K7 ACADEMY

Malware Researcher - Android

Overview

The Malware Researcher – Android programme is a specialised 7-day course that equips security professionals, mobile developers, and SOC analysts with practical skills to analyse, reverse-engineer, and understand Android malware. From APK internals and ZIP structure to known Android vulnerabilities and obfuscation techniques, this programme delivers hands-on expertise that is directly applicable to mobile threat intelligence and enterprise mobile security operations.

Mode	Duration	Level
Online/Offline Classes	40 Hours	Intermediate

Who Should Enrol?

- Android Developer/Mobile App Developer — understand how your apps can be weaponised
- Android Tester/Mobile App Tester/Android QA — identify malicious behaviour in apps
- Mobility Admin/SOC Device Manager — respond to mobile threats in enterprise environments
- Mobile Security Engineer/Enterprise Security Team — build mobile threat intelligence capability
- Malware Analysts — expand skills into the Android threat landscape
- Cyber Security Researchers — study real-world APK vulnerabilities and evasion techniques

Learning Outcomes

- Explain the Android security model — sandboxing, permissions, and app isolation
- Understand how Android malware spreads — sideloading, third-party stores, phishing
- Dissect APK file structure — Classes.dex, AndroidManifest.xml, META-INF, resources
- Use ADB and Android debugging tools for dynamic investigation
- Decompile and analyse DEX bytecode using dex2jar, Dexdump, and Jadx
- Identify and analyse known Android vulnerabilities (Master Key, Stagefright, AV Bypass)
- Parse and manipulate ZIP structure at the byte level to detect anomalies
- Understand the Android boot process and pre-boot persistence mechanisms
- Identify and break common code obfuscation techniques used by Android malware
- Use Genymotion and the Android Emulator for safe dynamic malware analysis

Modules

Module 1 — Introduction to Android Malware Analysis

- Android Security model
- Spreading and distribution
- Sideloading
- Android Root

Module 2 — APK File Structure

- Classes.dex
- AndroidManifest.xml
- META-INF
- Classes.dex file structure
- Analysis of APK

Module 3 — USB Debugging

- Android Debug Bridge

Module 4 — Tools

- Android SDK
- Emulator
- Dexdump.exe
- Dex2Jar Utility
- Genymotion

Module 5 — Vulnerabilities

- Master key vulnerability
- Filename length vulnerability
- Stagefright
- AV_Scanning_Bypass vulnerability

Module 6 — ZIP Structure

- End of Central Directory Header (EOCD)
- Central Directory File Header
- Local File Header

Module 7 — Android Boot Process

Module 8 — Obfuscation

- Obfuscation tools

Tools & Technologies Covered

Android SDK
Core development & analysis platform

ADB
Device debugging & forensic extraction

Android Emulator
Safe app detonation environment

Genymotion
Advanced Android emulation & network intercept

Dexdump.exe
DEX bytecode inspection

Dex2Jar
DEX to JAR conversion for decompilation

Jadx
APK decompiler — Java source output

APKTool
APK decoding, smali inspection & repackaging

ProGuard/DexGuard
Understanding obfuscation outputs

Wireshark
Network traffic analysis from emulator

Hex Editor (010 Editor)
Byte-level ZIP/DEX inspection

Career Opportunities

Role

- Android Malware Analyst
- Mobile Security Engineer
- SOC Analyst – Mobile Threat Intel
- Mobile Penetration Tester
- Threat Intelligence Researcher
- Enterprise MDM Security Specialist

Certification & Assessment

- Module-wise Knowledge Checks
- Practical Lab Reports — written analysis submitted for each lab exercise
- APK Analysis Assignment — full dissection and report on an assigned malicious APK
- Final Certification Exam — Passing Score: 70%

K7 ACADEMY

www.k7academy.com

202607163