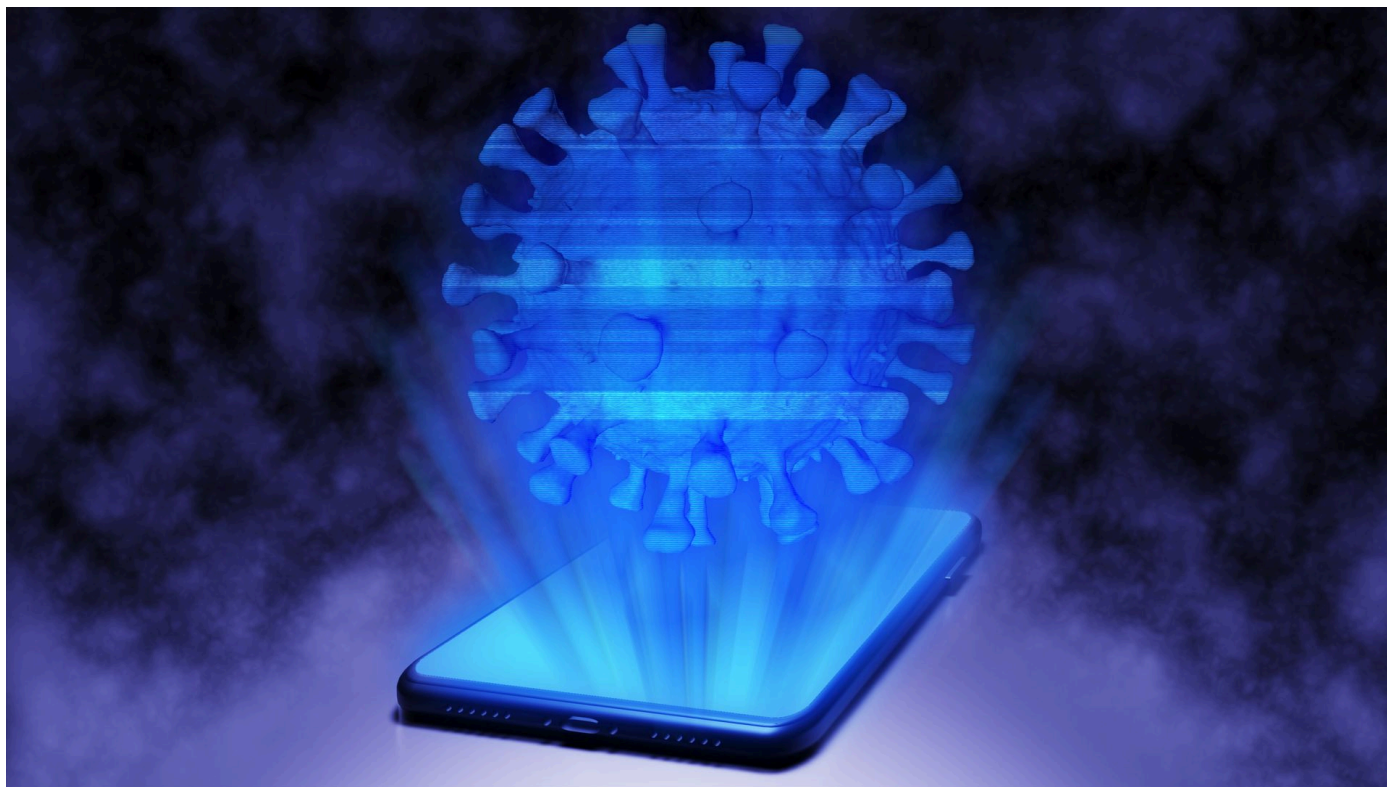


Android devices ship with firmware-level malware

 sophos.com/en-us/blog/android-devices-ship-with-firmware-level-malware

March 19, 2026



In late February 2026, SophosLabs analysts identified multiple detections on Android devices for malicious activity associated with the Keenadu backdoor. According to [Kaspersky](#), Keenadu is a firmware infection embedded in the `libandroid_runtime.so` (shared object library) that injects itself into the Zygote process. As Zygote is the parent process for all Android apps, an attacker effectively gains total control over an infected device. Keenadu acts as a downloader for second-stage malware modules that can be used to target the data in multiple applications. All Android apps rely on `libandroid_runtime.so` to run, so a copy of Keenadu is copied into the address space of every app installed on an infected device.

The code for Keenadu is located in a static library (`libVndxUtils.a`) on an infected device and relies on a malicious dependency that masquerades as legitimate MediaTek code. Based on artifacts associated with Keenadu's deployment, Kaspersky concluded that it was "integrated into the firmware during the build phase" in a supply chain compromise rather than subsequently installed through a compromised OTA (over-the-air) server.

The apps the malware targets depends on the modules the attacker chooses to download. Examples include storefronts like Shein, Temu, and Amazon. YouTube, Facebook, and the Digital Wellbeing app are all targeted with "clicker" modules, which perform ad fraud by silently

connecting to websites in the background to generate pay-per-click revenue. Another clicker module is embedded in the system launcher (com.android.launcher3) and appears designed to monetize each installation. One module targets the Google Chrome browser.

The infected devices detected by Sophos consistently involved two system-level APK files: PriLauncher.apk and PriLauncher3QuickStep.apk. These files were in system-level directories (e.g., /system/system_ext/priv-app/PriLauncher3QuickStep/PriLauncher3QuickStep.apk). [QuickStep](#) is the default Android system launcher and a core component of the [Android Open Source Project \(AOSP\)](#). The detections of these APK files as malicious suggest that these components were trojanized to run Keenadu on certain devices. The Sophos Intercept-X endpoint agent for Android does not block legitimate QuickStep versions.

As of March 4, Sophos X-Intercept telemetry listed over 500 unique compromised Android devices across nearly 50 models. The devices were mostly low-cost models produced by the following manufacturers: Allview, BLU, Dcode, DOOGEE, Gigaset, Gionee, Lava, and Ulefone. The list did not include Alldocube devices, despite Kaspersky reportedly observing Keenadu affect that manufacturer as well. The identified infections were spread globally, with devices located in 40 countries.

Organizations that allow users to access corporate resources from personal devices are at elevated risk. Although data exfiltration is from the device itself, threat actors could access a corporate network via exposed credentials stored in apps on the infected device.

SophosLabs analysts recommend following the steps outlined in knowledgeable article [KBA-000047016](#). Android users should install updated firmware if released by the vendor. Until the firmware has been updated, organizations should consider restricting affected models from accessing the corporate network.

The following Sophos protection relates to this threat:

Andr/Bckdr-SBS

The threat indicators in Table 1 can be used to detect activity related to this threat. Note that IP addresses can be reallocated. The domains and IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Cont
11eaf02f41b9c93e9b3189aa39059419	MD5 hash	Keer K50 (PriL

Indicator	Type	Conf
7db58b72a3493a86e847c3685eca74c690d50b55	SHA1 hash	Keer K50 (PriL
52db1f284a0dccbb750314cf765131a17a8284a2aeea04701a2b71f35fb9d9ee	SHA256 hash	Keer K50 (PriL
3c03168c98ad6111c3aa0a960f8b7eea	MD5 hash	Keer firmv (PriL
dcf2b51bfc43494bb27f5da26f3f706ca878d17e	SHA1 hash	Keer firmv (PriL
cdf1d41d732ba882184060933bec2c1f4b8eefc081c06471132a690f2205da31	SHA256 hash	Keer firmv (PriL
cb0d514d86ddf4f4345d25cef064863b	MD5 hash	Keer Armo (PriL
b73c94e56932f607108ec1efb74004c763a9e42b	SHA1 hash	Keer Armo (PriL
ab6d744dccf4c6266474df4b8aa3be6ae5663dbee39c579a552a4cfa1c1d12fd	SHA256 hash	Keer Armo (PriL
cd619b4e1e793f96eca877616a741bc1	MD5 hash	Keer Armo (PriL
c33b025bac789d3742278f784377fc36f83fd1ff	SHA1 hash	Keer Armo (PriL
da1c7f53add0abaa8a49b773e5cea9c9171799f644ec24e366aaf7ce29962a11	SHA256 hash	Keer Armo (PriL
b80b39ed95d54c8c1bf12e35f92e23cc	MD5 hash	Keer Armo (PriL

Indicator	Type	Cont
7eb32a90d556bb9954707014843a67f7039ea7f1	SHA1 hash	Keer Arm (PriL
34a0236b5c7b47577be4501e2c18908916ef9ec22032a6ea41b0ecceaf4e8d8a	SHA256 hash	Keer Arm (PriL
playstations[.]click	Domain name	C2 s back
uscellular[.]com	Domain name	C2 s back
gstatic2[.]com	Domain name	C2 s back
glogstatic[.]com	Domain name	C2 s back
yting2[.]com	Domain name	C2 s back
gmsstatic[.]com	Domain name	C2 s back
gsonx[.]com	Domain name	C2 s back
keepgo123[.]com	Domain name	C2 s back
sliidee[.]com	Domain name	C2 s back
newsroomlabss[.]com	Domain name	C2 s back
fbgraph[.]com	Domain name	C2 s back
dllpgd[.]click	Domain name	C2 s back
gvvt1[.]com	Domain name	C2 s back
proczone[.]com	Domain name	C2 s back

Indicator	Type	Conf
goaimb[.]com	Domain name	C2 s back
aifacecloud[.]com	Domain name	C2 s back
gbugreport[.]com	Domain name	C2 s back
tmgstatic [.]com	Domain name	C2 s back
fbsimg[.]com	Domain name	C2 s back
launcher[.]szprize[.]cn	Domain name	C2 s back
iboot[.]site	Domain name	C2 s back
67[.]198[.]232[.]187	IP address	C2 s back
67[.]198[.]232[.]4	IP address	C2 s back
110[.]34[.]191[.]82	IP address	C2 s back
110[.]34[.]191[.]81	IP address	C2 s back

Table 1: Indicators for this threat

About the author



[Sophos Counter Threat Unit Research Team](#)

[Sophos Counter Threat Unit™ \(CTU\)](#) researchers are recognized authorities in the cybersecurity field, regularly contributing expert analysis to global media, publishing technical analyses for the security community, and presenting about emerging threats at leading security conferences.

Backed by Sophos' advanced security technologies and a broad network of intelligence contacts and partners, the CTU™ plays a critical role in identifying and tracking threat actors and analyzing anomalous activity, uncovering new attack techniques, threats, and major shifts in the threat landscape.