TABLE OF CONTENTS

COVER

ORIGINALITY STATEMENT OF THE THESIS

THESIS SUPERVISOR'S APPROVAL

THESIS EXAMINATION COMMITTEE

ABSTRACT v

ABSTRAK vi

ACKNOWLEDGEMENTS.. vii

TABLE OF CONTENTS.. iix

LIST OF FIGURES xiv

LIST OF ABBREVIATIONS xix

CHAPTER I INTRODUCTION 1

1.1 Background 1

1.2 Problem Identification 5

1.3 Limitation of The Study.. 6

1.4 Problem Statement 8

1.5 Research Purpose 9

1.6 Research Objectives.. 10

1.7 Writing Structure 12

CHAPTER II LITERATURE STUDY 15

2.1 Log Analysis 15

2.1.1. Event Log Analyser 16

2.1.2. YARA Rules 18

2.1.3. Clustering Log Analysis 19

2.1.4. Thor Lite Scanner 20

2.2. Static Malware Analysis 20

2.3. Dynamic Malware Analysis 22

2.4.Hybrid Malware Analysis 24

2.5. SQL Injection Logs 25

2.5.1 Cross Site Scripting 26

2.5.2 Directory Traversal 27

2.5.3 Malicious URL Request 29

2.6. Malware entropy analysis 26

2.7. Code Cross-Reference Malware Analysis 32

2.7.1. IDA View-A Analysis 33

2.7.2 virustotal.com 33

2.7.3. Hybrid-analysis.com 36

2.7.4. Salt in Hash Strengthenin 37

2.7.5. MD5 (Message Digest Algorithm 5) 37

2.7.6. Distribution of File Extensions 40

2.7.7. Trojan Backdoor 40

2.7.8. Online Gambling 42

2.7.9. Malware Detection and Scoring 43

CHAPTER III RESEARCH METHODOLOGY 47

3.1.Stage Methodology 47

3.2.Data Collection 53

3.3.Tools and Methodology 58

a.Thor Lite Scanner 58

b.IDA Pro 56

c.VirusTotal.com 60

c.Hybrid-Analysis.com 62

d.Entrophy Analysis using IDAtropy plugin 63

3.4. Methodology 65

3.4.1.Clustering Log Analysis... 65

3.4.1.1. SQL Injection Logs Analysis 66

3.4.1.2. Directory Traversal Logs Analysis.. 68

3.4.1.3. Malicious URL Request Logs Analysis 70

3.4.1.4 Cross-Site Scripting (XSS) Log Analysis 73

3.4.2. Static Analysis 75

3.4.3. Dynamic analysis 77

3.4.4. Hybrid Analysis 78

3.4.5. The Cross-Reference and Code Analysis... 80

3.4.6.Entropy Analysis.. 83

3.5. Penetration Test.. 84

3.5.1. Stages of a penetration test using Burp Suite....................................... 84

3.5.2. Stages of a penetration test using Zed Attack Proxy (ZAP) 86

3.5.3 Stages of a penetration test using Acunetix 88

CHAPTER IV RESEARCH RESULTS AND DISCUSSION 86

4.1. Malware Distribution 90

4.2. Clustering Types of Attacks by Analyzing Server Logs............................... 99

4.2.1. SQL Injection.. 100

4.2.2. Cross site scripting... 110

4.2.3 Directory Traversal 118

4.2.4. Malicious URL Request... 123

4.3. Analysis Malicious Files.. 132

4.3.1. Static Analysis 132

a.File Name : Cina.php 132

b.File Name : js-site.web.php 138

c.File Name : nez.phtml 139

d.File Name : o.php 140

e.File Name : bash.alfa 142

f.File Name : perl.alfa 143

g.File Name : py.alfa 145

4.3.2. Dynamic Analysis 147

a.File Name : Cina.php 147

b.File Name : js-site.web.php 150

c.File Name : nez.phtml 152

d.File Name : o.php 155

e.File Name : bash.alfa 158

f.File Name : perl.alfa 161

g.File Name : py.alfa 162

4.3.3. Hybrid Analysis 165

a.File Name : Cina.php 165

b.File Name : js-site.web.php 166

c.File Name : nez.phtml 167

d.File Name : o.php 168

e.File Name : bash.alfa 169

f.File Name : perl.alfa 170

4.3.4. Analyzing Code and Functions 171

a.File Name : Cina.php 171

b.File Name : js-site.web.php 177

c.File Name : nez.phtml 180

d.File Name : o.php 181

e.File Name : bash.alfa 187

f.File Name : perl.alfa 192

g.File Name : perl.alfa 195

4.3.5. Entropy Analysis 197

a.File Name : Cina.php 197

b.File Name : js-site.web.php 199

c.File Name : nez.phtml 200

d.File Name : o.php 202

e.File Name : bash.alfa 204

f.File Name : perl.alfa 206

4.3.6. Penetration Test 208

a.Zed Attck Proxy (ZAP) 208

b.ACUNETIX Software 211

c.Burp Suite Software 215

CHAPTER V CONCLUSION AND RECOMMENDATION 219

5.1. Conclusion 219

5.2. Recommendations 221

REFERENCES

LIST OF FIGURES

Figure 1. 1 Websites that have been infiltrated with online gambling content............ 2

Figure 1. 2 Number and Value of Online Gambling Transactions (2017-2022) 3

Figure 1. 3 Website that has been infiltrated with online gambling content............... 4

Figure 1. 4 Research Flowchart on the Issue of Online Gambling Trojans.............. 10

Figure 1. 5 Research Objectives Flowchart 11

Figure 1. 6 Stage Methodology.. 49

Figure 2. 1 The display of Application process ……………………………………… 13

Figure 3. 1 Data Collection phase……………………………………………………..50

Figure 3. 2 Variety of tools 52

Figure 3. 3 Analysis stages.. 53

Figure 3. 4 Penetration Testing 56

Figure 3. 5 Apanel Dashboard 56

Figure 3. 6 Flow Chart Log Analysis.. 59

Figure 3. 7 Flow Chart IDA Pro and Hex View 60

Figure 3. 8 Flow Chart Virus Total Usage.. 58

Figure 3. 9 Flow Chart Analyse malware using Hybrid-Analysis.com 63

Figure 3. 10 Flow Chart Entrophy Analysis using IDAtropy 65

Figure 3. 11 Flow Chart Methodology Log Analysis 66

Figure 3. 12   Flow Chart Methodology Log Analysis 68

Figure 3. 13 Flow Chart Methodology Directory Traversal Logs Analysis 70

Figure 3. 14 Flow Chart Methodology Directory Traversal Logs Analysis 72

Figure 3. 15 Flow Chart Methodology Cross-Site Scripting (XSS) Log Analysis.... 75

Figure 3. 16 Flow Chart Static Analysis Methodology 77

Figure 3. 17 Flow Chart Hybrid Analysis Methodology 80

Figure 3. 18 Flow Chart Hybrid Analysis Methodology 83

Figure 3. 19 Flow Chart Entropy Analysis 84

Figure 3. 20 Flow Chart   penetration test using Burp Suite...................................... 86

Figure 3. 21 Flow Chart   penetration test using using Zed Attack Proxy (ZAP)..... 87

Figure 3. 22 Flow Chart   penetration test using using Acunetix.............................. 89

Figure 4. 1 Histogram MD5 Hashes and Score Distribution 90

Figure 4. 2   Distribution of Malware Score 91
Figure 4. 3   Distribution of file extensions 92
Figure 4. 4 Distribution of MD5 hash repeated 93
Figure 4. 5 Scatter Plot Cluster Base in Scores of malware files.............................. 94
Figure 4. 6 Directory infiltrated by an online gambling backdoor 95
Figure 4. 7 Directory view infiltrated with a script improving its ranking................ 96
Figure 4. 8 Contents of Folder infiltrated php extension gambling content files .. 96
Figure 4. 9 Display of a directory infiltrated by a backdoor trojan........................... 97
Figure 4. 10   Backdoor script display 97
Figure 4. 11 Backdoor script display 98
Figure 4. 12 htaccess display script file that has been modified by attacker 98
Figure 4. 13 Percentage IP address SQL Injection Logs 100
Figure 4. 14 Sactter Plot Transferred Bytes VS Status Code................................. 101
Figure 4. 15 Comparison of the number of HTTP requests with GET and POST . 103
Figure 4. 16 Number of HTTP status codes... 111
Figure 4. 17 Distribution of HTTP status codes 112
Figure 4. 18 Distribution of HTTP request types.. 115
Figure 4. 19 Precentage Directory Traversal Pie Chart 116
Figure 4. 20 The number of HTTP requests associated with various IP addresses 119
Figure 4. 21 Distribution of HTTP status codes in logs.. 119
Figure 4. 22 Comparing the number of GET and POST requests 120
Figure 4. 23 amount of data transferred (in bytes)... 121
Figure 4. 24 The directory suspected to be compromised by malware.................. 128
Figure 4. 25 Directory suspected to be compromised by malware......................... 129
Figure 4. 26 user interface of the malware... 145
Figure 4. 27 The user interface of the malware 148
Figure 4. 28 Directory suspected to be compromised by malware 149
Figure 4. 29 VirusTotal Graph from file nez.phtml... 150
Figure 4. 30 The user interface of the malware 152
Figure 4. 31 nez,phtml in directory web server 153
Figure 4. 32 The user interface of the malware 153

Figure 4. 33 file o.php in directory webserver 156
Figure 4. 34 VirusTotal Graph from file bash.alfa.. 156
Figure 4. 35 Malware bash.alfa in directory ALFA_DATA.................................. 157
Figure 4. 36 bash.alfa files in Directory web server 157
Figure 4. 37. VirusTotal Graph from file perl.alfa.. 158
Figure 4. 38 perl.alfa in directory web server 159
Figure 4. 39 VirusTotal Graph from file py.alfa 160
Figure 4. 40 . Malware py.alfa file in directory 162
Figure 4. 41 The scan results for the 'cina.php' file on www.hybrid-analysis.com 162
Figure 4. 42 The scan results for the 'cina.php' file on www.hybrid-analysis.com 163
Figure 4. 43T Scan results for the 'cina.php' file on www.hybrid-analysis.com 164
Figure 4. 44 The scan results for the 'cina.php' file on www.hybrid-analysis.com . 165
Figure 4. 45 The scan results for the 'cina.php' file on www.hybrid-analysis.com 166
Figure 4. 46 The scan results for py.alfa file on www.hybrid-analysis.com 167
Figure 4. 47 The IDA View-A interface of the o.php... 168
Figure 4. 48 .The Hex View-1 display of the o.php.. 171
Figure 4. 49 .The IDA View-A interface of the 'cina.php' file 174
Figure 4. 50 The Hex View-1 display of the js-site.web.php 175
Figure 4. 51 The IDA View-A interface of the nez.phtml file................................ 177
Figure 4. 52 The Hex View-1 display of the nez.phtml file 177
Figure 4. 53 IDA View-A interface of the o.php 178
Figure 4. 54 The Hex View-1 display of the o.php... 181
Figure 4. 55 The IDA View-A interface of the bash.alfa file 184
Figure 4. 56 The Hex View-1 display of the bash.alfa file 186
Figure 4. 57 The IDA View-A interface of the perl.alfa... 188
Figure 4. 58 The Hex View-1 display of the perl.alfa 189
Figure 4. 59 The IDA View-A interface of the py.alfa 191
Figure 4. 60 The Hex View-1 display of the py.alfa... 192
Figure 4. 61 Entropy level graph of the 'cina.php' file 193
Figure 4. 62 Graphical representation of the frequency distribution byte values   194
Figure 4. 63 The entropy level graph of the js-site.web.php................................... 195
Figure 4. 64 Graphical frequency distribution byte values file js-site.web.php ... 199

Figure 4. 65 The Hex View-1 display of nez.phtml file 200
Figure 4. 66 The entropy level graph of the nez.phtml file...................................... 197
Figure 4. 67 The entropy level graph of the o.php... 198
Figure 4. 68 Graphical frequency distribution byte values file o.php.................... 203
Figure 4. 69 .The entropy level graph of the bash.alfa file 204
Figure 4. 70 Graphical frequency distribution byte values bash.alfa file 205
Figure 4. 71 The entropy level graph of the perl.alfa... 206
Figure 4. 72 . Graphical frequency distribution byte values file   perl.alfa 207
Figure 4. 73 Burp Suite software Before and After Apache WAF enable.............. 210

UNIVERSITAS PELITA HARAPAN

LIST OF TABLES

Table 4. 1. Apache Access Logs - SQL Injection 104

Table 4. 2 . Apache Access Logs - SQL Injection 107

Table 4. 3 . Apache Access Logs - SQL Injection 109

Table 4. 4 Apache Access Logs - SQL Injection 110

Table 4. 5 Apache Access Logs - SQL Injection 109

Table 4. 6 Apache Access Logs - SQL Injection 110

Table 4. 7 Cross Site Scripting (XSS)... 113

Table 4. 8 Cross Site Scripting (XSS).. 114

Table 4. 9 Directory Traversal 117

Table 4. 10 Directory Traversal 122

Table 4. 11. Malicious URL Request 124

Table 4. 12 Malicious URL Request... 124

Table 4. 13 . Malicious URL Request 125

Table 4. 14 Malicious URL Request.. 126

Table 4. 15 Malicious URL Request.. 126

Table 4. 16 Malicious URL Request.. 127

Table 4. 17 Malicious URL Request... 127

Table 4. 18 Results of the file cina.php scan on VirusTotal.com 131

Table 4. 19 Results of the file js-site.web.php scan on VirusTotal........................ 134

Table 4. 20 Results of the file nez.phtml scan on VirusTotal.com 135

Table 4. 21 Results of the file o.php scan on VirusTotal.com 137

Table 4. 22 Results of the file bash.alfa scan on VirusTotal.com......................... 139

Table 4. 23 Results of the file perl.alfa on VirusTotal.com 141

Table 4. 24 Results of the file py.alfa scan on VirusTotal.com 143

Table 4. 25 Network Network Communication from malware 161

Table 4. 26 Results of Penetration Test using Zed Attack Proxy (ZAP) 204

Table 4. 27 ACUNETIX Scan Results.. 205

Table 4. 28 Burp Suit Penetration Test Result 208