Plataforma de
Aprendizaje Virtual

Conceptos Fundamentales sobre Ciberseguridad

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Unidad 3

El código malicioso o malware

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Unidad 3

El código malicioso o malware

Este manual se realizó con la colaboración de la Dirección Nacional de Ciberseguridad, perteneciente a la Subsecretaría de Tecnologías de la Información de la Nación.

El código malicioso o malware

Los códigos maliciosos o malware son programas que se utilizan para atacar dispositivos electrónicos sin el conocimiento del usuario. El atacante lo envía con el objetivo de dañar el sistema informático o espiar, robar, eliminar o modificar la información alojada en él.

Los equipos se infectan a partir de acciones tales como la descarga de un archivo o aplicación, o haciendo clic en un enlace o ingresando a un sitio web malicioso. Aunque muchas veces suele hablarse de "virus informáticos" para designar este tipo de código existen muchos tipos de malwares, de los cuales los virus son solamente uno de ellos. Más adelante veremos las particularidades y diferencias entre algunos de los códigos maliciosos más difundidos.

Un poco de historia

Aunque parezca una contradicción, el primer código malicioso de la historia no era dañino: surgió como un experimento del investigador estadounidense Bob Thomas Morris, en 1971. Este programa informático, apodado Creeper (enredadera, en inglés), no buscaba causar daño en las computadoras, sino más bien demostrar que un software podía ser capaz de recorrer una red saltando de una computadora a otra. De esta manera, Morris diseñó un programa que se introducía en una computadora, mostraba el mensaje "***I'm the creeper, catch me if you can!" ("¡soy la enredadera, atrápame si puedes!")***, y luego saltaba a otra computadora, borrándose del dispositivo anterior.

Si bien se trataba de un programa inofensivo y experimental, implicó un desafío para los investigadores de aquel entonces. Si existía un programa que se autorreplicaba, alguien debía encontrar la manera de frenarlo.

Fue el informático estadounidense Ray Tomlinson quien creó el Reaper (podadora, en inglés), también conocido como el primer programa antivirus de la historia. De esta forma, el Reaper lograba "podar la enredadera" propagada por el Creeper.

A partir de entonces, la historia de los códigos maliciosos comenzaría un camino de expansión, ahora sí con objetivos más dañinos. Con distintos niveles de complejidad y peligrosidad, algunos de ellos se hicieron muy conocidos debido a su alcance. Entre los más emblemáticos se encuentran el virus Rabbit (1974), el cual se multiplicaba como un conejo hasta dañar la computadora infectada; Elk Cloner (1982), primer virus de gran escala a nivel mundial; el Gusano Morris (1988), primer ejemplar de malware autorreplicable que afectó a Internet; CIH o Chernobyl73 (1998), primer virus capaz de borrar contenido de la memoria ROM BIOS; MyDoom (2004), un gusano informático de rápido contagio que se propagaba por correo electrónico; Zeuz (2013), con millones de infecciones en todo el mundo, y así una variedad extraordinaria.

Tipos de malware

Como mencionamos anteriormente, existen distintos tipos de softwares maliciosos, de los cuales los "virus informáticos" son solo uno de ellos. Lo que tienen en común entre todos ellos es que se instalan en los dispositivos electrónicos sin el consentimiento ni el conocimiento del usuario (a partir de acciones como la descarga de un archivo o aplicación, haciendo clic en un enlace o ingresando a un sitio web malicioso), e infectan el dispositivo en cuestión.

Ahora que ya conocimos un poco sobre el surgimiento y la historia del malware, veamos algunos de los tipos más difundidos:

Malware	Cómo funciona	Cómo infecta	El objetivo
Virus	Los virus están diseñados para copiarse a sí mismos y propagarse por la mayor cantidad de dispositivos posibles.	A través de mails u otros servicios web, así como por medio de dispositivos extraíbles (como memorias USB) e, incluso, a través de conexiones de red.	Puede llegar a modificar o eliminar archivos almacenados en el equipo. Son capaces de dañar un sistema, eliminando o corrompiendo datos esenciales para su correcto funcionamiento.
Troyanos	Los troyanos suelen infiltrarse en el dispositivo de la víctima presentándose como software legítimo, pero una vez instalado, se activan e infectan el equipo.	Por medio de archivos adjuntos de mails o desde páginas webs poco fiables. también pueden esconderse tras descargas de juegos, películas o aplicaciones no legítimas.	Generalmente buscan controlar los dispositivos, robar datos, introducir más códigos maliciosos en el equipo y propagarse a otros dispositivos.
Gusanos	Una vez ejecutado en un sistema, pueden modificar el código o sus características. Generalmente, pasan inadvertidos, hasta que su proceso de reproducción se hace evidente.	Mediante archivos adjuntos, redes de intercambio de archivos, y enlaces a sitios webs maliciosos, así como por medio de la conexión de dispositivos externos infectados (como USB).	El objetivo es replicarse e infectar a otros dispositivos. Son capaces de realizar cambios en el sistema de un equipo sin autorización.

Ransomware	Este tipo de malware consigue tomar el control de un dispositivo, para "secuestrar" archivos o datos valiosos, inhabilitando el acceso a la víctima. A cambio de recuperar el control y la información, los ciberatacantes suelen exigir el pago de un rescate.	A través de archivos adjuntos de mails o desde páginas webs poco fiables, escondiendose tras descargas de juegos, películas o aplicaciones no legítimas.	Buscan cifrar todos los archivos y carpetas de un dispositivo, impidiendo el acceso a ellos sin una clave. El atacante utiliza este tipo de malware para pedir una recompensa a cambio de desbloquar los archivos.
Keyloggers	Los Keyloggers realizan un seguimiento y registro de cada tecla que se pulsa en un equipo, sin el consentimiento de la víctima. Pueden alojarse tanto en un software, como en un hardware (por ejemplo, un dispositivo USB).	Por medio de archivos adjuntos de correos o desde páginas webs poco confiables, escondiendose tras distintos tipo de descargas (juegos, aplicaciones, películas). También pueden propagarse a través de dispositivos USB infectados.	Su objetivo es monitorizar la actividad de un dispositivo, para recoger datos e información confidencial. Los ciberatacantes pueden utilizar esta información para realizar distinto tipo de ataques, como robo de cuentas o de información bancaria.

En la siguiente unidad veremos algunos consejos de seguridad para prevenir este tipo de malwares.

¿Cómo saber si un dispositivo está infectado de malware?

Si bien no siempre es posible saber que un software malicioso se encuentra presente en un dispositivo, existen algunos síntomas que sí permiten dar cuenta de ello:

- El dispositivo empieza a funcionar más lento de lo normal. Como el malware se adueña de los recursos de procesamiento del dispositivo, muchas de sus capacidades quedan reducidas, por lo que puede notarse una ralentización repentina.
- Reducción repentina de espacio de almacenamiento. Muchos tipos de malware descargan e instalan archivos y contenido adicional en el dispositivo, generando una falta de espacio de almacenamiento.
- Aparecen ventanas emergentes y programas no deseados. Esta es la señal más clara de la presencia de malware: en el dispositivo comienzan a abrirse ventanas y anuncios emergentes, o aparecen descargados programas extraños.

Si bien estas son algunas de las señales de una posible presencia de malware, el hecho de que un dispositivo funcione lento o tenga poco espacio de almacenamiento puede deberse a otras razones. Por lo tanto, es recomendable realizar cada cierto tiempo una limpieza del dispositivo, para comprobar si de esta forma se restablece el normal funcionamiento.

Señales de que tu dispositivo puede estar infectado:

A) Rendimiento anómalo:

- **Lentitud general:** El dispositivo funciona lento, las aplicaciones tardan en abrirse, los sitios web se cargan con lentitud, etc.
- **Bloqueos frecuentes:** El dispositivo se bloquea con más frecuencia de lo normal.
- **Reinicios inesperados:** El dispositivo se reinicia sin tu intervención.
- **Consumo elevado de batería:** La batería se agota más rápido de lo normal, incluso sin usarlo mucho.

B) Comportamiento extraño:

- **Anuncios intrusivos:** Aparecen anuncios emergentes o publicidad no deseada incluso en aplicaciones que no sueles usar.
- **Aplicaciones desconocidas:** Encuentras aplicaciones instaladas en tu dispositivo que no recuerdas haber instalado.
- **Navegación web inusual:** El navegador se abre solo, te redirige a páginas web no deseadas o cambia la página web que estás visitando.
- **Enlaces fraudulentos:** Recibes mensajes de texto o correos electrónicos con enlaces que parecen ser de fuentes confiables pero que te llevan a sitios web peligrosos.

C) Otras señales:

- **Mensajes de error inusuales:** Aparecen mensajes de error que no habías visto antes.
- **Problemas para conectar a internet:** No puedes conectarte a internet o la conexión es muy lenta.
- **Ruidos extraños:** El dispositivo emite ruidos extraños.
- **Sobrecalentamiento:** El dispositivo se sobrecalienta sin motivo aparente.

Si sospechás que tu dispositivo está infectado:

- Descargá e instalá un antivirus: Existen muchos antivirus gratuitos y de pago disponibles. Elige uno de una empresa de confianza y analiza tu dispositivo en busca de malware.
- Actualizá el software: Asegúrate de que el sistema operativo y todas las aplicaciones estén actualizados a la última versión. Las actualizaciones de software suelen incluir parches de seguridad que pueden protegerte de las últimas amenazas.
- Eliminá aplicaciones sospechosas: Si has instalado alguna aplicación recientemente que crees que puede ser la causa de la infección, desinstalala.
- Cambiá tus contraseñas: Cambia las contraseñas de todas tus cuentas, especialmente las que usas en el dispositivo infectado.
- Respaldá tus datos: Antes de realizar cualquier otra acción, asegúrate de respaldar tus datos importantes.

Si no estás seguro de qué hacer, consultá a un experto. Si no te sentís cómodo solucionando el problema por tu cuenta, podés llevar tu dispositivo a un técnico informático o a una tienda especializada.

La mejor manera de protegerte contra el malware es prevenirlo. Tené cuidado con los sitios web que visitás, los archivos que descargás y los enlaces en los que hacés clic.

Mantené tu software actualizado y utilizá un antivirus de confianza.

Si sospechás que tu dispositivo está infectado, tomá medidas de inmediato para solucionarlo.

¡Ya casi terminamos! En la próxima unidad nos centraremos en algunos consejos de seguridad, tanto para navegar en internet, como para crear contraseñas seguras, proteger la información personal y qué hacer en caso de ser víctimas de un ciberataque.

Plataforma de
Aprendizaje Virtual

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología