# AOMEI Backupper update servers tampered with to deliver a backdoor



Attackers briefly altered files on AOMEI's update servers between May and July 2026, so copies of AOMEI Backupper that checked for updates in those windows received a backdoor.

- Attackers changed files on the vendor's own update servers.
- Each tampering window lasted roughly five to ten minutes and recurred between May and July 2026.
- Any Windows installation of AOMEI Backupper that checked for an update in a window would download and run a backdoor.
- The source names Google Threat Intelligence Group, Mandiant and ManageEngine's Threat Analysis team in connection with the findings.

## What was reported

According to The Hacker News, attackers repeatedly modified the files that AOMEI Backupper retrieves from the vendor's own update servers. The changes lasted only five to ten minutes at a time and occurred between May and July 2026.

The effect was that any copy of the Windows backup program that checked for an update during one of those short windows would download and run a backdoor. The source names Google Threat Intelligence Group, Mandiant and ManageEngine's Threat Analysis team in connection with the findings.

## Why it matters

The delivery route was the product's normal update mechanism, so the download came from a source the software already trusts. Backup tools typically run with high privileges and touch sensitive data, which makes a compromised installation a serious concern. The short windows also mean that exposure depends on when each machine happened to check for updates, so absence of obvious symptoms is not proof of safety.

The source excerpt does not provide indicators of compromise, affected version numbers or a vendor fix, so organisations should consult the full reporting and the vendor's own guidance.

## What to do next

Institutions should first establish whether AOMEI Backupper is installed anywhere in their estate, including on servers and on endpoints bought outside central procurement. Where it is present, review update activity for May to July 2026 and treat any host that checked for updates in that period as potentially affected until cleared.

## What to do now

1. Inventory all hosts running AOMEI Backupper, including servers and unmanaged endpoints.
2. Review update and network logs for May to July 2026 to find hosts that contacted the vendor's update servers.
3. Treat hosts that checked for updates in that period as potentially compromised and investigate them before trusting their backups.
4. Check the vendor's and researchers' published guidance for indicators of compromise and fixed versions.
5. Consider disabling automatic updates for backup tools until updates can be verified.