

Forum: [Hack Forums](#)

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

MadScientist - July 18, 2026, 10:28 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?

heatsuppressant - July 19, 2026, 9:03 am

If I was an exec at a major company I would most probably have everything on paper. So what i would do is in short break all of my devices and burn them.