

CS-011 · Malware

Virus informáticos

Código malicioso que se adhiere a un archivo anfitrión y se propaga cuando ese archivo se ejecuta.

[Read this reference sheet in English](#)

← CS-010

Ficha 11 de 15

CS-012 →

Resumen ejecutivo

Un virus informático es código malicioso que se inserta en un archivo o programa anfitrión legítimo y se ejecuta cuando ese anfitrión se abre. A diferencia de un gusano, el virus necesita que un usuario o un proceso lance el archivo infectado antes de poder propagarse. Una vez activo puede copiarse en otros archivos y entregar una carga que va de inofensiva a destructiva.

Qué es

Un virus informático es un tipo de malware que no puede existir por sí solo. Incrusta su código dentro de un anfitrión, como un programa ejecutable, un documento con macros o un sector de arranque, y se activa solo cuando ese anfitrión se abre o se ejecuta. Esa dependencia de un anfitrión y de la acción del usuario es lo que distingue a un virus de otras familias de malware. Los virus suelen organizarse en tres partes: un mecanismo de infección que encuentra nuevos anfitriones y se adhiere a ellos, un disparador que decide cuándo actúa la carga, y la carga misma, que es la acción que el virus realiza. Entre los tipos históricos habituales están los infectores de archivos, que se adhieren a programas, los virus de macros, que viven dentro de documentos de oficina, y los virus de sector de arranque, que se cargan antes del sistema operativo.

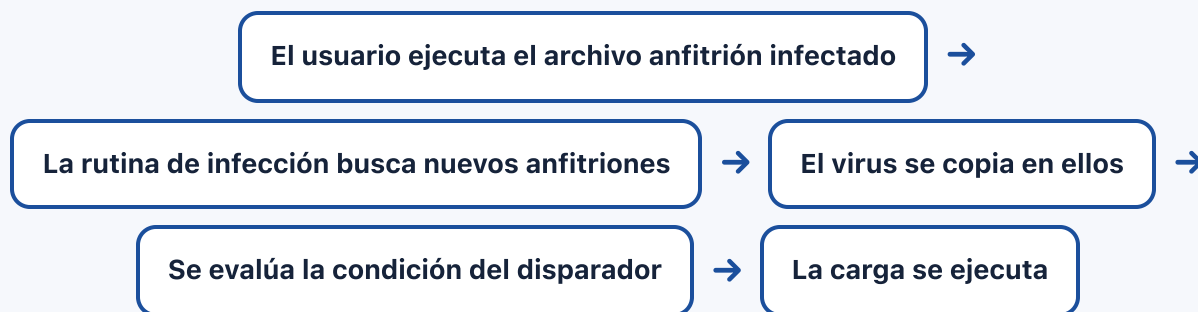
Por qué importa

Aunque los virus puramente autorreplicantes son hoy menos comunes que las amenazas combinadas, el concepto sigue siendo central en la forma en que los profesionales piensan el malware. Entender la infección, el disparo y la entrega de la carga es la base para analizar las amenazas actuales, que en su mayoría reutilizan esas ideas. Un solo archivo infectado compartido en una red puede interrumpir la operación, corromper datos y abrir el camino a un compromiso mayor. Para quien construye una carrera en seguridad, saber explicar cómo un virus se adhiere a un anfitrión y por qué importa la ejecución por parte del usuario es una expectativa básica en las entrevistas y en el trabajo.

■ Cómo funciona

Un virus arranca cuando un usuario ejecuta o abre un anfitrión infectado, por ejemplo al lanzar un programa o al habilitar las macros de un documento. La rutina de infección busca entonces otros anfitriones adecuados y escribe copias del virus en ellos, de modo que la infección puede propagarse cada vez que uno de esos archivos se usa. Muchos virus intentan evitar la detección cifrando o reorganizando su propio código, una técnica que se describe en general como polimorfismo o metamorfismo, para que cada copia se vea distinta ante los analizadores de firmas simples. La carga puede actuar de inmediato o esperar un disparador, como una fecha concreta, una cantidad de ejecuciones o una condición determinada. Como el virus viaja dentro de archivos legítimos, puede desplazarse por adjuntos de correo, unidades compartidas y medios extraíbles hasta donde lleguen esos archivos.

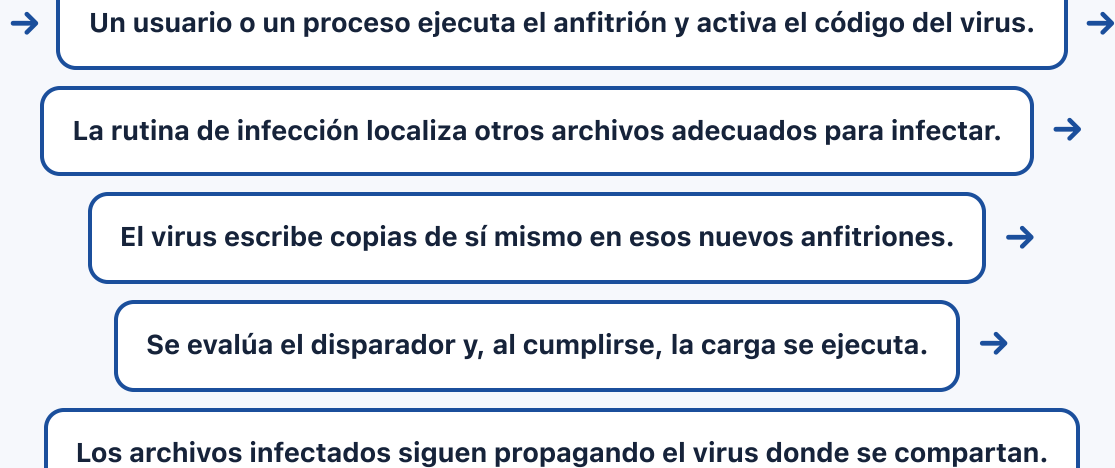
■ Diagrama de arquitectura



Un virus se propaga solo después de que se ejecuta un anfitrión infectado, y luego adhiere copias a nuevos anfitriones antes o después de disparar su carga.

■ Flujo de trabajo

Un archivo anfitrión infectado llega por correo, descarga, unidad compartida o medio extraíble.



■ Ataques frecuentes

- Virus de macros escondidos en documentos de oficina que corren al habilitar las macros
- Infectores de archivos que se adhieren a programas ejecutables y se propagan al lanzarse
- Infección del sector de arranque, que carga código malicioso antes del sistema operativo
- Archivos infectados propagados por adjuntos de correo y unidades de red compartidas
- Medios extraíbles como memorias USB que llevan archivos infectados entre sistemas

■ Errores frecuentes

- Habilitar macros en documentos de remitentes desconocidos o inesperados
- Ejecutar programas descargados de fuentes no confiables sin analizarlos
- Desactivar el antivirus o dejar que sus firmas queden desactualizadas
- Suponer que un solo producto antivirus atrapa todas las variantes
- Ignorar con qué facilidad viajan los archivos infectados en memorias USB y carpetas compartidas

■ Buenas prácticas

- Mantener la protección de endpoints instalada, activa y actualizada de forma automática
- Desactivar las macros de oficina por omisión y permitir las solo cuando se verifiquen
- Parchear sistemas operativos y aplicaciones para que no se abusen de fallas conocidas
- Aplicar el mínimo privilegio para que el código infectado no alcance con facilidad los archivos del sistema
- Analizar los medios extraíbles y las descargas antes de abrirlos
- Mantener copias de seguridad probadas para restaurar sin infección los archivos dañados

■ Lista de verificación

- ✓ Protección de endpoints desplegada en todos los dispositivos, con firmas actuales
- ✓ Ejecución de macros desactivada por política y controlada mediante ubicaciones confiables
- ✓ Sistemas operativos y aplicaciones parcheados según un calendario definido
- ✓ Los usuarios trabajan a diario sin derechos de administrador local
- ✓ Análisis de medios extraíbles exigido, o uso de medios extraíbles restringido
- ✓ Copias de seguridad probadas disponibles para restaurar archivos infectados o dañados

■ Herramientas recomendadas

Protección de endpoints o antivirus

Detecta y bloquea el malware de archivo conocido y sospechoso

Detección y respuesta en endpoints (EDR)

Vigila el comportamiento malicioso y permite contener y responder

Entorno aislado o servicio de detonación

Ejecuta un archivo sospechoso de forma segura para observar qué hace

Hash de archivos y consulta de reputación

Comprueba si un archivo se conoce como legítimo o como malicioso

■ Normas del sector

NIST SP 800-83

Guía para prevenir y manejar incidentes de malware en endpoints

NIST SP 800-61

Manejo de incidentes de seguridad, con contención y recuperación de malware

Controles Críticos de Seguridad del CIS

Defensas contra malware y configuración segura como salvaguardas prácticas

Relevancia profesional

Entender los virus es la base para analistas de SOC, personal de respuesta a incidentes y analistas de malware, que deben reconocer la infección, el disparo y el comportamiento de la carga. Los ingenieros de seguridad aplican este conocimiento al configurar las defensas de endpoint y endurecer sistemas, y los profesionales de GRC y auditoría se apoyan en él para evaluar si los controles contra malware están en su lugar. Para el público de GRC Careers, el conocimiento del malware es una expectativa habitual en puestos de seguridad y tecnología.

Preguntas de entrevista

- ¿Cuál es la diferencia entre un virus y un gusano?
- ¿Cuáles son las tres partes principales de un virus y qué hace cada una?
- ¿Por qué un virus suele requerir acción del usuario para propagarse?
- ¿Qué es un virus de macros y por qué los documentos son un portador frecuente?
- ¿Cómo ayuda el polimorfismo a un virus a evadir la detección por firmas?

Certificaciones relacionadas

CompTIA Security+
(GREM)

ISC2 Certified in Cybersecurity (CC)

GIAC Reverse Engineering Malware

Para profundizar

- [NIST SP 800-83: guía de prevención y manejo de incidentes de malware \(en inglés\)](#)
- [CISA: buenas prácticas de ciberseguridad \(en inglés\)](#)

■ Puntos clave

- Un virus se adhiere a un archivo anfitrión y necesita que ese anfitrión se ejecute para propagarse.
- Los virus tienen un mecanismo de infección, un disparador y una carga.
- Viajan dentro de archivos legítimos por correo, carpetas compartidas y medios extraíbles.
- Las defensas por capas de protección de endpoint, parches, mínimo privilegio y copias de seguridad funcionan mejor.
- Los fundamentos del malware sirven en puestos de SOC, respuesta a incidentes y análisis.

■ Preguntas frecuentes

- ▶ ¿Un virus es lo mismo que el malware?
- ▶ ¿Por qué los virus necesitan un archivo anfitrión?
- ▶ ¿El antivirus detiene todos los virus?

■ Carreras relacionadas

PUESTOS RELACIONADOS

Soc Analyst

Incident Responder

Malware Analyst

CERTIFICACIONES RELACIONADAS

CompTIA Security+

ISC2 Certified in Cybersecurity (CC)

GIAC Reverse Engineering Malware (GREM)

VACANTES ACTUALES

Las vacantes vigentes están en la bolsa de empleo.

[Ver todas las vacantes](#)

GUÍAS Y SALARIOS

[Vacantes en español](#)

[Glosario GRC](#)

[Empezar en privacidad](#)

[Cumplimiento por país](#)

RUTA DE APRENDIZAJE SUGERIDA

- 1 Afiance las bases con [CS-001 Ciberseguridad](#)
- 2 Estudie esta ficha: **Virus informáticos**
- 3 Profundice: [Troyanos](#)
- 4 Profundice: [Gusanos](#)
- 5 Valídelo: trabaje hacia **CompTIA Security+**
- 6 Encuentre el puesto: [vea las vacantes disponibles](#)

Las vacantes se publican en el idioma del empleador, por lo general en inglés.

FICHAS RELACIONADAS

[CS-012 Troyanos](#)

[CS-013 Gusanos](#)

[CS-014 Ransomware](#)

[CS-001 Ciberseguridad](#)

[CS-010 Higiene cibernética](#)

MÁS DE MALWARE

[CS-012 Troyanos](#)

[CS-013 Gusanos](#)

[CS-014 Ransomware](#)

[CS-015 Spyware](#)

Compartir

LinkedIn

Facebook

X

Correo