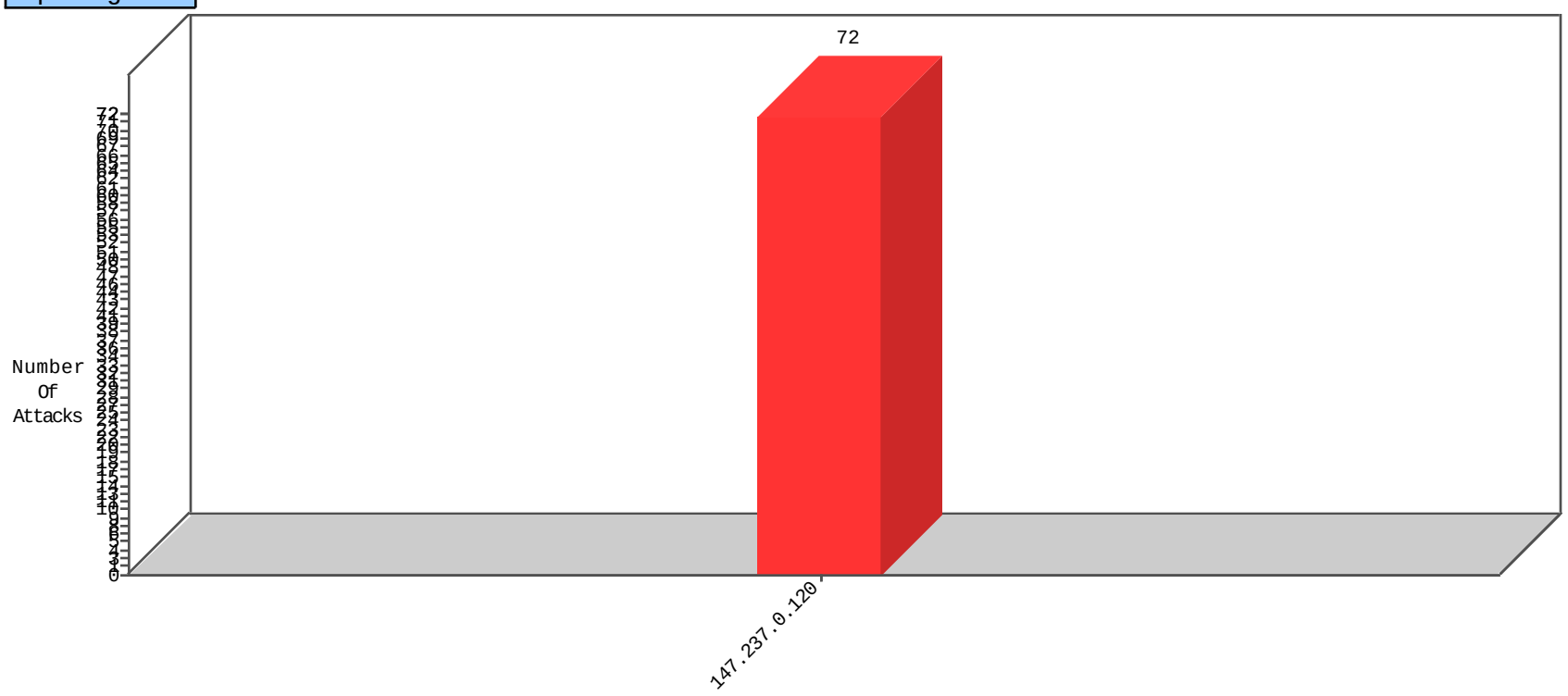
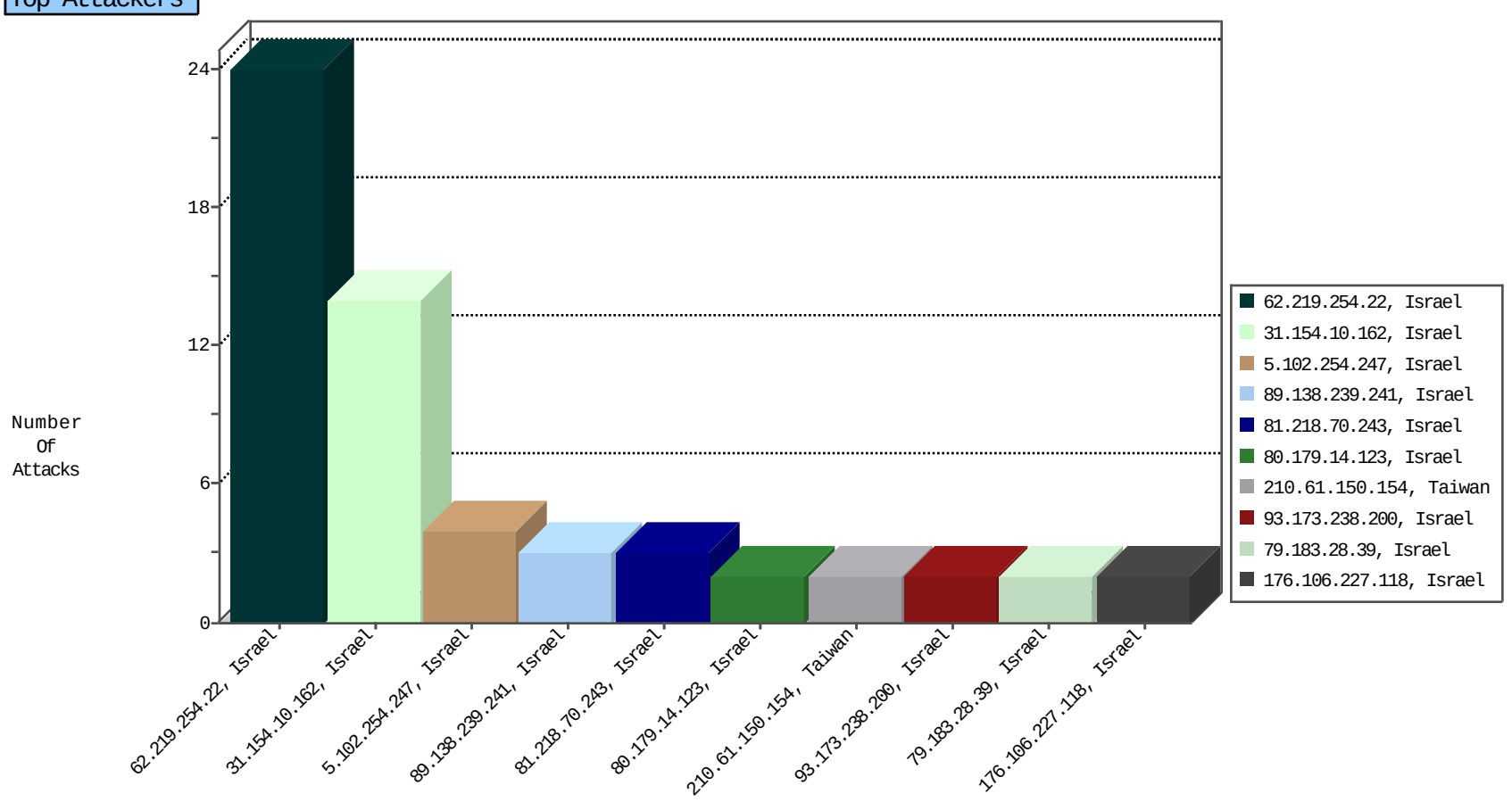
11-17-2015 to 11-18-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-17-2015 to 11-18-2015

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	BBL-Israel	24

11-17-2015 to 11-18-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
89.138.239.241	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	3
31.154.10.162	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	2

11-17-2015 to 11-18-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
5.102.254.247	Israel	147.237.0.120		GPL SCAN myscan	2
5.102.254.247	Israel	147.237.0.120		INDICATOR-SCAN myscan	2
46.151.55.35	Ukraine	147.237.0.120		ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.120		ET SCAN Potential VNC Scan 5800-5820	1
84.109.176.218	Israel	147.237.0.120		http_inspect: MULTIPLE HOST HEADERS DETECTED	1
210.61.150.154	Taiwan	147.237.0.120		ET SCAN NMAP -sS window 1024	1
213.169.149.80	Cyprus	147.237.0.120		ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.120		ET SCAN Potential SSH Scan	1
74.117.209.135	United States	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
95.105.15.110	Russian Federation	147.237.0.120		ET SCAN Potential SSH Scan	1
210.61.150.154	Taiwan	147.237.0.120		ET SCAN NMAP -sS window 4096	1

11-17-2015 to 11-18-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
79.177.163.227	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
185.120.126.39		147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
81.218.132.51	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1534
79.183.218.231	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1314
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1260
149.78.64.16	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1146
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1144
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	983
2.54.135.73	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	900
95.172.74.51	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	341
46.19.85.10	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	339
66.249.67.104	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	314
207.46.13.118	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	312
66.249.67.110	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	307
149.88.2.9	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	296
149.88.20.0	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	281
40.77.167.50	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	275
66.249.67.98	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	248
40.77.167.71	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	231
79.181.32.163	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
149.88.164.31	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	221
37.26.146.251	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	196
40.77.167.60	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	194
40.77.167.39	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	192
46.19.85.129	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	185
199.207.253.96	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	180
192.115.248.2	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	169
66.102.9.100	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	149
37.26.149.141	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	144
109.65.203.236	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
5.28.164.17	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.229.31.140	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
134.191.232.68	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	144
149.78.253.78	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	143
46.19.85.165	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	140
66.249.67.104	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	130
134.191.232.72	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	120
66.249.67.110	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	118
66.249.93.207	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	118
24.173.103.179	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	116
41.66.45.86	Cote D'Ivoire	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	109
17.78.99.192	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	109
38.127.167.44	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	108
142.162.40.193	Canada	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	108
46.19.85.129	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	106
66.249.93.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	102
66.249.67.98	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	102
79.161.20.58	Norway	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	100
66.102.9.80	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	97

11-17-2015 to 11-18-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.154.10.162	Israel	147.237.0.120		Unauthorized HTTP Method	Block	6
31.154.10.162	Israel	147.237.0.120		Multiple Unauthorized URL Access from 31.154.10.162	Block	5
77.127.89.214	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
81.218.70.243	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	2
93.173.238.200	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/homepage.aspx	Block	2
109.66.191.123	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/6_s3_	Block	1
79.183.28.39	Israel	147.237.0.120		Distributed PHP Attempt	Block	1
2.54.164.183	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1360-he/miluim.aspxâ€?â€Ž	Block	1
81.218.70.243	Israel	147.237.0.120		Multiple Unauthorized URL Access from 81.218.70.243	Block	1
176.13.8.115	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
79.183.28.39	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/ajax/pages/fan_status.php	Block	1
79.182.38.50	Israel	147.237.0.120		Distributed PHP Attempt	Block	1
176.106.227.118	Israel	147.237.0.120		PHP Attempt	Block	1
80.179.14.123	Israel	147.237.0.120		PHP Attempt	Block	1
79.182.38.50	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/ajax/pages/fan_status.php	Block	1
176.106.227.118	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/ajax/pages/fan_status.php	Block	1
80.179.14.123	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/ajax/pages/fan_status.php	Block	1
31.154.10.162	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/2/	Block	1

11-17-2015 to 11-18-2015