Software Malicioso (Malware)

Malware es un término general para referirse a cualquier tipo de "**mal**icious soft**ware**" (software malicioso) diseñado para realizar acciones dañinas en un sistema informático de forma intencionada (al contrario que el "software defectuoso") y sin el conocimiento del usuario (al contrario que el software potencialmente no deseado). Ejemplos típico de estas actividades maliciosas son el robo de información (p. ej. troyanos), dañar o causar un mal funcionamiento el sistema informático (p. ej. Stuxnet, Shamoon o Chernobyl), provocar un perjuicio económico, chantajear al propietario de los datos del sistema informático (p. ej. ransomware o programas de chantajeo), permitir el acceso de usuarios no autorizados, provocar molestias o una combinación de varias de estas actividades.

Durante los años 1980 y 1990, el malware era creado como una forma de vandalismo o travesura. Sin embargo hoy día la motivación principal es la obtención de un beneficio económico. En los últimos años está apareciendo malware asociado a amenazas persistentes avanzadas, que son campañas fuertemente orquestadas realizadas por grupos asociados a estados o a importantes instancias con poder, cuyo objetivo más habitual es el robo de información estratégica o producir daños en sistemas de organizaciones objetivo.

Las motivaciones más habituales para la creación de malware son:

- Experimentar al aprender. Por el ejemplo el Gusano Morris tuvo este origen
- Realizar bromas, provocar molestias y satisfacer el ego del creador. Ejemplos de este tipo de virus son Melissa y los llamados Virus joke.
- Producir daños en el sistema informático ya sea en el hardware (por ejemplo Stuxnet y Chernobyl), en el software (por ejemplo Ramen cambia la página inicial del servidor web), en los datos (por ejemplo Shamoon o Narilam buscan la destrucción de los datos) o provocando la caída de servidor (por ejemplo Code Red).
- Provocar una degradación en el funcionamiento del sistema. Por ejemplo consumiendo ancho de banda de la red o tiempo de CPU.
- Sacar beneficio económico. Por ejemplo:
    - Robando información (personal, empresarial, de defensa...) para luego usarla directamente en fraudes o revenderla a terceros. Al tipo de malware que roba información se le llama *spyware*.
    - Chantajeando al propietario del sistema informático. Por ejemplo el *ransomware*.
    - Presentar publicidad. A este tipo de malware se le llama *adware*.
    - Tomando control de computadoras para su explotación en el mercado negro. Estas computadoras infectadas zombis) son usadas luego para por ejemplo el envío masivo de correo basura, para alojar datos ilegales como pornografía infantil, distribuir malware (pago por instalación), o para unirse en ataques de denegación de servicio distribuido (DDoS).

Cuando el malware produce pérdidas económicas para el usuario o propietario de un equipo, también se clasifica como *crimeware* o software criminal. Estos programas suelen estar orientados a malversaciones financieras, la suplantación de identidad y el espionaje.

Algunos autores distinguen el malware del *grayware* (también llamados *greyware*, *graynet* o *greynet*), programas que se instalan sin la autorización usuario y se comportan de modo tal que resultan molestos o indeseables para el usuario, pero son menos peligrosos que los malware. En esta categoría, por ejemplo, se incluyen los programas publicitarios, marcadores, programas espía, herramientas de acceso remoto y virus de broma.

Hay distintos tipos de *malware* donde un caso concreto de *malware* puede pertenecer a varios tipos a la vez:

- **Virus**: secuencia de código malicioso que se aloja en un archivo ejecutable (huésped) de manera que al ejecutarse el programa también se ejecuta el virus. Tienen la propiedad de propagarse por reproducción dentro de la misma computadora.
- **Gusano**: *malware* capaz de ejecutarse por sí mismo. Se propaga por la red explotando vulnerabilidades, para infectar otros equipos.
- **Troyano**: programa que bajo apariencia inofensiva y útil tiene otra funcionalidad oculta maliciosa. Típicamente esta funcionalidad suele permitir el control de forma remota del equipo (administración remota) o la instalación de puertas traseras que permitan conexiones no autorizadas al equipo. No se reproducen. Los troyanos conocidos como *droppers* son usados para empezar la propagación de un gusano inyectándolo dentro de la red local de un usuario.
- **Bomba lógica**: programas que se activan cuando se da una condición determinada causando daños en el sistema. Las condiciones de ejecución típicas suelen ser que un contador llegue a un valor concreto o que el sistema esté en una hora o fecha concreta.
- ***Adware***: muestran publicidad no solicitada de forma intrusiva provocando molestias. Algunos programas *shareware* (modalidad de distribución de software, en la que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo o en algunas de las formas de uso) permiten usar el programa de forma gratuita a cambio de mostrar publicidad, en este caso el usuario consiente la publicidad al instalar el programa. Este tipo de *adware* no debería ser considerado *malware*, pero muchas veces los términos de uso no son completamente transparentes y ocultan lo que el programa realmente hace.
- ***Spyware***: envía información del equipo a terceros sin que el usuario tenga conocimiento. La información puede ser de cualquier tipo como por ejemplo datos personales, contraseñas, números de tarjetas de crédito, direcciones de correo electrónico (utilizable para enviarles correos basura) o información sobre páginas que se visitan (usable para seleccionar el tipo de publicidad que se le envía al usuario). Los autores de *spyware* que intentan actuar de manera legal pueden incluir unos términos de uso, en los que se explica de manera imprecisa el comportamiento del *spyware*, que los usuarios aceptan sin leer o sin entender. La mayoría de los programas *spyware* son instalados como troyanos junto a *software* deseable bajado de Internet. Otros programas *spyware* recogen la información mediante *cookies* de terceros o herramientas instaladas en navegadores web.
- ***Malvertising***: se aprovecha de recursos disponibles por ser un anunciante publicitario, para buscar puertas traseras y poder ejecutar o instalar otro *malware*. Por ejemplo un anunciante publicitario en una página web aprovecha una brecha de seguridad de un navegador para instalar *malware*.
- ***Ransomware* o criptovirus**: software que afecta gravemente al funcionamiento del equipo informático infectado (ejemplo encripta el disco duro o lo bloquea) infectado y le ofrece al usuario la posibilidad de comprar la clave que permita recuperar la información. En algunas versiones del *malware* (p. ej. Virus ucash) se enmascara el ataque como realizado por la policía y el pago como el abono de una multa por haber realizado una actividad ilegal como por ejemplo descarga de software ilegal.
- ***Keylogger***: software que almacena las teclas pulsadas por el usuario con el fin de capturar información confidencial como contraseñas o número de tarjeta de crédito o conversaciones de chat.

- ***Stealer***: roban información privada guardada en el equipo. Típicamente al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas recordadas, por ejemplo en los navegadores web o en clientes de mensajería instantánea (p. ej. Skype).
- ***Rogueware***: es un falso programa de seguridad que no es lo que dice ser, sino que es un malware. Por ejemplo falsos antivirus, antiespía, cortafuegos o similar. Estos programas suelen promocionar su instalación usando técnicas de *scareware*, es decir, recurriendo a amenazas inexistentes como por ejemplo alertando de que un virus ha infectado el dispositivo. En ocasiones también son promocionados como antivirus reales sin recurrir a las amenazas en la computadora. Una vez instalados en la computadora es frecuente que simulen ser la solución de seguridad indicada, mostrando que han encontrado amenazas y que, si el usuario quiere eliminarlas, es necesario la que compre una licencia para la versión de completa.
- ***Decoy* o señuelo**: software que imita la interfaz de otro programa para solicitar el usuario y contraseña y así poder obtener esa información.
- **Secuestrador de navegador**: son programas que realizan cambios en la configuración del navegador web. Por ejemplo, algunos cambian la página de inicio del navegador por páginas web de publicidad o páginas pornográficas, otros redireccionan los resultados de los buscadores hacia anuncios de pago o páginas de *phishing* bancario (persiguen el engaño a una víctima ganándose su confianza simulando pertenecer a una empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar, como revelar información confidencial o hacer *click* en un enlace).
- ***Wiper***: es un malware orientado al borrado masivo de datos. Por ejemplo discos duros o bases de datos.
- **Criptominado malicioso o *cryptojacking***: es un malware que se oculta en un ordenador y se ejecuta sin consentimiento utilizando los recursos de la máquina (CPU, memoria, ancho de banda,...) para la minería de criptomonedas y así obtener beneficios económicos. Este tipo de software se puede ejecutar directamente sobre el sistema operativo de la máquina o desde plataforma de ejecución como el navegador.
- ***Web skimming***: software que los atacantes instalan en aplicaciones webs de comercio electrónico con el fin de recopilar información de pago (datos personales y de tarjetas de crédito fundamentalmente) de los usuario que visiten dicho sitio web comprometido.
- **Apropiador de formulario**: software que permite robar información que es introducida en formularios web.

Conceptos relacionados

Relacionados con el malware hay una serie de conceptos informáticos:

- **Puerta trasera**. Vía alternativa de acceso que elude los procedimientos habituales de autenticación al conectarse a una computadora. En relación con el malware es frecuente que:
    - Un malware instale una puerta trasera para permitir un acceso remoto más fácil en el futuro
    - Se use una puerta trasera como vía para instalar un malware.
- ***Drive-by-Download***. Consiste en la descarga involuntaria de software proveniente de Internet. Es una vía típica para descargar malware, especialmente por descargas ocultas que se producen al navegar por ciertas páginas web. Por esta razón a los navegadores se les están agregando

bloqueadores *antimalware* que muestran alertas cuando se accede a una página maliciosa, aunque no siempre dan una total protección.

- ***Botnets***. Son redes de computadoras infectadas por malware, a las que se llama zombis, que pueden ser controladas a la vez por un individuo y realizan distintas tareas. Este tipo de redes son usadas para el envío masivo de *spam* o para lanzar ataques DDoS contra organizaciones como forma de extorsión o para impedir su correcto funcionamiento. La ventaja que ofrece a los *spammers* el uso de ordenadores infectados es el anonimato, que les protege de la persecución policial. Las *botnets* pueden ser usadas para actualizar el *malware* en los sistemas infectados manteniéndolos así resistentes ante antivirus u otras medidas de seguridad.
- **Vulnerabilidades**. Las vulnerabilidades son puntos débiles de un sistema informático que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Estas vulnerabilidades son aprovechadas por el malware para ejecutar su código maligno. Las vulnerabilidades suelen ser producidos por *errores de software*, sobre-privilegios de usuarios (usuarios a los que se les ha concedido más privilegios de los que se debería haber otorgado), sobre-privilegios de código (programas a los que se le ha concedido más privilegios del que se debería haber otorgado), ejecución por parte del usuario de software no confiable. Otro factor que afecta a la vulnerabilidad de un sistema complejo formado por varios ordenadores es que todos los ordenadores del sistema funcionen con el mismo software (homogeneidad). Por ejemplo, cuando todos los ordenadores de una red funcionan con el mismo sistema operativo, si se puede comprometer ese sistema, se podría afectar a cualquier ordenador que lo use.

Protección contra malware

Prevención

Siguiendo algunos sencillos consejos se puede aumentar considerablemente la seguridad de una computadora, algunos son:

- Tener el sistema operativo y el navegador web actualizados.
- Tener instalado un antivirus y un firewall y configurarlos para que se actualicen automáticamente de forma regular ya que cada día aparecen nuevas amenazas.
- Utilizar una cuenta de usuario con privilegios limitados. La cuenta de administrador solo debe utilizarse cuando sea necesario cambiar la configuración o instalar un nuevo software.
- Tener precaución al ejecutar software procedente de Internet o de medios extraíbles como memorias USB. Es importante asegurarse de que proceden de algún sitio de confianza.
- Una recomendación para tabletas, teléfonos celulares y otros dispositivos móviles es instalar aplicaciones de tiendas muy reconocidas como App Store, Google Play o Tienda Windows, pues esto garantiza un muy mínimo riesgo de contener *malware* alguno. También se puede instalar antivirus en estos dispositivos.
- Evitar descargar software de redes P2P (peer-to-peer, red de pares, red entre iguales o red entre pares), ya que realmente no se sabe su contenido ni su procedencia.
- Permitir JavaScript, ActiveX y cookies sólo en páginas web de confianza.
- Utilizar contraseñas de alta seguridad para evitar ataques de diccionario (método de *cracking* o descifrado de contraseñas que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario).

Es muy recomendable hacer copias de respaldo regularmente de los documentos importantes a medios extraíbles como *pen drives*, para poderlos recuperar en caso de infección por parte de algún malware, pero sólo si se tiene la seguridad de que esas copias están limpias.

Software anti-malware

- **Antivirus**. Son programas que detectan y eliminan o bloquean la actividad de malware. Puede proteger de varias formas:
    - Escaneando el tráfico procedente de la red en busca de *malware* que bloquea.
    - Interceptando intentos de ejecución automática no permitida.
    - Interceptando intentos de modificaciones no permitidas sobre aplicaciones importantes como el navegador web.
    - Detectando y eliminando o bloqueando *malware* que ya ha sido instalado en una computadora. Para ello analiza los programas instalados, el contenido del registro de Windows (para sistemas Windows), los archivos del sistema operativo y la memoria. Al terminar el escaneo muestra al usuario una lista con todas las amenazas encontradas y permiten escoger cuales eliminar o bloquear.
- **Antispyware**. Software que sirve para detectar, prevenir y eliminar *spyware*. Está centrado en este tipo de malware.
- **Virtualización**, permite dar acceso ilimitado pero sólo a recursos virtuales.
- **Aislamiento de procesos**, también conocido como sandbox.
- **Cortafuegos**. Software diseñado para controlar el tráfico de red. Ejemplos de funciones: filtrar paquetes de red sospechosos a partir de la información que contiene (por ejemplo dirección origen, dirección destino, tipo de mensaje,...), autenticación y autorización de accesos. Proporcionan cierto grado de protección frente a ataques de malware.
- **IDS** o **Sistemas de detección de intrusos**. Sistema que recolecta y analiza información con el objetivo de identificar posibles fallos de seguridad. Cuando detecta una acción sospechosa genera alarmas. La detección suele basarse en ver si el comportamiento se ajusta a algunos de los comportamientos típicos de malware que tiene en su base de datos, la detección de ciertas secuencias en el código y/o en el análisis estadísticos de parámetros (ancho de banda, protocolos y puertos usados, dispositivos conectados,...). Los tipos más habituales son:
    - **HIDS** o **IDS de host**. Reside en un equipo monitorizado y se encarga de analizar todos los logs para detectar actividades sospechas.
    - **NIDS** o **Sistemas de detección de intrusos en red**. Están conectados a un segmento de red y se encargan de detectar actividades sospechosas en el tráfico, como por ejemplo ataques de denegación de servicio, escáneres de puertos o intentos de acceso.
- **IPS** o **Sistemas de prevención de intrusos**. Hardware o software que tiene la habilidad de detectar ataques tanto conocidos como desconocidos y reaccionar a ellos para impedir su éxito. Suelen usar un software de cortafuegos asociado o trabajar de forma coordinada con un cortafuegos.