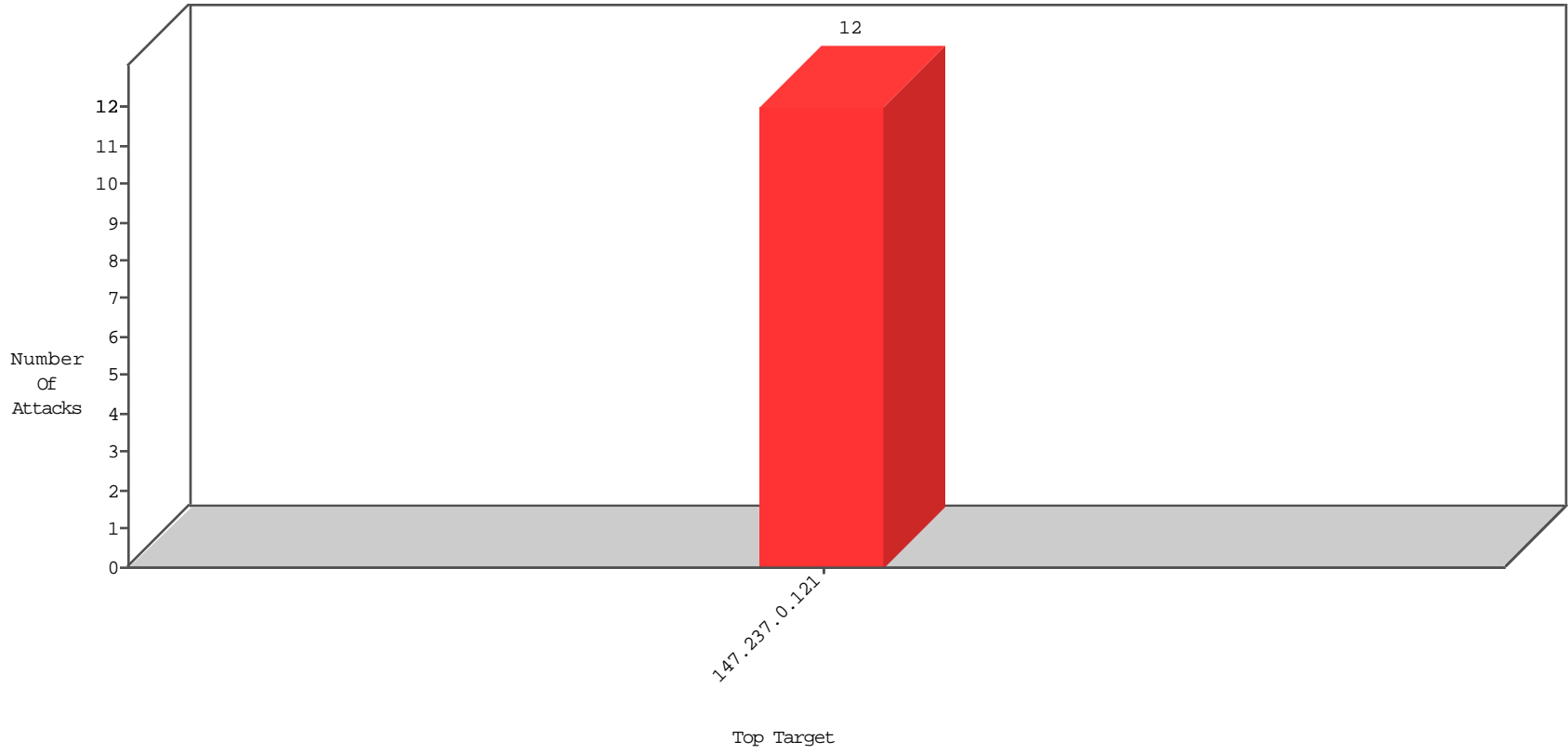


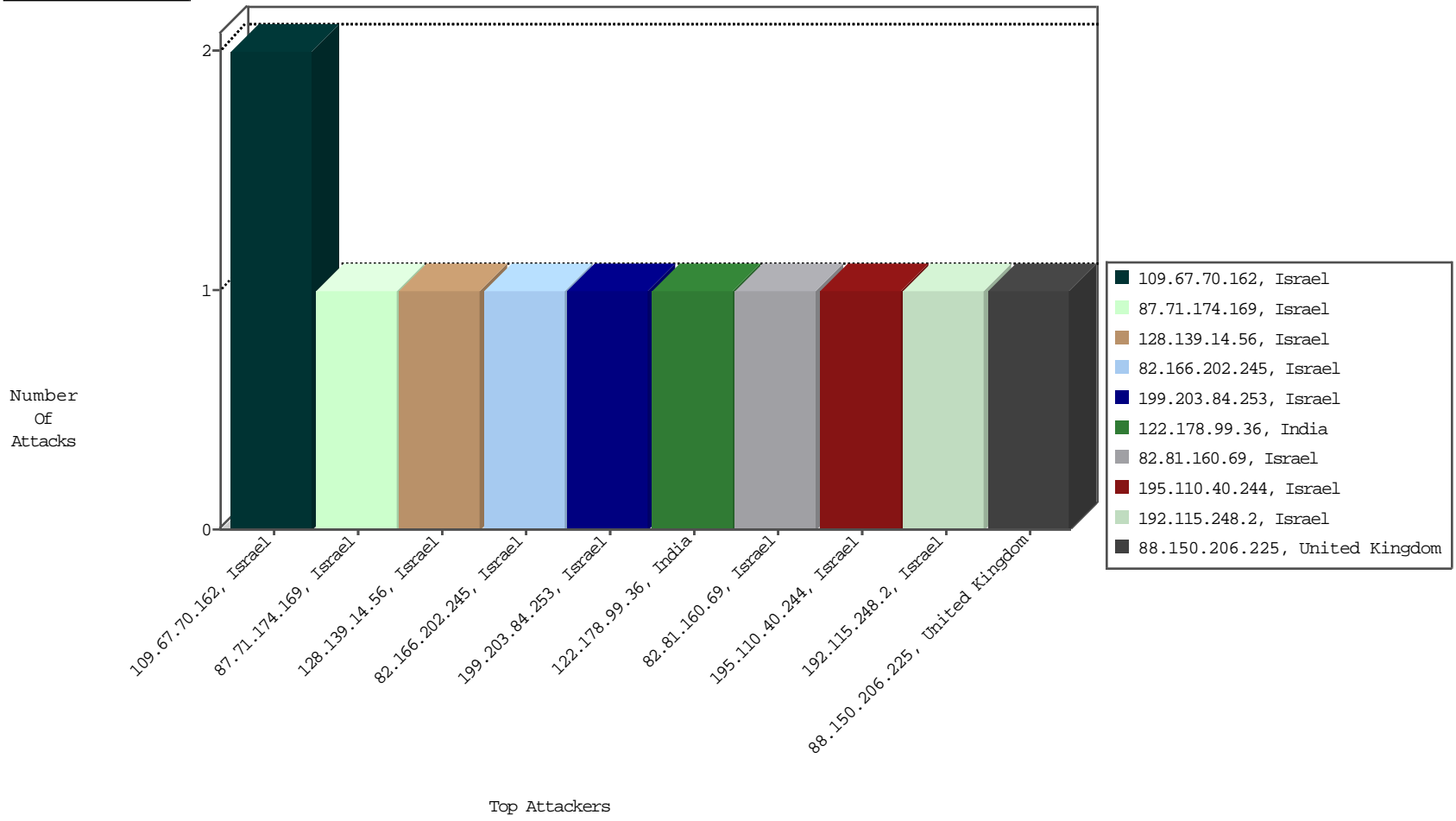
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
88.150.206.225	United Kingdom	147.237.0.121		Block_Udp_All_Nets	drop	NetV-London	1

04-10-2016-13:06:08 to 04-10-2016-14:06:08

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
122.178.99.36	India	147.237.0.121		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
167.220.196.142	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	166
2.54.148.77	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
74.91.23.166	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	117
17.78.122.156	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
2.53.26.118	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	50
192.115.177.203	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
2.53.26.118	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	47
193.62.194.254	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	43
109.64.21.57	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	35
2.53.26.118	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
2.53.26.118	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	25
149.88.148.33	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.88.62.22	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
23.81.90.154	United States	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	20
167.220.196.97	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
17.78.122.217	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.102.6.90	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
194.90.178.37	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	16
66.102.9.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
2.54.160.16	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	9
2.54.160.16	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	9
2.54.160.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.160.16	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	9
2.54.160.16	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.139.45	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	8
159.203.166.164	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	7
185.32.179.182	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.46.39.0	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	5
87.71.174.169	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	5
185.3.144.76	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	4
80.246.139.45	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	4
149.88.179.62	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4
87.71.174.169	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	4
31.210.186.50	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	4
199.203.215.1	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	3
199.203.215.1	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	3
37.46.38.207	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2
80.246.139.45	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.116.18.30	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
37.26.147.216	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
2.54.172.117	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.218.241.26	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.255.250	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
109.67.70.162	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
46.116.18.30	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
212.179.21.194	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.29	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.161	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.67.70.162	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesNames in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
195.110.40.244	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
82.81.160.69	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddPartnerAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	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
199.203.84.253	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/generalpetition	Block	1
82.166.202.245	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluim-ishi.aka.idf.il/ajax/order/confirmorder.aspx parameter accept	Block	1
149.50.32.26	Israel	147.237.0.121		Distributed Cookie Tampering on token: .ASPXAUTH	None	1
87.71.174.169	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
192.115.248.2	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected NA, Observed E769B52842D5E7FF6B1A557A82C7A4824970B40C4100A07565654B9E9E5D75976C66F407AF37 5976D9EBFFD8BEC87755957B3E8ACFCF00E7D5A3C4D915DE859DA4DEC5BF33CC648777347256 D1E29BDBC4E3BF129735EC3C791E1E92C87821F34DD6C391F0DD3DDB5A6F161675E0D00F740A 42F78E00F91DB068DD67D0FC55AB9E88D384F94381A5CFBD636DA1FFAB0EF1F1AFAD1175865B 73597F340FD217AC	None	1