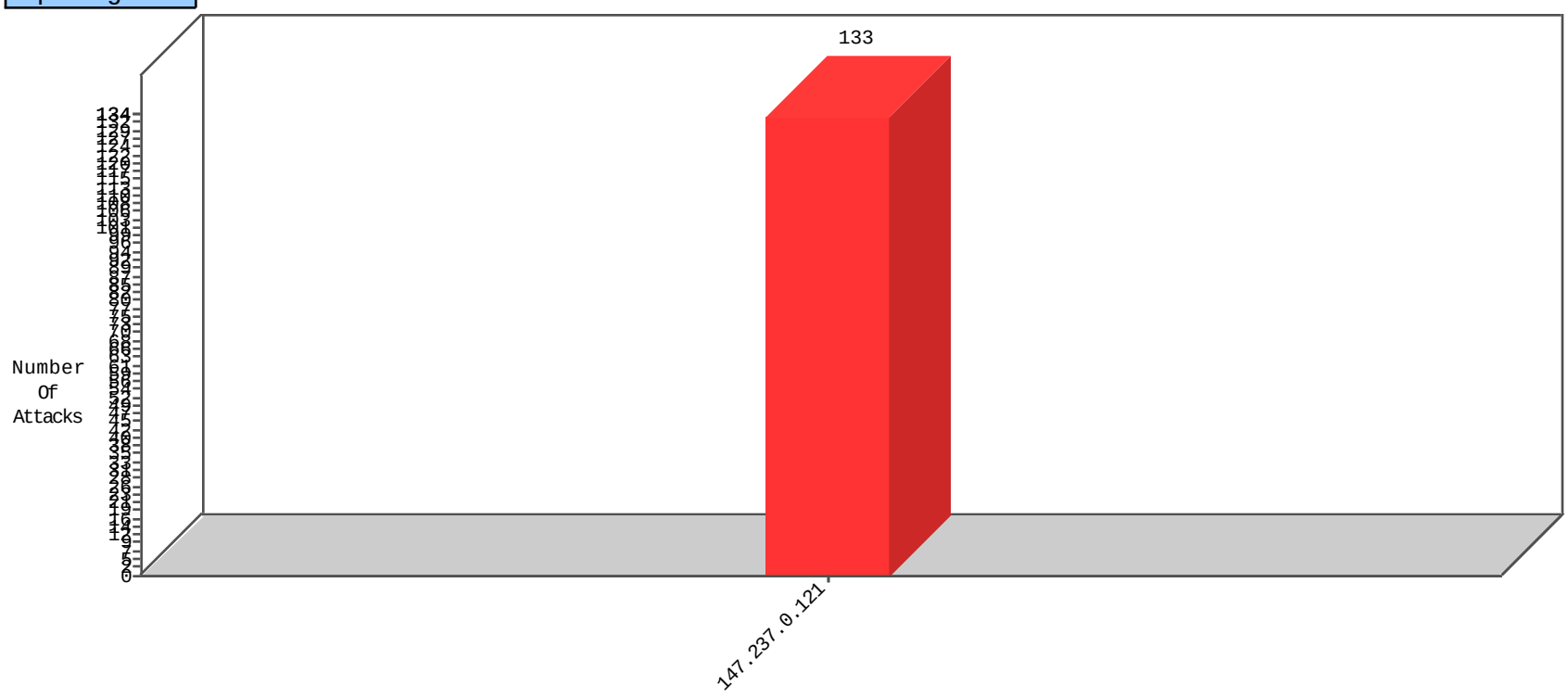
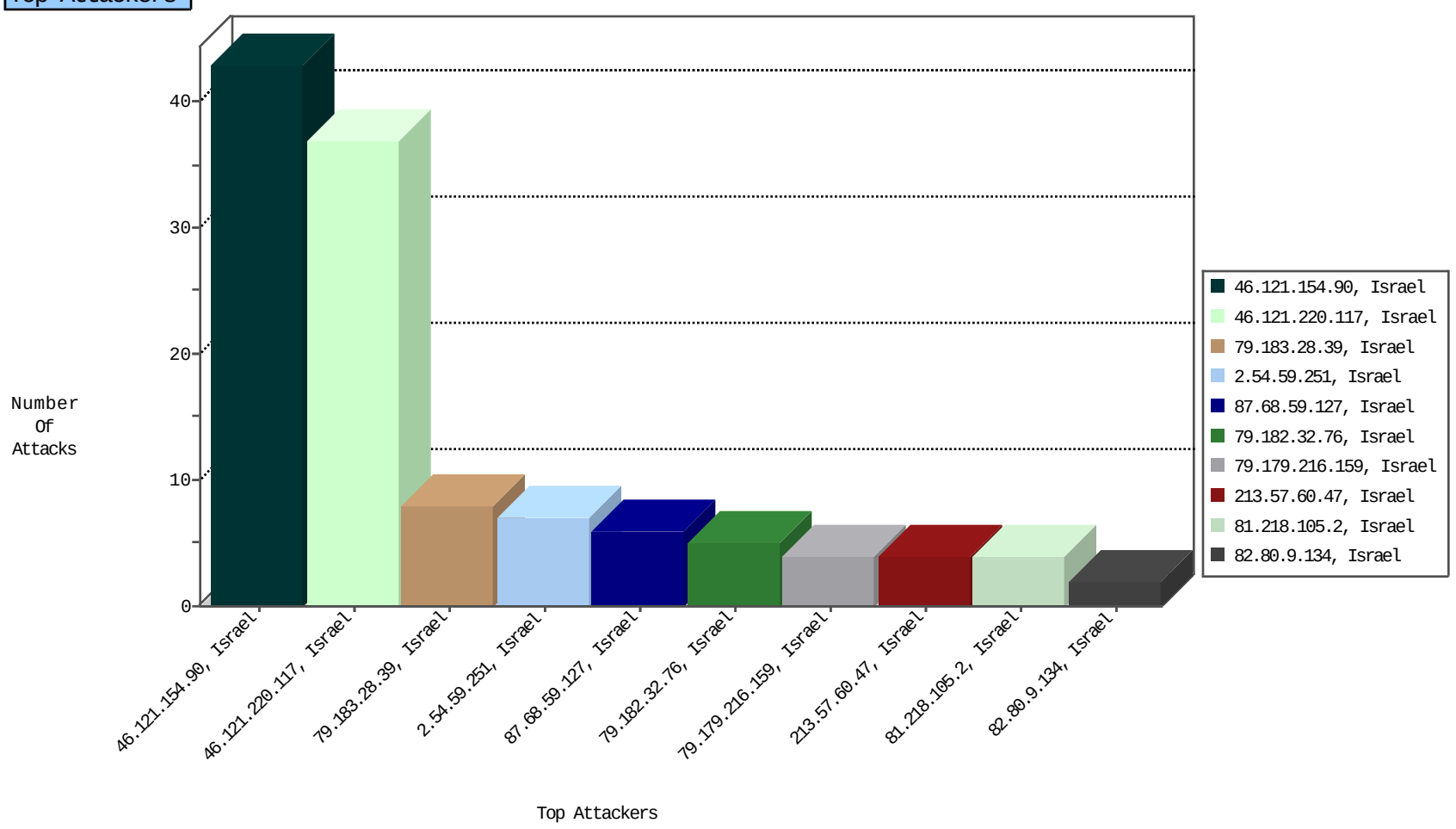
11-17-2015 to 11-18-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-17-2015 to 11-18-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.54.59.251	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	7
79.182.32.76	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	5

11-17-2015 to 11-18-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-17-2015 to 11-18-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
213.169.149.80	Cyprus	147.237.0.121		ET SCAN Potential SSH Scan	1
192.198.151.44	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
95.105.15.110	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1

11-17-2015 to 11-18-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3027
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2798
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2456
149.78.64.16	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1629
149.88.30.56	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	402
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	262
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	249
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	246
46.19.85.216	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
149.78.14.254	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	225
149.78.72.163	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	148
66.249.83.107	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	124
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	122
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	112
149.78.34.111	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	78
66.249.93.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
17.78.71.209	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	71
66.249.93.162	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
149.78.224.4	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
66.249.81.251	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	68
192.198.151.43	Europe	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	68
37.26.148.199	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	64
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
66.249.93.254	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
212.199.176.182	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	61
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
176.12.141.158	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	51
66.102.7.179	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
66.249.93.158	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
37.26.148.199	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	49
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	47
66.249.93.247	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
149.88.86.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
212.5.206.222	Slovakia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
188.93.56.123	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	40
66.249.83.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
79.176.172.104	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
132.64.73.12	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.9	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
2.54.62.23	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
82.166.22.14	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
149.78.244.215	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
176.13.16.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	30
132.76.50.6	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	29
66.249.83.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
176.12.141.102	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	27

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.121.220.117	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	23
46.121.220.117	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddBoardExamsPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	7
46.121.220.117	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	7
46.121.154.90	Israel	147.237.0.121		Multiple Illegal HTTP Version from 46.121.154.90	Block	4
46.121.154.90	Israel	147.237.0.121		Multiple Unknown HTTP Request Method from 46.121.154.90	Block	4
79.183.28.39	Israel	147.237.0.121		Distributed PHP Attempt	Block	4
46.121.154.90	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Method from 46.121.154.90	Block	4
79.183.28.39	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ajax/pages/fan_status.php	Block	4
46.121.154.90	Israel	147.237.0.121		Multiple Malformed URL from 46.121.154.90	Block	4
46.121.154.90	Israel	147.237.0.121		Multiple Abnormally Long Request from 46.121.154.90	Block	4
79.179.216.159	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	4
81.218.105.2	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddStudyPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	3
87.68.59.127	Israel	147.237.0.121		PHP Attempt	Block	3
87.68.59.127	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ajax/pages/fan_status.php	Block	3
46.121.154.90	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Value from 46.121.154.90	Block	2
213.57.60.47	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/ajax/pages/fan_status.php	Block	2
46.121.154.90	Israel	147.237.0.121		Multiple Illegal Byte Code Character in URL from 46.121.154.90	Block	2
46.121.154.90	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Name from 46.121.154.90	Block	2
46.121.154.90	Israel	147.237.0.121		Malformed URL [[#26]]Â´×€p$fÂ?mâ,¬Ö»Ö·[[[#18]]×°[[#6]][â€Ž×?e.jÂŒÂ¡×“ Â Â Â¾Ö³[[#28]]Â©jÂŽhÃ»Ö°pÂ?[[#30]]	Block	1
95.86.64.214	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1
46.121.154.90	Israel	147.237.0.121		Abnormally Long Request method	Block	1
213.57.60.47	Israel	147.237.0.121		Distributed PHP Attempt	Block	1
46.121.154.90	Israel	147.237.0.121		Illegal Byte Code Character in URL [[#26]]Â´×€p$fÂ?mâ,¬Ö»Ö·[[[#18]]×°[[#6]][â€Ž×?e.jÂŒÂ¡×“ Â Â Â¾Ö³[[#28]]Â©jÂŽhÃ»Ö°pÂ?[[#30]]	Block	1
31.154.174.124	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.121.154.90	Israel	147.237.0.121		Too Many Headers per Request - 33 Headers	Block	1
46.121.154.90	Israel	147.237.0.121		Multiple Malformed HTTP Header Line from 46.121.154.90	Block	1
95.86.64.214	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
46.121.154.90	Israel	147.237.0.121		Multiple Abnormally Long Header Line from 46.121.154.90	Block	1
82.80.9.134	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 82.80.9.134 (Unknown SSL Session)	None	1
46.121.154.90	Israel	147.237.0.121		Illegal Byte Code Character in Header Name Â•9uÂ„	Block	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
213.57.60.47	Israel	147.237.0.121		PHP Attempt	Block	1
46.121.154.90	Israel	147.237.0.121		Illegal HTTP Version ÂƒeWMÂ’[[#0]]ÂŠ_dH	Block	1
46.19.85.181	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
46.121.154.90	Israel	147.237.0.121		Unknown HTTP Request Method Â†Ã?r{[[#22]]Ã‘-Â”Â?4Ã¢lÂ³Ã“ÂŸ /eÂ?[[#22]]N{Ã¾w[[#20]]Â?Ã¹cÂ©"Â„{,Â¤Ã«v.ÂŸÂ?HÃžaqÃ¬[[#22]][[#1]].[[#14]]ÂŠ [[#15]]eÂ¦ÃªÂ¢@pÃ¯Â•Ã”m2DÂ¯Ã³Â•<F in URL [[#26]]Â´×€p$fÂ?mâ,¬Ö»Ö·[[[#18]]×°[[#6]][â€Ž×?e.jÂŒÂ¡×“Â Â Â¾Ö³[[#28]]Â©jÂŽhÃ»Ö°pÂ?[[#30]]	Block	1
109.64.62.178	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
46.121.154.90	Israel	147.237.0.121		Illegal Byte Code Character in Header Value	Block	1
82.80.9.134	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
62.219.169.218	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
46.121.154.90	Israel	147.237.0.121		NULL Character in Header Name at YÃ³`Ã–Â©Â¡Â¦[[#17]]Â^Ã¶Ã²[[#17]]Â¼Ã—HÂ›AÃ¡[[#6]]Â„ eb[[#29]]Ã¯Âªâ±Â…[[#1]]Â¶Â¬iSaÂ³Â™ÂŸÃ‚nÃ©Â?[[#17]]Ã€yFN[[#18]]$4Â“Ã¸ mÂµÃ·Â^ [[#27]]>+ÂµÂ²XX&Ã¤Ã‚[[#3]]*D{[[#28]]Â¾Ã©ugi;Â?Ã½Ã£Â£h,[[#3]]2Â²[[#5]][[#6]]Ã²Â, Ã-Ã¦Ã¿rÃ?][[#20]]6Ã¿Â„Ã¨Ã’Ã´Ã¿[[#30]])[[#7]]Ã–%Ã·[Â,[[#26]]JÃ«Ã?Â®Â«Ã‹Â“Â› G[[#19]]SÂ?Ã…M[[#1]]ÂŸo.Â?ÃžÃ·h6Â Â?[[#19]]wH[[#29]] Â„Ã†Ã¤Â‰Â,Â†Ã¢ÃŠÂ›Ã¸ ^Ãº;Ã©fgÃŸ=[[#6]][[#24]]Â^!Ã“[[#6]][[#3]]EÃŠÂ…'Â‹Â¾Ã¢XC.Âƒ [[#23]]pÃ?Â¦pÂ”}[[#14]]Ã»Ã‹ÂƒRÃ’hÃƒÂ¿Ã?Â?ÂŽ[[#30]]Â´Ã¬.ÃŒÂŠÃ£	Block	1
46.121.154.90	Israel	147.237.0.121		Malformed HTTP Header Line 4	Block	1
93.172.155.64	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1
81.218.105.2	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPermitFilesNames in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
46.121.154.90	Israel	147.237.0.121		Abnormally Long Header Line request header name	Block	1
46.121.154.90	Israel	147.237.0.121		Multiple NULL Character in Header Name from 46.121.154.90	Block	1
212.199.121.196	Israel	147.237.0.121		Parameter Type Violation __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
46.121.154.90	Israel	147.237.0.121		Illegal Byte Code Character in Method Â†Ã?r{[[#22]]Ã‘-Â”Â?4Ã¢lÂ³Ã“ÂŸ /eÂ?[[#22]]N{Ã¾w[[#20]]Â?Ã¹cÂ©"Â„{,Â¤Ã«v.ÂŸÂ?HÃžaqÃ¬[[#22]][[#1]].[[#14]]ÂŠ [[#15]]eÂ¦ÃªÂ¢@pÃ¯Â•Ã”m2DÂ¯Ã³Â•<F	Block	1
84.228.133.239	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
5.102.196.53	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtMosad in www.miluim-ishi.aka.idf.il/valtamrequest	Block	1
46.121.154.90	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1