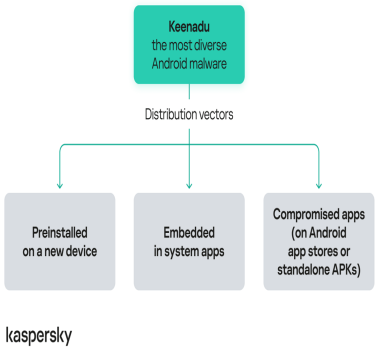

Kaspersky scopre Keenadu: un malware Android multifunzionale che puÃ² essere giÃ installato sui nuovi dispositivi

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky ha rilevato un nuovo malware per dispositivi Android, denominato Keenadu. Questo malware viene distribuito in diverse modalitÃ : puÃ² essere preinstallato direttamente nel firmware dei dispositivi, incorporato nelle app di sistema o persino scaricato da app store ufficiali come Google Play. Attualmente, Keenadu viene utilizzato per frodi pubblicitarie: gli aggressori sfruttano i dispositivi infetti come bot per generare clic sui link degli annunci. Tuttavia, puÃ² essere impiegato anche per scopi piÃ¹ dannosi, poichÃ© alcune varianti consentono il controllo completo del dispositivo della vittima.

A febbraio 2026, le soluzioni di mobile security di Kaspersky hanno rilevato oltre 13.000 dispositivi infettati da Keenadu. Il maggior numero di utenti colpiti Ã¨ stato osservato in Russia, Giappone, Germania, Brasile e Paesi Bassi, ma anche altri Paesi risultano coinvolti, tra cui lâ??Italia.

Integrato nel firmware del dispositivo

Analogamente alla backdoor Triada, rilevata da Kaspersky nel 2025, alcune versioni di Keenadu sono integrate nel firmware di diversi modelli di tablet Android durante una delle fasi della supply chain. In questa variante, Keenadu si presenta come una backdoor completamente funzionante, in grado di fornire agli aggressori il controllo illimitato sul dispositivo della vittima. PuÃ² infettare tutte le app presenti sul dispositivo, installare qualsiasi app tramite file APK e concedere loro tutte le autorizzazioni disponibili. Di conseguenza, tutte le informazioni presenti sul dispositivo, inclusi file multimediali, messaggi, credenziali bancarie, posizione e altri dati sensibili, possono essere compromesse. Il malware Ã¨ inoltre in grado di monitorare le query di ricerca inserite dallâ??utente nel browser Chrome in modalitÃ di navigazione in incognito.

Una volta integrato nel firmware, il malware si comporta in modo differente in base a diversi fattori. Non si attiva se la lingua impostata sul dispositivo Ã¨ uno dei dialetti cinesi e lâ??orario Ã¨ configurato su uno dei fusi orari della Cina. Inoltre, non si avvia se sul dispositivo non sono installati Google Play Store e Google Play Services.

Integrato nelle app di sistema

In questa variante, le funzionalitÃ di Keenadu risultano piÃ¹ limitate: non puÃ² infettare tutte le app presenti sul dispositivo ma, poichÃ© risiede allâ??interno di unâ??app di sistema, che gode di privilegi elevati rispetto alle normali applicazioni, puÃ² comunque installare app secondarie scelte dagli aggressori senza che lâ??utente ne sia a conoscenza.

Kaspersky ha inoltre individuato Keenadu incorporato in unâ??applicazione di sistema responsabile dello sblocco del dispositivo tramite riconoscimento facciale, consentendo potenzialmente agli aggressori di acquisire i dati facciali della vittima. In alcuni casi, Keenadu risultava integrato anche nellâ??app della schermata iniziale, responsabile dellâ??interfaccia della home.

Integrato nelle app distribuite tramite gli store Android

Gli esperti di Kaspersky hanno inoltre scoperto che diverse applicazioni distribuite su Google Play erano infettate da Keenadu. Si trattava di app dedicate alle telecamere domestiche intelligenti, scaricate oltre 300.000 volte. Al momento della pubblicazione, tali applicazioni sono state rimosse da Google Play.

Quando queste app vengono avviate, gli aggressori possono aprire schede invisibili del browser web al loro interno, utilizzate per navigare su diversi siti web senza che lâ??utente ne sia consapevole. Ricerche precedenti condotte da altri esperti di sicurezza informatica hanno dimostrato che applicazioni infette simili vengono distribuite anche tramite file APK autonomi o attraverso altri app store.

â??Come dimostrato dalla nostra recente ricerca, il malware preinstallato rappresenta un problema urgente su diversi dispositivi Android. Senza alcuna azione da parte dellâ??utente, un device puÃ² risultare infetto fin dal momento dellâ??acquisto. Ã? fondamentale che gli utenti comprendano questo rischio e utilizzino soluzioni di sicurezza in grado di rilevare questo tipo di malware. Probabilmente i fornitori non erano a conoscenza della compromissione della catena di approvvigionamento che ha consentito a Keenadu di infiltrarsi nei dispositivi, poichÃ© il malware imitava componenti di sistema legittimi. Ã? quindi essenziale controllare ogni fase del processo produttivo per garantire che il firmware del dispositivo non sia infettoâ?•, ha commentato Dmitry Kalinin, Security Researcher di Kaspersky.

Per proteggersi da queste minacce, Kaspersky consiglia di:

Per ulteriori informazioni Ã¨ possibile consultare il report completo su Securelist.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Febbraio 17, 2026
Autore
redazione