



TOP 10 tipos de Malware en el Q1 del 2025

www.dragonjar.org





Infostealers

Los stealers están diseñados para robar credenciales, cookies, historiales y wallets. En Q1 2025 encabezan el ranking con un salto brutal desde los 5.799 casos en Q1 2024. Su crecimiento del +521% refleja el auge del cibercrimen centrado en el robo de identidades digitales y accesos corporativos.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





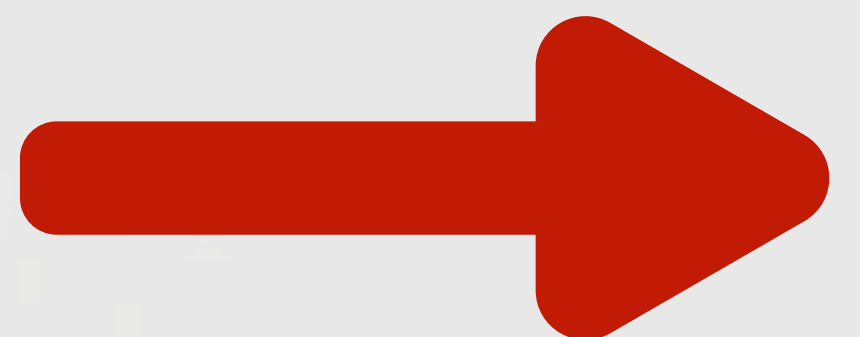
Loaders

Los loaders son malware que sirven como puerta de entrada para otras amenazas, como ransomware o stealers. Suben desde 4.770 en 2024 a más de 15 mil en 2025, un incremento del 225%. Su rol como “delivery” explica su protagonismo en campañas masivas automatizadas.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





RAT's

Los Remote Access Trojans permiten control total del sistema infectado. Pasan de 4.956 casos a más de 13 mil, creciendo un +165%. Esta herramienta sigue siendo clave para espionaje y persistencia en entornos comprometidos, usada tanto por actores APT como por ciberdelincuentes.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





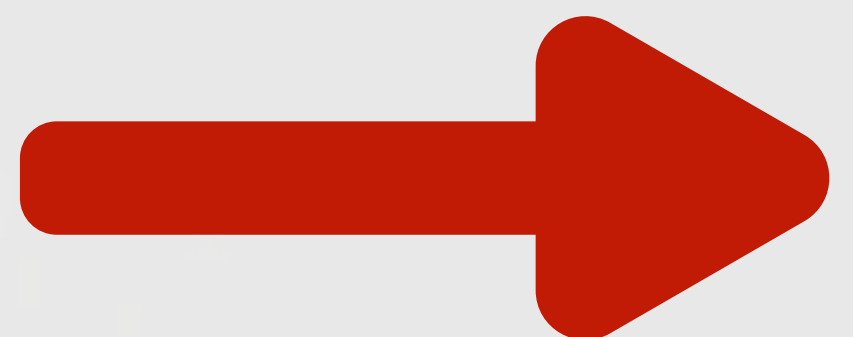
Ransomware

Aunque ha perdido atención mediática, el ransomware sigue muy activo. De 4.065 en Q1 2024 a más de 10 mil muestras en 2025 (+155%), se mantiene como una amenaza rentable. Su evolución incluye tácticas de doble extorsión y ataques dirigidos a infraestructuras críticas.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





Botnet

Las botnets no aparecían en el Top 2024 pero irrumpen con fuerza en 2025. Se utilizan para ataques DDoS, spam y minado ilegal. Su regreso podría estar ligado al crecimiento de dispositivos IoT mal asegurados y a campañas de propagación de malware a escala.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





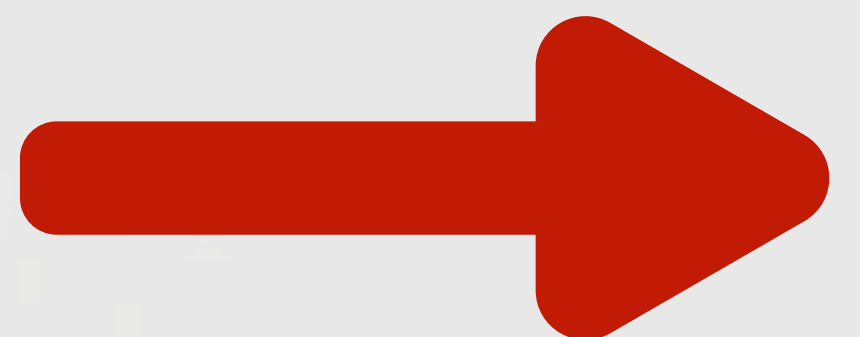
Keylogger

Los keyloggers registran pulsaciones del teclado para robar credenciales o espiar usuarios. Pasan de 1.682 a casi 4.500 muestras (+167.5%), mostrando un uso sostenido en campañas dirigidas y herramientas usadas por criminales con bajo presupuesto.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





Backdoor

Las puertas traseras permiten el acceso oculto y persistente al sistema. Aunque tenían apenas 587 casos en Q1 2024, suben a más de 2.000 (+255.9%). Se integran a menudo en malware personalizado y campañas APT para evitar la detección.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





Exploit

Los exploits aprovechan vulnerabilidades en software para ejecutar código malicioso. Su aparición en el ranking de 2025 muestra una explotación más activa de CVEs recientes, posiblemente favorecida por kits de exploits automatizados en foros underground.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





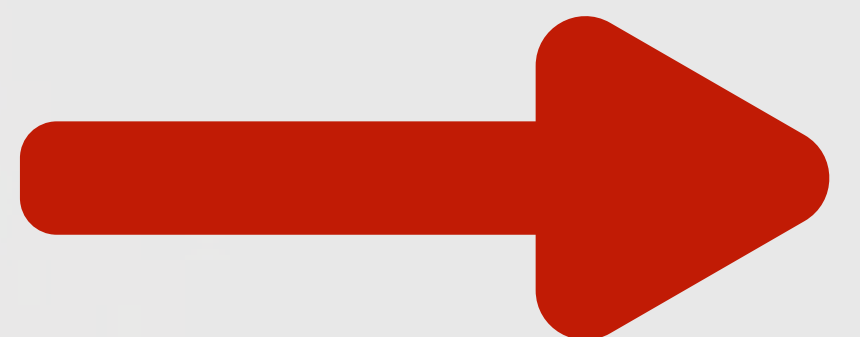
Adware

El adware, aunque menos sofisticado, sigue siendo molesto y persistente. Con casi 1.900 detecciones, su presencia en el top sugiere que aún se usa en campañas de monetización masiva, especialmente contra usuarios domésticos a través de descargas dudosas.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**





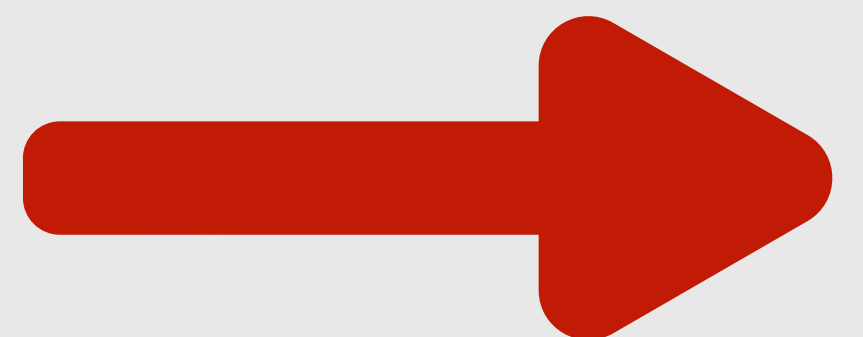
Troyano

Los troyanos bajan del 7.º lugar en 2024 (972 detecciones) al 10.º en 2025, con solo 542 muestras. El descenso del -44% podría indicar una migración hacia malware más especializado como stealers y loaders, reflejando una evolución en las tácticas ofensivas.

Referencias:

- *Top Malware Types in Q4 2024 by AnyRun <https://djar.co/2024Q1>*
- *Top Malware Types in Q4 2025 by AnyRun <https://djar.co/2025Q1>*

**TOP 10 tipos de Malware
en el Q1 del 2025**



¿Las credenciales de tu empresa han sido comprometidas por un malware infostealer?

Los infostealers llevan años siendo el malware mas popular en entornos reales y sandbox como Any.Run. Nosotros hemos reunido 7 TB de logs de infostealers y creado un sistema de informes automáticos que, te informará si tu cuenta o las de tu empresa ya fueron comprometidas



Visita djar.co/stealers para obtener tu informe personalizado gratis



***¿Quieres saber si tus
activos resistirían frente a
las amenazas más comunes
del momento, como
stealers, loaders o RATs?***

Hablemos...

Valentina Nieto F.

Directora Comercial

comercial@dragonjar.org

(+57) 304 384 9657

