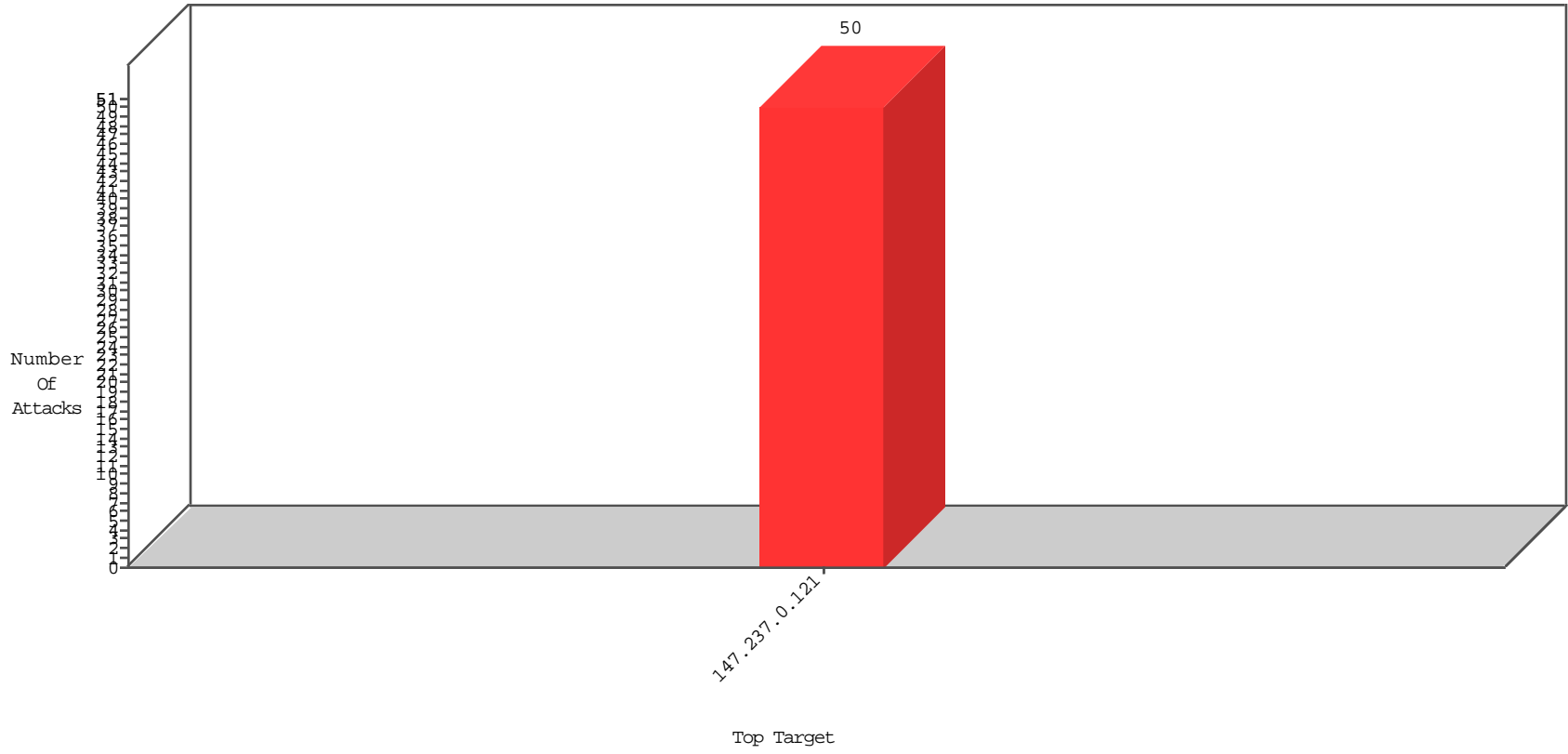


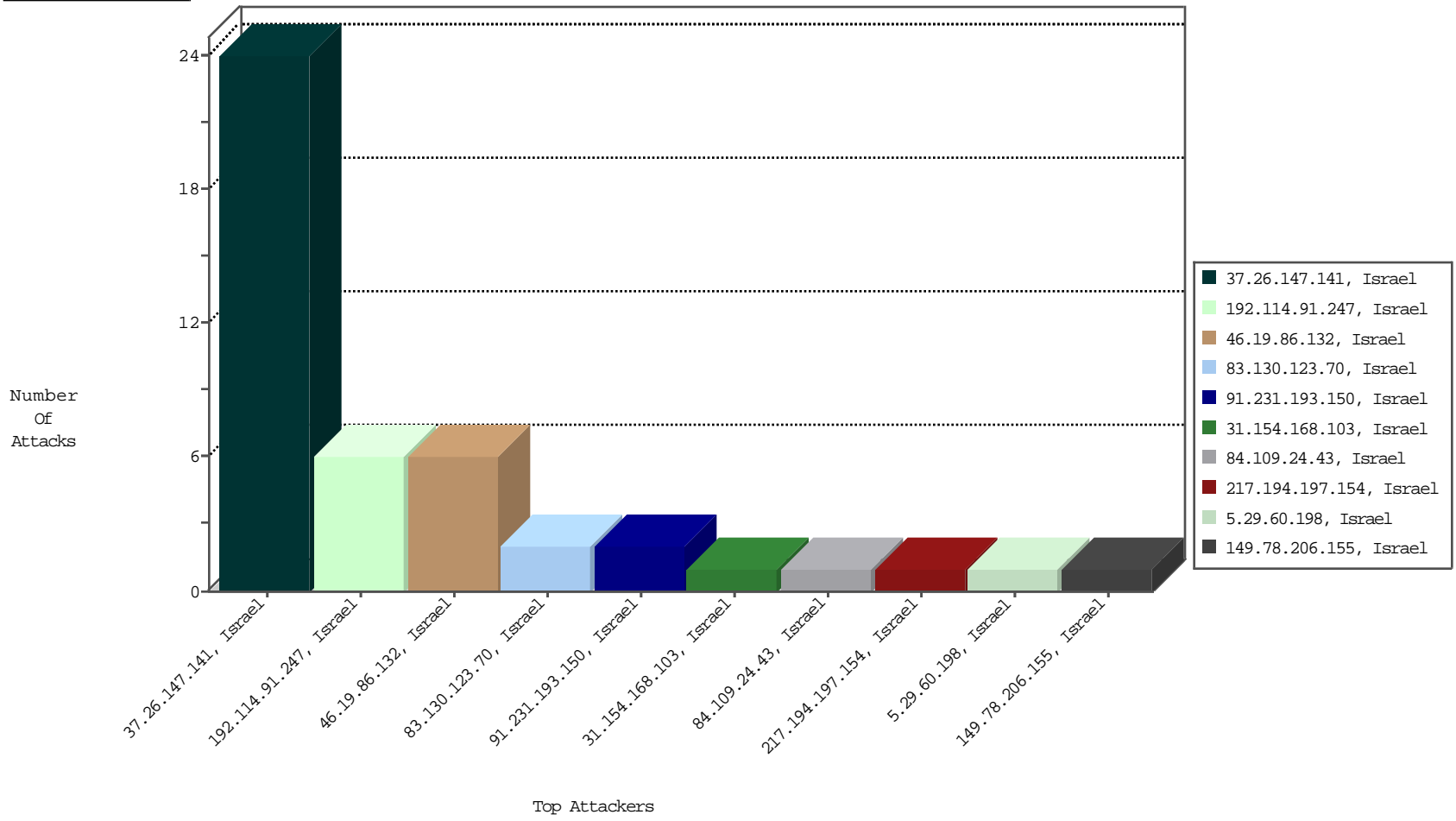
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
37.26.147.141	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	23
46.19.86.132	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	dest-reset	BBL-Israel	6

04-07-2016-13:06:00 to 04-07-2016-14:06:00

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
------------------	--------------	----------------	------	-----------	-------

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
149.88.146.176	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	511
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	448
199.207.253.101	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	336
66.249.78.244	United States	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
83.130.123.70	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
192.146.6.2	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	125
46.19.86.132	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
17.78.122.217	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	41
167.220.196.117	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	37
194.177.16.3	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	36
17.78.99.182	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	33
17.78.122.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.7.186	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
213.57.76.56	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	8
157.55.39.217	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	5
62.219.224.138	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.181.51.233	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.131.77	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	2
87.69.1.26	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
149.50.8.20	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
5.102.254.23	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.127	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.88.81.78	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.228.144.200	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.127	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

04-07-2016-13:06:00 to 04-07-2016-14:06:00

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
91.231.193.150	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.199.180.36	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
84.109.24.43	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
149.78.206.155	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
5.29.60.198	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
217.194.197.154	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
85.250.233.188	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.118.22.242	Israel	147.237.0.121		Parameter Type Violation accept in www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx	Block	1
31.154.168.103	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/login parameter ct100\$ContentPlaceHolder1\$txtPass	Block	1
195.62.30.20	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceHolder1\$txtPerutBakasha	Block	1
37.26.147.141	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$ct100 in www.miluim-ishi.aka.idf.il/form3010	Block	1
128.139.14.56	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPass in www.miluim-ishi.aka.idf.il/login	Block	1

04-07-2016-13:06:00 to 04-07-2016-14:06:00