Android Malware Stalkerware And Compromise

e-discovery.uk, Computer Forensics Lab. Published 2026-09-02.
https://e-discovery.uk/library/android-malware-stalkerware-and-compromise

ANDROIDMALWARE & STALKERWARE · A GUIDE FOR UK LAWYERSAndroid Malware, Stalkerware andCompromiseThe Open Platform's Larger Threat Surface, What Can Be Found, and the Dutyof Care That Comes FirstCOMPUTER FORENSICS LAB§ ABOUT THE AUTHORPREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAMESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURESANDROID STALKERWARE & MALWARE DETECTION SAFET Y-LED, VICTIM-CENTRED APPROACHCPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION§ CONTENTSIn this guide01 Executive summary02 The problem in plain English: openness cuts both ways03 How Android devices are compromised04 Detecting compromise: what Android lets you see05 Safety first: the duty of care06 Interpretation and honest limits07 Deployment: protecting the person, then the evidence08 Source architecture: where else the evidence lives09 Worked examples10 Common mistakes and technical limitations11 Questions to ask · Suggested wording12 Checklist and red flags · When to involve a digital forensic expert13 Frequently asked questions14 Glossary · References · Disclaimer · How a specialist laboratory can assist§ 01 · ORIENTATIONExecutive summaryThe headline point: Android's openness gives it a larger threat surface than iOS, sideloaded stalkerware andmalware are easier to install and sweeping permissions let them see a great deal, but the most commonsurveillance is still consumer stalkerware installed with physical access or the misuse of legitimate features,openness also lets an examiner inspect apps and permissions more fully, and, as on iOS, the person's safetycomes before the evidence.§ 02 · FIRST PRINCIPLESThe problem in plain English: openness cuts both ways§ 03 · HOWDEVICESARECOMPROMISEDHow Android devices are compromisedSTALKERWARE PERMISSIONS MISUSED FEATURES CONTROLLED MALWARE (RARE)ACCOUNT§ 04 · DETECTINGCOMPROMISEDetecting compromise: what Android lets you see§ 05 · SAFETYFIRSTSafety first: the duty of care§ 06 · INTERPRETATIONANDHONESTLIMITSInterpretation and honest limits§ 07 · DEPLOYMENTDeployment: protecting the person, then the evidence§ 08 · THEWIDERMAPSource architecture: where else the evidence livesEVIDENCE (APPS, FAMILY PROVIDER / OTHERTHE PHONE SHARING / STALKERWARE PHYSICAL /PERMISSIONS) SETUP DASHBOARD DEVICESGOOGLE SAFET YACCOUNT CONSIDERATION§ 09 · IN THE WILDWorked examplesEXAMPLE1 · THESTALKERWARETHEPERMISSIONSGAVEAWAYEXAMPLE2 · THE " SPYWARE " THATWASASHAREDGOOGLEACCOUNTEXAMPLE3 · THEBROADPERMISSIONSTHATWERELEGITIMATE§ 10 · WHEREITGOESWRONGCommon mistakes and technical limitationsCommon mistakesTechnical limitations§ 11 · INTERROGATORIES & DRAFTING AIDSQuestions to ask · Suggested wordingAsk your clientAsk the other side / in proceedingsAsk your e Discovery / forensic providerSUGGESTED WORDING · INSTRUCTIONFORANANDROIDSUSPECTED - COMPROMISEANA LY SIS§ 12 · QUICK CONTROLChecklist and red flags · When to involve a

digital forensicexpertThe Android suspected-compromise checklistRed flagsWhen to involve a digital forensic expert19. This guide continues the Android block. Through cflab.uk and e-discovery.uk, Android compromise work§ 13 · COMMON QUESTIONSFrequently asked questionsIs Android more vulnerable to stalkerware than iPhone?My client thinks their phone is being tracked. Where do we start?How can stalkerware be found on Android?Does an app with broad permissions prove it is spyware?What if the abuser controls the Google account?Should we just uninstall any stalkerware we find?§ 14 · REFERENCEGlossarySources and authoritative references35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guidesDISCLAIMER§ HOW A SPECIALIST LABORATORY CAN ASSISTWorking with Computer Forensics LabSpeak to a forensic examiner, not a salesperson.INSTRUCTTHELABNEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

Is Android more vulnerable to stalkerware than iPhone?

Its threat surface is larger, and its visibility is greater (

My client thinks their phone is being tracked. Where do we start?

With their safety, before any exam in at i on (

Does an app with broad permissions prove it is spyware?

No, permissions are necessary but not sufficient (

Should we just uninstall any stalkerware we find?

Not reflexively, because removal can escalate risk (