Cobalt Strike Beacon: What it is, how it’s used, and how to detect and contain

Gridinsoft Help Center

What it is

What you may notice

- Repeating, short network "check-ins" to odd domains/IPs (often over HTTPS or DNS)
- Legit tools (PowerShell, PsExec) launched in strange ways
- New services/scheduled tasks; security tools disabled or excluded

How it gets in

- Phishing documents and fake installers
- Exploited VPN/RDP or unpatched public apps
- Stolen admin credentials from earlier malware

If you suspect Beacon (quick response)

- Isolate the host from the network-don’t just kill the process.
- Collect evidence first (memory, logs), then remove persistence (tasks/services).
- Reset credentials from a clean admin box; rotate keys/tokens.
- Hunt laterally-assume more than one foothold.
- Engage your IR team; block C2 domains/IPs at the firewall/DNS.

Prevent it

- Patch internet-facing systems; lock down or remove unused remote access.
- Enforce MFA, least privilege, and admin "jump" workstations.
- Monitor for beaconing patterns and unusual admin tool usage.
- Use EDR with script logging (PowerShell, AMSI) and DNS filtering.
- Train staff to spot phishing; test restores from offline backups.