

AOMEI Backupper update servers abused to deliver malware in supply chain attacks



Attackers briefly altered configuration files on AOMEI's servers between April and July 2026, pushing the CROSSROAD downloader and SHINYROAD backdoor to AOMEI Backupper users. Organizations using the software should hunt for compromise.

- Attacks ran between April and July 2026 and abused the update and notification systems of AOMEI Backupper, a Windows backup and disk-cloning application.
- Two configuration files, `down_html.ini` and `Notifycfg.ini`, were briefly modified, and the expected checksum was changed so the malicious archive passed verification.
- Three exposure windows of 5 to 10 minutes were identified: May 28, July 16 and July 20.
- The malware included the CROSSROAD downloader and the SHINYROAD backdoor, which abuses Radmin components; the actor is tracked as UNC7017.

- A server-side fix does not remove malware already installed on endpoints, according to ManageEngine.

What happened

Researchers at ManageEngine's Threat Analysis Lab, working with Google's Threat Intelligence Group and Mandiant, reported that attackers compromised the servers AOMEI uses to feed its Backupper software. Rather than replacing files permanently, they briefly altered two configuration files and then restored them within minutes, which made detection difficult.

One file controls where update packages are downloaded from; the other governs notifications and can trigger content to run on the computer. The attackers redirected the software to a malicious ZIP archive, changed the expected checksum so it passed verification, and used the notification mechanism to run the payload without user interaction.

Impact

The malware delivered was the CROSSROAD downloader, which profiled the machine, fetched more components and persisted through a scheduled task, and the SHINYROAD backdoor, which used legitimate Radmin components to reach an attacker-controlled server. On July 20, Google also saw an attempt to capture Windows NTLM hashes through a WebDAV resource.

Affected organizations were found in several countries, including the United States, Australia, India, Singapore, Spain and Switzerland, across IT services, telecommunications and higher education. Google described the attacks as opportunistic, so other organizations that checked for updates during the short windows may also be affected.

Vendor status

AOMEI says it upgraded and verified its servers and that its CTO is leading an investigation. It has not confirmed how attackers gained access or whether the issue is fully resolved. ManageEngine stresses that securing the servers stops new infections but does not clean machines that already received the malware.

What to do now

1. Inventory all endpoints running AOMEI Backupper, including unmanaged or departmental installs.
2. Review the indicators published by Google and ManageEngine and hunt for suspicious scheduled tasks, unexpected executables in AOMEI directories, and Radmin installations not approved by IT.
3. Check proxy and DNS logs for connections to the reported IP address and hostnames since April 2026.
4. If compromise is found, isolate the host, preserve evidence, reset credentials exposed on it and treat NTLM hashes as potentially captured.

5. Consider suspending automatic updates and notifications for this product until the vendor publishes its findings, and add third-party update channels to supplier risk reviews.