

Forum: [Hack Forums](#)

Thread: [You're infected by malware you suspect nation state, what do you do?](#)

MadScientist - July 18, 2026, 10:24 pm

Scenario: You're a exec at a major company - you're roofied - you wake up confused and your phones funny.

What steps are you taking to monitor the device?

setting up intercept linux hotspot and copying all data for archiving;

What are you doing to copy the data to retain it(IE dd, tools, etc)?

What tools are you running to monitor network activity, catch get and posts, detect protocol calls and packet data?

On android see what services are calling what (non root), or rootkit analysis and detecting deep hands on or ABD installed backdoors?

Whats your go-to reverse engineering/malrev tools?

Guns3524 - July 21, 2026, 2:49 am

hi yeah im assuming the worst in this situation...

immediate steps:

- airplane mode right away
- copying data on linux using dd or dc3dd or tools like Magnet AXIOM
- on android: adb pull + dd on partitions if i can

network monitoring:

- linux hotspot + wireshark + tcpdump
- mitmproxy to catch protocols and requests

android device analysis:

- without root: adb shell dumpsys to see running services and apps
- with root: checking for rootkits and weird processes
- looking for adb backdoors magisk stuff and suspicious apks

malware analysis tools i usually go with:

ghidra jadx frida + objection and radare2

DamonLopez - July 26, 2026, 5:14 am

If I genuinely suspected a nation-state level compromise, my priority wouldn't be proving it myself. I'd isolate the device from every network, avoid interacting with it any further, and preserve its current state as much as possible. Every extra action risks overwriting evidence or triggering additional malware behavior. I'd also assume any credentials used on that device were exposed and change them from a separate trusted system. Unless you have a proper forensic lab, it's very easy to contaminate evidence while trying to investigate. At that level, involving an experienced incident response team is usually far more valuable than relying on a long list of tools. The process and chain of evidence matter just as much as the technical analysis.

