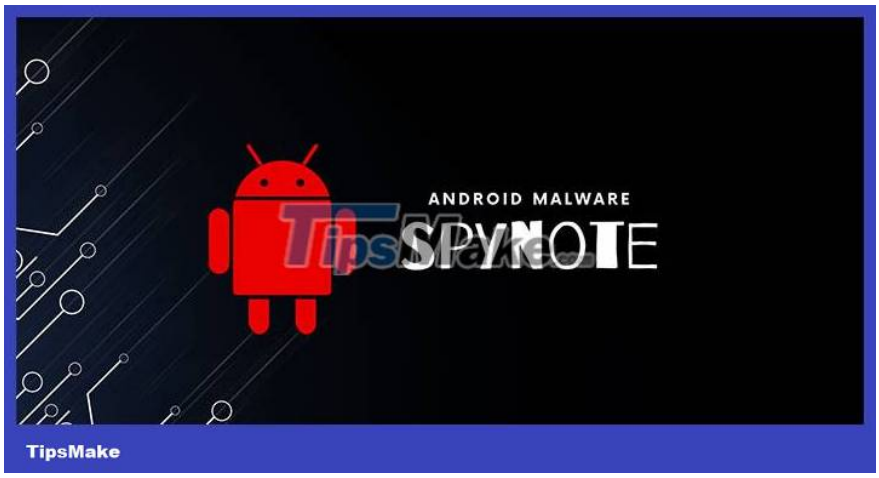
Warning: SpyNote phone eavesdropping software is extremely dangerous and difficult to remove

Security researchers at F-Secure have just issued a warning about a malware designed to eavesdrop on phones called SpyNote.

This malware is distributed through SMS messages and phishing campaigns that trick victims into clicking on attached links or installing malware.



During installation, SpyNote will ask users for permission to access call logs, cameras, SMS messages and external storage. SpyNote has the ability to 'hide' from the main interface of the phone, so it is very difficult to detect.

According to researcher Amit Tambe (F-Secure), SpyNote can be launched via an external trigger.

Removing SpyNote is relatively difficult because this malware works hidden in the background and prevents users when uninstalled. When users access Settings - Apps to uninstall applications, SpyNote abuses the BIND_ACCESSIBILITY_SERVICE permission to close the menu screen to prevent uninstallation.

In case this application is turned off, the Broadcast Receiver (an important component on the Android operating system, allowing the system or other applications to distribute events to the application) will automatically relaunch SpyNote.

SpyNote is especially dangerous because after being granted initial permissions, they will use these permissions to grant themselves additional powers such as eavesdropping on phone calls, taking screenshots, and recording keystrokes. via MediaProjection API.

To remove this malware, the victim's only option is to restore factory settings, which means losing all data.

You finished reading the article "**Warning: SpyNote phone eavesdropping software is extremely dangerous and difficult to remove**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
