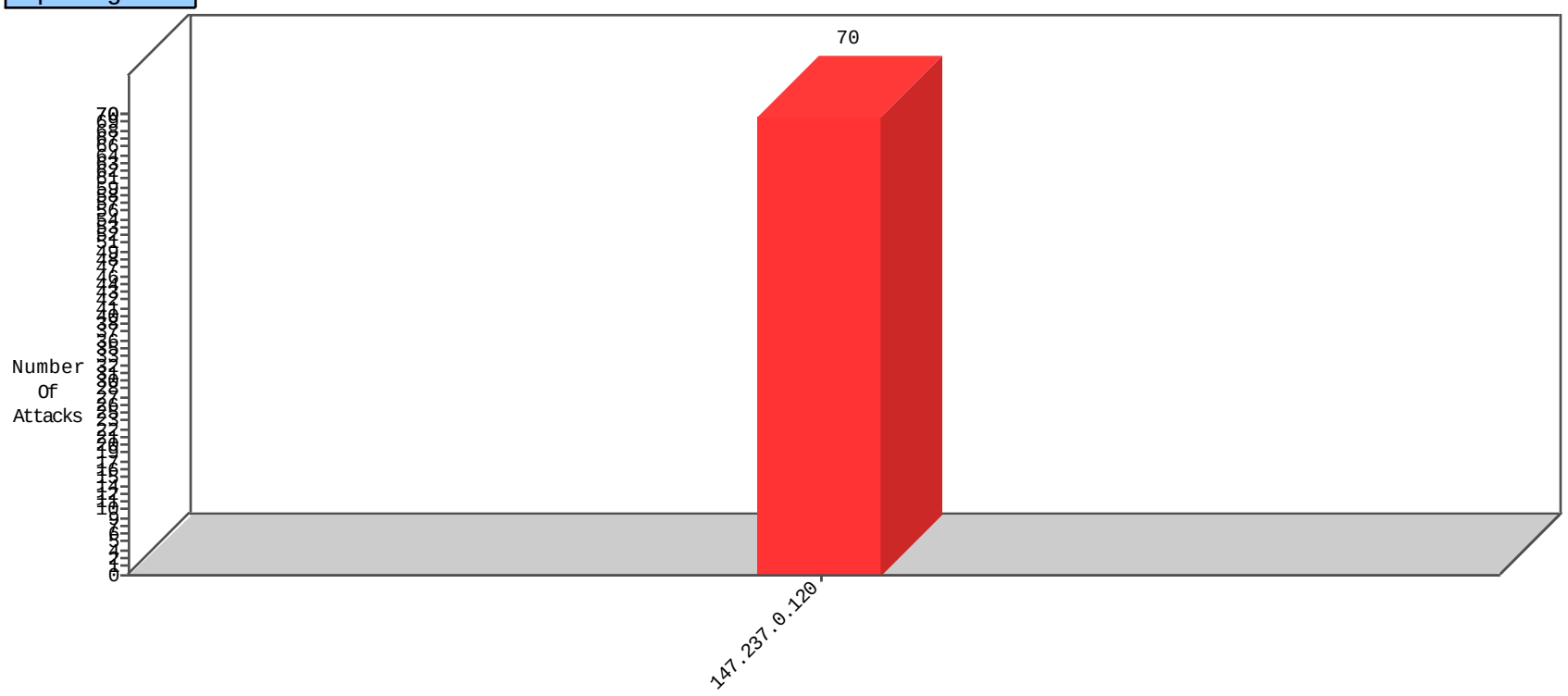
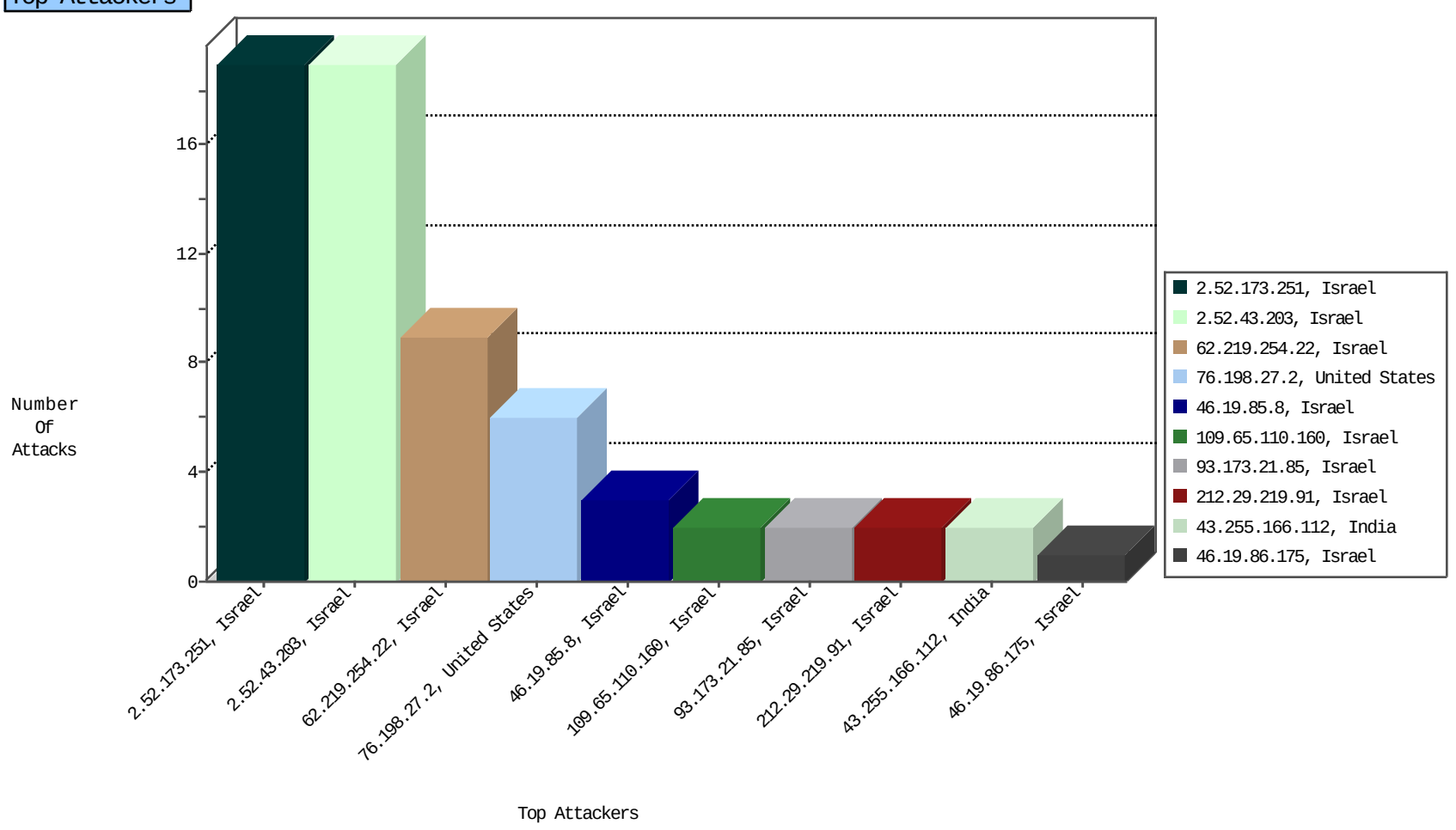
11-24-2015 to 11-25-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-24-2015 to 11-25-2015

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	9
76.198.27.2	United States	147.237.0.120		Invalid TCP Flags	drop	BBL-Frankfurt	6

11-24-2015 to 11-25-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

11-24-2015 to 11-25-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
2.52.173.251	Israel	147.237.0.120		POLICY-OTHER TCP packet with urgent flag attempt	19
43.255.166.112	India	147.237.0.120		ET SCAN Potential SSH Scan	2
109.65.110.160	Israel	147.237.0.120		ET SCAN NMAP -sA (2)	2
31.6.71.154	Poland	147.237.0.120		ET SCAN NMAP -sS window 1024	1
74.117.209.136	United States	147.237.0.120		ET SCAN NMAP -sS window 1024	1
212.7.199.208	Netherlands	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1

11-24-2015 to 11-25-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.81.227	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	7148
69.41.14.215	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	7094
66.249.81.224	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	6752
66.249.81.230	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	6522
2.52.11.222	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3869
149.78.22.6	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2761
31.171.244.115	Switzerland	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2681
149.78.47.62	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2669
79.183.163.198	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.52.170.120	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
81.218.187.153	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.182.137.195	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
149.78.218.180	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2280
149.88.168.236	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1524
76.198.27.2	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1087
85.132.43.59	Azerbaijan	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	909
46.19.86.17	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	900
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	897
85.115.52.201	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	775
149.78.41.248	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	443
149.88.67.137	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	440
108.171.128.188	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	433
193.242.218.25	Switzerland	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	378
90.181.168.124	Czech Republic	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	366
74.125.57.102	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	364
149.78.213.37	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	332
46.19.86.31	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	295
46.19.85.216	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	289
149.78.68.216	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	277
149.88.82.13	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	257
66.249.81.224	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	225
149.78.239.91	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	220
86.28.243.252	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	212
66.249.81.227	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	211
66.249.81.230	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	209
149.78.24.54	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	206
66.249.73.212	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	197
199.115.114.229	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	194
149.78.37.8	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	185
149.78.125.159	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	182
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	178
90.181.168.126	Czech Republic	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	153
2.52.144.245	Israel	147.237.0.120		SYN Attack	SYN -> SYN-ACK -> RST	reject	144
2.54.32.96	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.73.220	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	138
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	127
123.243.140.218	Australia	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	125
195.55.86.146	Spain	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	122
51.175.93.165	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	120
46.19.86.31	Israel	147.237.0.120		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	119

11-24-2015 to 11-25-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
2.52.43.203	Israel	147.237.0.120		Multiple Unauthorized URL Access from 2.52.43.203	Block	18
93.173.21.85	Israel	147.237.0.120		Multiple Unauthorized URL Access from 93.173.21.85	Block	1
212.29.219.91	Israel	147.237.0.120		Multiple _vti_ from 212.29.219.91	Block	1
46.19.85.8	Israel	147.237.0.120		Malformed URL	Block	1
93.173.21.85	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/ufi/reaction/	Block	1
2.52.43.203	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/4/2024.pd	Block	1
46.19.85.8	Israel	147.237.0.120		Unknown HTTP Request Method _pk_ses.104.b624=* in URL	Block	1
109.66.100.95	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
2.52.136.76	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.86.175	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
212.29.219.91	Israel	147.237.0.120		Multiple Unauthorized URL Access from 212.29.219.91	Block	1
46.19.85.8	Israel	147.237.0.120		Abnormally Long Request method	Block	1

11-24-2015 to 11-25-2015