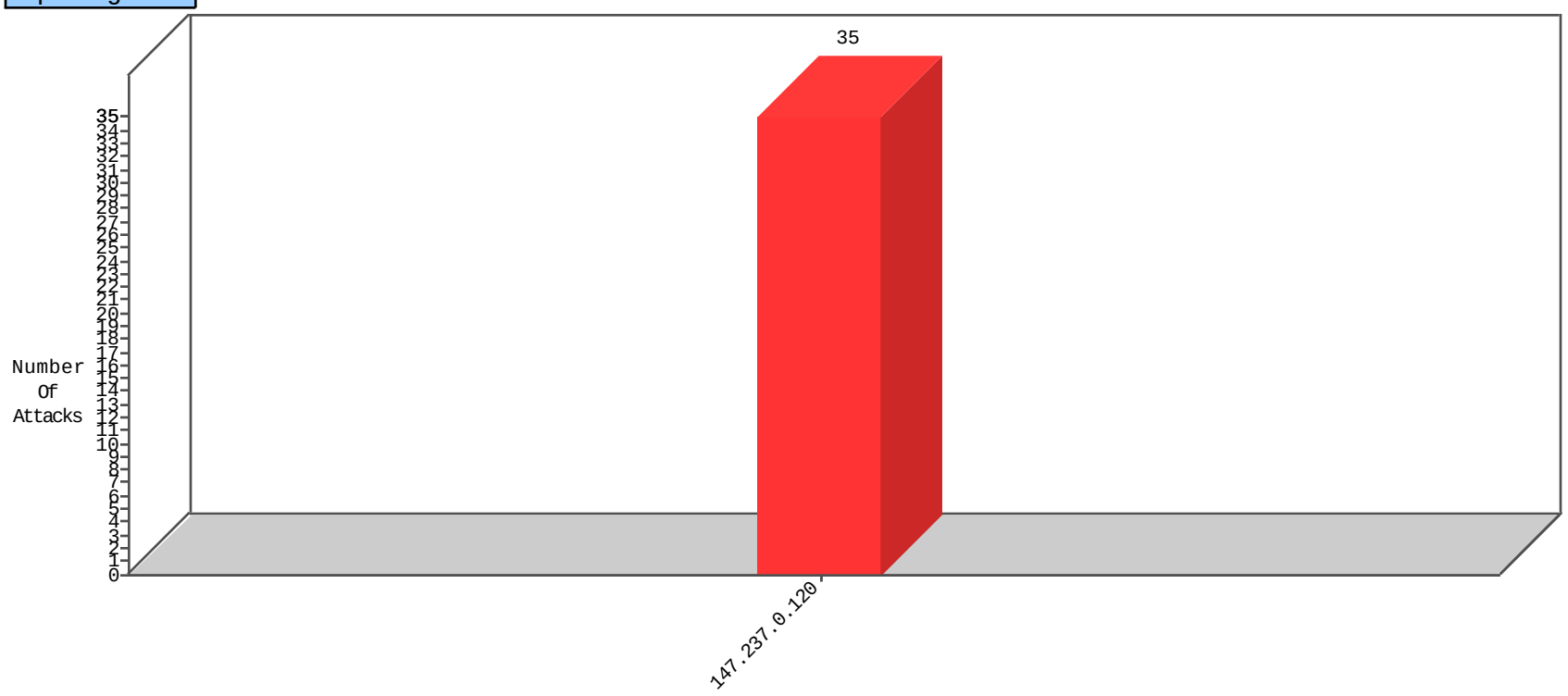
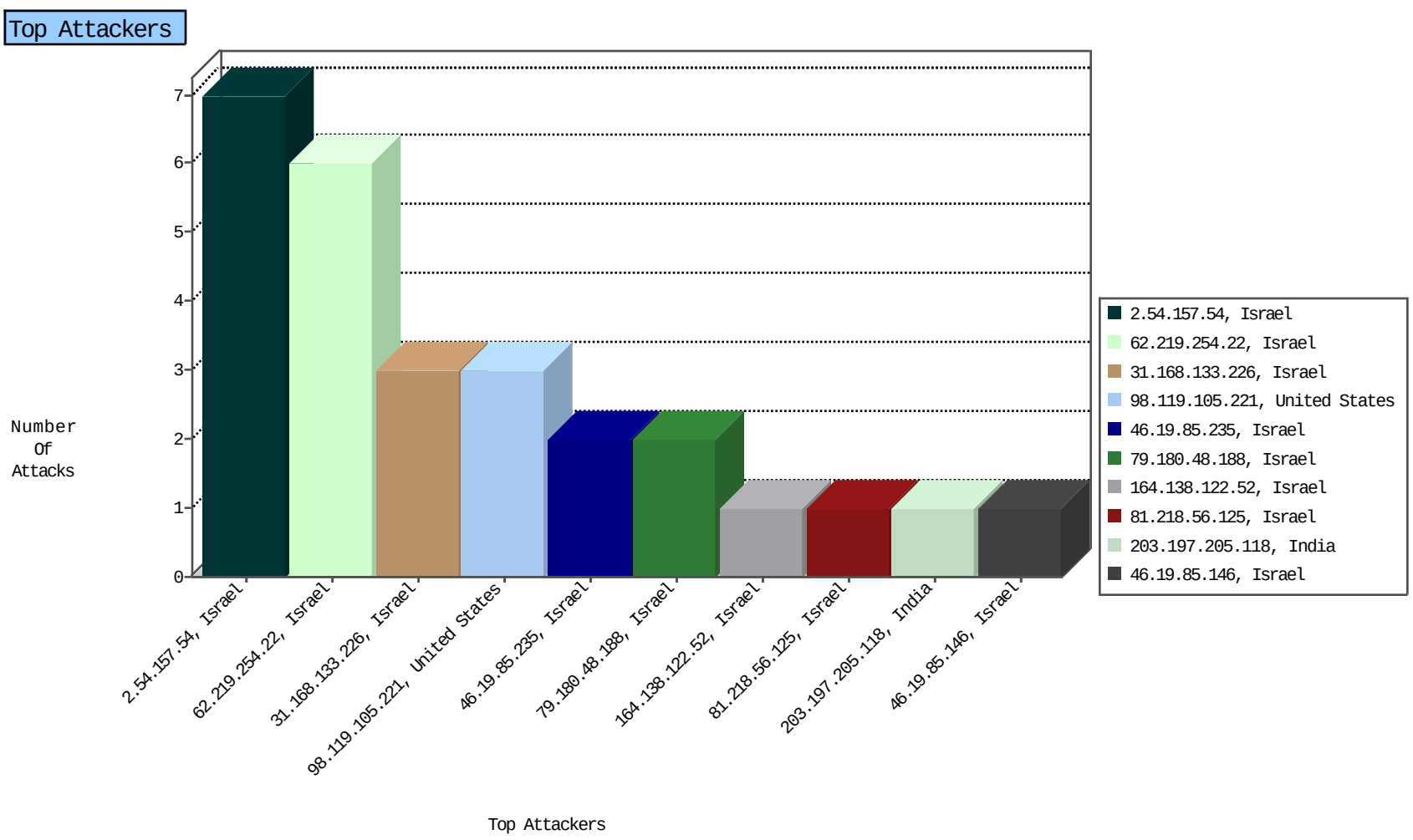
11-18-2015 to 11-19-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-18-2015 to 11-19-2015

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	6
31.168.133.226	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	3
81.218.56.125	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	1
108.161.253.41	United States	147.237.0.120		L4 Source or Dest Port Zero	drop	BBL-Israel	1

11-18-2015 to 11-19-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-18-2015 to 11-19-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
79.180.48.188	Israel	147.237.0.120		ET SCAN NMAP -sA (2)	2
203.197.205.118	India	147.237.0.120		ET SCAN NMAP -sS window 4096	1
69.30.246.210	United States	147.237.0.120		ET SCAN Potential SSH Scan	1
98.119.105.221	United States	147.237.0.120		ET SCAN NMAP -f -sS	1
98.119.105.221	United States	147.237.0.120		ET SCAN NMAP -sS window 4096	1
45.79.142.96		147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
98.119.105.221	United States	147.237.0.120		ET SCAN NMAP -sS window 2048	1

11-18-2015 to 11-19-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2890
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2703
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1837
79.178.198.128	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1440
46.19.85.29	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	1238
46.19.85.140	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	729
169.230.90.218	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	710
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	300
157.55.39.77	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	288
149.88.20.0	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	248
149.88.233.187	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	244
40.77.167.66	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	235
176.13.6.205	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	232
109.186.160.242	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	229
79.182.135.246	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
24.12.74.89	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	223
40.77.167.73	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	212
46.19.86.1	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	206
79.182.123.60	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	196
134.191.249.24	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	192
66.249.93.203	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	176
46.19.86.1	Israel	147.237.0.120		Bad TCP sequence	Invalid sequence number	monitor	171
192.146.6.2	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	166
199.207.253.96	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	160
66.249.67.98	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	158
66.249.81.224	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	151
79.181.15.85	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
46.19.86.1	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.66.103.96	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.182.100.248	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.67.104	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	136
66.102.9.90	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	135
149.78.13.236	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	130
149.78.140.51	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	129
66.249.93.207	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	127
2.54.179.97	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
125.19.102.130	India	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	117
176.13.6.205	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	alert	114
149.88.127.66	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	114
66.249.93.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	111
98.108.203.44	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	106
207.46.13.171	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	106
193.6.168.41	Hungary	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	105
93.173.143.99	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	104
79.178.198.128	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	100
2.54.175.64	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
85.64.89.139	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	86
85.64.89.139	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	alert	86
46.19.86.225	Israel	147.237.0.120		Bad TCP sequence	Invalid sequence number	monitor	84
46.19.86.225	Israel	147.237.0.120		Bad TCP sequence	Invalid ACK number	monitor	84

11-18-2015 to 11-19-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.54.157.54	Israel	147.237.0.120		Multiple Unauthorized URL Access from 2.54.157.54	Block	7
192.116.232.69	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/894-he/miluim.aspx	Block	1
46.19.85.146	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1361-he/miluim.aspxâ€?â€Ž	Block	1
109.67.133.223	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/main/home/default.aspx	Block	1
199.203.215.1	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/miluim.aspx	Block	1
46.19.85.235	Israel	147.237.0.120		Malformed URL	Block	1
164.138.122.52	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspx&sa=u&ved=0cagqfjaaahukewjfuo_qzjrjahue6rqkhse-dxk&sig2=jhhtd88lpyft__mth-nbhw&usg=afqjcnernh23git69bvqc8ggaxyqqn74qq	Block	1
46.19.85.235	Israel	147.237.0.120		Unknown HTTP Request Method sdch in URL	Block	1
176.13.6.172	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1	Block	1
93.113.125.11	Romania	147.237.0.120		Unauthorized URL Access to /readme_for_decrypt.txt	Block	1

11-18-2015 to 11-19-2015