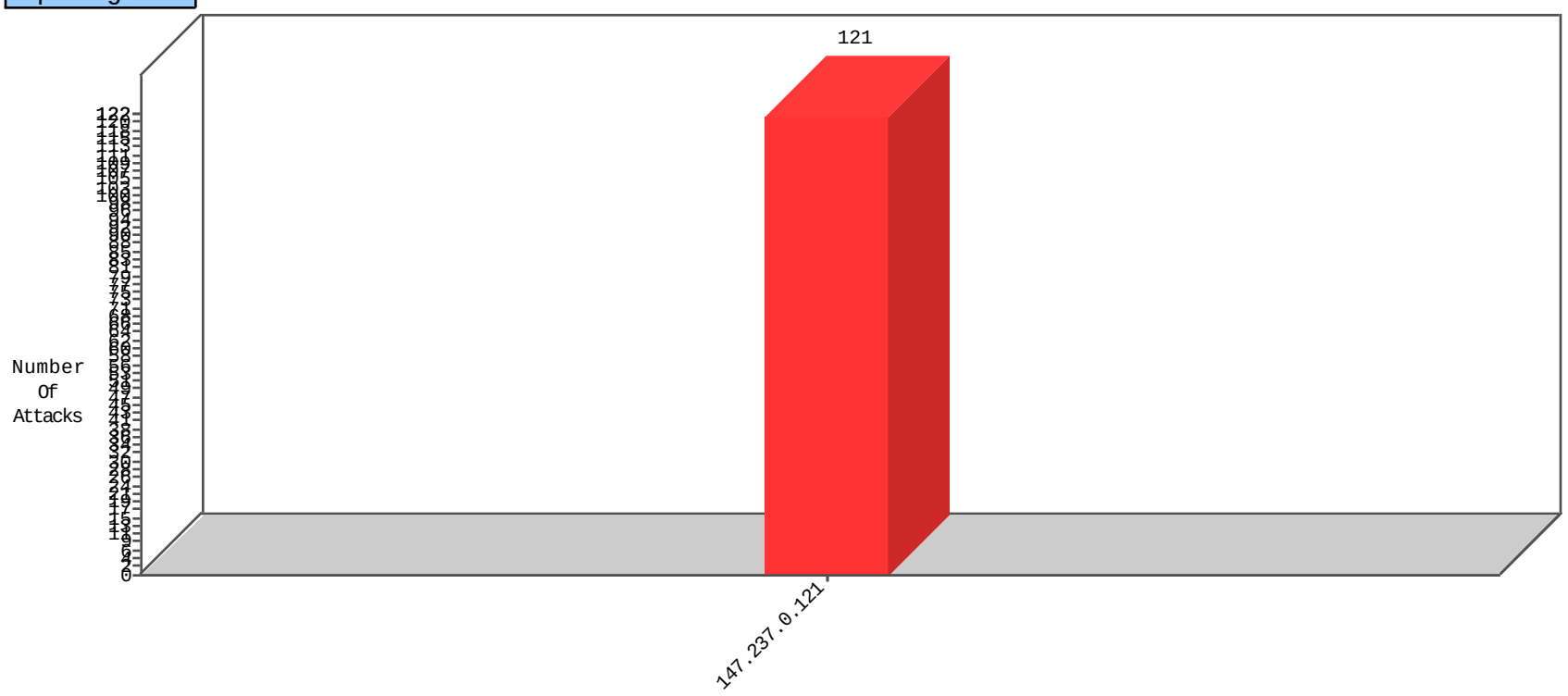
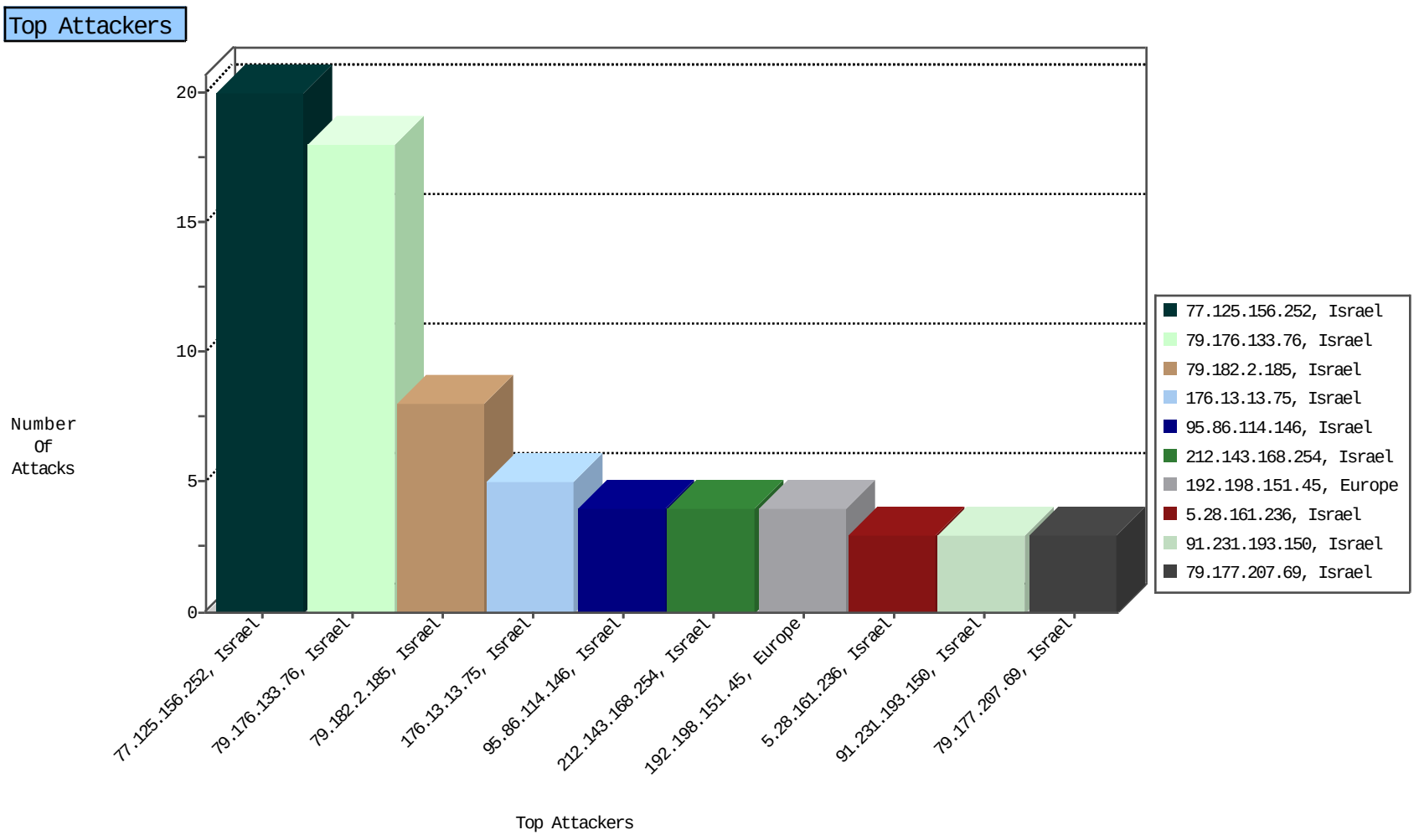
02-11-2016 to 02-12-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-11-2016 to 02-12-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
77.125.156.252	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	20
79.176.133.76	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	18
176.13.13.75	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	5

02-11-2016 to 02-12-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

02-11-2016 to 02-12-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	4
180.97.106.37	China	147.237.0.121		ET SCAN Potential SSH Scan	1

02-11-2016 to 02-12-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.88.28.233	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2069
149.88.6.6	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1416
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1283
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	779
194.42.67.50	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	586
139.181.48.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	514
134.191.232.70	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	481
181.141.14.135	Colombia	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	479
149.78.23.60	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	422
149.88.3.74	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	387
149.88.7.132	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	379
77.125.156.252	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	378
165.225.80.60	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	365
46.19.86.53	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	351
149.78.226.41	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	322
149.78.32.19	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	287
149.78.93.152	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	272
149.78.47.198	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	262
149.88.21.171	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	241
149.78.234.95	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	220
140.242.217.2	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	195
149.78.238.182	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	181
149.78.234.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	179
46.19.86.14	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
149.88.8.145	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
149.78.48.204	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	161
165.225.76.60	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
192.54.144.229	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	143
149.78.139.79	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	117
149.78.80.42	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	110
194.136.140.158	Finland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.88.5.63	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	105
149.78.34.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
82.80.33.138	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	86
2.54.169.56	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
108.171.133.166	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
17.78.99.52	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	80
149.88.44.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	77
108.171.128.166	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	76
212.235.103.211	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	69
81.218.241.25	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	65
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	63
149.88.89.230	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
40.114.210.53	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	60
109.66.149.86	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	54
149.88.112.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
37.142.216.5	Israel	147.237.0.121		Bad TCP sequence		monitor	49
149.78.197.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	48
17.78.123.15	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.143.168.254	Israel	147.237.0.121		Unauthorized HTTP Method	Block	4
95.86.114.146	Israel	147.237.0.121		Suspicious Response Code	Block	4
79.177.207.69	Israel	147.237.0.121		Suspicious Response Code	Block	3
5.28.161.236	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	3
79.176.192.175	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	2
62.219.44.242	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
192.198.151.44	Europe	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtTitle	Block	2
2.54.137.192	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.170.139	Israel	147.237.0.121		Suspicious Response Code	Block	2
109.253.210.135	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	2
85.64.225.242	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
37.142.134.34	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddIDCardDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
192.115.132.226	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
91.231.193.150	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 91.231.193.150 (Unknown SSL Session)	None	1
5.28.174.168	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
79.181.123.245	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
77.127.210.64	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.86.23	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
212.235.91.200	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	1
109.65.116.30	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
31.44.141.87	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
2.52.140.28	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.108.249.169	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
62.219.111.31	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
37.142.134.34	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
91.231.193.150	Israel	147.237.0.121		SSL Untraceable Connection - Unknown SSL Session	None	1
5.29.158.184	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
79.181.231.6	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
77.127.218.60	Israel	147.237.0.121		Unknown Parameter ch in www.miluim-ishi.aka.idf.il/login	Block	1
62.0.28.165	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
213.8.39.241	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
109.66.209.201	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected D0BDE1775D1ABD1FCE3895F0493DFAB01DF1A6B520783AC30E1734412F12AE3434CE7253885D2BF60ACA36C1D640B318F0FA523D5B9C175B20F5D71AB44A3DA7C7FDDDC48E3D0EB27FB3672DDDAC8F7A792DF106D0734ABDEC7EAF50D4E074A04682D6A101C1C1F3E4073816817735C4937E3863E91B08B7B5EFD86E566A3260, Observed E182F6D535C0BC894205AE4DE085690136ECB18A7BB709331D86CCDAE788FF9BBE60F2DEBC8702AF656128642EB2762984E0A225A7E3D8079DE9CC1068561FD1433CEF98EA1771C0BF755B101A33BC6F59BADCDC40B382FA7C09BC41F56673C79E3BB7	None	1
31.168.14.82	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
85.64.225.242	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 42594A3BF55790F1394C94E63AE91D2763FA012C6BCB640E208ADA9E659B5F0EAFB8DCD323C08FED41595C93B231DBACEB67D034D3FFEC92AFBFE59AB4C15AC903D841EC4BCE0C7234BAB1B91D56FD78F78FB959A6217C19543DF2A62834549C94D4465CC1868D61B1F4B0C5AB56C822635DB46650B00883A2C20F08B1617607, Observed 7CFF21D606A72F3DA3C36C22A55E46CC2E2EE49AE8EA5D839EFF9DDFCCC364C3716BE4C018260D1654DDEA4B16517D640334620B2717C8466BA7D95975026BBE5BB06DABF7898413380FB30D4EB3EB219E3BD39D7EB369E2B413B92CF0AE3CB5E17D64	None	1
79.178.189.112	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
62.219.135.44	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
37.142.134.34	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
91.231.193.150	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.32.229	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
77.127.218.60	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
62.0.34.93	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
37.142.68.50	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
79.179.15.135	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected F7C2D8C65D3701917882E48B43DE8F21B71417B1DED0F9872BA5469A6B8679943B65B3A53D3AE2E982F409648DCEC1CEBFC4233AAE903A781C4136EAE23959E6DCFB3072C12698ECA0C36159C2C5A5C58393CA80DE89F89568663B99F8ECDF168C3F93735CC80D3676B963B9A4AA1E0A43CD2EF0F7F0971A64F1074D09FD06D2, Observed 0AEA91DE2E29FC6923468904CB2DBB6099BE55587EB30D46E10C936B5C24828513F1EC5D7B5289354CBAFC4F3F322680244D2186F7EDCDBC62158B71B58B7A4BF9FF44E9B76E017C64A508C3DCAE5F997E4DDBAD5BA0A6925A74A8B26F0E828DD24FDC	None	1
77.125.81.165	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.102	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.143.169.21	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
5.255.253.47	Russian Federation	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.161.46	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1