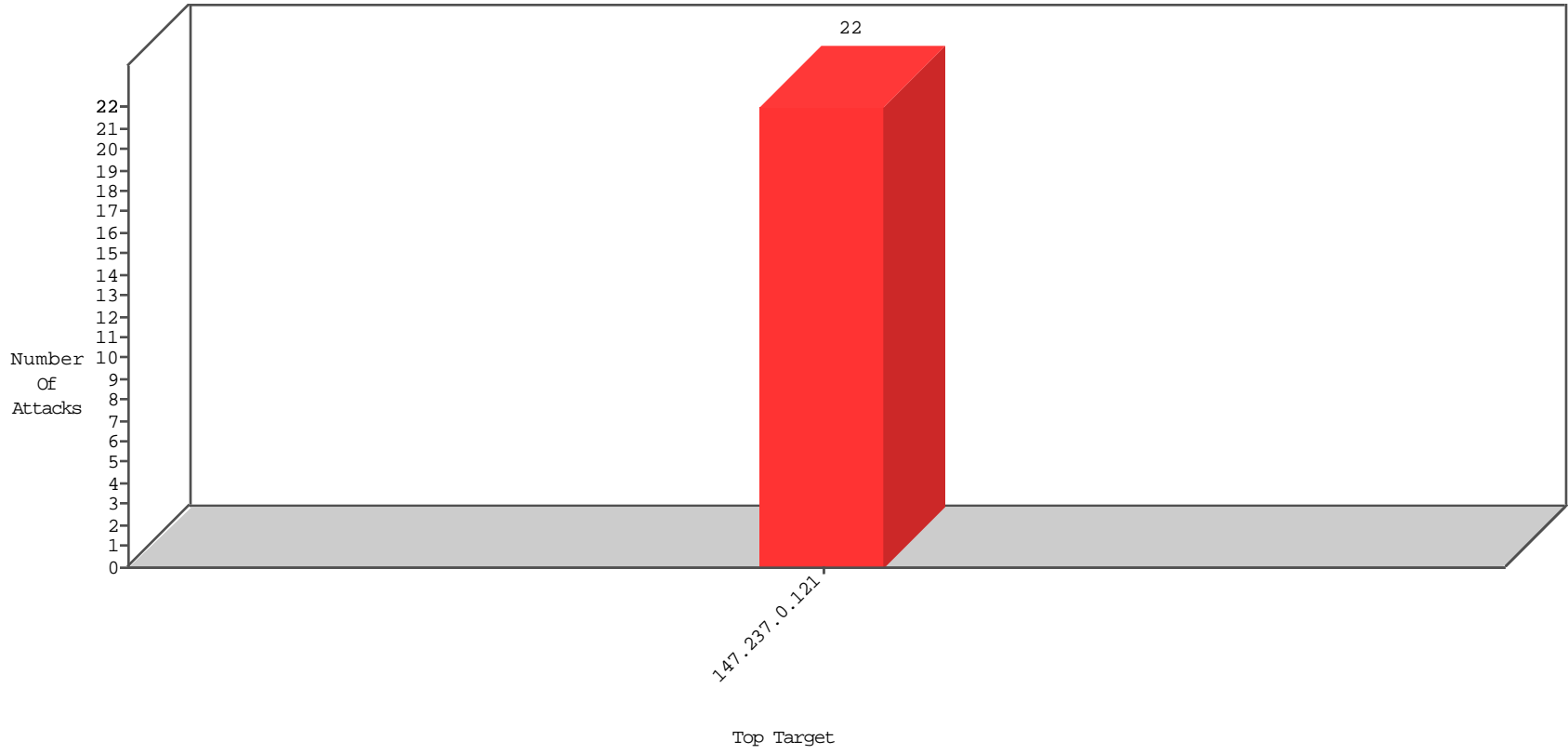


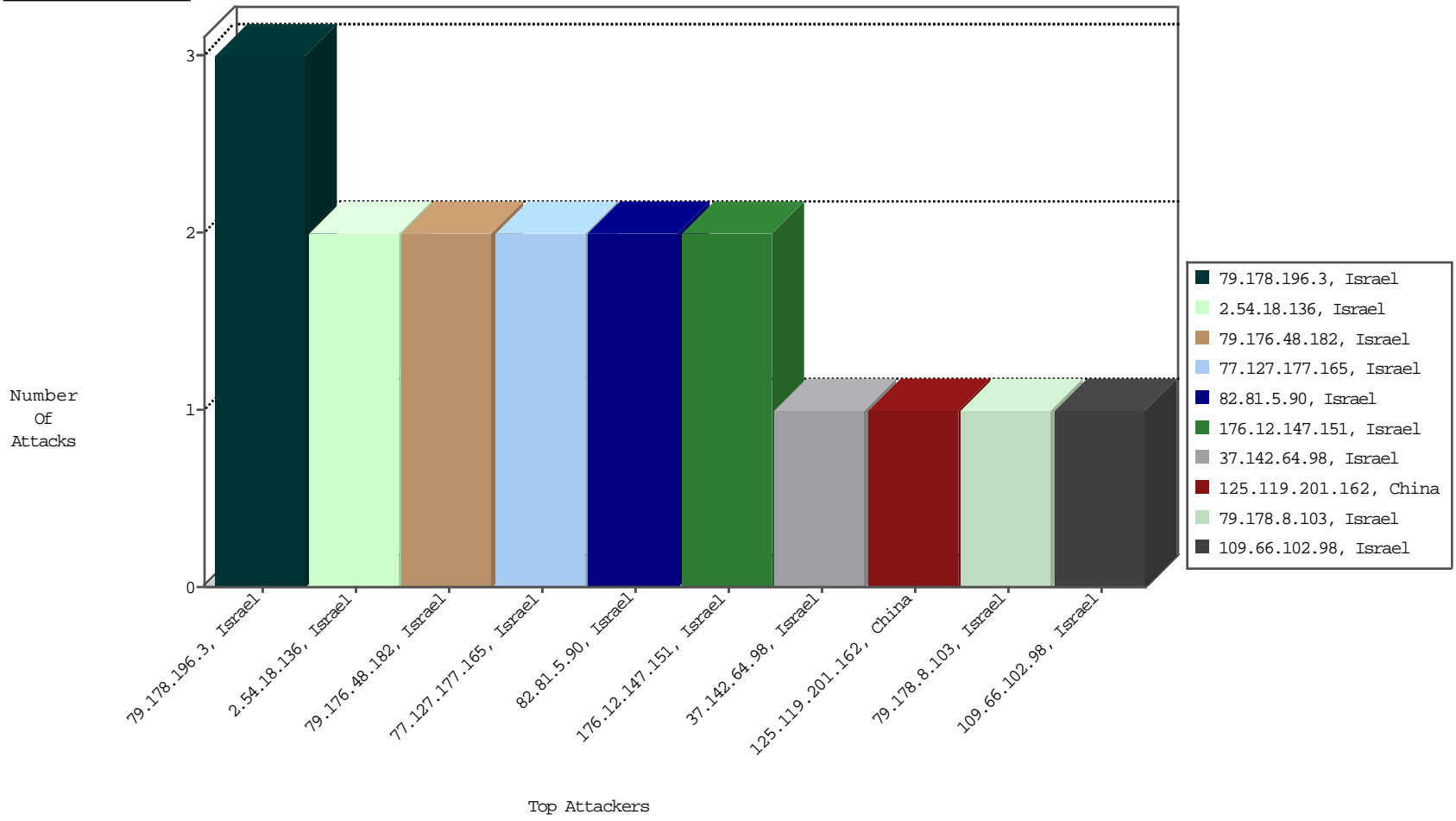
# Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-12-2015 to 12-13-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
------------------	--------------	----------------	------	-----------	---------------	----------------------	-------

12-12-2015 to 12-13-2015

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
59.45.79.117	China	147.237.0.121		ET SCAN Potential SSH Scan	1
125.119.201.162	China	147.237.0.121		ET SCAN Potential SSH Scan	1
203.251.250.133	Korea, Republic of	147.237.0.121		ET SCAN Potential SSH Scan	1
104.200.78.34	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
202.194.40.14	China	147.237.0.121		ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1267
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	1106
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	818
94.44.252.118	Hungary	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	598
64.79.85.205	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	558
46.19.86.228	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
149.88.63.144	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
149.78.192.98	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
46.19.85.235	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.78.244.197	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	140
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	126
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	122
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	119
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	116
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	114
149.78.241.12	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	109
62.77.209.221	Hungary	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	108
66.249.93.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	106
66.249.83.107	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
46.19.85.181	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
157.55.39.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	86
149.88.6.5	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	62
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	61
217.69.133.251	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
149.88.122.81	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	52
149.88.116.181	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.78.240.184	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
66.249.64.170	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
2.52.186.142	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.66.109	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	34
66.249.93.23	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
213.8.204.7	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	25
149.78.253.32	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	25
188.120.148.152	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	22
217.69.133.252	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
217.69.133.191	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
149.154.167.163	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
149.78.233.91	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.93.51	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
149.78.63.20	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	18
66.249.83.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
149.88.226.235	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
109.65.220.27	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	14
66.249.64.170	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	14
217.69.133.253	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
89.139.179.241	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	13
89.139.179.241	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	13
66.102.9.44	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	13
159.203.135.155	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	12

12-12-2015 to 12-13-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
176.12.147.151	Israel	147.237.0.121		Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.196.3	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.178.196.3 (sigalgs DoS Attack)	None	1
37.142.64.98	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
109.66.102.98	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$Submit1 in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	1
79.176.48.182	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.6.64	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.178.196.3	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
77.127.177.165	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 77.127.177.165 (sigalgs DoS Attack)	None	1
79.178.8.103	Israel	147.237.0.121		Unknown Parameter ct100_ContentPlaceHolder1_fuAddStudyEmploymentPermitDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1
2.54.18.136	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 2.54.18.136 (sigalgs DoS Attack)	None	1
82.81.5.90	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 82.81.5.90 (sigalgs DoS Attack)	None	1
77.127.177.165	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.178.196.3	Israel	147.237.0.121		Cookie Injection on cookie .ASPXAUTH with value 88B4602990F58B8AED7455782CDAECB82AACD6AE0DE371C3EE7BD0D144427B940F7F557D2C0749988D60CF8AB6EE2FBC36BBAEB021736F3053C770738D8278A188695772C41BA51DD853F8D0D3D10FEEA7DDDEF9793FDC3EE6D25DB8B3A5D90EC80225B460AF3D1648CFDF1E7EB38C88CF5BB07A2E478290E3F870074C96EEA95D8A8A63801F31C28831D4EAD1B292CC90BE6A4F25FB8845C50E93075CACB24D	None	1
2.54.18.136	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
82.81.5.90	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.176.48.182	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected , Observed 1EAL69382276CE06B26B0C6EC9B20E749366422E63D0F3695773709564B1AFF386BD8936CE166E7A568957E29B69594CA811960EF106329927F3C703E9B1A269EA467B44CB695A6A3A14C50B6A8A6F255AE8DD2EC8A2B81B4067BD8BAD6222DB413BD527E51A4E25D58229F83CE0CC68509FB9718620E89AA12FEF22A199D247EBCEF7F4DCF10964937381D243F544ED8D3C4B8A6C7940ACEED5B3BBDBB282A6	None	1

12-12-2015 to 12-13-2015