

CS-015 · Malware

Spyware

Software que recoge en secreto información sobre una persona o un dispositivo, sin su consentimiento.

[Read this reference sheet in English](#)

← CS-014

Ficha 15 de 15

Final →

Resumen ejecutivo

El spyware es software malicioso que recoge en silencio información sobre un usuario o un dispositivo y la envía a un tercero sin permiso. Puede capturar pulsaciones de teclas, credenciales, hábitos de navegación, archivos y capturas de pantalla. Como está construido para pasar desapercibido, el spyware suele funcionar mucho tiempo antes de que alguien note la pérdida de datos.

Qué es

El spyware es una categoría de malware cuyo objetivo principal es la vigilancia y el robo de datos, no la interrupción inmediata. En lugar de cifrar archivos o tumbar sistemas, trabaja para mantenerse invisible y poder seguir observando. La familia cubre varios tipos que se solapan: los registradores de teclas, que graban cada pulsación; los ladrones de información, que cosechan contraseñas guardadas y datos del navegador; las cookies de seguimiento y los componentes de adware, que perfilan el comportamiento para la publicidad; y los programas de acecho, que una persona instala en el dispositivo de otra para vigilarla. Parte del spyware llega empaquetado dentro de software gratuito de apariencia legítima, mientras que otras variantes se entregan por phishing, descargas maliciosas o la explotación de una vulnerabilidad.

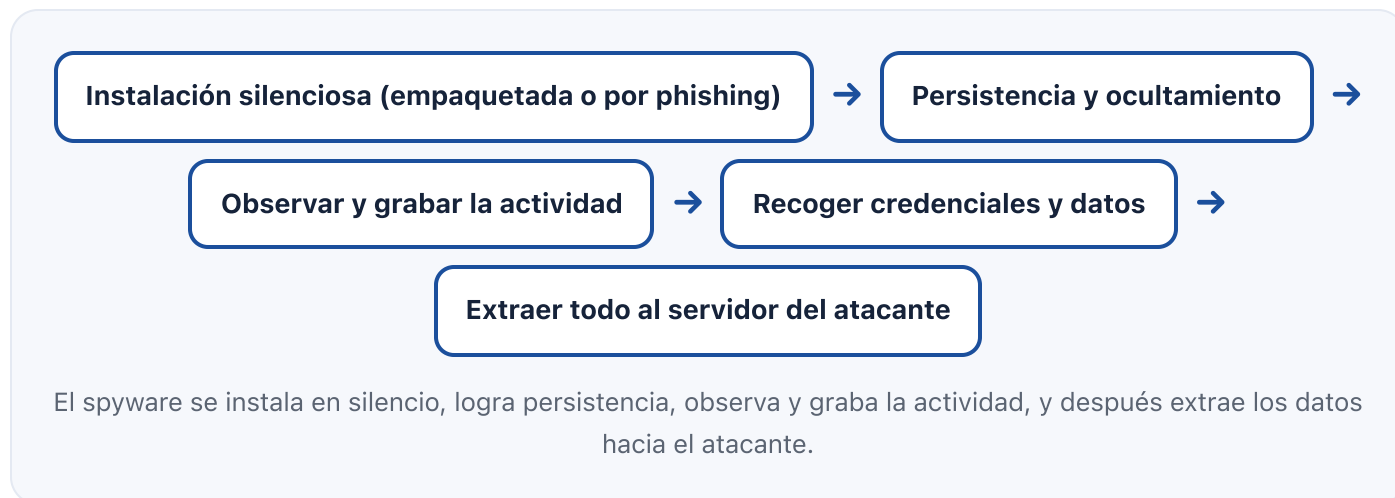
Por qué importa

El daño del spyware suele ser silencioso y acumulativo. Las credenciales robadas pueden reutilizarse para entrar al correo, la banca y los sistemas corporativos, y los datos de negocio capturados pueden llevar a fraude, espionaje o una brecha mayor. Para una organización, un ladrón de información en una sola computadora portátil puede exponer a la vez las contraseñas de decenas de servicios internos y en la nube, y convertir un endpoint infectado en un problema de toda la red. Los programas de acecho plantean además preocupaciones serias de seguridad personal y de orden legal. Para los profesionales, entender el spyware es central en la defensa de endpoints, la respuesta a incidentes y el trabajo de privacidad, porque el objetivo del atacante es ver todo lo que ve la víctima.

■ Cómo funciona

El spyware primero establece un punto de apoyo, a menudo engañando al usuario para que ejecute un instalador o viajando junto con otro software. Una vez en marcha, intenta lograr persistencia para sobrevivir a los reinicios y después empieza a recoger lo que fue diseñado para robar: pulsaciones de teclas, contenido del portapapeles, credenciales guardadas o capturas de pantalla. Los datos recogidos se preparan de forma local y luego se envían, o se extraen, hacia un servidor que el atacante controla, con frecuencia disfrazados dentro de tráfico web de apariencia normal para no despertar sospechas. Muchas variantes también intentan esconder sus archivos y procesos, desactivar las herramientas de seguridad y actualizarse, para que quien defiende tenga más dificultad en encontrarlas y eliminarlas.

■ Diagrama de arquitectura



■ Flujo de trabajo

Aislar el dispositivo afectado de la red para detener la extracción de datos.



Confirmar la infección con un análisis actualizado de endpoint o antimalware y la revisión de los registros.



Identificar a qué pudo acceder el spyware, en especial credenciales guardadas y archivos sensibles.



Eliminar el spyware y sus mecanismos de persistencia, o reinstalar el dispositivo si no se puede restablecer la confianza.



Restablecer toda contraseña y token de sesión que pudieran haberse capturado, empezando por el correo y las cuentas de administración.



Revisar cómo llegó, cerrar esa vía y vigilar una posible reinfección.

■ Ataques frecuentes

- Registradores de teclas que graban usuarios, contraseñas y mensajes al escribirse
- Ladrones de información que toman contraseñas guardadas del navegador, cookies y datos de autocompletado
- Descargas maliciosas y software con la licencia saltada que traen spyware oculto
- Adjuntos o enlaces de phishing que instalan una carga de vigilancia
- Programas de acecho instalados en un dispositivo para vigilar a una persona concreta

■ Errores frecuentes

- Suponer que un dispositivo silencioso es un dispositivo limpio, cuando el spyware se diseña para no hacer ruido

- Limpiar el malware y no rotar nunca las credenciales que pudo haber robado
- Instalar software gratuito de fuentes no confiables sin leer qué trae empaquetado
- Ignorar los permisos del navegador y del móvil que conceden acceso amplio a los datos
- Confiar en un solo análisis en lugar de confirmar con detección por capas

■ Buenas prácticas

- Usar detección y respuesta en endpoints (EDR) o un antimalware de buena reputación, y mantenerlo actualizado
- Instalar software solo de fuentes oficiales y confiables, y revisar los permisos que solicita
- Exigir autenticación multifactor, para que las contraseñas robadas no basten por sí solas
- Usar un gestor de contraseñas en lugar de guardar credenciales en el navegador
- Parchear sin demora sistemas operativos, navegadores y aplicaciones para cerrar vías de entrada
- Formar a los usuarios para reconocer el phishing y las descargas riesgosas

■ Lista de verificación

- ☒ EDR o antimalware desplegado y al día en todos los endpoints
- ☒ Autenticación multifactor activada en el correo y en las cuentas de administración y financieras
- ☒ Instalación de software restringida a fuentes confiables o a un catálogo aprobado
- ☒ Guardado de contraseñas en el navegador desactivado, a favor de un gestor de contraseñas
- ☒ Un proceso para restablecer credenciales tras cualquier sospecha de infección por spyware
- ☒ Dispositivos móviles revisados en busca de aplicaciones inesperadas y permisos excesivos

■ Herramientas recomendadas

**Detección y respuesta en endpoints
(EDR)**

Antimalware o antivirus

Analiza y elimina el spyware y los ladrones de información conocidos

Detecta el comportamiento de vigilancia y permite contener y responder

Gestor de contraseñas con MFA

Reduce el valor de las credenciales robadas y evita guardarlas en el navegador

Monitorización de red

Señala conexiones de salida inusuales que pueden indicar extracción de datos

■ Normas del sector

NIST SP 800-83

Guía para prevenir y manejar incidentes de malware, spyware incluido

NIST SP 800-61

Ciclo de manejo de incidentes que se usa para responder a las infecciones

Controles Críticos de Seguridad del CIS

Salvaguardas prácticas como las defensas contra malware y la gestión de cuentas

■ Relevancia profesional

El spyware aparece a diario para los analistas de SOC que clasifican alertas, el personal de respuesta a incidentes que dimensiona la pérdida de datos, los analistas de malware que hacen ingeniería inversa de muestras y los ingenieros de seguridad que endurecen endpoints. A los profesionales de privacidad y de GRC también les importa, porque amenaza de forma directa los datos confidenciales y puede activar deberes de notificación de brechas, y ese es el público al que sirve GRC Careers.

■ Preguntas de entrevista

- ¿En qué se diferencia el spyware del ransomware en objetivos y comportamiento?
- ¿Qué es un ladrón de información y por qué una sola portátil infectada es más grave de lo que parece?
- ¿Cómo determinaría a qué datos pudo acceder un spyware?

- ¿Por qué restablecer las credenciales es un paso crítico tras una infección por spyware?
- ¿Qué controles reducen el impacto de las contraseñas robadas?

Certificaciones relacionadas

CompTIA Security+
(GREM)

ISC2 Certified in Cybersecurity (CC)

GIAC Reverse Engineering Malware

Para profundizar

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

Puntos clave

- El spyware roba información en silencio: prioriza el sigilo sobre la interrupción.
- Una sola infección por un ladrón de información puede exponer credenciales de muchos servicios a la vez.
- Eliminar el malware no basta: hay que rotar todas las credenciales robadas.
- La autenticación multifactor y un gestor de contraseñas amortiguan el daño.
- Es un tema central en la defensa de endpoints, la respuesta a incidentes y la privacidad.

Preguntas frecuentes

► ¿Cómo sé si un dispositivo tiene spyware?

► ¿El adware es lo mismo que el spyware?

► ¿Restablecer las contraseñas resuelve un problema de spyware?

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 aparecen en la versión web. Vea la bolsa de empleo para los puestos vigentes de GRC y seguridad.

[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: **Spyware**
- 3 Profundice: [Troyanos](#)
- 4 Profundice: [Ciberseguridad](#)
- 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-001 Ciberseguridad](#)[CS-010 Higiene cibernética](#)

MÁS DE MALWARE

CS-011 Virus informáticos

CS-012 Troyanos

CS-013 Gusanos

CS-014 Ransomware

← CS-014

Ficha 15 de 15

Final →

Compartir

LinkedIn

Facebook

X

Correo