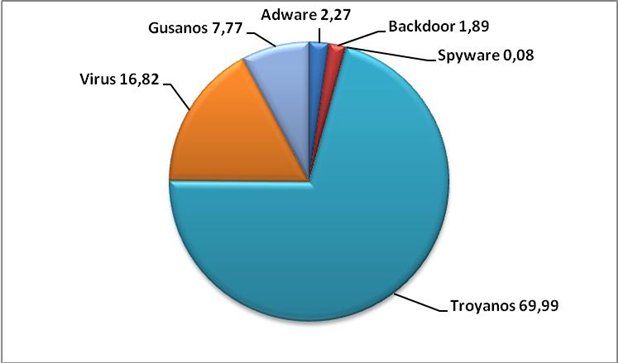
Software malicioso

Como su nombre indica, es un software que se ha creado con malas intenciones y que lo que busca es dañar nuestro ordenador, bien atacando a una funcionalidad o componente específico o bien entorpeciendo nuestra experiencia como usuario.  Muchas veces nos ocurre que al instalar un programa nos caen de rebote otros no deseados y puede deberse a un despiste nuestro a la hora de instalarlo (muchos están camuflados en el instalador como una opción más) o porque la página web aloja sin saberlo uno de estos bichitos.

Lo que debemos tener claro es que hay que protegerse y prestar atención a la [seguridad de nuestro dispositivo y navegador](https://blog.miamigoelinformatico.com/5-consejos-reforzar-la-seguridad-navegador/).Cada día se generan alrededor de 73.000 [nuevos malware](http://www.pcactual.com/articulo/actualidad/noticias/8186/cada_dia_crean_73000_nuevos_ejemplares_malware.html) con lo que imaginaros las probabilidades que tenemos de sufrir uno de estos ataques. A continuación os comentamos los más conocidos y algunos recientes que están causando estragos en la actualidad.

[](http://www.pcactual.com/articulo/actualidad/noticias/8186/cada_dia_crean_73000_nuevos_ejemplares_malware.html)

*Porcentaje de tipos de software malicioso. Fuente: PC Actual.*

Virus

Los podríamos considerar los padres de todos los malware. Se trata de un tipo de programa que se instala en tu ordenador sin tu autorización y que altera su funcionamiento.

Spyware

Conocidos comúnmente como espías, son programas cuyo objetivo es recolectar información personal tuya sin que lo sepas y enviarla a su creador. Evidentemente el creador tendrá intenciones fraudulentas.

Troyano

Como su nombre indica, hacen uso del engaño para llegar hasta nosotros sin delatarse. Parece inofensivo pero dentro puede contener la caja de Pandora. Un programa de este tipo puede manipular nuestros archivos, borrarlos e incluso pasar el control del ordenador a un tercero, para pesadilla nuestra. A diferencia de los virus no se propaga de un ordenador a otro.

Keylogger

Son las bestias que controlan las pulsaciones que realizamos sobre el teclado, es decir, registran las teclas que pulsamos para hacerse, por ejemplo, con nuestras contraseñas. También pueden averiguar las webs que has visitado, los correos que has leído o los archivos que has consultado (abierto). Pueden considerarse una especie de spyware y son peor que una vecina cotilla.

Phishing

Básicamente es una suplantación de identidad. Seguramente os sonará, ya que desde el nacimiento de la banca online es un software que ha proliferado más. Normalmente el criminal se hace pasar por una persona o empresa de confianza a través de un correo, manipulado previamente para dar el pego. Son bastantes ingeniosos a la hora de hacernos caer en sus redes. Casos de phishing suelen ser escribir por un problema técnico donde debemos especificar cierta información, recomendaciones de seguridad que implican proporcionar contraseñas, inminente desactivación del producto, falsas ofertas, etc. Recuerda que cualquier compañía de confianza no va a solicitarte información personal a través de un correo, así que cuando te pidan darla, sospecha.

Ransomware

Es un programa malicioso que restringe el acceso a determinados archivos o determinadas partes del sistema y pide un rescate para eliminar dicha restricción. Algunos de estos programas incluso cifran los archivos del sistema operativo inutilizándolo.  Se suele propagar como un gusano (de ordenador a ordenador) lo que lo hace más peligroso. En los últimos tiempos están aprovechando incluso vulnerabilidades en softwares que utilizamos casi a diario. Un caso muy conocido fue el de la difusión de este malware a través de [emails simulando ser Correos](http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/).

Mazar

Es un tipo de malware que se instala en tu smartphone Android y borra sus datos. Pero también puede acceder a nuestro registro de llamadas, realizar las que le parezca y fisgonear nuestros mensajes. La forma de propagarse, aunque cueste creerlo, es a través de SMS. Y es que por más que su uso haya decaído con la llegada de Whatssap, Telegram o Hangout la realidad es que todavía se utilizan. Suele ser un mensaje inofensivo y al abrir el enlace que acompaña redirige a la descarga Tor (que permite acceder a Internet de forma privada y anónima) y, a continuación, se descarga el software malicioso. Así que precaución.

Adware

Son programas que muestran publicidad web durante la navegación o instalación de un programa en beneficio lucrativo de sus creadores. Podríamos incluirlo dentro de la familia de troyanos. El año pasado apareció una nueva variante infernal para los usuarios de Android. Se trata de un programa capaz de convertirse a sí mismo en una aplicación del sistema, que viene a indicar que para el usuario resulta  casi imposible eliminarlo. Es más, al tener privilegios de tipo administrador no tiene que bombardearnos constantemente con publicidad y nos será más complicado darnos cuenta de que estamos infectados. Se descubrió que este tipo de programa se esconde dentro del código de aplicaciones tan conocidas como Candy Crush, Google Now, Facebook, o Twitter entre otras. Importante destacar que las versiones infectadas no estaban en Google Play, sino que estaban disponibles en páginas de terceros. Así que pon atención a las páginas orígenes de tus descargas y procura hacerlo siempre desde las oficiales.

AceDeceiver

Este es un nuevo malware que ha disparado todas las alarmas en los usuarios IOS, que se consideraban prácticamente intocables hasta ahora. Aunque ya ha sido retirada por Apple de su Store os contamos que estaba camuflado bajo una aplicación de fondos de pantallas. Su objetivo era robar las credenciales de Apple del usuario para hacer uso malintencionado de ellas.