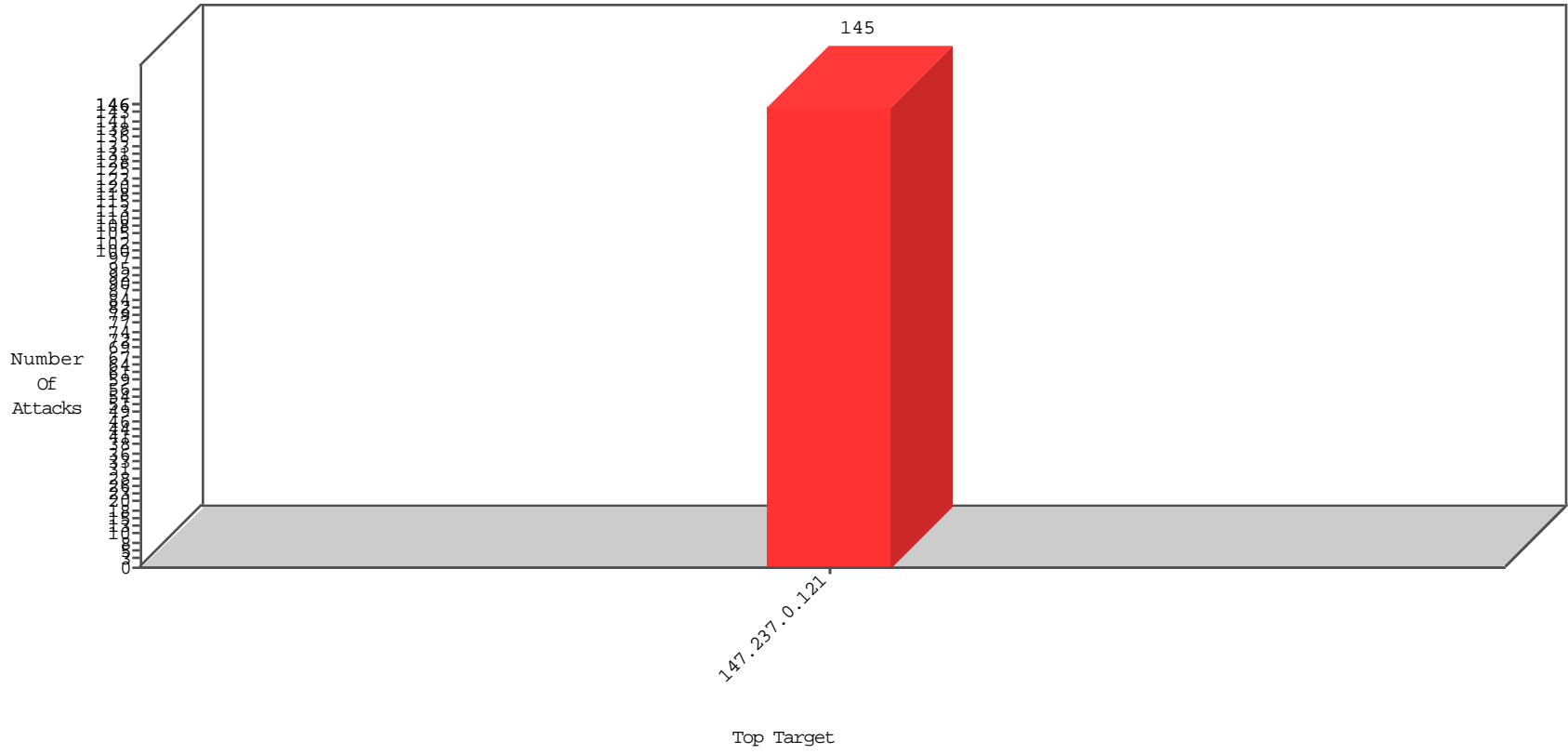


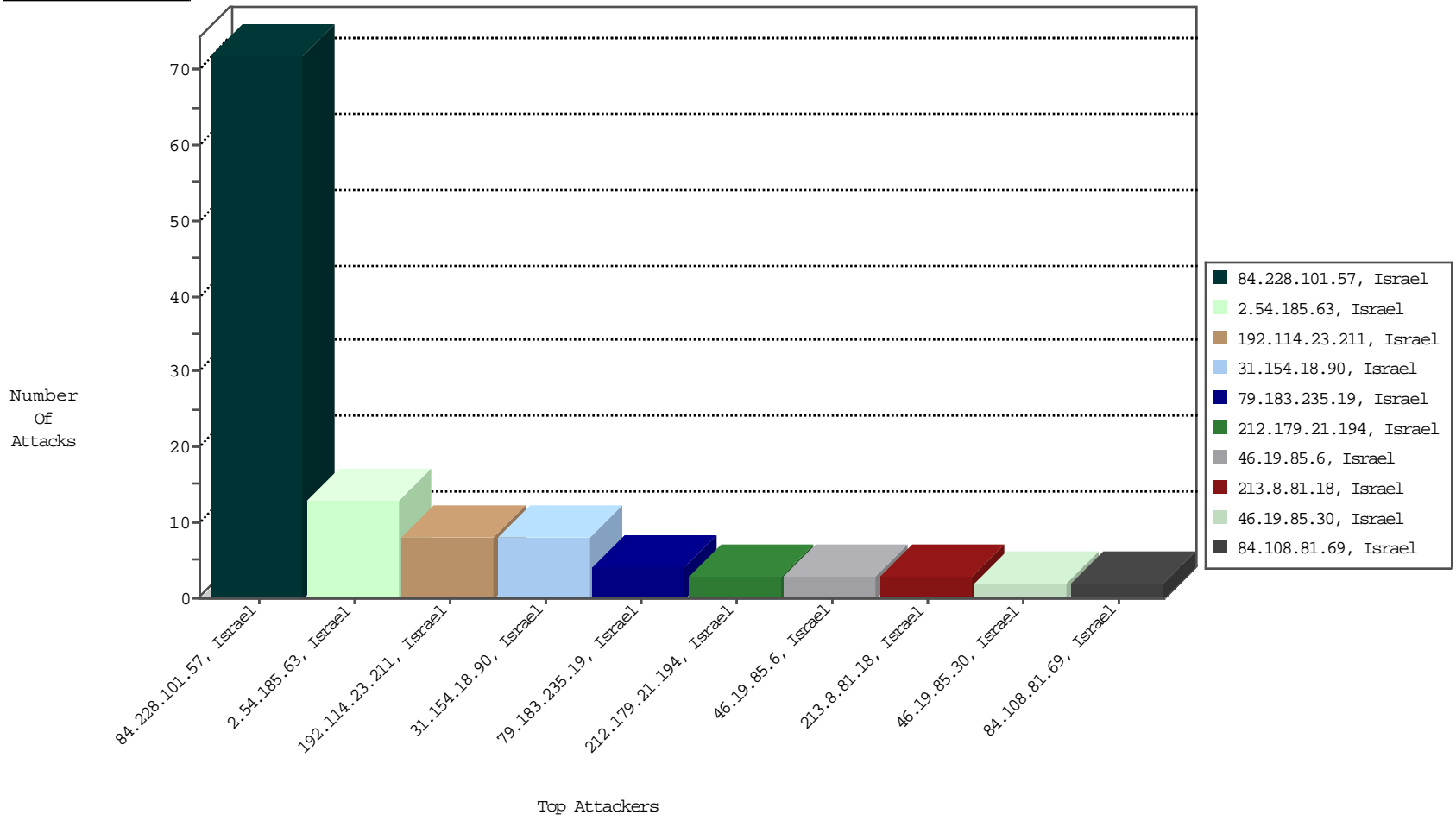
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-14-2015 to 12-15-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
2.54.185.63	Israel	147.237.0.121		Anomaly-SSL-renegotiation-Cli	source-dest-reset	DP-Tehila	13

12-14-2015 to 12-15-2015

Top Attackers In IPS

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

12-14-2015 to 12-15-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
94.102.48.195	Netherlands	147.237.0.121		ET SCAN NMAP -sS window 1024	1
213.85.31.170	Russian Federation	147.237.0.121		ET SCAN Potential VNC Scan 5900-5920	1
104.209.183.157	United States	147.237.0.121		ET SCAN Potential SSH Scan	1
220.231.195.122	China	147.237.0.121		ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.85	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4350
66.249.93.83	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	4263
66.249.93.89	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3098
107.92.63.26	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	468
72.179.171.55	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	468
84.228.101.57	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	369
66.249.93.83	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	343
66.249.93.89	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	321
149.78.255.48	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	318
178.164.228.225	Hungary	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	288
2.54.52.25	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
149.78.233.24	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	275
66.249.93.85	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	260
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	225
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	222
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	205
108.225.17.34	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	162
2.54.156.41	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.185.63	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
37.26.147.251	Israel	147.237.0.121		SYN Attack		reject	121
149.78.236.253	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
149.78.103.175	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	102
78.131.24.205	Hungary	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	96
17.78.72.138	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	64
192.115.177.202	Israel	147.237.0.121		SYN Attack	SYN -> SYN-ACK -> RST	reject	49
149.78.241.12	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	45
149.88.89.180	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
217.69.133.250	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	44
17.78.68.137	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	42
54.88.168.129	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	36
109.65.180.24	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
82.81.23.71	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.228.90.179	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	36
66.249.93.23	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	32
149.88.126.93	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	31
50.152.173.56	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	28
66.249.93.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	27
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	26
66.102.9.33	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	24
149.88.123.52	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	22
149.88.5.39	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
157.55.39.61	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	20
66.249.66.105	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
79.176.49.101	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	17
66.249.93.93	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	17
2.54.185.63	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	16
5.102.254.110	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	16
149.78.86.10	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16
66.249.93.51	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	16

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
84.228.101.57	Israel	147.237.0.121		NULL Character in Header Name at ...	Block	1
79.183.235.19	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 79.183.235.19 (sigalgs DoS Attack)	None	1
46.19.85.30	Israel	147.237.0.121		Multiple Untraceable SSL Sessions from 46.19.85.30 (sigalgs DoS Attack)	None	1
192.114.5.10	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
84.228.101.57	Israel	147.237.0.121		Illegal HTTP Version	Block	1
87.69.148.16	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
84.228.101.57	Israel	147.237.0.121		NULL Character in Query String on ...	Block	1
83.130.113.213	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
84.228.101.57	Israel	147.237.0.121		Multiple NULL Character in Method from 84.228.101.57	Block	1
31.168.81.166	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
176.12.136.60	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Malformed HTTP Header Line 22	Block	1
84.228.101.57	Israel	147.237.0.121		Illegal Byte Code Character in Query String ...	Block	1
84.228.101.57	Israel	147.237.0.121		Unknown HTTP Request Method ...	Block	1
84.228.101.57	Israel	147.237.0.121		NULL Character in Header Name at ...	Block	1
79.183.235.19	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
46.19.85.30	Israel	147.237.0.121		SSL Untraceable Connection - sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.0.121		Illegal HTTP Version ...	Block	1
94.230.86.211	Israel	147.237.0.121		Parameter Type Violation ct100_ContentPlaceHolder1_fuAddAddressAppendixIDDocs&FilesToSend in www.miluim-ishi.aka.idf.il/login	Block	1