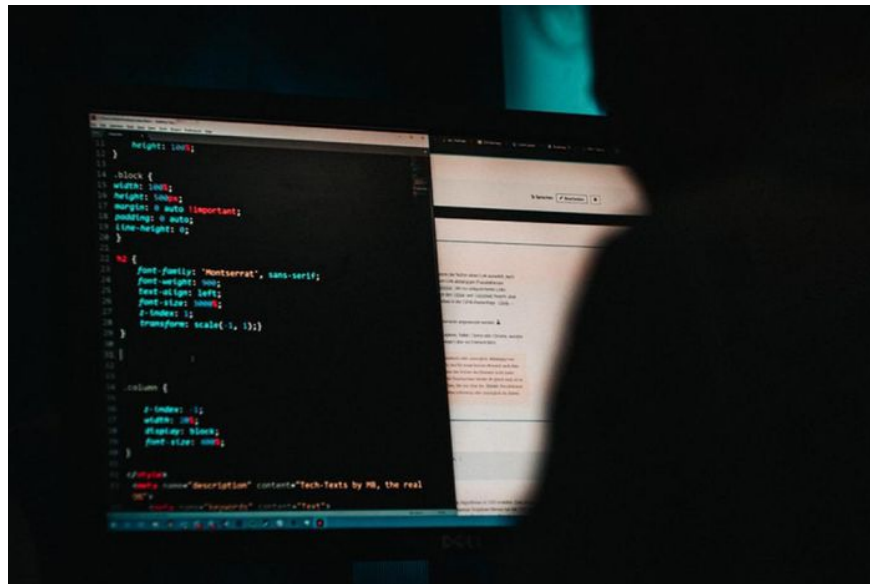


A malware warning can get rid of Android device data

A new malware has been discovered capable of disguising itself as Software Update for a user's Android device.

This extremely powerful malware is capable of stealing all the data stored on a user's device, including messages, photos, browser access history, **WhatsApp** messages, and more. It even has the ability to take complete control of an infected Android device.



Researchers at Zimperium's **zLabs** have discovered the Software Update malware can act as a remote access **Trojan** (RAT). This means that malware can receive and execute commands from a remote server and retrieve data stored on their device. It can also track device location and secretly record or phone calls.

Malware is complex and sophisticated. After hacking into Android device, it starts looking for any activity of interest, such as phone calls, it will automatically record and upload to server as encrypted ZIP file . The file is immediately deleted after the upload is completed so that no traces are left behind.

The fake Software Update uses social engineering to gain access to Accessibility Services permissions on the compromised Android device. This allows it to read and collect messages across multiple messaging apps like WhatsApp by scanning the screen. On rooted Android devices, malware can steal WhatsApp database files. It also actively steals clipboard data.

To deceive users, this malware disguised by displaying Software Update looks a lot like how update notifications from Google would show up on Android devices.



zLabs has confirmed to Google that the Software Update malware was never available as part of any app on the Google Play Store. It's mostly packed with apps outside of the Play Store, so unless a user regularly downloads apps from third parties and unknown sources, they don't need to be overly concerned. This malware appears to have been created with an intentional attack due to its complexity and sophistication.

The best way to keep a user's Android device safe from malicious apps and malware is to make sure you only install apps from the Google Play Store. Google periodically scans all the apps on the Play Store to make sure they're safe. Additionally, users should install the latest available security patch for their Android device to ensure all known security vulnerabilities are fixed.

You finished reading the article "**A malware warning can get rid of Android device data**" 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.