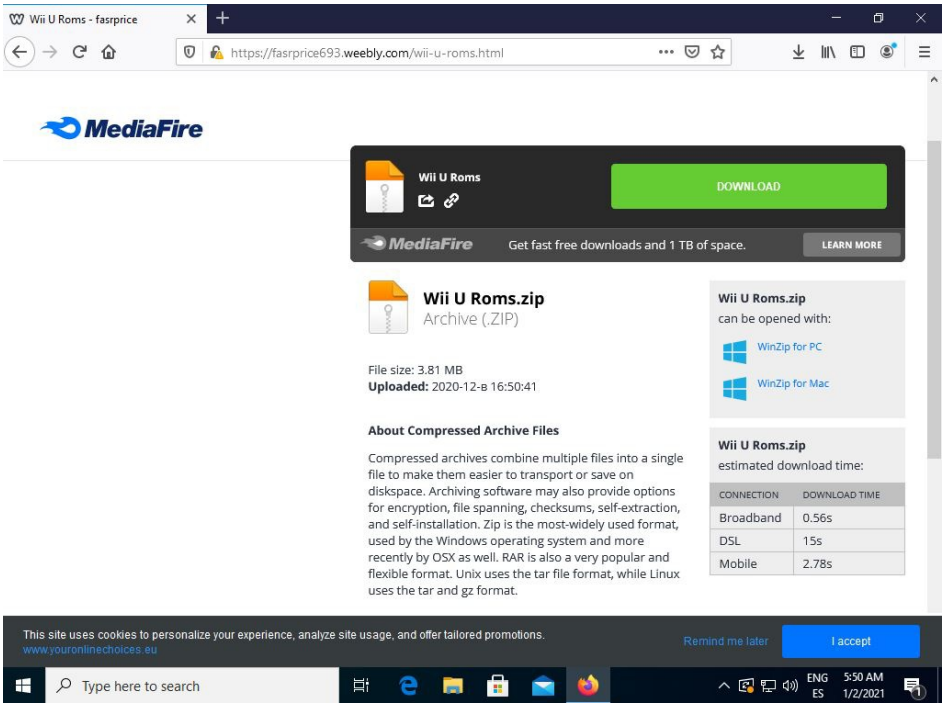


Como ya he dicho, las páginas de descargas son muy peligrosas y es preferible evitar

usarlas.

Phishing scam

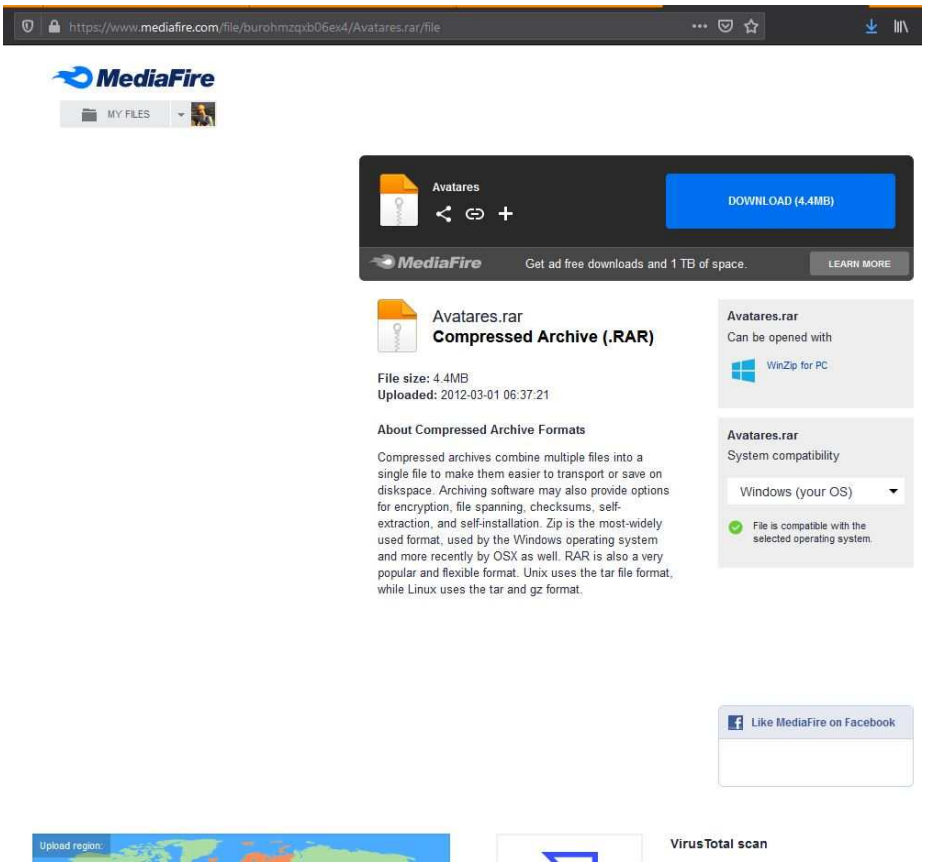
El “phishing” es una técnica de engaño mediante la cuál un atacante hace creer a su víctima que está visualizando una página legal, pero que en realidad es **una copia falsa de la página. Se suele usar para robar datos de acceso a sitios web, datos bancarios, o en éste caso hacernos descargar malware**.



La página de descarga de Mediafire, totalmente inofensiva... ¿verdad?

En éste caso, y mediante un enlace de descarga falso, una página nos redirige a otra página que, en apariencia, **parece una descarga de la página de Mediafire**, un servicio de alojamiento de archivos “en la nube”. La manera de detectar que se trata de una página falsa, aparte de que hay algunas diferencias entre ésta y la original en el diseño, **es en la dirección de la página**.

Ojo a la barra de dirección del navegador. Nos indica que **nos encontramos en un subdominio que pertenece a weebly.com**. Weebly es un servicio de alojamiento web gratuito, lo que quiere decir que el atacante ha creado una copia falsa de Mediafire en un servidor web gratuito, para hacernos creer que estamos en una descarga real de Mediafire. **El dominio original de Mediafire es mediafire.com**. Además, el certificado SSL no es válido. Observa cómo es la página original en comparación con la copia:

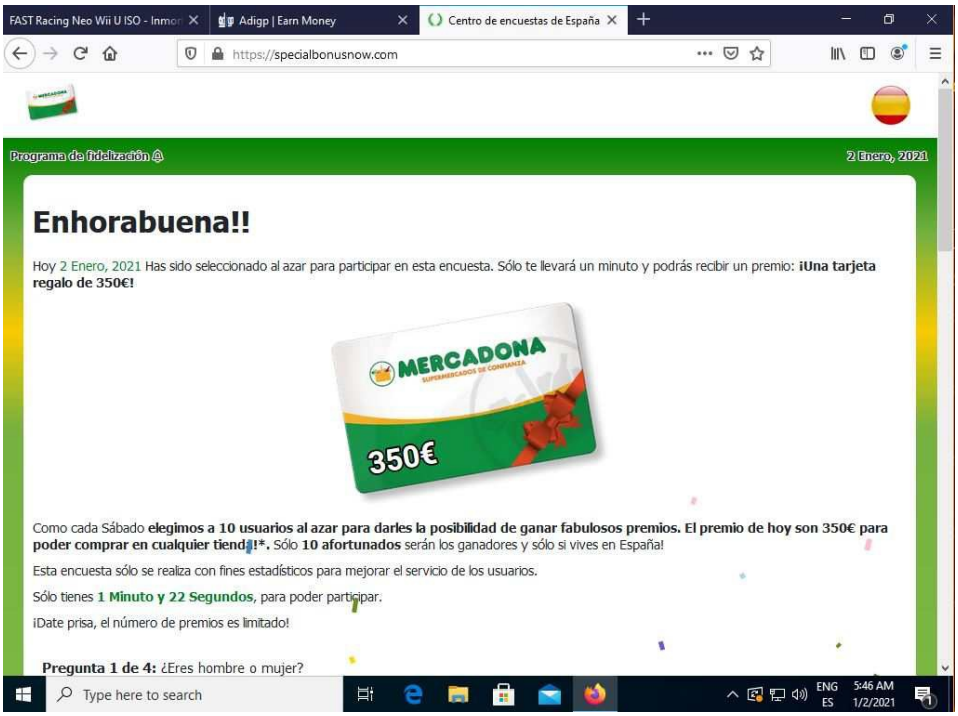


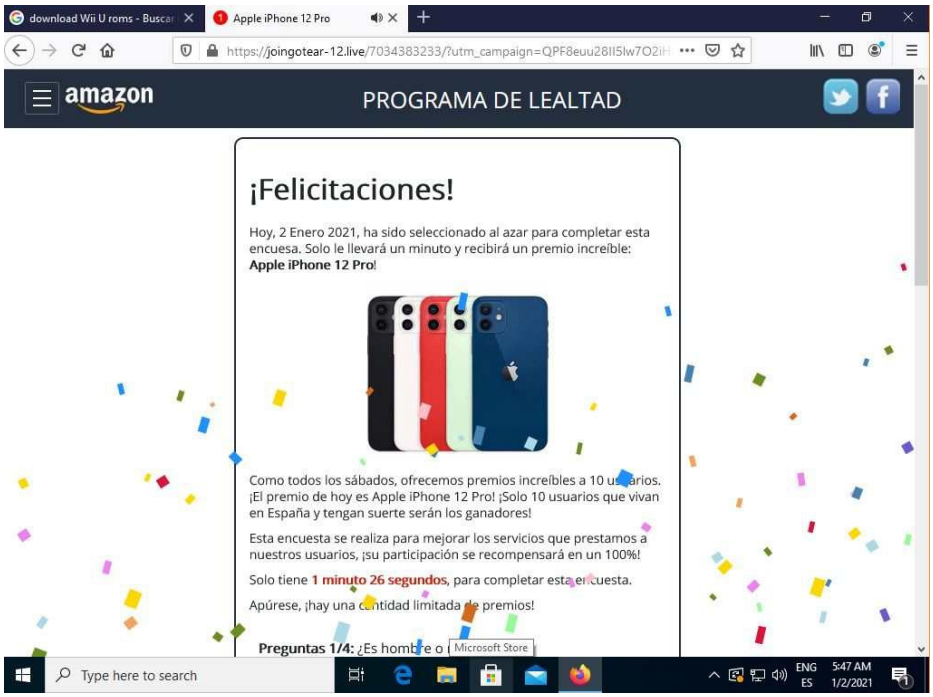
Esta es la página original de descarga de Mediafire. Y el dominio es mediafire.com.

Afortunadamente, **Weebly ya ha retirado la página falsa** de su servicio. Pero ándate con ojo, los atacantes abren páginas como ésta cada hora. **Tú puedes ser su próxima víctima.**

"¡Enhorabuena! ¡Eres el visitante 1,000,000!"

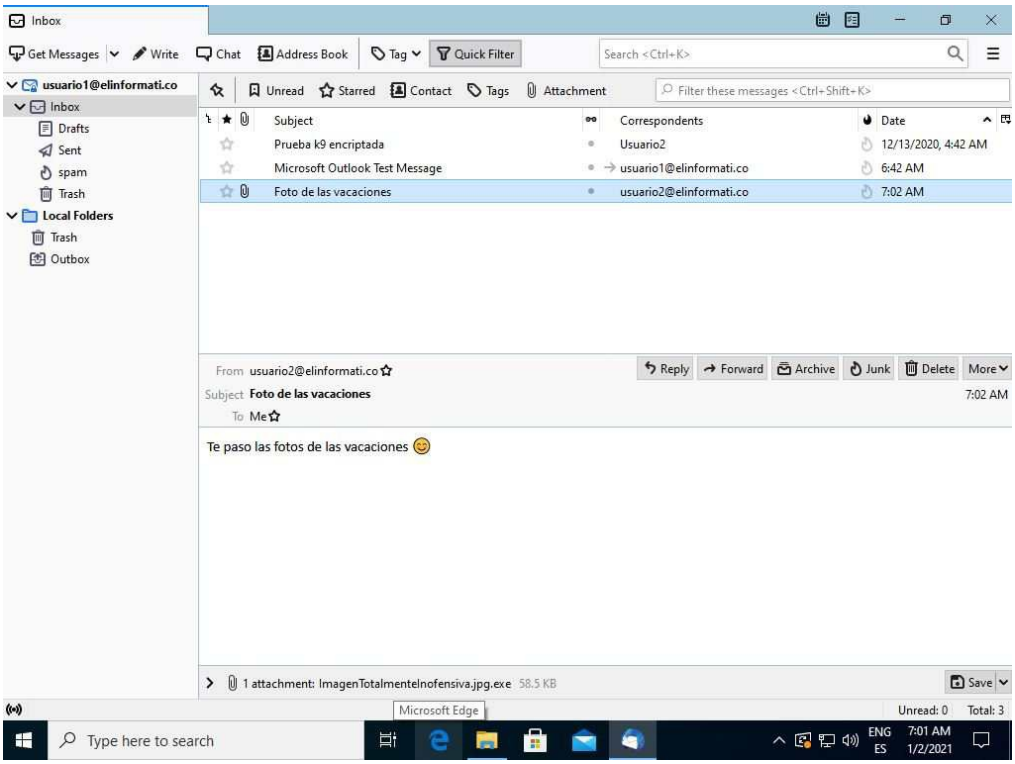
Esta estafa es clásica en internet. Al entrar en una página o seguir un enlace, la página nos indica que somos los elegidos para recibir un premio. Normalmente te ofrecen realizar una encuesta para poder acceder al "premio", **tras la cual te piden tus datos personales** (Correo, número de teléfono, etc). Ya te puedes imaginar para qué usan los atacantes éstos datos, pero **si piensas que te vas a llevar un premio, entonces estás muy equivocado/a.**





NUNCA y bajo ningún concepto accedas a realizar éstas encuestas ni mucho menos a dar datos personales a nadie en internet, ya que con esos datos te podrían meter en un buen lio.

Correos y mensajes infectados



Recreación de un mensaje infectado

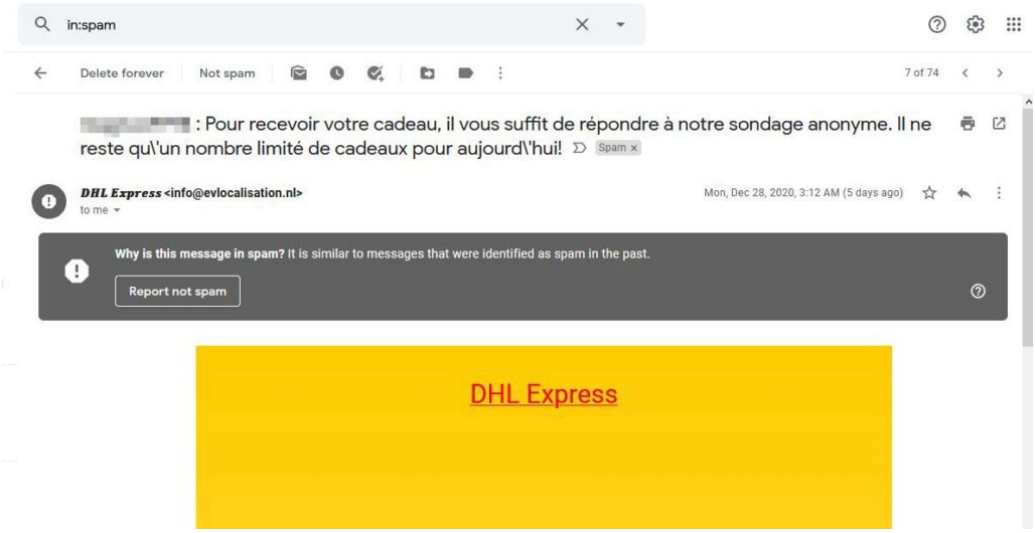
Este ataque es ya un vector de ataque clásico. La mayoría de gestores de correo bloquean automáticamente los archivos ejecutables, pero a algunos se les pueden escapar algunas cosas, **sobre todo en móviles**. No sólo se realiza mediante correo electrónico, **a veces el atacante puede hacerse pasar por alguno de tus contactos en WhatsApp o Telegram y mandarte un mensaje con un enlace a un sitio infectado**. Puede que incluso infectando el equipo de alguno de tus contactos, te mande un mensaje a través de WhatsApp o un correo haciéndose pasar por tu contacto.

> Por archivo ejecutable entendemos cualquier archivo que el sistema operativo pueda "ejecutar" como software. Es decir, un programa o aplicación. Estos archivos pueden tener extensión .exe, .dll (Aunque son librerías dinámicas de Windows, internamente son ejecutables), .jar, .bat, .vbe, o .apk en sistemas Android. Pero en ocasiones ocultan con trucos la extensión para aparentar ser archivos inofensivos. Los ejecutables ELF en Linux no tienen extensión. MIRA BIEN si los archivos que descargas tienen alguna de éstas extensiones al final del mismo.

Aunque el archivo aparenta ser otra cosa mediante el uso de dobles extensiones, **se trata de un ejecutable y hay que tener mucho cuidado, ya que**

seguramente se trate de un malware.

En ocasiones puede ocurrir que se mande un archivo con extensión inofensiva, pero que esté infectado de alguna manera (Por ejemplo, una bomba ZIP). Aunque lo más común es que nos intenten atacar mediante algún enlace, puede que incluso en un intento de hacerse **con nuestra información personal mediante ataque de phishing**. Si tienes gmail y vas a la carpeta de spam, es muy probable que encuentres una buena ristra de mensajes de éste tipo.

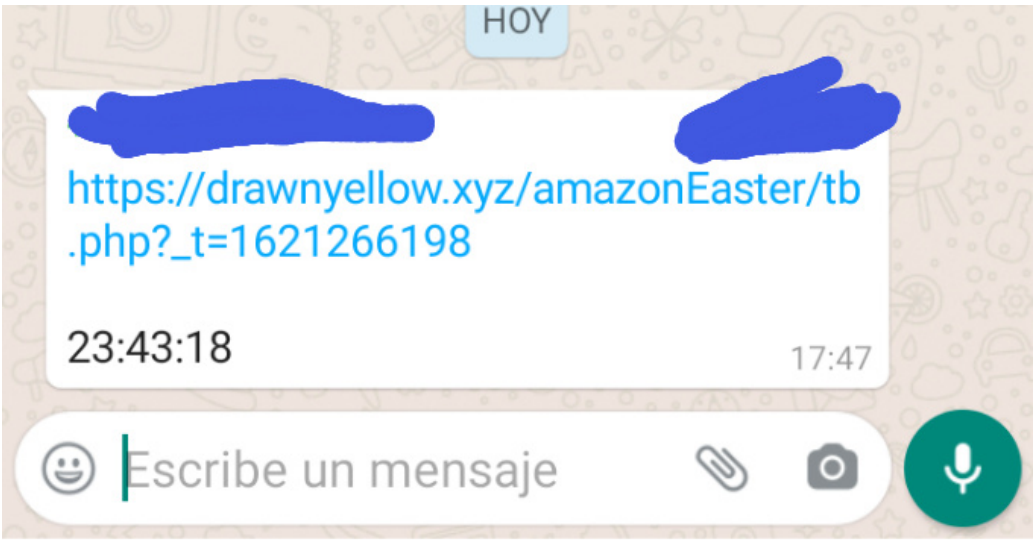


La información del remitente ni siquiera se corresponde con la de DHL.

Siempre desconfía de cualquier enlace o archivo adjunto que no hayas solicitado directamente a tus contactos, por mucho que la apariencia del mensaje sea de fiar. Pregunta a tus contactos antes de abrir nada, si el mensaje lo han mandado ellos realmente. Nunca se sabe cuándo uno de tus contactos ha podido infectarse.

Lo mejor para evitar éste problema es usar GPG para encriptar tus correos y firmarlos. Se puede hacer también en Android. Así podrás desconfiar de cualquier mensaje que no esté cifrado.

En el caso de **Whatsapp**, a veces podemos recibir un mensaje similar al siguiente:



Mensaje con un enlace sospechoso

En ocasiones el enlace puede ir acompañado de algún mensaje anunciando que la compañía está regalando dinero o productos y que hay que acudir al enlace para poder acceder a la oferta. **Esto es una estafa, y al hacer click en el enlace, podrías infectar tu telefono con algún tipo de malware**.

NUNCA abras direcciones web sospechosas ya que es probable que contengan algún tipo de malware.

ANTERIOR

Cómo usar el gestor de contraseñas KeePass

SIGUIENTE

Acerca de la nueva política de “privacidad” de WhatsApp

Buscar ...

Entradas Recientes

- Encriptación LUKS con CRYPTSETUP
- Se acabaron las bromas. A partir de ahora vas a estar constantemente vigilado en todas partes.
- Microsoft anuncia su nueva versión de su sistema operativo: Windows 11

- La historia de Internet en España
- Terminología moderna usada en tecnología digital
- Desactiva la ejecución de JavaScript de los archivos PDF, en Firefox y TOR browser.

Categorías

Actualidad | Android | Básicos | Ciberseguridad | Criptografía | Emulación / Virtualización | FOSS | Hacking | Informática | Internet | Juegos | Opinion | Otros | Personal | Privacidad | Programación | Tecnología | Time Machine | Tutoriales

RSS

Subscribirse al feed RSS