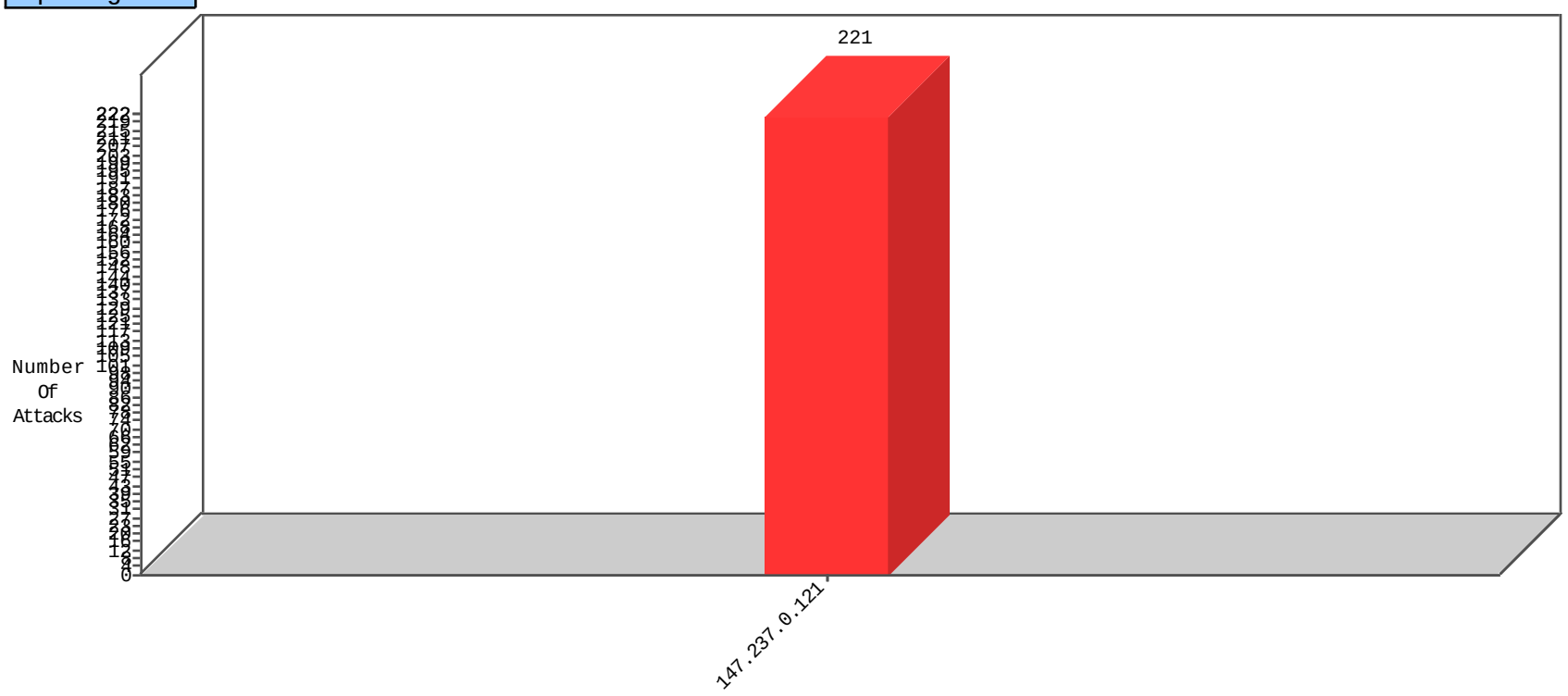
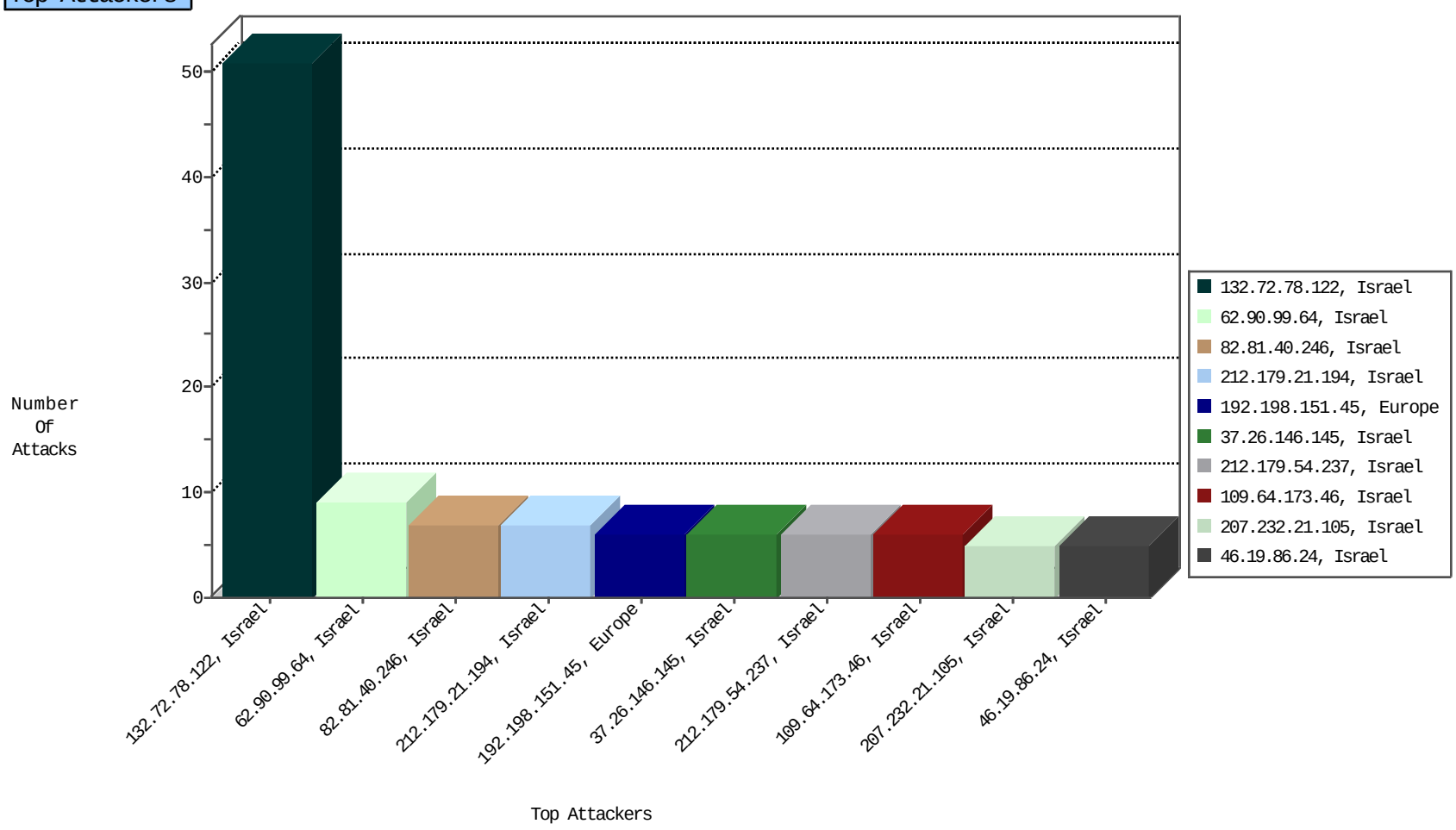
02-10-2016 to 02-11-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-10-2016 to 02-11-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.81.40.246	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	7
37.26.146.145	Israel	147.237.0.121		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	6
212.179.54.237	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	6
79.178.56.146	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	3
79.183.154.79	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BBL-Israel	2

02-10-2016 to 02-11-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

02-10-2016 to 02-11-2016

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)	6
66.249.81.254	United States	147.237.0.121		ET SCAN NMAP -sA (2)	1
109.235.254.181	Turkey	147.237.0.121		ET SCAN NMAP -sS window 1024	1
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
109.235.254.181	Turkey	147.237.0.121		ET SCAN NMAP -f -sS	1
109.235.254.181	Turkey	147.237.0.121		ET SCAN NMAP -sS window 2048	1

02-10-2016 to 02-11-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
165.225.76.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1663
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	835
149.88.146.176	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	575
149.78.93.183	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	544
199.207.253.101	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	498
149.78.60.229	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	411
165.225.80.69	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	402
63.99.16.220	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	397
149.78.34.82	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	384
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	371
108.171.128.165	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	342
192.88.162.1	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	333
82.166.140.117	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	333
149.88.154.143	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	325
144.24.20.230	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	309
149.78.143.90	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	308
46.5.0.6	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	280
149.78.245.36	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	274
149.78.18.192	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	273
149.78.197.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	241
149.78.46.50	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	220
193.222.161.6	Switzerland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	196
2.52.190.66	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
189.203.255.99	Mexico	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	177
149.78.184.96	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	169
149.78.186.225	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
149.78.31.201	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	158
92.111.149.92	Netherlands	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	156
77.127.44.226	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
149.78.40.74	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	152
2.54.131.248	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
188.6.184.175	Hungary	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	128
149.88.101.173	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	121
90.206.225.31	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	120
78.48.250.153	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
167.220.196.138	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	86
149.88.202.196	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
149.88.30.232	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	83
149.88.44.189	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
149.78.35.26	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	79
93.73.2.157	Ukraine	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	77
149.78.27.2	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	75
93.85.92.218	Belarus	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.88.141.241	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
149.78.245.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	70
149.88.13.66	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	67
149.78.102.251	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	66
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	57
149.78.239.124	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56
149.88.196.149	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	56

02-10-2016 to 02-11-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
132.72.78.122	Israel	147.237.0.121		Too Many of the Same Response Code (404) in Session from 132.72.78.122	Block	50
109.64.173.46	Israel	147.237.0.121		Suspicious Response Code	Block	6
46.19.86.24	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	4
62.219.44.242	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	4
192.198.151.44	Europe	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected 520E8083647F28171DD714D51B1257C4CD512DB1F29C4B79433F2F9C543EE2D990D91724DB6397B5D8D909FD9265B26198FC372D2CB5B6BB2F54416E15FFA6794397B4CF19D73F163C2CBA89EFF07F8AC27D8DA5786B2B84979B25052FA9CF997001125B80527821665A3C7967C2A3B51830340119331105F36C329D4A26B8B0, Observed 149EAED771573D571BE012D9D9CE05223358A79F01F01B28AC912FE29447053AFB4AC20DFB4DEF4530D7CCCCB488CF8CE19B8E5EA8F614CBD3138B0809C4849FEB9A07B4C4074C997E613A2B42C0E286AED6A731113C86D867B899DBA6025F4204A2B7	None	3
147.234.241.1	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	3
109.67.208.64	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	3
62.90.99.64	Israel	147.237.0.121		Suspicious Response Code	Block	3
213.57.34.171	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
212.179.21.194	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddTimetableDocs&FilesToSend in www.miluim-ishi.aka.idf.il/uploadregister.axd	Block	2
95.35.0.216	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
207.232.21.105	Israel	147.237.0.121		Distributed Unknown Parameter on miluim-ishi.aka.idf.il/shamapchange parameter __EVENTTARGET	Block	2
138.134.102.16	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
5.29.38.47	Israel	147.237.0.121		Suspicious Response Code	Block	2
85.64.216.238	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/changeunit	Block	2
79.180.155.239	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
62.219.50.56	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	2
212.235.56.185	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
62.90.58.17	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	2
192.198.151.44	Europe	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	2
79.182.176.18	Israel	147.237.0.121		Suspicious Response Code	Block	2
46.19.86.157	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.21.194	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTimetableFilesNames in www.miluim-ishi.aka.idf.il/valtamrequest	Block	2
31.154.29.94	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.69.105.56	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
207.232.21.105	Israel	147.237.0.121		Unknown Parameter ctl00$s_id in www.miluim-ishi.aka.idf.il/shamapchange	Block	1
2.54.58.45	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
193.169.70.108	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
84.108.117.227	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/gen204	Block	1
79.182.210.37	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
185.27.105.95	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
109.186.167.8	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
77.126.10.110	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
46.117.4.163	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
31.168.66.36	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.86.22	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.108.104.201	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 84.108.104.201 (sigalgs DoS Attack)	None	1
192.115.190.190	Israel	147.237.0.121		Unknown Parameter _ in www.miluim-ishi.aka.idf.il/newpassword/forgotpassword	Block	1
79.179.60.48	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
212.199.118.130	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.65.124.199	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
87.69.136.250	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
46.19.86.33	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
212.179.21.194	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
193.238.190.30	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
84.108.161.46	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
81.218.190.37	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
188.120.154.220	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
132.72.78.122	Israel	147.237.0.121		Too Many 404: Response Code per Session	Block	1
77.127.176.185	Israel	147.237.0.121		Parameter Type Violation ctl00_ContentPlaceHolder1_fuAddAddressAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
213.57.142.166	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
62.0.102.190	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
212.179.21.194	Israel	147.237.0.121		Unknown Parameter ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/smsverify	Block	1
95.86.83.221	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
37.46.43.10	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
207.232.21.105	Israel	147.237.0.121		Unknown Parameter __EVENTARGUMENT in www.miluim-ishi.aka.idf.il/shamapchange	Block	1
84.108.104.201	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.65.126.248	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
93.172.53.122	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.104	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1

02-10-2016 to 02-11-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/shamapchange	Block	1
5.102.197.227	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
194.90.25.90	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
84.228.196.177	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
82.80.153.251	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00$txtNewPass1 in www.miluim-ishi.aka.idf.il/personalsettings	Block	1
192.115.190.190	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 192.115.190.190 (Open Mode)	None	1
79.176.208.111	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
217.132.58.82	Israel	147.237.0.121		Distributed Unauthorized URL Access on www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
212.199.118.130	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddMarriageCertDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
85.250.242.142	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
46.19.86.24	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
207.232.21.105	Israel	147.237.0.121		Unknown Parameter __EVENTVALIDATION in www.miluim-ishi.aka.idf.il/shamapchange	Block	1
2.52.163.154	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.104.201	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.147.0	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
77.125.90.243	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
212.235.98.139	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
94.230.86.2	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
195.212.29.172	Europe	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
85.64.86.22	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 85.64.86.22 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
82.80.196.44	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
192.115.190.190	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
132.73.205.94	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
79.176.209.82	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
217.132.97.85	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/shamapchange	Block	1
212.199.118.130	Israel	147.237.0.121		Unknown Parameter ctl00_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
109.65.31.234	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1

02-10-2016 to 02-11-2016