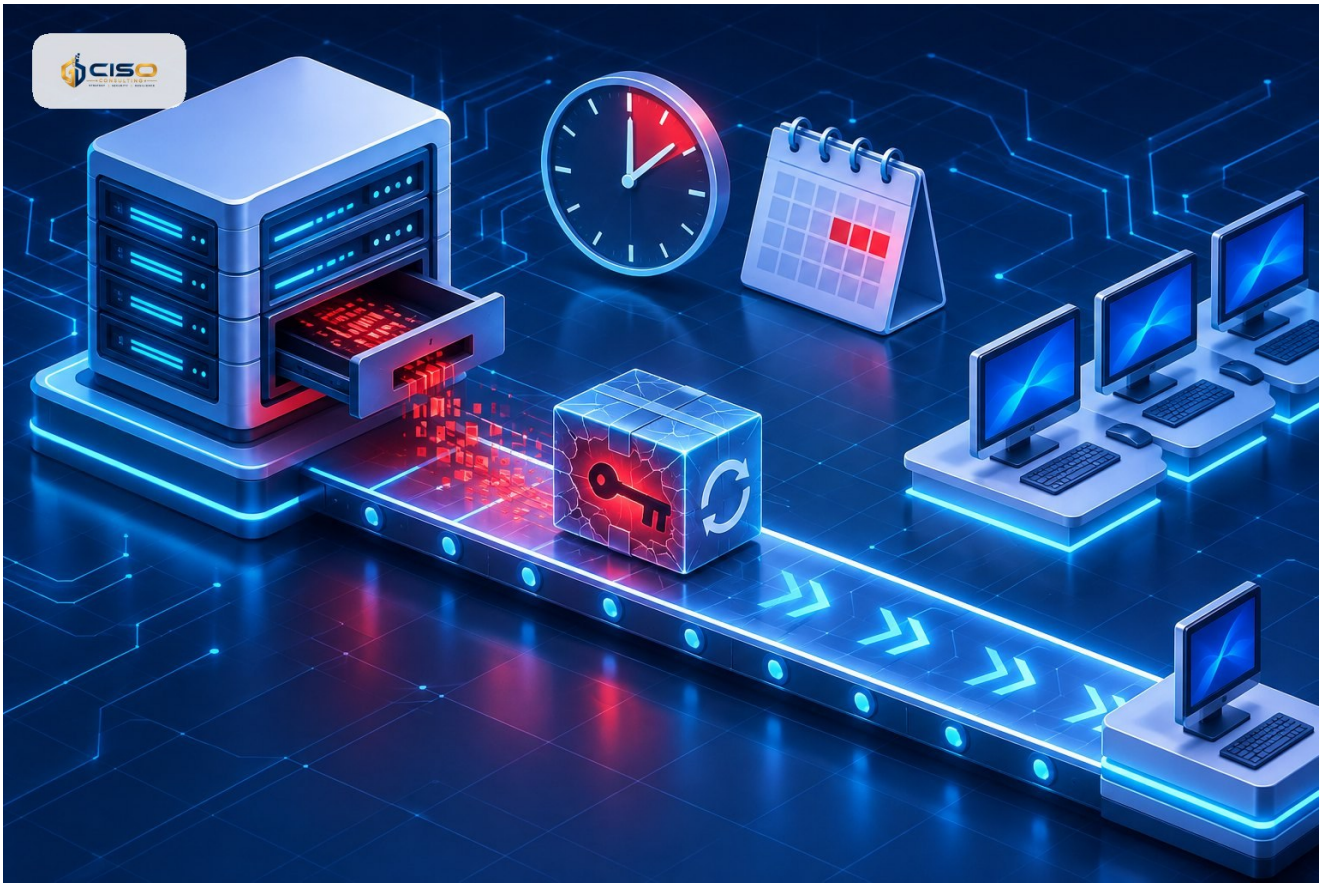
AOMEI Backupper update servers briefly tampered with to deliver a backdoor



Attackers altered files on AOMEI Backupper's vendor update servers in short windows between May and July 2026. Copies of the program that checked for updates in those windows could download and run a backdoor.

- Attackers changed files on the vendor's own update servers, not on a third-party site.
- Each tampering window lasted about five to ten minutes and recurred between May and July 2026.
- Any Windows installation that checked for an update during a window could fetch and run a backdoor.
- The source names Google Threat Intelligence Group, Mandiant and ManageEngine's Threat Analysis team among those involved in the reporting.

What was reported

According to The Hacker News, attackers repeatedly modified the files that AOMEI Backupper, a Windows backup program, retrieves from the vendor's own update servers. The changes were made in short windows of roughly five to ten minutes, repeated between May and July 2026.

Any installation that checked for an update during one of those windows would download and run a backdoor instead of a legitimate update. The report credits Google Threat Intelligence Group, Mandiant and ManageEngine's Threat Analysis team in connection with the findings.

Why it matters

Backup software typically runs with high privileges and has broad access to data, so a compromised update channel is a serious route into an environment. Because the windows were brief, an organisation could have been exposed without any obvious sign, and absence of alerts does not confirm safety.

The source excerpt does not give technical indicators, the backdoor's name, or the affected version numbers, so those details should be sought from the vendor and the original researchers.

Recommended approach

Institutions should first establish whether AOMEI Backupper is present anywhere in their estate, including on administrator workstations and servers that are not centrally inventoried. Where it is present, review whether automatic update checks occurred between May and July 2026 and treat those hosts as potentially affected until verified.

What to do now

1. Inventory every host running AOMEI Backupper, including unmanaged workstations and servers.
2. Identify hosts where update checks may have run between May and July 2026 and treat them as potentially compromised until verified.
3. Contact the vendor and review the original researchers' reporting for indicators of compromise, then hunt for them in endpoint and network logs.
4. Pause automatic updates for the product until the vendor confirms the update channel is clean.
5. Verify that backups taken from potentially affected hosts are intact and stored separately from production credentials.