kaspersky
expert training

Mobile malware reverse engineering

Course program

№	Track	What you will learn	What you will practice	Lesson	Practice	Evaluation
0	Introduction	• About your trainer • Course roadmap • Course structure	–	Intro	–	–
				Introduction to virtual lab	–	–
1	Mobile malware essentials	• Android security models: DAC/MAC, SafetyNet, “unknown sources” • The Android package structure manifest with entry points, Dalvik bytecode and native code • Static analysis tools • Dynamic analysis tools	–	Mobile malware essentials: Android	–	Knowledge check: mobile malware essentials
				Mobile malware essentials: iOS	–	–
2	DuKong: sophisticated Android espionage campaign	• Surface entropy, signature, strings and unpacking • Manifest research, suspicious permissions, broadcast receivers and services • Decompilation procedure	• Static analysis of Dalvik bytecode • Analyzing native libraries • Understanding staging concept: payload decryption	DuKong: the story	–	–
				Introduction to DuKong	Lab: introduction to DuKong	Quiz
				Solution: Introduction to DuKong. Stager functionality	–	–
				DuKong: payload decryption	Lab: DuKong payload decryption	Checkpoint quiz
				Solution: decryption. DuKong payload analysis	–	–
				DuKong: wrap-up	–	–

№	Track	What you will learn	What you will practice	Lesson	Practice	Evaluation
3	LightSpy	Structure of the most popular packer for Android Dynamic file analysis	• Qihoo packer JIANGU basic concept and footprints location • Unpacking using dynamic instrumentation with Frida framework • Logging web requests using dynamic instrumentation featuring Frida framework	LightSpy: the story	Lab: LightSpy. Surface analysis	Checkpoint quiz
				Solution: surface analysis. LightSpy unpacking	Lab: LightSpy. Payload analysis	Quiz
				LightSpy: wrap-up	—	
4	MagicKarakurt	Java native interface connection Ghidra JNI correct code decompilation	• Advanced static analyzing of Android native shared libraries using Ghidra • Static decrypting of configuration files using Python • Frida framework to dump configuration file • Dynamic instrumentation for configuration file dumping using Frida framework	MagicKarakurt: the story. Surface analysis	Lab: MagicKarakurt. Surface analysis	Quiz
				Solution: surface analysis. Dive into native	—	—
				Dynamic config dumping	Lab: MagicKarakurt. Dynamic config dumping	Checkpoint quiz
				Back to Java	—	—
				MagicKarakurt: wrap-up	—	—
5	LightSpy iOS	How to deal with iOS malware Objective—C selector calls	• Advanced static analysis of Mach—o binaries • Dealing with msgSend selector calls using Ghidra plugins: restoring cross references • Static config file decryption using Cyberchef or any other suitable tool	LightSpy iOS: the story	Lab: LightSpy iOS. Surface analysis	Checkpoint quiz
				• Solution: surface analysis • Code analysis	—	—
				LightSpy iOS: wrap-up	—	—
6	Course Summary	Summary	Trainer ‘s closing remarks	—	—	—

Thank you!

kaspersky.com

Discord server: kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky