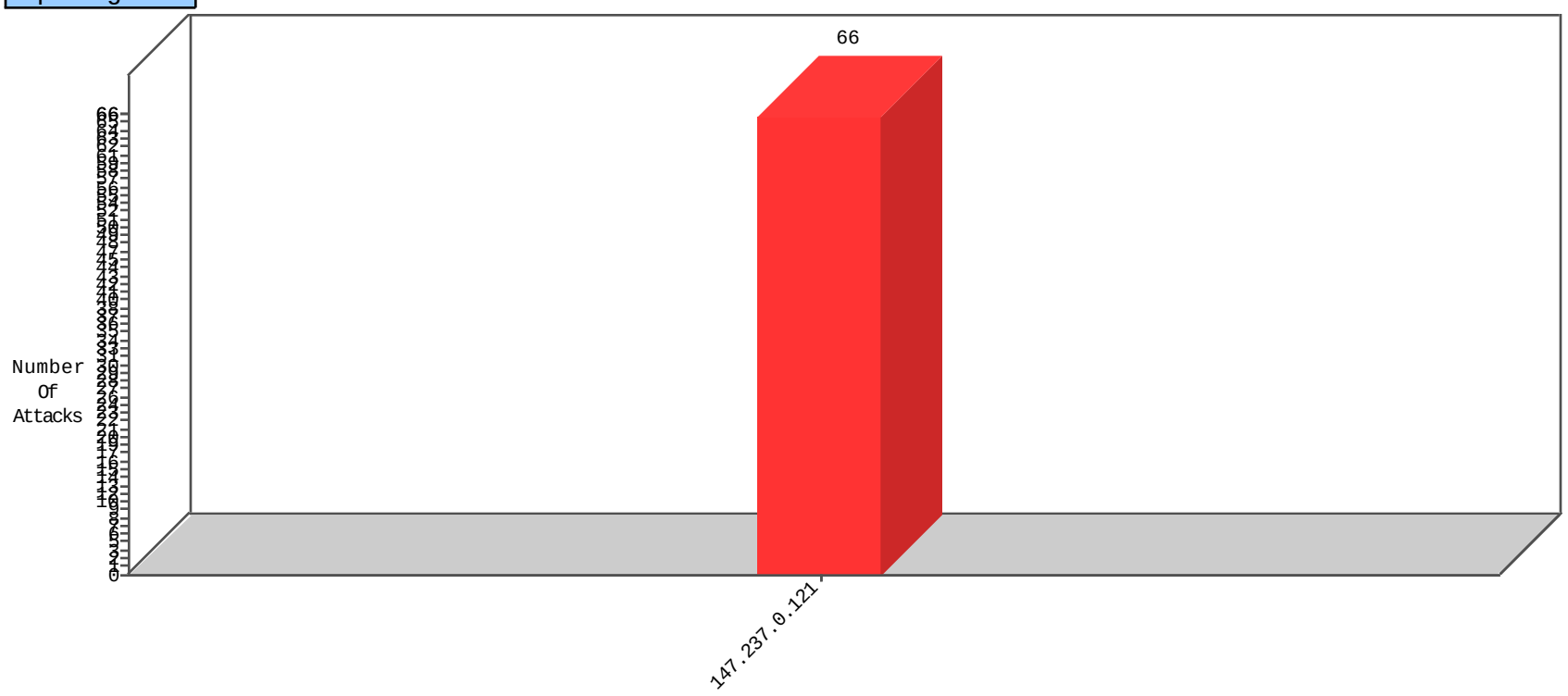
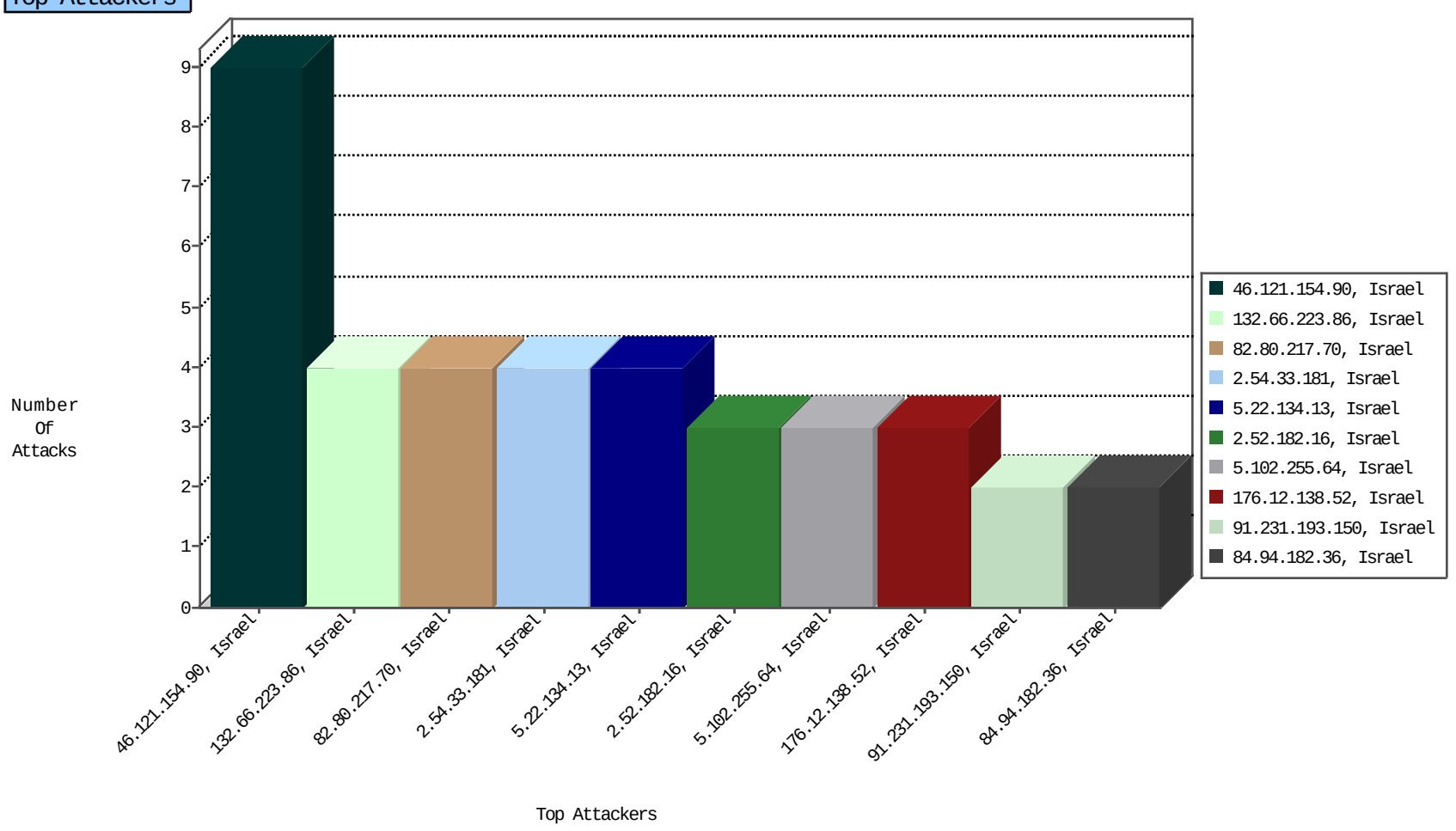
12-02-2015 to 12-03-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



12-02-2015 to 12-03-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3

12-02-2015 to 12-03-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

12-02-2015 to 12-03-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
5.22.134.13	Israel	147.237.0.121		GPL SCAN myscan	2
5.22.134.13	Israel	147.237.0.121		INDICATOR-SCAN myscan	2
91.201.236.114	Ukraine	147.237.0.121		ET SCAN NMAP -sS window 1024	1
122.231.3.92	China	147.237.0.121		ET SCAN Potential SSH Scan	1

12-02-2015 to 12-03-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.153	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2877
66.249.93.145	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2705
66.249.93.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2504
66.249.93.153	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	349
149.88.149.123	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	333
2.202.128.95	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	328
66.249.93.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	296
66.249.93.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	281
192.146.6.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	217
149.78.221.136	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	200
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	193
194.42.67.50	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	172
46.19.85.205	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	145
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	69
149.78.234.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	65
149.88.132.190	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.88.202.196	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	59
149.78.34.51	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
108.171.128.175	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49
40.77.167.14	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
149.88.213.210	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
185.27.105.169	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	36
66.249.66.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
66.249.81.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
149.88.101.24	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
149.88.73.71	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
212.150.125.84	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
62.90.54.54	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	24
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
31.168.226.178	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	20
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
81.218.97.6	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	18
66.249.66.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
66.249.93.241	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
93.173.229.254	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	16
66.249.81.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
66.249.66.105	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
46.116.245.86	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	14
108.161.241.23	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12
217.69.133.248	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11
66.249.81.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	11

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.54.33.181	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	4
2.54.172.210	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.126.93.207	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPermitFilesNames in www.miluim-ishi.aka.idf.il/valtamrequest	Block	2
176.12.138.52	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 176.12.138.52 (sigalgs DoS Attack)	None	2
62.219.99.130	Israel	147.237.0.121		Suspicious Response Code	Block	2
62.219.169.218	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
46.121.154.90	Israel	147.237.0.121		Malformed HTTP Header Line 1	Block	1
213.151.59.151	Israel	147.237.0.121		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 213.151.59.151	Block	1
132.66.223.86	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
5.102.255.64	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.0.32	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$Submit1 in www.miluim-ishi.aka.idf.il/changeunit	Block	1
87.69.106.146	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
82.80.217.70	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/rules.abe	Block	1
46.121.154.90	Israel	147.237.0.121		Unknown HTTP Request Method Âƒ5Ã«,qÃ¬ÂªGÂ»[[#1]]Ã¶Â-[[#14]]Ã£Â™G:,Â‰ ;Ã¾Â®Ã¦E5Ã?Ã²Y[[#3]]Âˆ[[#24]]ÂªÂ [[#5]]Â½Ã°&9Â±LOÂ™6)Â…ÂµÃŸÃš)ÃºaÃ§-ÂŒ 6ToÂ?[[#12]]Â?/)O\ÃƒÂ¹1-Â¶Ã?Ã´Â€ÃŸÃœ}Âœ5I3dÂŠÂµÃ–[[#3]]Â¾Â‡MÃ“ÃšÃ³<cÃ·[[#18]]Ãœ [[#1]]Ã‰m[[#18]]Ã-[[#25]]Ã¨Ã,Â»*]XÂ«][[#21]]Ã?<,Ã«BÂŠ#Ã«}gsh2Ã?ÂºÃ,	Block	1
176.13.5.82	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.121.154.90	Israel	147.237.0.121		Abnormally Long Request method	Block	1
132.66.223.86	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
84.94.182.36	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.52.182.16	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.52.182.16 (sigalgs DoS Attack)	None	1
46.121.154.90	Israel	147.237.0.121		Malformed URL	Block	1
132.73.195.66	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
46.19.86.23	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.4.90	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.231.193.150	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 91.231.193.150 (Unknown SSL Session)	None	1
82.81.8.151	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 82.81.8.151 (Unknown SSL Session)	None	1
62.90.147.209	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
46.121.154.90	Israel	147.237.0.121		Illegal Byte Code Character in Header Name	Block	1
192.115.67.2	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 192.115.67.2 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
132.66.223.86	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
5.102.255.64	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
84.228.235.204	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
2.52.182.16	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.176.21.12	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
46.121.154.90	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.121.154.90 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
46.19.86.111	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
91.231.193.150	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
82.81.8.151	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
46.121.154.90	Israel	147.237.0.121		Illegal Byte Code Character in Method Âƒ5Ã«,qÃ¬ÂªGÂ»[[#1]]Ã¶Â-[[#14]]Ã£Â™G:,Â‰ ;Ã¾Â®Ã¦E5Ã?Ã²Y[[#3]]Âˆ[[#24]]ÂªÂ [[#5]]Â½Ã°&9Â±LOÂ™6)Â…ÂµÃŸÃš)ÃºaÃ§-ÂŒ 6ToÂ?[[#12]]Â?/)O\ÃƒÂ¹1-Â¶Ã?Ã´Â€ÃŸÃœ}Âœ5I3dÂŠÂµÃ–[[#3]]Â¾Â‡MÃ“ÃšÃ³<cÃ·[[#18]]Ãœ [[#1]]Ã‰m[[#18]]Ã-[[#25]]Ã¨Ã,Â»*]XÂ«][[#21]]Ã?<,Ã«BÂŠ#Ã«}gsh2Ã?ÂºÃ,	Block	1
192.115.67.2	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
132.66.223.86	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
5.102.255.64	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
87.69.103.137	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.182.16	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.55.225	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.121.154.90	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.12.138.52	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.121.154.90	Israel	147.237.0.121		Abnormally Long Header Line request header name	Block	1
2.54.129.79	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.49.103	Israel	147.237.0.121		Unknown Parameter gfe_rd in www.miluim-ishi.aka.idf.il/	Block	1
84.94.182.36	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.94.182.36 (sigalgs DoS Attack)	None	1