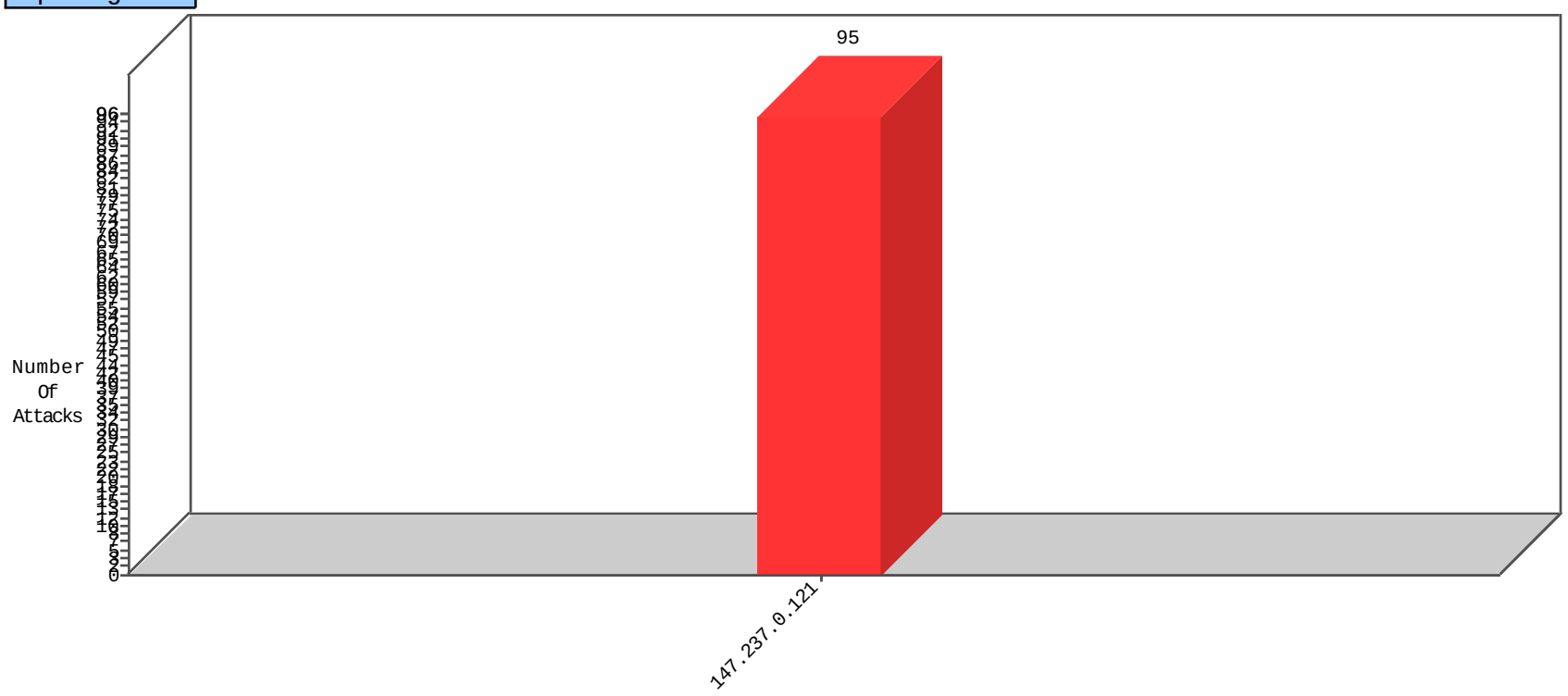
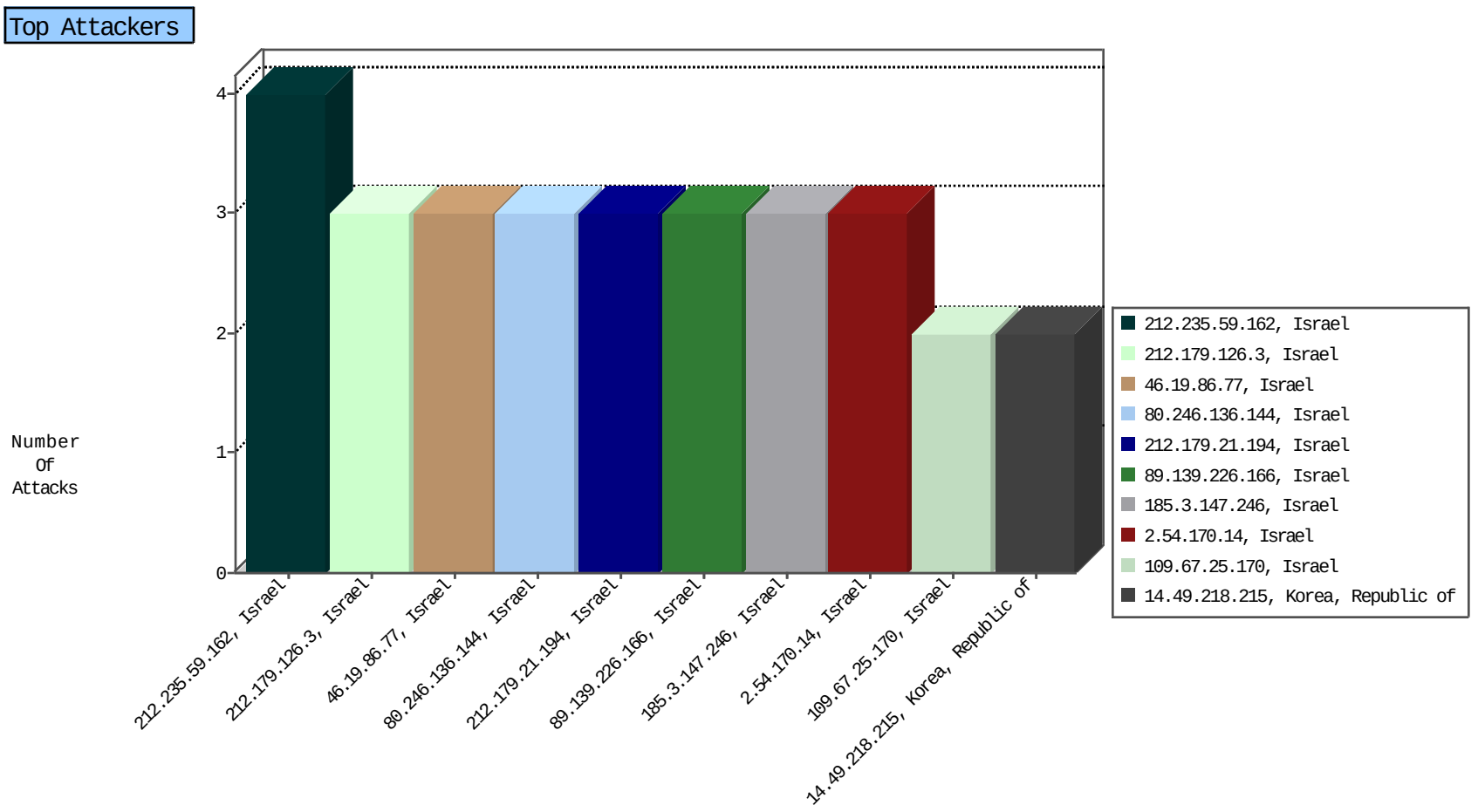
01-06-2016 to 01-07-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



01-06-2016 to 01-07-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
14.49.218.215	Korea, Republic of	147.237.0.121		Frk_Under_Attack_Con_Tcp	drop	BBL-Frankfurt	2

01-06-2016 to 01-07-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

01-06-2016 to 01-07-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
89.248.162.131	Netherlands	147.237.0.121		ET SCAN Potential SSH Scan	1
188.227.16.76	Russian Federation	147.237.0.121		ET SCAN Potential SSH Scan	1
208.67.1.94	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
24.121.225.29	United States	147.237.0.121		ET SCAN NMAP -sS window 1024	1
174.142.97.6	Canada	147.237.0.121		ET SCAN Potential SSH Scan	1
192.198.151.45	Europe	147.237.0.121		ET SCAN NMAP -sA (2)	1
219.138.49.165	China	147.237.0.121		ET SCAN Potential SSH Scan	1

01-06-2016 to 01-07-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1896
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1607
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1402
149.78.29.41	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	915
149.88.13.144	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	672
2.52.178.45	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
110.173.190.4	India	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	436
213.8.204.37	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
192.114.23.208	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	243
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	235
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	203
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	166
149.78.62.113	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	160
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	141
2.52.24.221	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	140
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	129
149.78.47.118	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	113
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	107
149.78.29.95	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	100
194.90.119.124	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	61
40.77.167.95	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
157.55.39.75	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
2.52.178.45	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.182.229.1	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
40.77.167.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
149.78.236.247	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	29
149.88.190.121	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
173.245.115.78	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
37.26.146.146	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
149.78.31.17	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
138.134.192.10	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	26
149.88.20.22	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
79.181.127.122	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	25
192.114.91.232	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	25
66.249.64.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
192.117.110.4	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
2.52.24.221	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	22
2.52.24.221	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	22
2.52.24.221	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	22
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
66.249.64.175	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
149.78.60.229	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
37.46.39.182	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	18
209.135.211.211	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.81.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.69.106	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
149.78.109.19	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15
54.243.190.43	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	15

01-06-2016 to 01-07-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.235.59.162	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	4
212.179.21.194	Israel	147.237.0.121		Suspicious Response Code	Block	3
212.179.126.3	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	3
185.3.147.246	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	3
80.246.136.144	Israel	147.237.0.121		Suspicious Response Code	Block	3
89.139.226.166	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	3
62.219.115.220	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	2
213.8.245.50	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	2
80.74.103.200	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	2
82.166.237.252	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
31.154.17.182	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	2
109.67.25.170	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	2
2.54.170.14	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.94.172.77	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	2
199.203.215.1	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	2
212.150.161.210	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
81.218.71.132	Israel	147.237.0.121		Double URL Encoding - parameter: ReturnUrl in www.miluim-ishi.aka.idf.il/login	Block	1
194.90.15.61	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
147.235.236.1	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.19.86.77	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
2.54.176.122	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.126.149	Israel	147.237.0.121		Distributed Double URL Encoding	Block	1
84.109.16.83	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https:/www.miluim-ishi.aka.idf.il/	Block	1
212.143.90.173	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
79.181.135.240	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtTitle in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
192.114.105.254	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
46.19.86.209	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.209 (sigalgs DoS Attack)	None	1
31.168.13.78	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.253.159.73	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
93.172.247.177	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
2.52.154.4	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
82.166.200.226	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
77.127.200.1	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
194.177.16.3	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
165.72.200.11	Europe	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.77	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.109.70	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
109.66.215.51	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
84.111.180.87	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
212.143.186.38	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
46.19.86.209	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.118.36.53	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
37.26.147.241	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
132.68.141.22	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
93.173.8.210	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 93.173.8.210 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
2.54.170.14	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.177.209.236	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
198.20.69.74	United States	147.237.0.121		Unauthorized URL Access to 147.237.0.121/	Block	1
46.19.86.83	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.83 (sigalgs DoS Attack)	None	1
87.68.252.85	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$ctl00 in www.miluim-ishi.aka.idf.il/form3010	Block	1
2.52.143.73	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.52.143.73 (sigalgs DoS Attack)	None	1
212.143.186.38	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
46.121.223.148	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
192.198.151.44	Europe	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ctl00$ContentPlaceHolder1$txtPerutBakasha	Block	1
132.76.50.5	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
46.19.86.77	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.86.77 (sigalgs DoS Attack)	None	1
93.173.8.210	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
212.199.106.82	Israel	147.237.0.121		Unknown Parameter returnurl in www.miluim-ishi.aka.idf.il/login	Block	1
79.181.135.240	Israel	147.237.0.121		Parameter Type Violation ctl00$ContentPlaceHolder1$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
185.127.10.35		147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/form3010 parameter ctl00$ContentPlaceHolder1$ctl00	Block	1
46.19.86.83	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1

01-06-2016 to 01-07-2016

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.168.13.78	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
109.253.159.73	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 109.253.159.73 (sigalgs DoS Attack)	None	1
2.52.143.73	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1

01-06-2016 to 01-07-2016