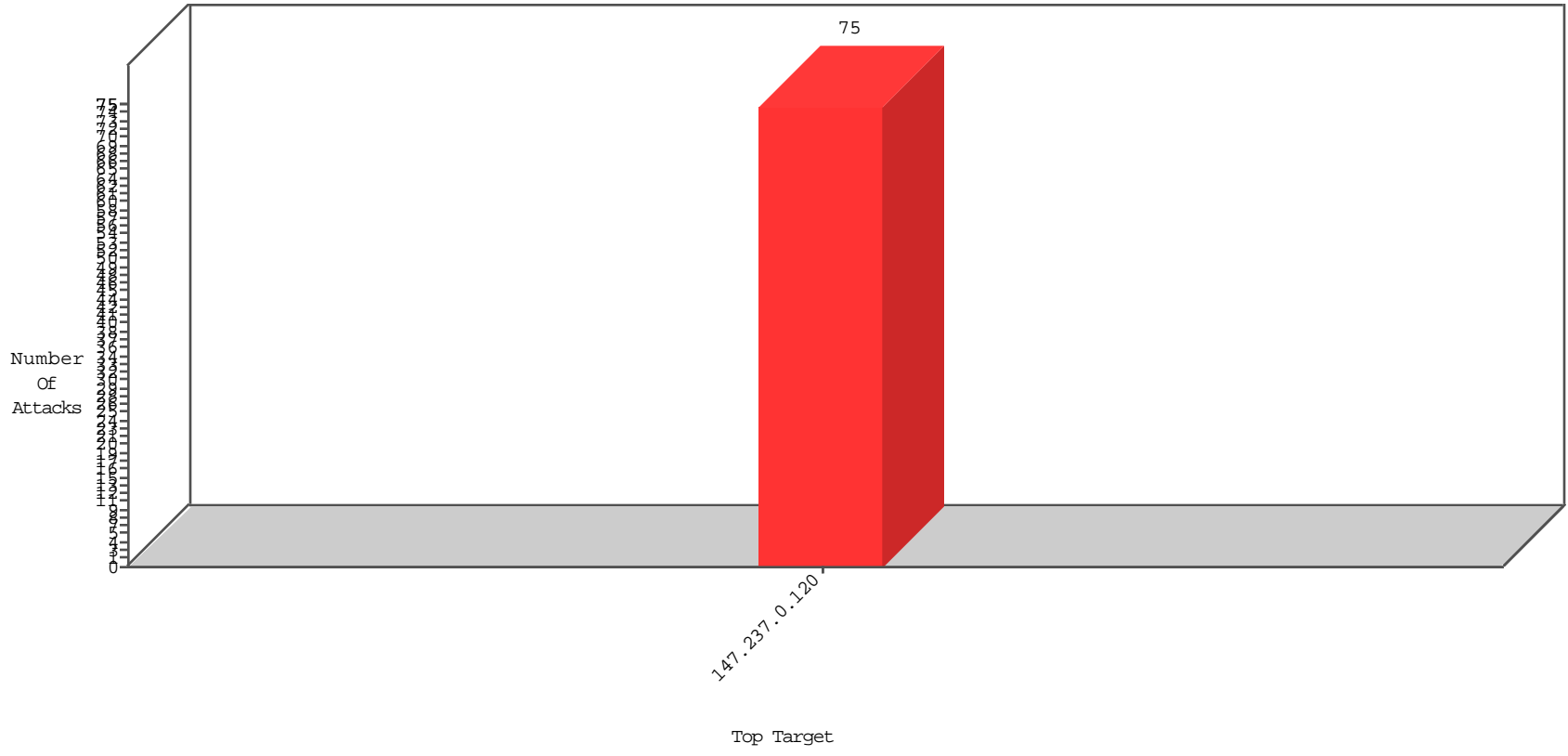


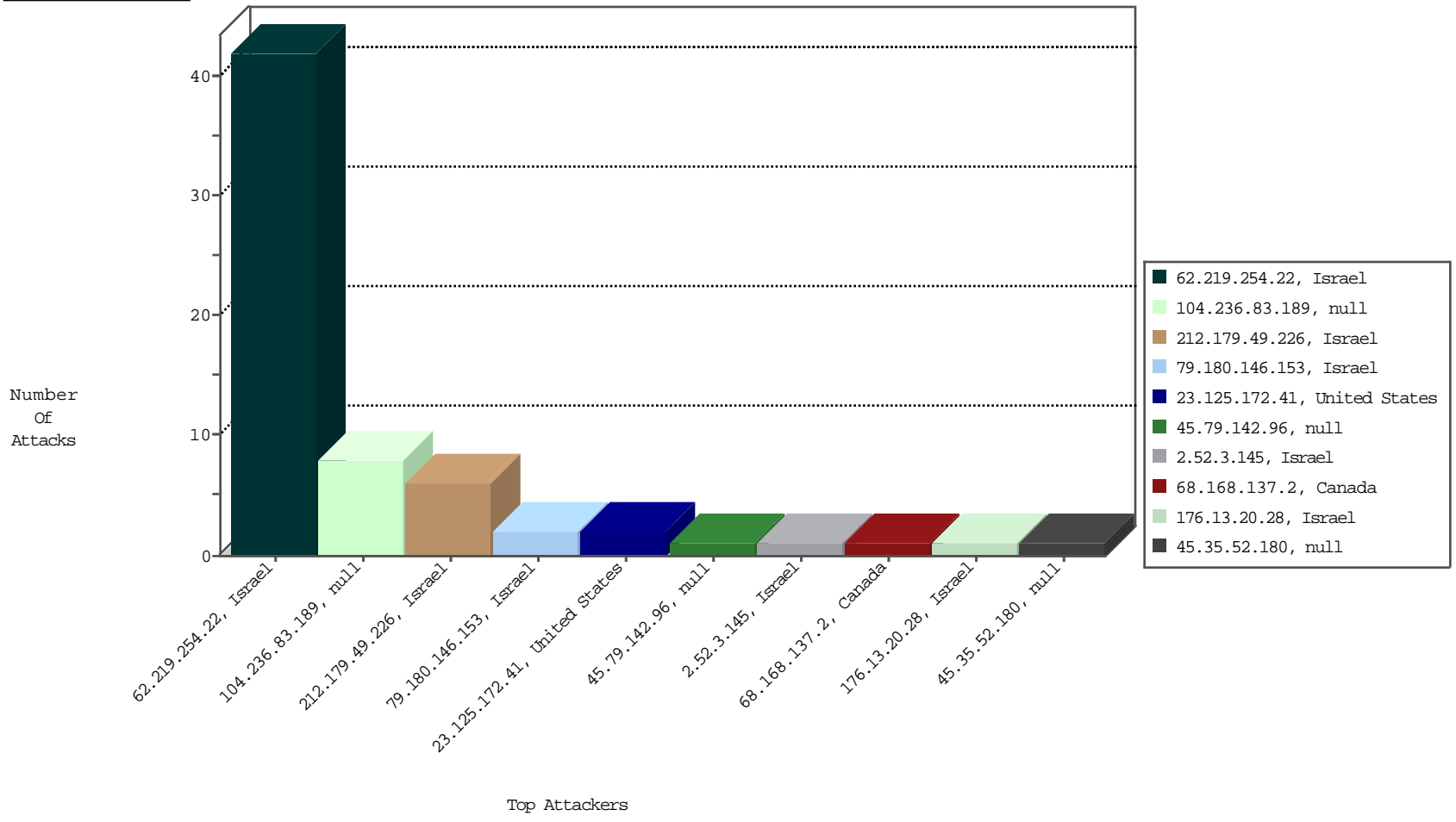
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



11-19-2015 to 11-20-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
62.219.254.22	Israel	147.237.0.120		Block_Udp_All_Nets	drop	EEL-Isreal	42

11-19-2015 to 11-20-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.49.226	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	2

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
23.125.172.41	United States	147.237.0.120		ET SCAN NMAP -sS window 4096	1
45.35.52.180		147.237.0.120		ET SCAN Potential SSH Scan	1
68.168.137.2	Canada	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
113.108.21.16	China	147.237.0.120		ET SCAN Potential SSH Scan	1
23.125.172.41	United States	147.237.0.120		ET SCAN NMAP -sS window 1024	1
37.49.224.135	Netherlands	147.237.0.120		ET SCAN Potential SSH Scan	1
45.79.142.96		147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
101.4.136.68	China	147.237.0.120		ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	3802
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	3605
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	3019
2.54.36.89	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2501
213.8.44.241	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
157.55.39.19	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1948
168.63.137.102	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1737
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1037
157.55.39.77	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	712
207.46.13.128	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	639
207.46.13.57	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	625
77.125.102.165	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
144.24.20.231	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	428
149.78.95.93	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	403
1.136.96.157	Australia	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	400
149.88.21.176	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	396
149.88.216.49	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	390
207.46.13.171	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	364
207.46.13.120	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	294
40.77.167.11	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	293
157.55.39.208	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	279
207.46.13.19	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	253
149.78.249.154	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	236
37.26.149.182	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
149.78.18.50	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	223
173.38.209.9	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	204
137.71.226.54	Ireland	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	200
149.78.246.250	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	197
37.26.148.161	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	196
66.249.93.207	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	193
66.249.93.203	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	191
149.88.229.197	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	180
66.249.93.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	169
80.254.150.79	France	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	160
164.144.48.13	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	146
79.179.58.215	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.182.181.98	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.94.194.202	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
157.55.39.18	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	141
149.78.32.196	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	131
66.102.9.80	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	130
167.220.196.72	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	125
46.19.85.191	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	122
46.19.85.191	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	alert	121
46.19.85.143	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	121
149.78.2.63	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	119
46.19.86.238	Israel	147.237.0.120		Bad TCP sequence	Invalid sequence number	monitor	117
66.102.9.90	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	117
149.78.240.247	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	113
46.19.86.238	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	110

11-19-2015 to 11-20-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
104.236.83.189		147.237.0.120		Multiple Unauthorized URL Access from 104.236.83.189	Block	7
79.180.146.153	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1359-he/miluim.aspx	Block	2
212.179.49.226	Israel	147.237.0.120		Unauthorized HTTP Method	Block	2
212.179.49.226	Israel	147.237.0.120		Multiple Unauthorized URL Access from 212.179.49.226	Block	1
109.67.58.218	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1358-he/miluim.aspx?aeZ	Block	1
46.19.86.253	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1361-he/miluim.aspx?aeZ	Block	1
87.68.247.102	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?aeZ	Block	1
176.13.6.172	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1	Block	1
46.121.138.133	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1358-he/miluim.aspx?aeZ	Block	1
212.179.49.226	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1
2.52.3.145	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?aeZ	Block	1
176.13.20.28	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1358-	Block	1
79.177.115.85	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?aeZ	Block	1
104.236.83.189		147.237.0.120		Unauthorized URL Access to miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
31.168.11.194	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?aeZ	Block	1

11-19-2015 to 11-20-2015