Advanced Persistent Threat (APT): What it is, how it works, and how to defend against it

Gridinsoft Help Center

What it is

How it works

- Initial access: spear-phishing, stolen credentials, or a zero-day.
- Persistence & stealth: "living off the land" tools, scheduled tasks, legit admin utilities.
- Lateral movement: hop between systems, escalate privileges, map crown jewels.
- Exfiltration: compress, stage, and quietly send data out.

What you might notice

- Unusual admin logins at odd hours
- New scheduled tasks, services, or remote connections
- Legit tools (PowerShell, PsExec) used in suspicious ways
- Data spikes to unknown destinations

If you suspect an APT

- Isolate affected systems; don’t tip off the attacker with broad resets.
- Collect evidence (logs, memory, timelines) before changes.
- Reset creds from a clean host; rotate keys/tokens.
- Hunt laterally-assume multiple footholds.
- Engage IR specialists and notify stakeholders as required.

Strengthen your defenses

- EDR/XDR + threat hunting; enable detailed logging (auth, PowerShell, DNS, proxy).
- MFA everywhere, least privilege, and privileged access workstations.
- Patch fast on internet-facing apps; inventory and segment critical data.
- Email and identity security: protect against spear-phishing and token theft.
- Practice: tabletop exercises and restore drills for backups.