MALICIOUS WHATSAPP, TELEGRAM FOUND PREINSTALLED ON CHEAP ANDROID PHONES

Vairav Cyber Security News Report

Date: April 16, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A major supply chain security incident has been uncovered involving low-cost Android smartphones preloaded with trojanized versions of WhatsApp and Telegram. According to Doctor Web researchers, Chinese-manufactured phones have been shipping since June 2024 with malware-laced apps containing a cryptocurrency clipper dubbed **Shibai**. This malware silently replaces cryptocurrency wallet addresses in messages and harvests sensitive data, resulting in unauthorized asset transfers and major data exfiltration.

The compromised devices, often branded under **SHOWJI** and designed to mimic flagship models like Samsung's S23 Ultra or Huawei's Note 13 Pro, are manipulated at the firmware level before being sold. An estimated **$1.6 million in cryptocurrency** has been stolen by the attackers over the past two years, highlighting the effectiveness of the operation.

Figure 1: Product descriptions in bad Russian boasting "Fast Tastydragon CPU" [sic!] and "50 million cameras" [even sic'er!]

INCIDENT ANALYSIS

The attack campaign hinges on malware embedded directly into the firmware of low-end Android smartphones sold globally. The threat actors target the ROM-level software supply chain, ensuring that trojanized apps like WhatsApp are installed before the devices even reach consumers.

The malware is injected using LSPatch, an open-source project for modifying Android apps. The Shibai Trojan hijacks the update mechanism to silently download malicious payloads from attacker-controlled servers. It uses chat message interception to identify Ethereum and Tron wallet addresses and replaces them in transit to reroute funds to attacker wallets. The user sees their correct wallet address, while the recipient sees the substituted attacker address, making detection nearly impossible. In addition to wallet manipulation, the malware:

- Exfiltrates all WhatsApp messages
- Uploads .jpg, .png, and .jpeg files from common image directories
- Scans stole images for mnemonic recovery phrases
- Sends collected data to a wide network of 60+ C2 servers
- Uses over 30 domains for malware distribution

Affected apps include not only messaging services but also QR scanners and other utilities, about 40 modified APKs have been identified so far.

IMPACT AND EXPLOITATION

- **Financial Theft**: Over **$1.6 million** siphoned from users' cryptocurrency wallets.
- **Privacy Breach**: Exfiltration of sensitive user data, personal images, and messages.
- **Supply Chain Compromise**: Malware embedded during manufacturing, beyond the user's control.
- **Brand Abuse**: Victims believe they're using legitimate WhatsApp or Telegram apps on Android 14.
- **Widespread Scope**: Phones sold under multiple brand names, with spoofed system info to mimic high-end models.

RECOMMENDED ACTIONS

1. **Avoid untrusted devices:** Purchase smartphones only from reputable manufacturers and authorized sellers.
2. **Verify system specs:** Use verified apps and tools to confirm Android version and hardware details.
3. Install official apps: Only install messaging apps from the official Google Play Store or app developers' websites**.**
4. **Monitor transactions:** Always double-check wallet addresses before sending cryptocurrency.
5. **Update and reset:** If using a suspicious device, perform a factory reset and flash with verified firmware.
6. **Deploy endpoint protection:** Use mobile antivirus software capable of detecting clippers and spyware.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://thehackernews.com/2025/04/chinese-android-phones-shipped-with.html

https://news.drweb.com/show/?lng=en&i=15002&c=5

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com