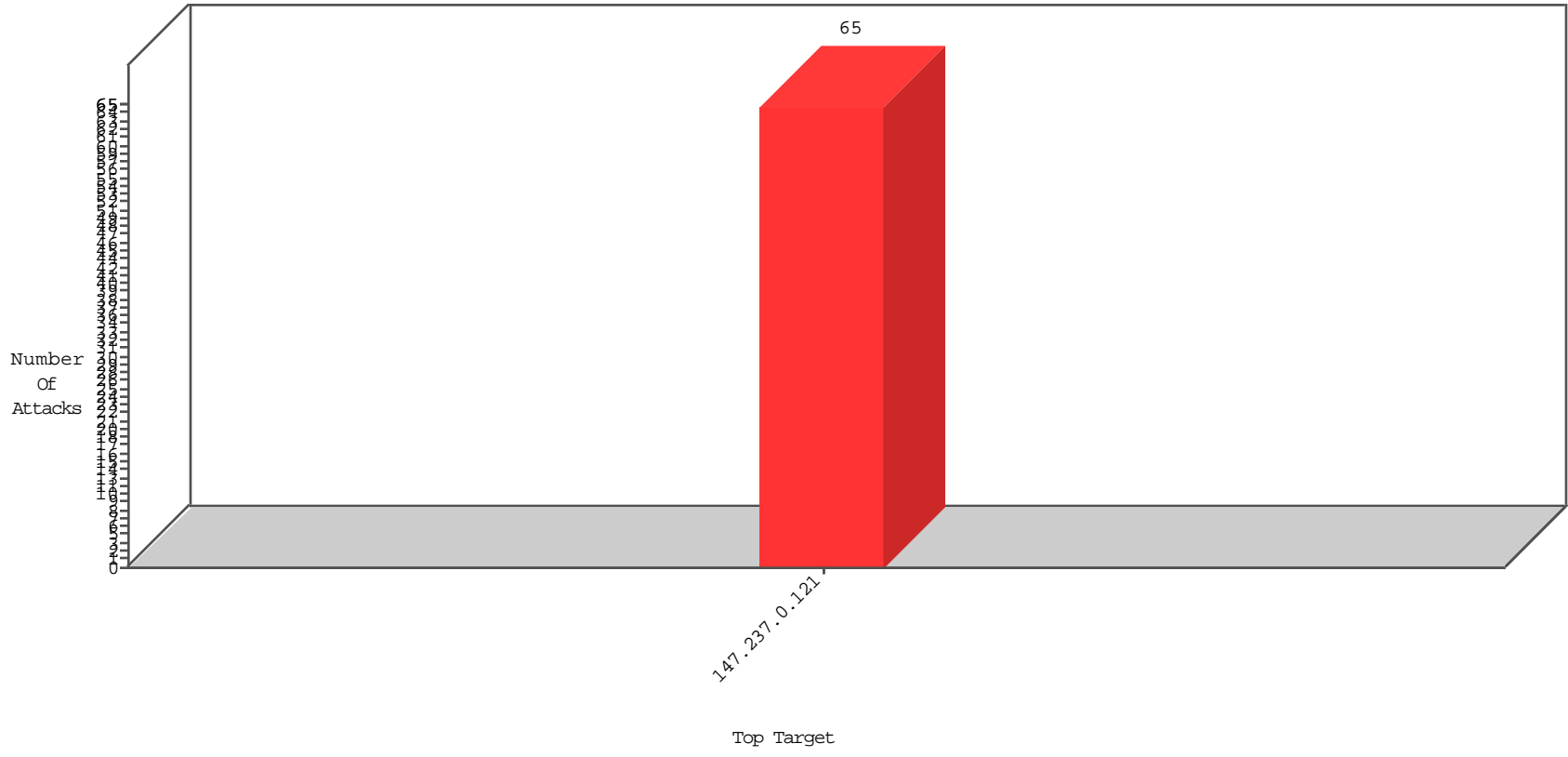


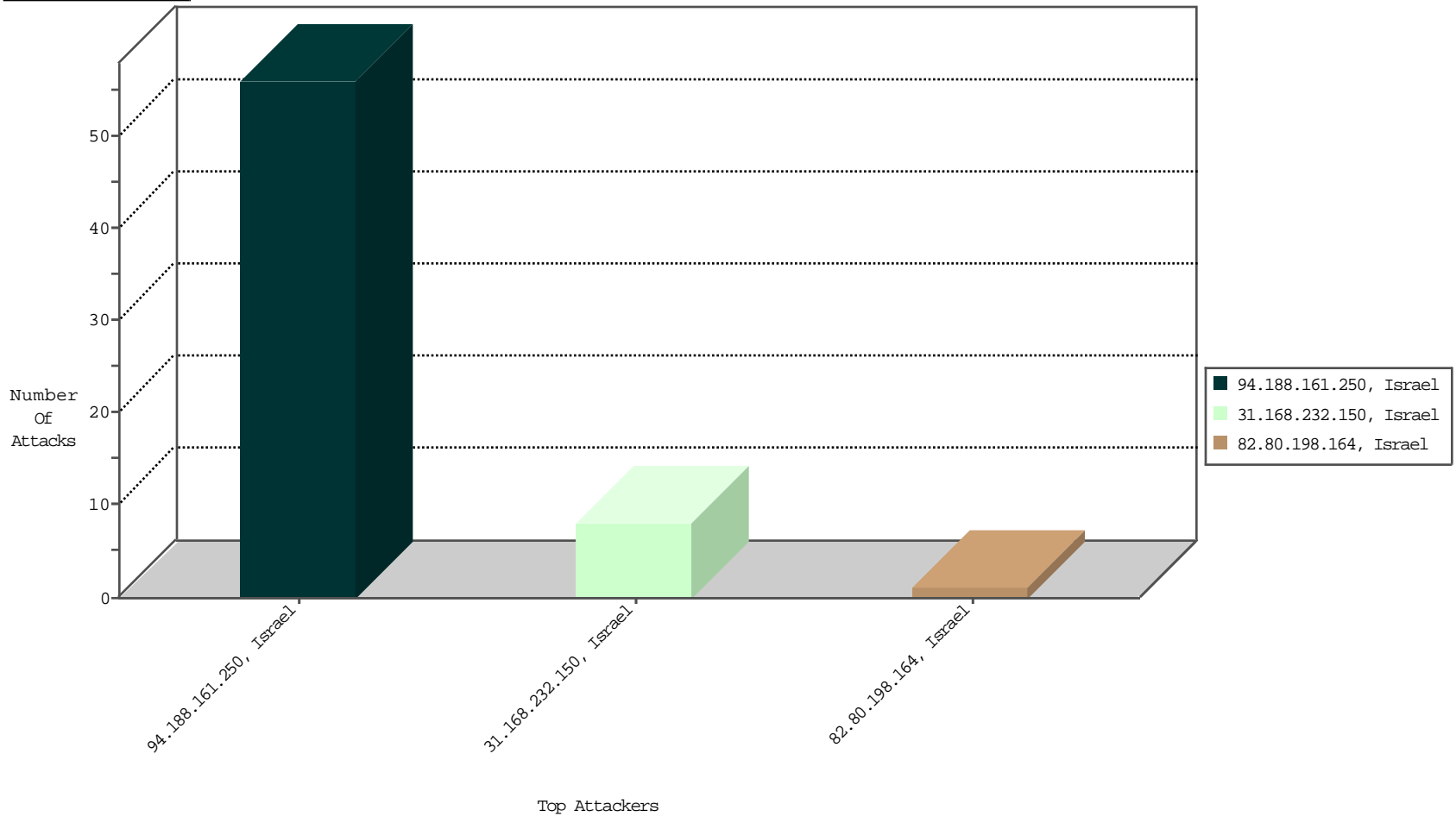
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
31.168.232.150	Israel	147.237.0.121		Block_Udp_All_Nets	drop	EEL-Isreal	8

04-07-2016-15:06:01 to 04-07-2016-16:06:01

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
199.207.253.101	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	547
212.179.50.200	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	232
199.207.253.96	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	180
54.240.197.227	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	165
93.172.246.14	Israel	147.237.0.121		Bad TCP sequence		monitor	144
54.240.197.226	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	74
149.88.140.207	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	73
130.119.13.66	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	46
85.68.1.30	France	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
93.172.246.14	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	36
93.172.246.14	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
93.172.246.14	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
17.78.99.182	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	35
94.188.161.250	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	32
54.240.197.225	Ireland	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
149.88.242.84	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
149.88.86.132	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	19
149.88.40.45	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	10
84.229.248.7	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	4
142.105.39.9	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4
212.25.82.123	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	4
84.229.248.7	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	4
84.229.248.7	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	4
193.37.129.170	Israel	147.237.0.121		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.67.154.47	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.6	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
62.128.48.34	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
5.29.52.29	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1
109.67.154.47	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
194.90.66.15	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
5.29.52.29	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
212.179.21.194	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.227	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.67.154.47	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	1
193.37.129.170	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
94.188.161.250	Israel	147.237.0.121		Multiple Malformed URL from 94.188.161.250	Block	5
94.188.161.250	Israel	147.237.0.121		Multiple Unknown HTTP Request Method from 94.188.161.250	Block	5
94.188.161.250	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Method from 94.188.161.250	Block	5
94.188.161.250	Israel	147.237.0.121		Multiple Abnormally Long Request from 94.188.161.250	Block	4
94.188.161.250	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Name from 94.188.161.250	Block	4
94.188.161.250	Israel	147.237.0.121		Multiple Abnormally Long Header Line from 94.188.161.250	Block	4
94.188.161.250	Israel	147.237.0.121		Distributed Parameter Type Violation on www.miluum-ishi.aka.idf.il/generalpetition parameter ct100\$ContentPlaceholder1\$txtPerutBakasha	Block	3
94.188.161.250	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 94.188.161.250 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
94.188.161.250	Israel	147.237.0.121		Multiple Illegal Byte Code Character in URL from 94.188.161.250	Block	2
94.188.161.250	Israel	147.237.0.121		Multiple NULL Character in Header Name from 94.188.161.250	Block	2
94.188.161.250	Israel	147.237.0.121		Multiple Illegal Byte Code Character in Header Value from 94.188.161.250	Block	2
94.188.161.250	Israel	147.237.0.121		NULL Character in URL	Block	1
94.188.161.250	Israel	147.237.0.121		Illegal Byte Code Character in Parameter Name [[#30]]HD>[[#25]]!`µ°[[#23]] !¶[[#22]] [[#20]][[#8]]~r'x [[#24]]w\$%·*[[#22]]± a·'W@%E ¶y in	Block	1
82.80.198.164	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
94.188.161.250	Israel	147.237.0.121		Malformed HTTP Header Line 3	Block	1
94.188.161.250	Israel	147.237.0.121		Illegal Byte Code Character in Header Name [[#22]]δ²Q+jØ·«\$Eè[[#26]]^'...%ž+[[#28]]Æ@·xârF3	Block	1
94.188.161.250	Israel	147.237.0.121		Unknown HTTP Request Method ·8øø[[#6]]epUrFÿ[[#6]]¹_†@'c{vî@>~lvW?æ7[[#4]]è	Block	1
94.188.161.250	Israel	147.237.0.121		Illegal Byte Code Character in Query String [[#30]]HD>[[#25]]!`µ°[[#23]] !¶[[#22]] [[#20]][[#8]]~r'x [[#24]]w\$%·*[[#22]]± a·'W@%E ¶y on	Block	1
94.188.161.250	Israel	147.237.0.121		Abnormally Long Header Line request header name	Block	1
94.188.161.250	Israel	147.237.0.121		NULL Character in Header Name at ù3,£[[#11]][[#20]]ÖÁ¼ÑÈ[[#5]]Èî"[[#0]];kfc	Block	1
94.188.161.250	Israel	147.237.0.121		Multiple Illegal HTTP Version from 94.188.161.250	Block	1
94.188.161.250	Israel	147.237.0.121		Malformed URL	Block	1
94.188.161.250	Israel	147.237.0.121		Illegal Byte Code Character in Header Value	Block	1
94.188.161.250	Israel	147.237.0.121		Multiple NULL Character in Method from 94.188.161.250	Block	1
94.188.161.250	Israel	147.237.0.121		Illegal Byte Code Character in URL	Block	1
94.188.161.250	Israel	147.237.0.121		Abnormally Long Request method	Block	1
94.188.161.250	Israel	147.237.0.121		NULL Character in Method U·A,,P»5Wq*`îifèYž`Td'v^!%æ''°)[[#4]][[#12]]ó)ýÈ,2Š,Ð¶, G=dW:tba-É_,-ð@Òqý¶, [[#0]]^[[#0]]E[[#11]]%e ,8šmÄ)5"[[#29]]x±-h[[#28]]Èøq+[[#6]]e{ts'É'[[#16]]@[[#6]]bj<)[[#19]]#í,[[#1]]žE^²[[#15]]È¼µ*f+Y""	Block	1
94.188.161.250	Israel	147.237.0.121		Multiple Malformed HTTP Header Line from 94.188.161.250	Block	1
94.188.161.250	Israel	147.237.0.121		Illegal Byte Code Character in Method ·8øø[[#6]]epUrFÿ[[#6]]¹_†@'c{vî@>~lvW?æ7[[#4]]è	Block	1
94.188.161.250	Israel	147.237.0.121		Illegal HTTP Version	Block	1