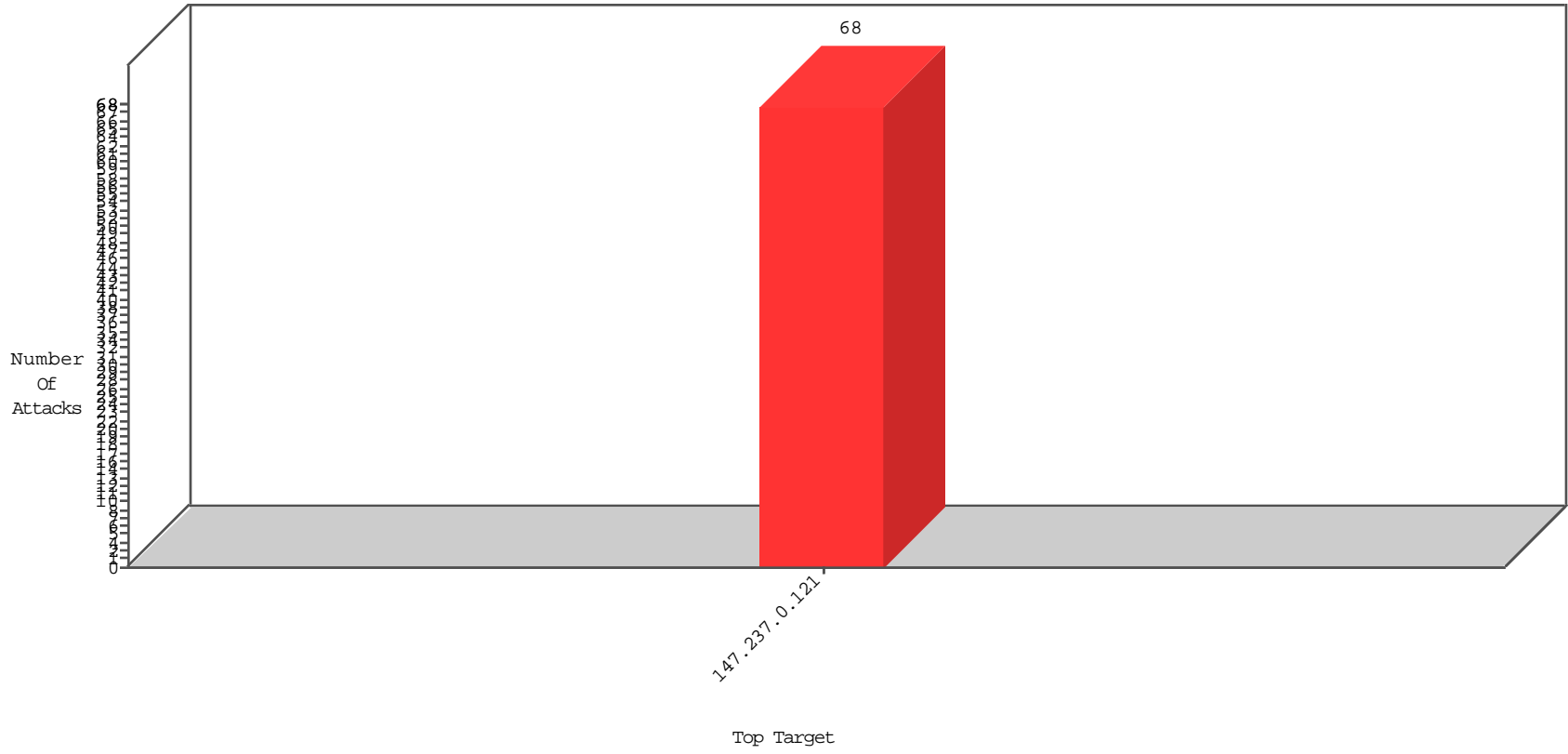


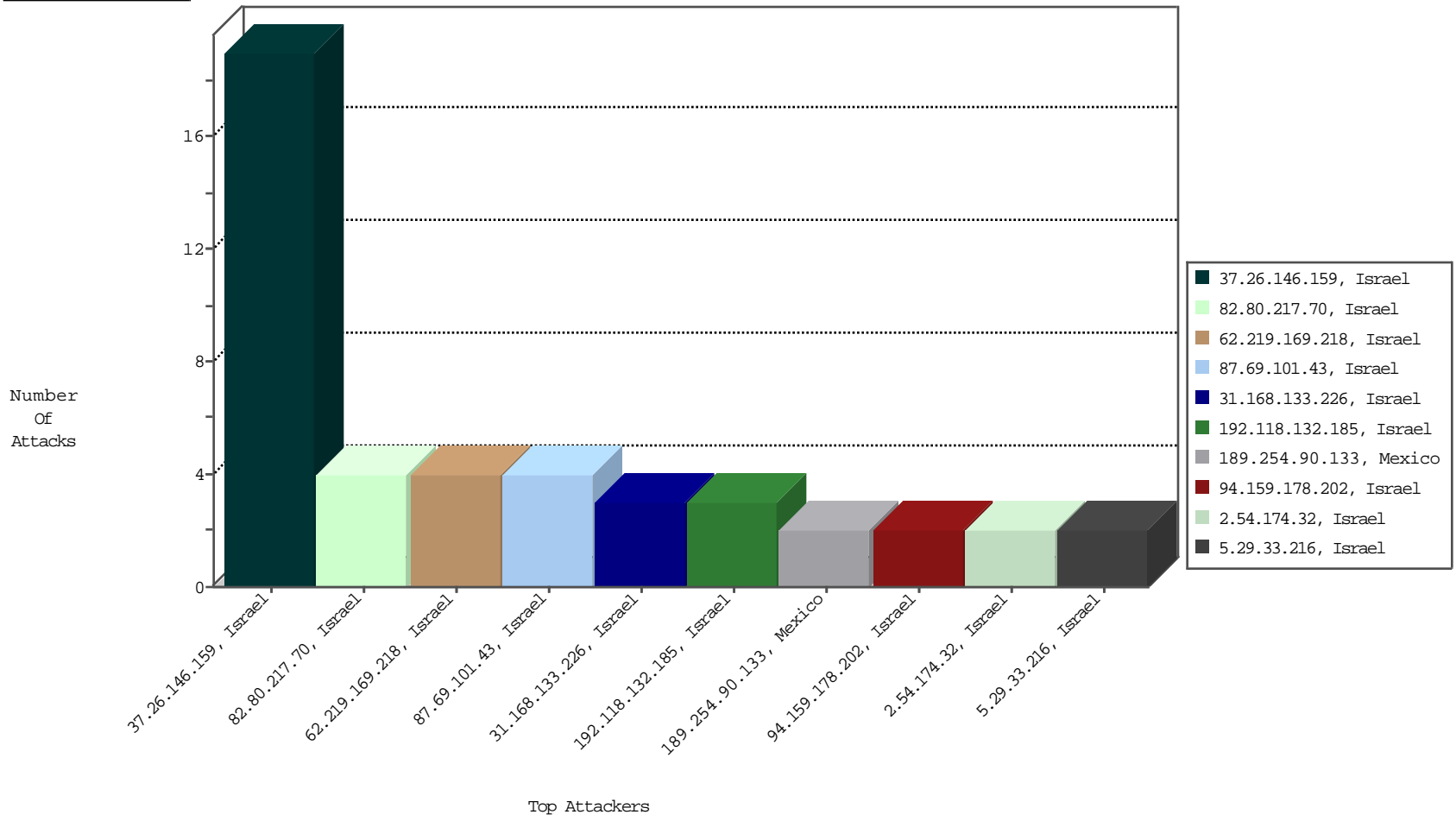
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
37.26.146.159	Israel	147.237.0.121		Invalid TCP Flags	drop	BEL-Frankfurt	19
82.80.217.70	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	3
192.118.132.185	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	3
31.168.133.226	Israel	147.237.0.121		Block_Udp_All_Nets	drop	BEL-Israel	3

11-15-2015 to 11-16-2015

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
125.65.165.215	China	147.237.0.121		ET SCAN Potential SSH Scan	1
189.254.90.133	Mexico	147.237.0.121		ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.0.121		ET SCAN NMAP -sS window 1024	1
189.254.90.133	Mexico	147.237.0.121		ET SCAN NMAP -sS window 1024	1
221.205.92.176	China	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
66.249.93.154	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	3351
212.25.84.200	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	2824
66.249.93.146	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2465
66.249.93.150	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	2313
212.25.84.200	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	1225
212.25.84.200	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	1225
85.115.52.201	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	932
149.78.76.61	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	864
149.78.245.119	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	551
149.78.34.111	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	334
66.249.93.150	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	328
165.225.72.71	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	315
66.249.93.146	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	277
109.66.151.230	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	270
66.249.93.154	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	266
149.78.238.95	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	233
212.166.55.48	Belgium	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	225
149.88.20.108	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	224
149.78.253.215	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	206
13.21.125.9	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	192
2.54.53.212	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
149.78.225.176	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	179
62.219.169.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	160
66.102.9.74	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	146
109.64.52.233	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	144
109.64.52.233	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	144
80.246.137.120	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
62.219.169.218	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	125
109.64.52.233	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	122
155.56.68.219	Germany	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	104
79.181.55.107	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	103
66.249.81.130	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
66.102.6.149	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	101
149.78.50.57	Israel	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	95
185.24.76.132	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	81
80.246.136.9	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
2.52.174.196	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
46.19.85.92	Israel	147.237.0.121		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
79.181.55.107	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	71
91.228.248.251	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	66
185.24.76.132	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	alert	64
185.24.76.132	Israel	147.237.0.121		Bad TCP sequence	Invalid sequence number	monitor	64
176.13.1.4	Israel	147.237.0.121		Bad TCP sequence	Invalid ACK number	monitor	59
217.69.133.21	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	55
66.102.9.97	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	53
134.191.249.39	United Kingdom	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
66.102.9.50	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	51
192.118.132.243	Israel	147.237.0.121		Bad TCP sequence	SYN retransmit with different window scale	monitor	50
66.102.9.87	United States	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	50
217.69.133.249	Russian Federation	147.237.0.121		Geo-location enforcement	Geo-location inbound enforcement	drop	49

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
62.219.169.218	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesNames in www.miluim-ishi.aka.idf.il/medicalcommitteerequest	Block	4
87.69.101.43	Israel	147.237.0.121		Cookie Tampering on cookie .ASPXAUTH: Expected F72C0802CDD657B47EB9F2DC3A5E03E094F3A7ED3DA53E6DC1BC1BED9AE56861E2627580ABBD523B3145A93967120E1737BD4724B076794E8B9F4AD18476D322018434B731E951804FC6A82CCB6C762739A73225F0C4BF18F455DE87E0F41B2D26E9172306738F15993182759527E7933A9797C0D0D02CD4DEC4B3A84CF2F407, Observed EEF504F2AFF6F7874DA5F1BD64EEAE55339249C2512DF0F344B5979E24EF4A97B9306DAEFACD2865483E60604E290CF20AE0E643F81C0D38D039638D855999722B6D5EE3F185EC54684632664667DC47D4644B06BCE092714D0E46DAD3CC5D671C1F6D	None	4
79.181.115.30	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	2
94.159.178.202	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	2
5.29.33.216	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/æ?æž	Block	2
2.54.174.32	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPerutBakasha in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	2
82.80.217.70	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/rules.abe	Block	1
5.28.174.210	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
80.178.148.243	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
212.117.136.8	Israel	147.237.0.121		Unknown Parameter prm in www.miluim-ishi.aka.idf.il/login	Block	1
83.130.100.207	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
79.182.27.155	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
109.66.206.50	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
81.218.101.2	Israel	147.237.0.121		SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.35.246	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtFilesNames in www.miluim-ishi.aka.idf.il/mentalhealthofficercontacting	Block	1
84.108.10.95	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.182.184.88	Israel	147.237.0.121		Unknown Parameter yom in www.miluim-ishi.aka.idf.il/login	Block	1
46.19.86.114	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
176.228.65.73	Israel	147.237.0.121		Unauthorized URL Access to www.miluim-ishi.aka.idf.il/https://www.miluim-ishi.aka.idf.il/	Block	1
81.218.154.15	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
79.178.178.120	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
2.54.179.155	Israel	147.237.0.121		SSL Untraceable Connection - Open Mode	None	1
79.182.206.6	Israel	147.237.0.121		Parameter Type Violation ct100\$ContentPlaceHolder1\$txtNewPass1 in www.miluim-ishi.aka.idf.il/changepassword/newpassword	Block	1
62.128.45.222	Israel	147.237.0.121		Untraceable SSL Sessions: Open Mode	None	1
185.120.126.43		147.237.0.121		SSL Untraceable Connection - Open Mode	None	1