# Ghostware - What it is, why it’s hard to catch, and how to defend against it

Gridinsoft Help Center

## What it is

Ghostware is stealthy malware built to avoid detection. It slips into high-value targets like companies or governments, quietly collects sensitive data, then wipes or hides traces so traditional antivirus has little to find.

## How it works - quick tour

- Low-noise tactics - blends in with normal processes and traffic
- Living-off-the-land - uses built-in tools instead of obvious malware files
- Log tampering - clears or alters records to erase its footsteps
- Timed activity - works in short bursts to dodge monitoring

## What you might notice

- Occasional login prompts or re-auth requests you didn’t start
- Gaps in logs or disabled auditing on key systems
- Strange after-hours network traffic from sensitive hosts
- Security tools turned off or set to permissive modes

## If you suspect it - first moves

- Isolate likely affected systems and preserve memory and logs.
- From a clean admin box, rotate credentials and tokens.
- Review outbound connections, block suspicious domains/IPs, and collect samples.
- Engage incident response to hunt for persistence and rebuild from clean images if needed.

## Prevent it

- MFA everywhere and least-privilege access for admins.
- Use EDR/XDR that monitors behavior and command-line activity.
- Turn on centralized logging with write-once storage and alert on log tampering.
- Patch fast on internet-facing apps and keep endpoints updated.
- Segment networks and restrict egress so sensitive systems can’t freely call out.