

Fileless Attacks: What they are, how they work, and ways to stop them

Gridinsoft Help Center

What it is

A fileless attack runs malicious code directly in memory or abuses built-in tools (PowerShell, WMI, Office macros) so there's little or nothing written to disk. That stealth lets it slip past traditional antivirus and move quickly inside a network.

How it works

- A booby-trapped page, email, or doc launches scripts in memory.
- Legit tools are abused to download commands, dump creds, or move laterally ("living off the land").
- Persistence hides in scheduled tasks, registry, or legit admin tools - not obvious EXE files.

What you may notice

- Brief command windows flashing, odd PowerShell activity
- Security tools disabled or failing to update
- New scheduled tasks/services; spikes in CPU or network from system processes
- Alerts about script hosts or encoded commands

If you suspect it

- Disconnect from the network.
- Run a reputable EDR/anti-malware scan; reboot and scan again.
- Inspect Startup, Scheduled Tasks, services, and Office add-ins; remove unknowns.
- From a clean device, change passwords and enable MFA.
- Review logs/DNS for suspicious domains and block them.

Prevent it

- Disable macros by default; allow only signed scripts.
- Constrain PowerShell (Constrained Language Mode), restrict WMI/PSRemoting.
- Keep OS, Office, browsers, and drivers updated.
- Use EDR that monitors script behavior and command-line anomalies.
- Apply least privilege; limit local admins and use application allow-listing.