Códigos maliciosos

El código malicioso es lo que vulgarmente conocemos como **virus o malware.**

Se debe tener especial atención por parte de las empresas tanto públicas como privadas en asegurar que sus herramientas y dispositivos aseguren una integridad, confidencialidad y disponibilidad de los datos.

No olvidemos que los datos de una empresa son lo que garantizan la continuidad de la misma.

Una pérdida o robo de los mismos, perjudicaría gravemente a la empresa afectando tanto a su reputación como a la actividad normal de su empresa, pudiendo significar incluso el cierre del negocio.

¿Qué es el código malicioso o malware?
Son programas que tienen como objetivo acceder a tu sistema sin que detectes su presencia.
En función de la intención del Cracker, el programa podría:

- Robar credenciales, datos bancarios, información…
- Creación de redes con ordenadores botnet.
- Cifrado del contenido. Con esto se intenta que los usuarios paguen un rescate por sus datos.

¿Qué tipos de código malicioso existen?

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 fichero ejecutable (huésped) de manera que al ejecutar el programa también se ejecuta el virus. Tienen las propiedades 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 permiten usar el programa de manera 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, información industrial, datos personales, contraseñas, 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. Sin embargo, otras veces el spyware proviene de programas famosos de pago (ej. Red Shell fue distribuido a través de la plataforma Steam por los propios desarrolladores de juegos). El spyware suele estar centrado en obtener tipos específicos de información. Según como operan o la clase de información al que está orientado, tenemos distintos tipos de spyware. Hay que tener en cuenta que un spyware concreto puede ser de varios tipos a la vez. Algunos de los tipos más frecuentes son: **Keylogger, Banking Trojan, Password Stealer,Cookies de seguimiento..**

- **Malvertising:** se aprovecha de recursos disponibles por ser un anunciante publicitario, para buscar puertas traseras y poder ejecutar o instalar otro malware. Por ejemplo, anunciante publicitario en una página web aprovecha brecha de seguridad de navegador para instalar malware.

- **Ransomware o criptovirus:** software que afecta gravemente al funcionamiento del ordenador infectado (Por ejemplo: cifra el disco duro o lo bloquea) infectado y le ofrece al usuario la posibilidad de comprar la clave que permita recuperarse de 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.

- **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 versión de completa, la cual es de pago.
- **Decoy o señuelo**: software que imita la interfaz de otro programa para solicitar el usuario y contraseña y así poder obtener esa información.

- **Dialer:** toman el control del módem dial-up, realizan una llamada a un número de teléfono de tarificación especial, muchas veces internacional, y dejan la línea abierta cargando el coste de dicha llamada al usuario infectado. La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos, pero que solo permiten el acceso mediante conexión telefónica. Actualmente la mayoría de las conexiones a Internet son mediante ADSL y no mediante módem, lo cual hace que los dialers ya no sean tan populares como en el pasado.

- **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.

- **Wiper:** es un malware orientado al borrado masivo de datos. Por ejemplo, discos duros o bases de datos.

- **Clipper "malware".** Es un malware que se aprovecha de que los usuarios tienden a, en lugar de insertar manualmente, copiar cierto tipo de informaciones en el portapapeles (en inglés clipboard) y luego la utilizan pegándola en donde necesitan. Lo que hace este tipo de malware es monitorizar el portapapeles y cuando su contenido se ajusta a ciertos patrones lo reemplaza de manera oculta con lo que el atacante quiera. El uso más habitual de este tipo de aplicaciones es el secuestro de transacciones de pago al cambiar el destino de estas.