Snowblind malware

October 27, 2025 • vajiramandravi.com

About Snowblind malware:

- It is a new **Android malware** that uses a built-in Android security feature to bypass anti-tamper mechanisms and steal banking credentials.
- This malware **exploits a built-in security feature** to bypass anti-tamper protection in apps handling sensitive information.
- It works by **repacking an app** so it is unable to detect the use of accessibility features that can be used to extract sensitive information like login credentials and get remote access to the app.
- It exploits a **feature called 'seccomp'**, which stands for '**secure computing'**.
    - It is part of the underlying Linux kernel and the Android operating system and is used to check applications for signs of tampering.
- The security firm discovered that **Snowblind injects a piece of code** that loads before seccomp initialises the anti-tampering measures. This enables the malware to bypass security mechanisms and utilize accessibility services to remotely view the victim's screen.
- Snowblind can also **disable biometric and two-factor authentication**, two security features commonly used by banking apps to thwart unauthorised access. Like typical Android malware, Snowblind infects users who install apps from untrusted sources.

While the security firm was unable to identify how many devices are affected by the new malware, it says that Snowblind is mostly **active in Southeast Asia.**

Q1: What is the Raccoon Stealer?

Raccoon Stealer is a kind of malware that steals various data from an infected computer. It is a classic example of information-stealing malware, which cybercriminals typically use to gain possession of sensitive data saved in users' browsers and cryptocurrency wallets.

Source: Snowblind malware uses an Android security feature to bypass security

---