Quick Heal Warns of Android Cryptojacker Masquerading as Axis Bank App

This sophisticated miner takes into consideration the fact that users may suspect unusual activity once they pick up the phone; hence, the mining is designed to stop the mining as soon as the device is unlocked.

Quick Heal Technologies Limited has uncovered a highly evasive Android cryptojacking campaign hiding behind a fake banking application. The malware, distributed via a phishing site impersonating Axis Bank, leverages device-lock events to launch sustained cryptocurrency mining operations that silently drain resources and risk permanent hardware damage.

During routine threat intelligence monitoring, researchers at Seqrite Labs, India's largest malware analysis facility, encountered a phishing domain, getxapp[.]in, hosting an app labeled "Axis Card." Upon installation outside official app stores, the application presented a counterfeit update screen but delivered no banking functionality. Instead, it embedded the open-source XMRig miner to initiate Monero mining as soon as the user locked their device.

By continuously monitoring battery level and screen-lock status, the malware allocates over 2.3 GB of RAM and eight CPU threads after each lock event, rapidly increasing device temperature from 32 °C to 45 °C within 30 minutes. This sophisticated miner takes into consideration the fact that users may suspect unusual activity once they pick up the phone; hence, the mining is designed to stop the mining as soon as the device is unlocked. This is done to avoid identification and detection of the mining on the device.

The intelligent measures incorporated in Quick Heal Mobile Security identify and flag this threat as Android.Dminer. A, blocking both installation and execution of the malicious payload. It also prevents the download of encrypted native libraries from hosting sites on GitHub, Cloudflare Pages, and the attacker's own uasecurity[.]org domain.

Quick Heal Mobile Security's real-time behavioral analysis detects unauthorized background processes, suspicious permissions such as REQUEST_INSTALL_PACKAGES, and abnormal network connections to Monero pool endpoints at pool.uasecurity.org:9000.

Quick Heal Technologies Limited urges Android users to install applications only from trusted Google Play and Apple App stores, scrutinize any unexpected update prompts, and maintain up-to-date mobile security software.

Users experiencing rapid battery depletion, device overheating, or performance lag should run a full malware scan immediately and consider a factory reset after backing up critical data. Victims of this or similar malware campaigns are encouraged to report incidents to cybercrime.gov.in or the national helpline at 1930