

Infostealers

Malware that quietly steals saved passwords, cookies and crypto wallets, then sells the access to fraudsters and ransomware crews.

WHAT IT IS

An infostealer is malware that secretly harvests saved logins, session cookies, card data and cryptocurrency wallets from a device, then sends the logs to an attacker. Most are rented as a service, so one infection on a single laptop can expose email, cloud consoles and banking.

WHY IT MATTERS

54%

of ransomware victims had their domain show up in infostealer logs before the attack

Verizon DBIR, 2025

165+

organisations exposed when infostealer-stolen credentials with no MFA were used to breach Snowflake customer accounts

CISA alert, 2024

1.7M+

instances where the LummaC2 stealer was used to steal information

FBI, 2025

WHAT HAPPENED

In October 2024, Operation Magnus saw Dutch police and the FBI, coordinated by Eurojust, disrupt the RedLine and Meta infostealers, seizing servers and back-end data tied to millions of victims, and charges were unsealed against an alleged RedLine developer. Even so, logs stolen before the takedown still circulate today (Eurojust).

RED FLAGS TO WATCH FOR

Infostealers are built to be silent, so watch the accounts, not just the laptop.

- A monitoring alert that your email or password has appeared in a leak or stealer log.
- Logins from odd locations, or two active sessions on one account at once.
- Password-reset or MFA prompts you did not trigger.
- A browser extension, scheduled task or app that nobody installed.

THE ONE RULE THAT STOPS IT

Turn on phishing-resistant multi-factor authentication on every account, including SaaS and cloud consoles.

THEN BUILD THE HABIT AROUND IT

- Stop saving corporate passwords in browsers and give staff a managed password manager.
- Monitor for exposed credentials and rotate them fast. Treat any leaked credential as already compromised.

- Shorten sessions and revoke them on risk signals, so a stolen cookie expires quickly.
- Run EDR, limit admin rights and block cracked or pirated software, a common infostealer carrier.

MYTHS AND FACTS

MYTH

MFA makes infostealers harmless.

FACT

Stolen session cookies can resume a logged-in session without the password or a second factor.

MYTH

If my antivirus is clean, I was not infected.

FACT

Many stealers run in seconds and self-delete. Credential monitoring often catches what the endpoint misses.

MYTH

An old leaked password is no longer a risk.

FACT

Stolen credentials work until they are changed. The 2024 Snowflake breaches used credentials harvested years earlier.

THE LEGAL DUTY

Under Cybersäkerhetslagen and NIS2, a significant incident means a 24-hour early warning to MCF (formerly MSB) and a 72-hour notification. If personal data is exposed, GDPR Article 33 adds a separate 72-hour notice to IMY.

GET HELP

If credentials are already circulating, eBuilder Security can help you find exposed logins, lock down access and meet your reporting duties.

[Read the Full Article →](#)