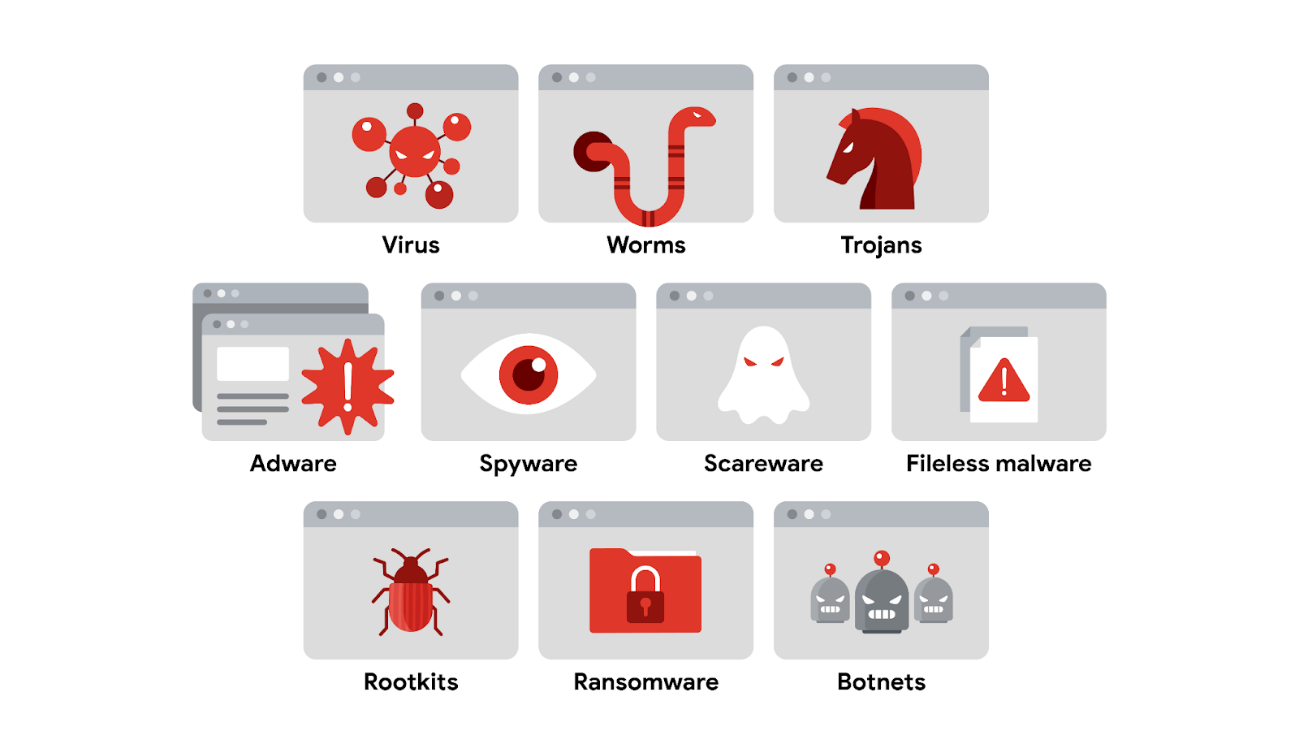
**Introducción al malware**

Anteriormente, aprendiste que el **malware** es un software diseñado para dañar dispositivos o redes. Desde su primera aparición en computadoras personales hace décadas, se desarrolló una gran cantidad de cepas de malware. Ser capaz de identificar diferentes tipos de malware y comprender las formas en que se propagan te ayudará a mantenerte alerta y al corriente como profesional de seguridad.



**Virus**

Un **virus** es un código malicioso escrito para interferir con las operaciones informáticas y causar daños a los datos y al software. Para poder propagarse y causar daños, este tipo de malware debe ser instalado por el usuario a quien el ataque apunta. Una de las muchas formas en que los virus se propagan es a través de campañas de phishing, en las que se ocultan enlaces maliciosos dentro de vínculos o archivos adjuntos.

**Gusano**

Un **gusano** es un software malicioso que se puede duplicar y propagar por sí mismo a través de sistemas. De manera similar a los virus, un gusano debe ser instalado por el usuario a quien está dirigido el ataque, y también se puede propagar mediante tácticas como el correo electrónico malicioso. Dada la capacidad que tiene un gusano de propagarse por sí solo, los ataques a veces están dirigidos a dispositivos, unidades o archivos que tienen acceso compartido a través de una red.

Un ejemplo muy famoso es el gusano Blaster, también conocido como Lovesan, Lovsan o MSBlast. A principios de la década de 2000, este gusano se extendió en computadoras con sistemas operativos Windows XP y Windows 2000, y forzó a los dispositivos a un bucle continuo de apagado y reinicio. Si bien no dañó los dispositivos infectados, logró extenderse a cientos de miles de usuarios en todo el mundo. Desde el gusano Blaster original, se implementaron muchas variantes que pueden infectar computadoras modernas.

**Nota:** Los gusanos fueron ataques muy populares a mediados de la década de 2000. Sin embargo, desde hace unos años, se utilizan con menos frecuencia.

**Troyano (caballo de Troya)**

Un **troyano**, también llamado **caballo de Troya**, es un software malicioso (malware) que se parece a un archivo o programa legítimo. Esta característica se relaciona con la forma en que los troyanos se propagan. De forma similar a los virus, los atacantes entregan este tipo de malware oculto en descargas de archivos y aplicaciones. Los atacantes se apoyan en el hecho de engañar a usuarios desprevenidos para que crean que están descargando un archivo inofensivo, cuando en realidad están infectando su propio dispositivo con malware que puede usarse para espiarlos, otorgar acceso a otros dispositivos y más.

**Adware**

El software respaldado por publicidad, o **adware**, es un tipo de software legítimo que a veces se utiliza para mostrar publicidad digital en las aplicaciones. Los desarrolladores de software suelen usar el adware como una forma de reducir sus costos de producción o hacer que sus productos sean gratuitos para el público, lo que también se conoce como “freeware” o “shareware”. En estos casos, los desarrolladores monetizan su producto a través de los ingresos publicitarios en lugar de cobrarles a sus usuarios.

El adware malicioso pertenece a una subcategoría de malware conocida como **aplicación potencialmente no deseada (PUA)**. Una PUA es un tipo de software no deseado que se incluye con programas legítimos y que puede mostrar anuncios, causar la ralentización del dispositivo o instalar otro software. Los atacantes a veces ocultan este tipo de malware en programas gratuitos con diseño inseguro, para ser ellos quienes moneticen los anuncios, en lugar del desarrollador. Esto funciona incluso cuando el usuario se ha negado a recibir anuncios.

**Spyware**

Al igual que el adware, el **spyware** es un tipo de software malicioso que se usa para recabar y vender información sin consentimiento. También se considera un PUA. El spyware se oculta comúnmente en el *bundleware*, un software adicional que a veces se incluye dentro de otras aplicaciones. Los PUA como el spyware se han convertido en un serio desafío en el ecosistema del desarrollo de software de código abierto. Esto se debe a que los desarrolladores tienden a no considerar cómo otras personas podrían hacer un abuso o un mal uso de su software.

**Scareware**

Otro tipo de PUA es el **scareware**. Esta clase de software malicioso emplea tácticas para asustar a los usuarios con el fin de que infecten su propio dispositivo. El scareware los engaña al mostrarles advertencias falsas que parecen provenir de empresas legítimas. El correo electrónico y las ventanas emergentes son solo algunas de las maneras en las que el scareware se propaga. Ambos pueden usarse para entregar advertencias con afirmaciones falsas de que los archivos o los datos del usuario están en riesgo.

**Software malicioso sin archivos**

El **software malicioso sin archivos** (o malware sin archivos) no necesita que el usuario lo instale porque utiliza programas legítimos que ya están instalados para infectar una computadora. Este tipo de infección reside en la memoria, por eso el malware nunca toca el disco duro. En este sentido, es diferente de los otros tipos de software maliciosos, que se almacenan dentro de un archivo en el disco. Estas infecciones sigilosas, en cambio, entran en el sistema operativo o se esconden dentro de aplicaciones de confianza.

**Consejo profesional:** El software malicioso sin archivos se detecta mediante la realización de análisis de memoria, para lo que se requiere de experiencia con sistemas operativos.

**Rootkits**

Un **rootkit** es un software malicioso que proporciona acceso administrativo y remoto a una computadora. La mayoría de los atacantes utilizan rootkits para abrir una especie de puerta trasera a los sistemas, lo que les permite instalar otras formas de malware o realizar ataques de seguridad de red.

Este tipo de software malicioso suele propagarse por una combinación de dos componentes: un dropper y un loader (cargador). Un **dropper** es un programa o archivo que se utiliza para instalar un rootkit en un equipo de destino. Un **loader** es un código malicioso que se activa después de que el usuario inicia un programa dropper.

**Secuestro de datos (Ransomware)**

El **ransomware** es un ataque en el que los agentes de amenaza cifran los datos de una organización y exigen un pago (rescate) para restablecer el acceso a ellos. Según la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), los delitos de ransomware están en aumento y son cada vez más sofisticados. Este tipo de infecciones puede causar un daño considerable a una organización y a sus clientes. Un ejemplo es el ataque [WannaCry](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack), que encripta la computadora de una víctima hasta que se paga un rescate en criptomonedas.

**Botnet**

Una **botnet** (“red de bots”) es un conjunto de computadoras infectadas con software malicioso que están bajo el control de un solo agente de amenaza, conocido como el “bot-herder” (pastor de bots). A menudo, los virus, gusanos y troyanos se utilizan para propagar la infección inicial y convertir los dispositivos en un bot para el bot-herder. Luego, el atacante utiliza protocolos de uso compartido de archivos, correo electrónico o aplicaciones de redes sociales para crear nuevos bots y hacer crecer la botnet. Cuando un objetivo, sin saberlo, abre el archivo malicioso, la computadora, o el bot, vuelve a transmitir la información al bot-herder, que puede ejecutar comandos en la computadora infectada.

**Conclusiones clave**

Existe una variedad asombrosa de software malicioso que puede propagarse de múltiples maneras. El malware es una amenaza compleja que puede requerir de una especialización propia dentro de la ciberseguridad. El [curso introductorio de INFOSEC sobre análisis de malware](https://www.infosecinstitute.com/skills/courses/malware-analysis-introduction/) es un lugar posible para aprender más al respecto. Incluso sin una especialización en el análisis de malware, reconocer los tipos de software malicioso y cómo se propagan es una parte importante de la defensa contra estos ataques, en tu trabajo como analista de seguridad.