Trending

Seqrite Warns of New Android Threat Exploiting Trust in mParivahan App

Seqrite has uncovered a dangerous new variant of malware masquerading as the Indian government's official 'NextGen mParivahan' application.

Seqrite has uncovered a dangerous new variant of malware masquerading as the Indian government's official 'NextGen mParivahan' application. Researchers at Seqrite Labs, India's largest malware analysis facility, identified the threat during routine threat-hunting operations, revealing its use of advanced technical evasion methods to steal sensitive user data, including SMS messages, UPI PINs, and notifications from popular apps like WhatsApp, Amazon, and Gmail. The malware's operators exploit public trust in digital governance initiatives, distributing fake traffic violation alerts via SMS to trick users into installing malicious apps.

The malware employs a multi-layered approach to avoid detection. By creating malformed APK files with invalid compression methods, it bypasses standard analysis tools used by cybersecurity researchers while remaining fully functional on Android devices running version 9 or later.

One variant dynamically generates its command-and-control server URLs through native code stored in a library file, making it nearly impossible to trace communications using static analysis. Another variant uses a two-stage deployment process, where an initial dropper app disguised as a routine update installs a hidden payload that exfiltrates data to a Firebase database controlled by attackers.

This malware represents a significant leap in technical sophistication. Attackers are not just relying on social engineering but are actively exploiting subtleties in how Android processes files. Their ability to hide critical infrastructure within native code and abuse compression standards shows a deep understanding of system vulnerabilities.

The malware's operators further ensure persistence by configuring it to automatically restart after device reboots, maintaining long-term access to stolen data. Researchers at Seqrite Labs also revealed its focus on notifications from over 15 applications. Users may

unknowingly grant access to their messages, payment alerts, and social media activity, thinking they are complying with a legitimate government service.

The emergence of this fake **'NextGen mParivahan'** application highlights the need for continuous education and advanced mobile security solutions. Seqrite recommends that Android users exercise extreme caution when downloading apps outside official stores and verify unexpected traffic violation notices directly through the Ministry of Road Transport & Highways' website. Using robust security solutions such as Quick Heal Mobile Security for Android, can help detect this threat early on, providing real-time protection against such attacks. Enterprises are recommended using Seqrite's comprehensive endpoint security solutions which are capable of preemptively blocking malicious APKs and associated servers.