

CS-012 · Malware

Troyanos

Malware disfrazado de algo útil que ejecuta código dañino una vez que el usuario lo instala.

[Read this reference sheet in English](#)

[← CS-011](#)

Ficha 12 de 15

[CS-013 →](#)

Resumen ejecutivo

Un troyano es malware que se disfraza de software legítimo o deseable para engañar al usuario y lograr que lo instale y lo ejecute. Su nombre viene del caballo de Troya y se apoya en el engaño, no en la autorreplicación. Una vez ejecutado puede abrir una puerta trasera, robar datos, descargar más malware o dar al atacante el control remoto del dispositivo.

Qué es

Un troyano, a veces llamado caballo de Troya, es software malicioso que se presenta como algo que el usuario quiere: una herramienta gratuita, un juego, una aplicación con la licencia saltada, una actualización de software o un adjunto de correo. Se engaña al usuario para que lo instale, y ese es el punto central de la técnica. A diferencia de un virus o un gusano, un troyano no se propaga por sí mismo. Depende por completo de la ingeniería social para llegar a un sistema. Los troyanos suelen describirse por lo que hacen más que por cómo se propagan, y por eso los profesionales hablan de categorías como los troyanos de acceso remoto, que dan control al atacante, los troyanos bancarios, que roban credenciales financieras, los descargadores, que traen más malware, y los soltadores, que instalan otras cargas.

Por qué importa

Los troyanos son una de las formas más comunes en que los atacantes logran su primer apoyo en un sistema, justamente porque explotan la confianza humana y no una falla técnica. Un disfraz convincente puede sortear a un usuario prudente y llevar a credenciales robadas, cuentas vaciadas, despliegue de ransomware o acceso oculto de larga duración. Como la entrega depende del engaño, ningún parche por sí solo resuelve el problema, lo que vuelve esenciales la concientización y los controles por capas. Para los profesionales de seguridad, reconocer las tácticas de los troyanos es central para entender cómo empiezan las intrusiones y cómo cerrarlas temprano.

■ Cómo funciona

Un troyano llega a la víctima por un canal que parece confiable: un sitio de descargas, un adjunto de phishing, un aviso de actualización falso o software empaquetado con otro. El usuario lo instala o lo ejecuta creyendo que es legítimo. En ese momento el código malicioso oculto corre con los privilegios que tenga el usuario. Según su tipo, el troyano puede abrir una puerta trasera para el control remoto, registrar pulsaciones de teclas, extraer archivos, o descargar e instalar más malware. Muchos troyanos trabajan para pasar desapercibidos: disfrazan sus procesos, establecen persistencia para sobrevivir a un reinicio y se comunican en silencio con un servidor del atacante para recibir instrucciones. Como un troyano no puede replicarse solo, los atacantes lo distribuyen a gran escala con campañas de correo basura, anuncios maliciosos y sitios web comprometidos.

■ Diagrama de arquitectura



■ Flujo de trabajo

Un atacante empaqueta código malicioso dentro de algo que parece legítimo. →

El troyano se entrega por phishing, descargas, actualizaciones falsas o software empaquetado.

→ Se engaña al usuario para que lo instale o lo ejecute. →

El código oculto corre con los privilegios del usuario. →

El troyano abre una puerta trasera, roba datos o descarga más malware. →

Establece persistencia y se comunica con el atacante para recibir instrucciones.

■ Ataques frecuentes

- Troyanos de acceso remoto que dan al atacante control oculto de un dispositivo
- Troyanos bancarios que roban credenciales de acceso y financieras
- Descargadores y soltadores que instalan ransomware u otro malware
- Actualizaciones falsas y aplicaciones con la licencia saltada que llevan cargas ocultas
- Adjuntos de correo maliciosos disfrazados de facturas, currículos o documentos

■ Errores frecuentes

- Instalar software desde fuentes de descarga no oficiales ni confiables
- Confiar en avisos de actualización falsos que aparecen al navegar
- Abrir adjuntos de remitentes inesperados sin verificarlos
- Realizar las tareas diarias con derechos de administrador local
- Suponer que un programa es seguro porque parece funcionar como se anuncia

■ Buenas prácticas

- Instalar software solo de proveedores oficiales y tiendas de aplicaciones confiables

- Mantener la protección de endpoints activa, con firmas actuales y detección por comportamiento
- Aplicar el mínimo privilegio para que el código instalado tenga un alcance limitado
- Usar listas de permitidos de aplicaciones para bloquear ejecutables no aprobados donde sea práctico
- Capacitar a los usuarios para reconocer actualizaciones falsas, señuelos y adjuntos sospechosos
- Vigilar las conexiones de salida en busca de comunicación inesperada con servidores desconocidos

■ Lista de verificación

- ✓ Software obtenido solo de ubicaciones oficiales o aprobadas
- ✓ Protección de endpoints con detección por comportamiento activada
- ✓ Los usuarios trabajan por omisión sin derechos de administrador local
- ✓ Listas de permitidos o control de aplicaciones aplicados donde sea viable
- ✓ Actividad de red de salida vigilada en busca de conexiones sospechosas
- ✓ La capacitación en seguridad cubre actualizaciones falsas y adjuntos maliciosos

■ Herramientas recomendadas

Detección y respuesta en endpoints (EDR)

Detecta el comportamiento malicioso tras la ejecución y permite contenerlo

Listas de permitidos de aplicaciones

Evitan que corran programas no aprobados, troyanos incluidos

Entorno aislado o servicio de detonación

Ejecuta de forma segura un instalador sospechoso para revelar su comportamiento oculto

Monitorización de red

Señala conexiones de salida inesperadas usadas para mando y control

■ Normas del sector

NIST SP 800-83

Guía para prevenir y manejar malware, incluidos los instaladores engañosos

NIST SP 800-61

Marco de manejo de incidentes para contener un compromiso y recuperarse

MITRE ATT&CK

Cataloga técnicas del adversario como el mando y control y la persistencia

■ Relevancia profesional

Los troyanos son un tema central para analistas de SOC y personal de respuesta a incidentes, que investigan cómo empezó una intrusión y qué hizo el malware después de ejecutarse. Los analistas de malware hacen ingeniería inversa de troyanos para entender sus capacidades, y los ingenieros de seguridad diseñan listas de permitidos y controles de mínimo privilegio para bloquearlos. Los profesionales de GRC usan este conocimiento para evaluar los controles de malware y de concientización. Al público de GRC Careers le sirve reconocer cómo el engaño impulsa las intrusiones reales.

■ Preguntas de entrevista

- ¿En qué se diferencia un troyano de un virus y de un gusano?
- ¿Qué es un troyano de acceso remoto y por qué es peligroso?
- ¿Por qué la concientización del usuario importa tanto para defenderse de los troyanos?
- ¿Cómo pueden el mínimo privilegio y las listas de permitidos reducir el impacto de un troyano?
- ¿Qué señales podrían indicar que un troyano se comunica con un atacante?

■ 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 \(en inglés\)](#)
- [MITRE ATT&CK \(en inglés\)](#)

■ Puntos clave

- Un troyano se disfraza de software útil para engañar al usuario y lograr que lo instale.
- No se autorreplica y depende por completo del engaño.
- Una vez ejecutado puede abrir puertas traseras, robar datos o instalar más malware.
- Las defensas combinan fuentes confiables, mínimo privilegio, listas de permitidos y concientización.
- Los troyanos son una causa principal del acceso inicial en las intrusiones reales.

■ Preguntas frecuentes

► ¿Por qué se llama troyano?

► ¿Un troyano puede propagarse por sí solo?

► ¿Qué es un troyano de acceso remoto?

■ 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: **Troyanos**
- 3 Profundice: [Virus informáticos](#)
- 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-011 Virus informáticos](#)

[CS-013 Gusanos](#)

[CS-014 Ransomware](#)

[CS-001 Ciberseguridad](#)

MÁS DE MALWARE

[CS-011 Virus informáticos](#)

[CS-013 Gusanos](#)

[CS-014 Ransomware](#)

[CS-015 Spyware](#)

Compartir

LinkedIn

Facebook

X

Correo