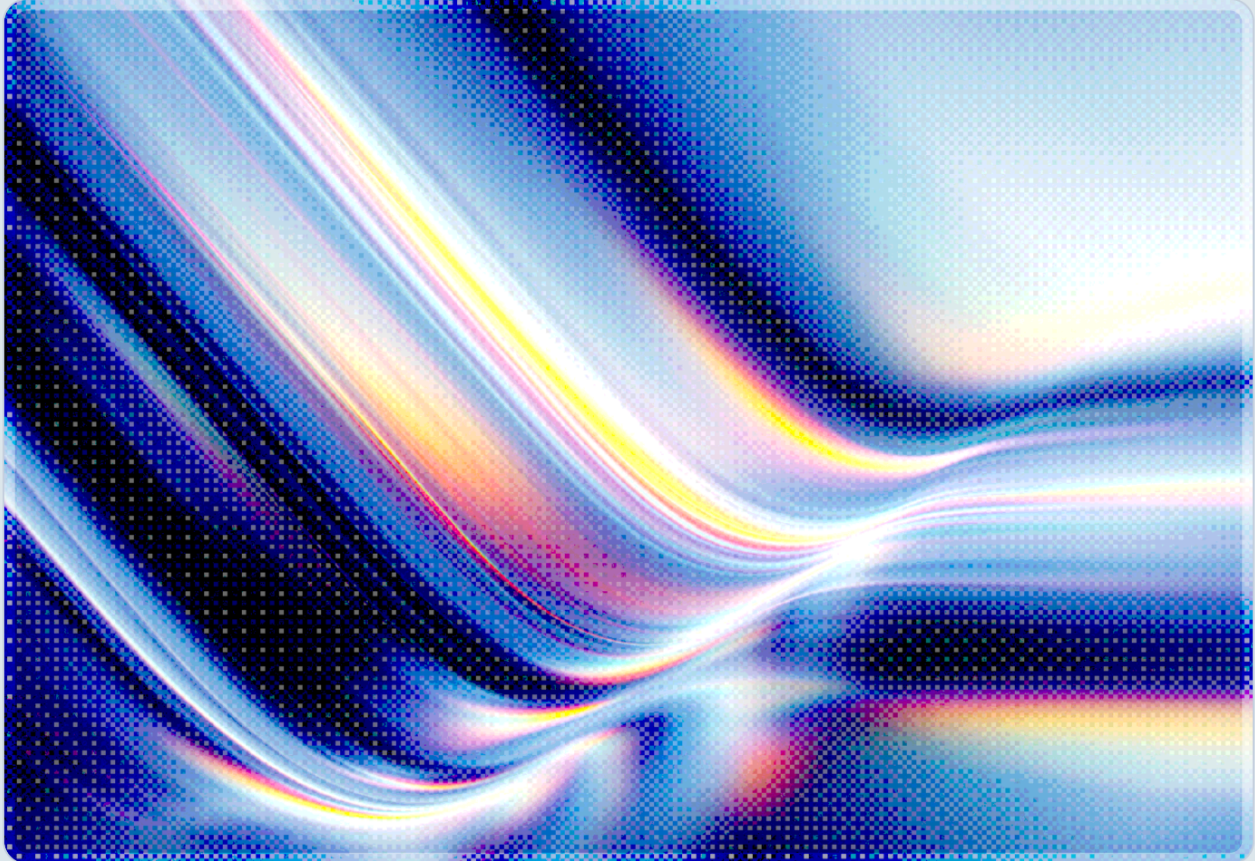


Pre-Compromised Hardware: Firmware Malware Shipped to Buyers

Security Implications and Guidance on Preinstalled Firmware
Implants and Reseller-Channel Risk

2026-10-13

 AI-assisted Rapid Research



CSAI

cloud
security
alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

Several independently documented Android malware families have been found in device firmware before the device reached its purchaser. Triada, Keenadu and, most recently, Midnight Mimosa were reported as embedded in the system image [1][3][5][7], while BADBOX 2.0 devices were either configured with malicious software before purchase or infected when they downloaded backdoored apps during setup [2]. Because the malicious code sits in the system image, standard remediation such as uninstalling an app, running an endpoint scanner or performing a factory reset generally does not remove it. Reflashing trusted firmware, or retiring the device, is the usual remedy [3][4].

Public reporting places the Keenadu implant at the firmware build or ROM-supply stage [3][4], and Kaspersky hypothesizes a pre-sale supply chain compromise for Triada, with the observation that stores may not know they are selling affected devices [1]. Reseller-level tampering cannot be ruled out in every case, and the sources do not establish how each affected device reached its buyer. For a buyer, the practical exposure is the same either way: the sales channel is where the risk is realized. Budget tablets, phones, TV boxes and similar devices bought online are commonly reported carriers, and Sophos notes that remote workers and small-business contractors buy the affected models [4]. The sources cited here do not include a published enterprise breach traced to a preinstalled implant, so enterprise relevance is an inference from where these devices are sold and used.

The controls that matter most are procurement-side: buy from authorized channels, require certified or attested firmware, and treat unmanaged consumer-grade devices as untrusted on enterprise networks. These controls are supported most directly by the Triada and BADBOX evidence and reduce risk without guaranteeing protection against build-stage implants.

Background

Hardware supply chain compromise is an old concern. CSA's work on firmware integrity in cloud data centers already identified supply chain compromise and unverified first-instruction integrity as risks to server platforms, and anchored its recommendations to the NIST platform firmware resiliency guidelines [9][10]. Reporting since 2025 suggests that the consumer-grade variant of the problem now operates at

considerable scale. Rather than targeted interdiction of a specific shipment, the reported cases involve a backdoor present in the firmware image that a low-cost manufacturer or ROM vendor ships, with the product then sold in volume through marketplaces and online stores.

Triada provided an early, well-documented example. In spring 2025, as reported by Bleeping Computer, Kaspersky described counterfeit smartphones imitating popular brands, sold at discount prices through online stores, that arrived with Triada embedded in the firmware. Kaspersky counted at least 2,600 infections, mainly among Russian users, and estimated that the trojan had stolen at least \$270,000 in cryptocurrency, though it cautioned that the true total is unknown because of the difficulty of tracing Monero transactions. Its working hypothesis was a compromised supply chain at some point before sale, so that "even the stores may not realize" what they are selling [1]. The malware operated inside Android's system framework, so the only reported fix was reflashing the ROM [1].

BADBOX and its successor BADBOX 2.0 extended the pattern to a wider range of product categories. The FBI's June 2025 public service announcement described compromised TV streaming devices, digital projectors, aftermarket vehicle infotainment systems and digital picture frames, mostly manufactured in China, which were either configured with malicious software before purchase or infected during setup when they downloaded backdoored apps [2]. The bureau described a botnet of "millions of infected devices" without giving a precise figure [2]. Google subsequently filed suit against 25 unidentified individuals alleged to operate the botnet, citing more than 10 million affected devices running Android Open Source Project builds that lacked Play Protect certification [6]. The operators allegedly sold access to compromised home networks as residential proxies and used the devices for ad fraud [2][6].

Security Analysis

Recent Campaigns: Keenadu and Midnight Mimosa

Kaspersky's February 2026 report on Keenadu is the most detailed public account of how a firmware implant can be introduced. According to the report, a malicious static library was linked into the build, ending up inside `libandroid_runtime.so`, a core Android runtime library. From there the code injects into the Zygote process, which is the parent of every Android application, much as Triada does, and so gains access to every app launched on the device [3]. Kaspersky found that the firmware images it examined, including those delivered by over-the-air updates, carried valid digital signatures. It reasoned that compromising an update server alone would not have been enough to inject the code, and concluded that the Trojan was most probably integrated during the firmware build phase [3]. As of its

report, Kaspersky counted 13,715 affected users, with the highest concentrations in Russia, Japan, Germany, Brazil and the Netherlands, and tied Keenadu to the same ecosystem as BADBOX, Triada and VoId through shared code and module downloads [3][7].

Sophos' independent telemetry gave a different cut of the same threat. Its analysts found Keenadu on more than 500 devices as of early March 2026, spanning roughly 50 models from budget brands across about 40 countries, and described the infection as occurring during manufacturing [4]. This is consistent with Kaspersky's build-phase conclusion. Sophos' principal enterprise concern was that remote workers and small-business contractors buy these inexpensive models, so that compromised devices can become entry points into business networks even when no corporate data resides on them directly [4].

Bitdefender's Midnight Mimosa research, reported by SecurityWeek on October 9, 2026, shows that the problem remains active. Bitdefender observed malware preinstalled in the firmware of budget Android devices built on MediaTek platforms, with compromised devices seen across more than 150 countries over roughly two years, led by Mexico and France [5]. The implant runs as a persistent system app that cannot be removed through normal uninstall, holds system-level privileges to install and remove apps, grant permissions and load remotely supplied code, and is used for ad fraud and for assembling botnets that can be rented to other actors [5]. It also disables Google Play Protect during malicious installations, and the reporting describes 13 Google Play apps with identical ad-fraud code under two developer accounts, suggesting a secondary distribution channel that overlaps with the preinstalled one [5]. Several of these details, including the duration and the Google Play apps, rest on a single secondary report, and the stage at which the implant entered the supply chain is not clearly established in public coverage.

Why the Reseller Channel Matters

The phrase "reseller implant" suggests a downstream actor tampering with goods. The evidence summarized here does not establish that mechanism. Keenadu and Sophos' findings point to the firmware build or ROM-supply stage [3][4], and Kaspersky's hypothesis for Triada is a supply chain compromise before sale, with retailers possibly unaware [1]. The Triada devices, however, were counterfeit units whose makers and sellers are not shown to be distinct, and some BADBOX devices were infected at first setup through downloaded apps rather than at build time [2]. Reseller-level tampering therefore cannot be ruled out in every case. The distinction affects remediation but not exposure. A buyer purchasing through an unauthorized marketplace seller cannot distinguish a clean device from an infected one at the point of sale, and the lowest-priced listings appear to be where affected products concentrate: the Triada devices were sold at discount through unofficial online channels rather than through authorized distributors [1], and the FBI lists unfamiliar brands, non-certified Android builds and disabled Play Protect among its indicators [2].

The channel also shapes who bears the cost. Consumers and small organizations are the usual purchasers, yet their devices may connect to the same networks, cloud accounts and identity providers as managed endpoints. BADBOX 2.0's proxy business model illustrates the consequence: the compromised device becomes an egress point for third-party traffic from inside the buyer's network and can obscure attacker activity behind residential addresses [2][6]. Because these devices are sold to consumers and small organizations, a plausible enterprise scenario is an unmanaged infected tablet in a conference room or a contractor's phone holding a session token for a SaaS tenant. This is an inference; no published enterprise breach case is cited here.

Why Detection Is Difficult

Firmware-level implants defeat the controls most organizations rely on. Because the code is part of the trusted system image, endpoint tools running above the operating system have limited ability to inspect or remove it, and an implant inside the Zygote process can observe or alter any application [3]. A factory reset is unlikely to help because the system partition is restored from the same image. Kaspersky's own mitigation options for Keenadu were to check for a clean manufacturer update, attempt a clean firmware installation at the risk of bricking the device, or stop using the device until the firmware is replaced [3]. Indicators that remain observable are largely behavioral and network-side, such as unexplained outbound traffic, which the FBI lists among its indicators [2].

It is worth stating the limits of current evidence. Public counts are telemetry from specific vendors' customer bases and so likely understate the true population; the figures above should not be summed or compared directly. Attribution of the botnet families to a single operator is also contested in the sources, which describe shared code and infrastructure rather than a confirmed single group [3]. The enterprise relevance of consumer-grade Android devices is inferred from where they are sold and used, not from published case studies of corporate breaches via preinstalled implants.

Summary of Documented Cases

The table below summarizes the four campaigns discussed above. Counts come from different vendors' telemetry and from different time periods, so they should not be summed.

Campaign	Reported by	Device types	Notable details
Triada (counterfeit phones)	Kaspersky, as reported by Bleeping	Counterfeit smartphones sold online	At least 2,600 infections; at least \$270,000 stolen; suspected supply chain compromise

Campaign	Reported by	Device types	Notable details
	Computer, 2025 [1]		
BADBOX 2.0	FBI, Google, 2025 [2][6]	TV boxes, projectors, car infotainment, picture frames	Millions of devices; 10+ million per Google's complaint; residential proxy and ad fraud
Keenadu	Kaspersky, Sophos, 2026 [3] [4]	Budget tablets and phones	Build-stage implant in <code>libandroid_runtime.so</code> ; 13,715 users (Kaspersky)
Midnight Mimosa	Bitdefender, as reported by SecurityWeek, October 2026 [5]	Budget MediaTek Android devices	150+ countries; system app disables Play Protect; botnet rental

Recommendations

Immediate Actions

Organizations should begin by inventorying the consumer-grade Android devices, such as tablets, TV boxes, projectors, digital signage and aftermarket infotainment units, that connect to corporate or remote-worker networks, starting with the models and brands named in the vendor reports above [3][4] [5]. Devices from affected brands or with non-certified Android builds should be blocked from corporate resources until their firmware provenance is verified, a cautious step consistent with Sophos' concern about affected Keenadu models [4]. Security teams should also review egress logs for unexplained outbound traffic from such devices, the behavioral indicator the FBI highlights [2]. Where an infection is confirmed, Kaspersky's options apply in order: check for a clean vendor update, attempt a clean reflash while accepting the risk of bricking, and otherwise stop using the device [3]. Retiring the device is the fallback when no clean firmware exists.

Short-Term Mitigations

Procurement policy should limit purchases of endpoint, IoT and network hardware to authorized distributors and resellers, and should reject marketplace listings from third-party sellers for anything that will touch a business network. Buyers can also require that Android devices be certified by Google, since the BADBOX 2.0 devices described in Google's complaint were AOSP builds without Play Protect certification [6], and the FBI cites non-certified builds as an indicator [2]. These controls are supported by the Triada and BADBOX evidence. The sources do not establish whether Keenadu and Midnight Mimosa devices reached buyers through authorized channels or lacked certification, and Midnight Mimosa disables Play Protect after installation, so the controls reduce risk but are not proof against build-stage implants.

Network segmentation helps contain what cannot be prevented: unmanaged IoT and BYOD devices belong on isolated VLANs with default-deny egress, and device posture checks in conditional access can refuse tokens to devices that cannot attest to a known-good OS build. Where mobile device management is feasible, enrollment should require hardware-backed attestation, not only an agent that runs inside the possibly compromised operating system. Attestation has limits, however: if a manufacturer's build pipeline is compromised, as Kaspersky's finding of validly signed infected images indicates for Keenadu [3], attestation may certify a malicious build, so it should be paired with behavioral monitoring.

Strategic Considerations

The structural issue is that firmware can be signed and shipped by low-cost manufacturers with little visibility into build provenance, as the validly signed Keenadu images show [3]. Enterprises can address this contractually by requiring suppliers to provide firmware software bills of materials, signed build attestations, and notification obligations when a compromise is discovered, consistent with NIST's guidance on cybersecurity supply chain risk management [8]. For server and network equipment, the protection, detection and recovery model in NIST SP 800-193 provides a basis for acceptance testing, including verification of firmware measurements against vendor-published values at receipt [9][10]. Because valid signatures did not indicate a clean image in the Keenadu case, organizations should monitor device behavior after update and not rely on signature verification alone [3]. As a forward-looking consideration, and not a finding of the cited sources, AI-enabled agents and local inference devices may increasingly run on commodity hardware, in which case the same provenance requirements would apply to edge AI deployments.

CSA Resource Alignment

CSA's position paper, [Firmware Integrity in the Cloud Data Center](#), is the most directly relevant prior work. It frames firmware integrity around protection, detection and recovery and discusses supply chain compromise, unsigned option ROMs and first-instruction integrity as risks to server platforms [10]. The cases in this note apply the same concerns to consumer-grade endpoints, where none of those assurances are present, and the paper's procurement-oriented approach (requiring verifiable firmware integrity of vendors) transfers to the acceptance-testing steps above.

CSA's [AI Controls Matrix \(AICM\) v1.1](#) provides the control structure for the supplier-side recommendations, particularly its supply chain and third-party risk domains, and CSA's STAR program offers a model for requiring documented, assessed assurance from suppliers [11]. CSA's recent threat notes on software supply chain compromise, such as [Sapphire Sleet Poisons Mastra AI npm Supply Chain](#) [12], illustrate the same trust-in-upstream failure at the package level, and read alongside this note they make the case for provenance verification across software and hardware alike.

References

- [1] Bleeping Computer. "[Counterfeit Android devices found preloaded with Triada malware.](#)" BleepingComputer, April 2025 (reporting Kaspersky research).
- [2] FBI Internet Crime Complaint Center. "[Alert I-060525-PSA: BADBOX 2.0 Targets Home Networks.](#)" IC3, June 5, 2025.
- [3] Kaspersky GReAT. "[Keenadu the tablet conqueror and the links between major Android botnets.](#)" Securelist, February 17, 2026.
- [4] Sophos. "[Android devices ship with firmware-level malware.](#)" Sophos, March 2026.
- [5] SecurityWeek. "[Pre-Baked Firmware Malware Hits Budget Android Devices in 150+ Countries.](#)" SecurityWeek, October 9, 2026 (reporting Bitdefender research).
- [6] SecurityWeek. "[Google Sues Operators of 10 Million Device BadBox 2.0 Botnet.](#)" SecurityWeek, July 2025.
- [7] Security Affairs. "[Keenadu backdoor found preinstalled on Android devices, powers ad fraud campaign.](#)" Security Affairs, February 2026.
- [8] NIST. "[SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.](#)" NIST, May 2022.
- [9] NIST. "[SP 800-193: Platform Firmware Resiliency Guidelines.](#)" NIST, May 2018.
- [10] Cloud Security Alliance. "[Firmware Integrity in the Cloud Data Center.](#)" CSA.
- [11] Cloud Security Alliance. "[AI Controls Matrix v1.1.](#)" CSA.
- [12] Cloud Security Alliance. "[Sapphire Sleet Poisons Mastra AI npm Supply Chain.](#)" CSA, 2026.