

TABLE OF CONTENTS

01	Introduction	
	Intro	03
	Code	04
	POC & Detection	05
02	ETW Components	
	Intro	06
	Code	07
	POC & Detection	08
03	ETW Interceptor	
	Intro	09
	Code	10
	POC & Detection	11
04	Creating fake Events with ETW	
	Intro	12
	Code	13
	POC	14
05	ETWHash	

TABLE OF CONTENTS

06 Disable ETW

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

07 Exercise

08 Conclusions