Gatekeeper XProtect And MacOS Malware Artefacts

e-discovery.uk, Computer Forensics Lab. Published 2026-09-02.
https://e-discovery.uk/library/gatekeeper-xprotect-and-macos-malware-artefacts

GATEKEEPER, XPROTECT & MACMALWARE · A GUIDE FOR UK LAWYERSGatekeeper, XProtect and macOS MalwareArtefactsWhat Ran, What Was Blocked, and Whether "a Virus Did It" Holds UpCOMPUTER FORENSICS LAB§ ABOUT THE AUTHORPREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAMFULL CHAIN-OF-CUSTODY DOCUMENTATION§ CONTENTSIn this guide01 Executive summary02 The problem in plain English: Macs get malware, and "a virus did it" gets raised03 How Gatekeeper and XProtect work04 What the artefacts show: ran, blocked, quarantined05 Investigating a genuine compromise06 Testing the "a virus did it" claim07 Deployment: breach, c a us at i on and the malware defence08 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: Macs get malware, and Apple's Gatekeeper and XProtect leave artefacts showing whatran, was blocked or was quarantined, so those artefacts, with the wider record, both help investigate a genuinecompromise and allow the "a virus did it" defence to be tested even-handedly, at honest confidence.§ 02 · FIRST PRINCIPLESThe problem in plain English: Macs get malware, and "a virus didit" gets raised§ 03 · HOW THEY WORKHow Gatekeeper and XProtect workD OWN LOAD QUARANTINE GATEKEEPER XPROTECT RAN / BLOCKED§ 04 · WHATTHEARTEFACTSSHOWWhat the artefacts show: ran, blocked, quarantined§ 05 · INVESTIGATINGACOMPROMISEInvestigating a genuine compromise§ 06 · TESTINGTHEVIRUSDEFENCETesting the "a virus did it" claim§ 07 · DEPLOYMENTDeployment: breach, c a us at i on and the malware defence§ 08 · THEWIDERMAPSource architecture: where else the evidence livesEVIDENCE SECURIT Y LOGS / FIREWALLMAC SYSTEM NETWORK /ARTEFACTS MEMORY LOGSEND POINT / BACKUPS / MANAGEDAV TOOLS SNAPSHOTS CONSOLE§ 09 · IN THE WILDWorked examplesEXAMPLE1 · THEGENUINECOMPROMISERECONSTRUCTEDEXAMPLE3 · THEMALWAREDEFENCETHEEVIDENCESUPPORTED§ 10 · WHEREITGOESWRONGCommon mistakes and technical limitationsCommon mistakesTechnical limitations§ 11 · INTERROGATORIES & DRAFTING AIDSQuestions to ask · Suggested wordingAsk your clientAsk your opponentAsk your e Discovery / forensic provider§ 12 · QUICK CONTROLChecklist and red flags · When to involve a digital forensicexpertThe Mac security and malware checklistRed flagsWhen to involve a digital forensic expert19. The laboratory investigates malware and does not create or deploy it. Through cflab.uk and e-discovery.uk,§ 13 · COMMON QUESTIONSFrequently asked questionsDo Macs really get malware?What do Gatekeeper and XProtect actually record?Someone says "a virus did it". How do you test that?If malware is found, does that prove it was responsible?Isn't the expert just there to defeat the virus defence?Why the urgency about not shutting the Mac down?§ 14 ·

REFERENCEGlossarySources and authoritative referencesDISCLAIMER§ HOW A SPECIALIST LABORATORY CAN ASSISTWorking with Computer Forensics Lab19. The laboratory investigates malware and does not create or deploy it. This guide completes the macOSSpeak to a forensic examiner, not a salesperson.INSTRUCTTHELABNEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

Someone says "a virus did it". How do you test that?

Even-handedly, by asking specific questions (

Why the urgency about not shutting the Mac down?

Because compromise evidence is often volatile (