

CS-013 · Malware

Gusanos

Malware autorreplicante que se propaga por las redes sin necesitar un archivo anfitrión ni la acción del usuario.

[Read this reference sheet in English](#)

[← CS-012](#)

Ficha 13 de 15

[CS-014 →](#)

Resumen ejecutivo

Un gusano es malware autónomo que se copia a sí mismo y se propaga de computadora a computadora por una red, a menudo sin ninguna acción del usuario. A diferencia de un virus, no necesita un archivo anfitrión al que adherirse, y a diferencia de un troyano, no depende del engaño. Su autorreplicación puede consumir el ancho de banda, sobrecargar sistemas y entregar una carga a gran escala en muy poco tiempo.

Qué es

Un gusano informático es un programa autocontenido que se reproduce y se desplaza entre sistemas por su cuenta. Esa independencia es su rasgo definitorio: un virus debe adherirse a un anfitrión y esperar que ese anfitrión se ejecute, pero un gusano lleva todo lo que necesita y puede propagarse de forma automática. Varios de los brotes más dañinos de la historia de la seguridad fueron gusanos, porque podían extenderse por una red entera en minutos sin que nadie hiciera clic en nada. Los gusanos suelen viajar explotando una vulnerabilidad de software, abusando de recursos y servicios de red compartidos o, en algunos casos, enviando copias de sí mismos por correo. Un gusano también puede llevar una carga, como instalar una puerta trasera, soltar ransomware o construir una red de equipos controlados.

Por qué importa

La velocidad y la autonomía hacen que los gusanos sean peligrosos de una forma singular. Como se autorreplican sin acción del usuario, un solo sistema sin parchear puede sembrar un brote que se propaga más rápido de lo que quien defiende puede responder a mano. Los gusanos pueden saturar redes, tumbar servicios y entregar cargas destructivas en miles de equipos. Su historia es un argumento duradero a favor de parchear sin demora, segmentar la red y poder aislar sistemas con rapidez. Para los profesionales, los gusanos ilustran por qué los controles proactivos y la planificación de la contención importan tanto como la detección.

■ Cómo funciona

Un gusano suele empezar en un sistema comprometido y de inmediato busca nuevos objetivos. Explora la red en busca de equipos alcanzables y de una debilidad concreta que sabe aprovechar, como una vulnerabilidad sin parchear o un servicio expuesto. Cuando encuentra un objetivo, se copia allí y se ejecuta, y la nueva copia repite el proceso, lo que produce un crecimiento exponencial. Como cada equipo infectado se convierte en una fuente nueva de infección, la contención suele depender de eliminar la debilidad de fondo y de cortar las rutas que el gusano usa para viajar. Algunos gusanos incluyen una carga que actúa junto con la propagación, mientras que otros se concentran solo en extenderse y en informar al atacante.

■ Diagrama de arquitectura



■ Flujo de trabajo

Un gusano se activa en un equipo comprometido. →

Explora la red en busca de sistemas alcanzables y de una debilidad conocida. →

Explota una vulnerabilidad o abusa de un servicio o recurso compartido expuesto. →

Se copia al equipo nuevo y se ejecuta allí. →

La copia nueva empieza a explorar y a propagarse de forma independiente. →

Cualquier carga, como una puerta trasera o ransomware, se entrega en el camino.

■ Ataques frecuentes

- Explotar vulnerabilidades sin parchear expuestas a la red para propagarse de forma automática
- Abusar de recursos compartidos y servicios de red abiertos para copiarse entre equipos
- Enviar copias de sí mismo de forma masiva para propagarse por correo
- Soltar ransomware o puertas traseras como carga durante la propagación
- Consumir ancho de banda y recursos hasta interrumpir la operación

■ Errores frecuentes

- Dejar sin parchear los sistemas expuestos a internet frente a fallas que los gusanos explotan
- Operar redes planas, sin segmentación que frene la propagación lateral
- Exponer servicios y recursos compartidos innecesarios a la red general
- No tener una forma de aislar rápido los sistemas infectados durante un brote
- Confiar solo en la detección, sin un plan de contención y recuperación

■ Buenas prácticas

- Parchear sin demora, con prioridad a las fallas expuestas a la red y explotables de forma remota
- Segmentar las redes para que un brote no se propague libremente por todo el entorno
- Desactivar o restringir servicios, puertos y recursos compartidos innecesarios
- Desplegar detección en el endpoint y en la red para atrapar actividad anómala y rápida
- Preparar y ensayar un plan de contención para aislar sistemas con rapidez
- Mantener copias de seguridad probadas para reconstruir sin infección los sistemas afectados

■ Lista de verificación

- ✓ Sistemas expuestos a la red parcheados frente a vulnerabilidades explotadas conocidas
- ✓ Segmentación de red implementada para limitar el movimiento lateral
- ✓ Servicios, puertos y recursos compartidos innecesarios desactivados o restringidos
- ✓ Detección afinada para notar la exploración y la replicación rápidas
- ✓ Procedimiento documentado y ensayado para aislar equipos infectados
- ✓ Copias de seguridad probadas disponibles para reconstrucciones limpias

■ Herramientas recomendadas

Escáner de vulnerabilidades

Encuentra las fallas sin parchear que los gusanos suelen explotar

Detección y respuesta de red (NDR)

Nota la exploración rápida y el movimiento lateral que producen los gusanos

Detección y respuesta en endpoints (EDR)

Detecta y contiene la actividad del gusano en cada equipo

Segmentación de red y firewalls

Limita las rutas que un gusano puede usar para propagarse

■ Normas del sector

NIST SP 800-83

Guía para prevenir y manejar malware, incluidas las amenazas de propagación rápida

NIST SP 800-61

Manejo de incidentes, contención y recuperación de brotes

Controles Críticos de Seguridad del CIS

Gestión de parches y defensas de red que limitan la propagación

Relevancia profesional

Los gusanos son un estudio clave para analistas de SOC y personal de respuesta a incidentes, que deben detectar la propagación rápida y contenerla antes de que desborde la red. Los ingenieros de seguridad aplican sus lecciones con parches, segmentación y endurecimiento de servicios, y los analistas de malware examinan el código del gusano para entender su propagación y su carga. Los profesionales de GRC usan escenarios de gusanos para justificar los controles de parches y de segmentación. Al público de GRC Careers le deja un modelo claro de por qué importa la velocidad de respuesta.

Preguntas de entrevista

- ¿En qué se diferencia un gusano de un virus y de un troyano?
- ¿Por qué los gusanos pueden propagarse sin ninguna acción del usuario?
- ¿Cómo ayuda la segmentación de red a contener un brote de gusano?
- ¿Por qué parchear sin demora es especialmente importante frente a los gusanos?
- ¿Qué pasos daría para contener un gusano que se propaga por una red?

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 gusano es malware autónomo que se autorreplica y se propaga por las redes.
- No necesita archivo anfitrión y a menudo tampoco acción del usuario, a diferencia de un virus o un troyano.
- La autorreplicación puede causar brotes más rápidos de lo que la respuesta manual aguanta.
- Parchear, segmentar y aislar con rapidez son las defensas más fuertes.
- Los gusanos muestran por qué los controles proactivos y el plan de contención son esenciales.

Preguntas frecuentes

► ¿Cuál es la diferencia principal entre un gusano y un virus?

► ¿Por qué se consideran tan peligrosos los gusanos?

► ¿Cómo se detiene un brote de gusano?

Carreras relacionadas

PUESTOS RELACIONADOS

Soc Analyst

Incident Responder

Security Engineer

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: **Gusanos**
- 3 Profundice: [Virus informáticos](#)
- 4 Profundice: [Troyanos](#)
- 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-012 Troyanos](#)

[CS-014 Ransomware](#)

[CS-001 Ciberseguridad](#)

MÁS DE MALWARE

[CS-011 Virus informáticos](#)

[CS-012 Troyanos](#)

[CS-014 Ransomware](#)

[CS-015 Spyware](#)

Compartir

LinkedIn

Facebook

X

Correo