

TABLE OF CONTENTS

01	The Anatomy of a YARA Rule	
	Intro	03
	Code	04
	POC & Detection	05
02	Pattern Matching and Condition Logic	
	Intro	06
	Code	07
	POC & Detection	08
03	Modules, Imports...	
	Intro	09
	Code	10
	POC & Detection	11
04	Writing a Basic YARA Rule	
	Intro	12
	Code	13
	POC	14
05	Using Hex Patterns in Rules	

TABLE OF CONTENTS

06 File Type and Magic Header Matching

- Data Obfuscation via Encoding 03
- Domain Generation Algorithms (DGAs) 05

07 Case Insensitivity and String Modifiers

08 PE Module Basics

09 Import Table and Function Detection

10 Matching Specific Compile Timestamps

11 Exercise

12 Conclusions