Malware Analysis & Reverse Engineering

Course program

№	Track	What you will learn	Lesson	Practice	Evaluation
0	Introduction	• About your trainer • Course roadmap • Course structure	Introduction	—	—
			Introduction to virtual lab	—	—
1	Chafer	• How to analyze the Windows Crypto API functions and calls • About PE compiled with gcc: segments, DWARF debug data, names mangling • How to resolve standard enumerators to make code more readable • How to determine the encryption algorithms and keys	Chafer: campaign against diplomatic entities	—	Knowledge check
			Chafer: debug data	—	Knowledge check
			Chafer: understanding the enumerator value meaning	Lab: time to determine the encryption algorithm Solution: time to determine the encryption algorithm	Quiz
				Lab: more functions and IoCs Solution: more functions and IoCs	Quiz
			Chafer: summary	—	Quiz Checkpoint quiz
2	LuckyMouse	• How to combine static and dynamic analysis with with disassembler, debugger and hex editor • How to follow all the Windows dynamic libraries search order hijacking steps • How to find custom decryption routines (implemented without CryptoAPI this time) • How to dump the PE file from memory • after self-decryption • How to add structures to the IDA database like you did for enumerators in Chafer	LuckyMouse: national level data center attack	—	—
			LuckyMouse: surface analysis	Lab: surface analysis	Quiz
			LuckyMouse: reducing the amount of code under analysis	Lab: now it's time for the disassembler	Quiz
			LuckyMouse: combination of static and dynamic analysis	Lab: prepare to dump	Quiz
			LuckyMouse: dumping from memory	Lab: dumping the next stager	Quiz Checkpoint quiz
			LuckyMouse: summary	—	—

№	Track	What you will learn	Lesson	Practice	Evaluation
3	Biodata Exploit	• Files don't have to be executable to • analyze them in the disassembler • The nature of the exploits, how they • initially start and operate • "One asm instruction after another" • analysis, like you would do in any real case	Biodata exploit: the story of one geographically targeted campaign	Lab: analyzing the document in IDA	Quiz
			Biodata exploit: popular tricks in exploits with FS:[ ]	Lab: analyzing the exception handler	Quiz
			Biodata exploit: Egg hunting	Lab: analyzing the Egg Hunter	Quiz
			Biodata exploit: PE header parsing analysis	Lab: analyzing the function resolver	Quiz Checkpoint quiz
			Biodata exploit: summary	—	—
4	Topinambour	• How interpreted samples differ from compiled ones • .NET samples analysis with DnSpy • Static and dynamic scripts deobfuscation	Topinambour: .NET Story In Which KopiLuwak Meets RocketMan	—	—
			Topinambour: the tool to analyze .NET bytecode	Lab: dropper analysis	Quiz
			Topinambour: gathering file and network IoCs	Lab: backdoor and script	Quiz
			Topinambour: time for deobfuscation	Lab: dynamic RC4 decryption	Quiz Knowledge check Checkpoint quiz
			Topinambour: summary	—	—
5	Biodata Trojan	• Reverse-engineering sometimes involves looking at less popular languages like Delphi	Biodata Trojan: using IDA Pro's scripting abilities to automate string decryption	—	Knowledge check
				Lab: biodata Trojan. Step 1 Solution: biodata Trojan. Step 1	Quiz

№	Track	What you will learn	Lesson	Practice	Evaluation
			IDA scripting &important API functions	Lab: biodata Trojan. Step 2 Solution: biodata Trojan. Step 2	Quiz Checkpoint quiz
			Biodata Trojan: summary	—	—
6	DeathStalker	• How DeathStalker, a mercenary APT, breaches law offices and wealth management firms with custom tooling • How LNK-based infection chains work and how to approach them • How to deobfuscate PowerShell scripts • Common techniques like dead-drop resolvers used by APTs and red teams	DeathStalker: a Mercenary's infection chain	Lab: DeathStalker. Step 1 Unpacking the LNK and reaching powersing Solution: DeathStalker. Step 1 Unpacking the LNK and reaching powersing	Quiz
				Lab: DeathStalker. Step 2. Reversing powersing Solution: DeathStalker. Step 2. Reversing powersing	Quiz Checkpoint quiz
			DeathStalke: summary	—	—
7	MontysThree	• How to deal with steganography • How to dump embedded encryption keys • How to migrate definitions between samples with header files	MontysThree: industrial espionage case	Lab: import the header and apply the structure	—
			MontysThree: bitmap file structure	Lab: understand steganography algorithm	—
			MontysThree :steganography algorithm	—	Quiz
			MontysThree: here comes the Kernel module	Lab: export the encryption keys	Quiz
			MontysThree: the BLOBs with encryption keys	Lab: the final step to understanding the config encryption	Quiz Checkpoint quiz

№	Track	What you will learn	Lesson	Practice	Evaluation
			MontysThree: a little bit of C++ to parse the tasks	Lab: Google cloud communications	Quiz Checkpoint quiz
			MontysThree: summary	—	—
8	Lazarus Group	• Reverse-engineering x64 malware • How to reconstruct a custom network protocol from a malware sample	Lazarus group: a post-exploitation tool	Lab: Lazarus' post-exploitation tool. Step 1 Solution: Lazarus' post-exploitation tool. Step 1	Quiz
				Lab: Lazarus' post-exploitation tool. Step 2 Solution: Lazarus' post-exploitation tool. Step 2	Quiz
				Lab: Lazarus' post-exploitation tool. Step 3 Solution: Lazarus' post-exploitation tool. Step 3	Quiz Checkpoint quiz
			Lazarus group: summary	—	—
9	Cloud Snooper	• Reverse-engineering Linux programs • Recognizing variants of open-source trojans • Analyzing network protocols used by backdoors • What rootkits are and how they work	Cloud snooper: a Linux Rootkit and its userland companions	Lab: cloud snooper. Userland component 1	Quiz
			Cloud snooper: tsh	Lab: cloud snooper. Snoopy_client	Quiz
			Cloud snooper: "snoopy_client"	Lab: cloud snooper. Kernel module	Quiz
			Cloud snooper: summary	—	Checkpoint quiz

№	Track	What you will learn	Lesson	Practice	Evaluation
10	Cyclades’s Triad	• New obfuscation tricks used by attackers to frustrate reverse-engineering efforts and additional IDA Python tips to overcome them • How to work with shellcodes • What “Reflective DLL loading” is and how it works • Advanced Hex-Rays Decompiler techniques	Cycldek’s triad	Lab: Cycldek’s triad. Step 1 Solution: Cycldek’s triad. Step 1	Quiz
				Lab: Cycldek’s triad. Step 2 Solution: Cycldek’s triad. Step 2	Quiz
				Lab: Cycldek’s triad. Step 3 Solution: Cycldek’s triad. Step 3	Quiz
			Cycldek’s triad: step 4	Lab: Cycldek’s triad. Step 4	Quiz
			Cycldek’s triad: summary	—	Checkpoint Quiz
11	Bonus Track: Go Malware	• How to reverse-engineer Go malware • The fundamentals of the Go language	Golang malware: theory	Lab: Sunshuttle. Step 1 Solution: Sunshuttle. Step 1	Quiz
				Lab: Sunshuttle. Step 2 Solution: Sunshuttle. Step 2	Quiz
				Lab: Sunshuttle. Step 3 Solution: Sunshuttle. Step 3	Quiz
				Lab: Sunshuttle. Step 4	Quiz
			Reverse-engineering Golang malware: Sunshuttle. Summary	—	—
			Course summary	—	—

Own the knowledge, outsmart the threat.

kaspersky.com

Discord server: kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky