Keenadu malware found preinstalled on more than 220,000 Android devices



Kaspersky reports Keenadu on over 220,000 Android devices in the first ten months of 2026, planted in firmware via the supply chain. Organisations buying devices in bulk should test samples and keep continuous protection.

- Keenadu was found on more than 220,000 Android devices in the first ten months of 2026.
- With Triada, it accounts for 88% of devices found with preinstalled malware this year; monthly detections have grown more than 2.5 times in a year.
- The malware sits in the system partition, so antivirus and the OS cannot remove it, and reflashing may not help.
- Tested Keenadu backdoors stayed dormant for about two and a half months before activation, likely to evade detection.

> - Most known attacks used it for ad fraud, but its modular design lets attackers push further modules.

Kaspersky reports that new Android devices can leave the factory with malware already in their firmware. According to the company, the number of such devices detected each month has grown more than 2.5 times over the past year.

What was found

Keenadu reached more than 220,000 devices in the first ten months of 2026. Together with the older Triada family, it was present on 88% of devices found with preinstalled malware this year. About twenty distinct Triada variants appeared in 2026.

Keenadu uses a modular design similar to Triada's, allowing attackers to deliver extra modules and inject them into target apps. The backdoor versions Kaspersky examined stayed silent for about two and a half months before the command-and-control servers ordered activation, a delay the researchers believe was meant to avoid detection. Most known attacks involved ad fraud, such as fake clicks.

Why it matters for organisations

These infections arrive through the supply chain: a manufacturer may install the malware deliberately, a contractor may supply malicious firmware to a legitimate brand, or a build component may be compromised. Once the malware is in the system partition, Kaspersky says antivirus tools and the OS cannot remove it, and some Trojans survive reflashing.

For companies issuing devices to staff, the risks include slower phones, hidden ads, hijacked accounts, stolen cryptocurrency and leaked corporate data. Devices can also be enlisted into proxy networks or DDoS botnets. Kaspersky advises inspecting and pilot-testing sample units before bulk orders, but notes this does not replace security software, since a supplier may send clean samples and update systems can themselves be attacked.

What to do now

1. Inspect and pilot-test sample units before any bulk purchase of phones, tablets or other connected devices.
2. Do not rely on sample testing alone; keep continuous security software and monitoring on every issued device.
3. Review device suppliers and their firmware supply chain as part of third-party risk assessment.
4. Monitor issued devices for unusual behaviour such as slowdowns, unexpected ads, account takeovers or odd network traffic.
5. Treat devices with suspected preinstalled malware as non-recoverable and plan replacement rather than relying on reflashing.