Time Bomb - what it is, warning signs, and how to prevent timed attacks

Gridinsoft Help Center

Time Bomb

What it is

A time bomb is malware (or a hidden malicious feature) set to go off at a specific date or time. Until that moment, it stays quiet, then runs its payload - deleting files, encrypting data, stealing info, or opening a back door. It’s a time-based version of a "logic bomb." Quick explainer and examples: https://gridinsoft.com/time-bomb

Why it matters

Because it sleeps first, normal use can look safe during testing. When the timer hits, damage happens fast and all at once - perfect for sabotage, ransom demands, or wiping traces after an intrusion.

How it works Trigger set: code checks the system clock or a counter (days since install).

- Timer sources: Scheduled Task/cron, startup scripts, or a hidden check inside an app/add-in.

- Go-time: runs the payload (encrypt, delete, exfiltrate, or install more malware).

- Hide: may reset the clock check, disable logs, or remove itself afterward.

Red flags

- Unknown Scheduled Tasks/cron jobs set for a future date or repeating at odd hours.

- Programs that behave differently after a specific date or number of launches.

- Files modified in a burst at the same timestamp across many folders.

- Compile/metadata timestamps that don’t match the rest of the system or vendor.

Do it right

- Review and clean Scheduled Tasks/cron, startup items, and login scripts regularly.

- Use reputable security software with behavior rules for mass file changes and script abuse.

- Keep good, offline backups and test restores - timers can trigger destructive wipes.

- Lock down admin rights and code execution (allowlisting, signed scripts only).

- If you suspect a time bomb, isolate the device, collect logs, and scan from a clean environment.