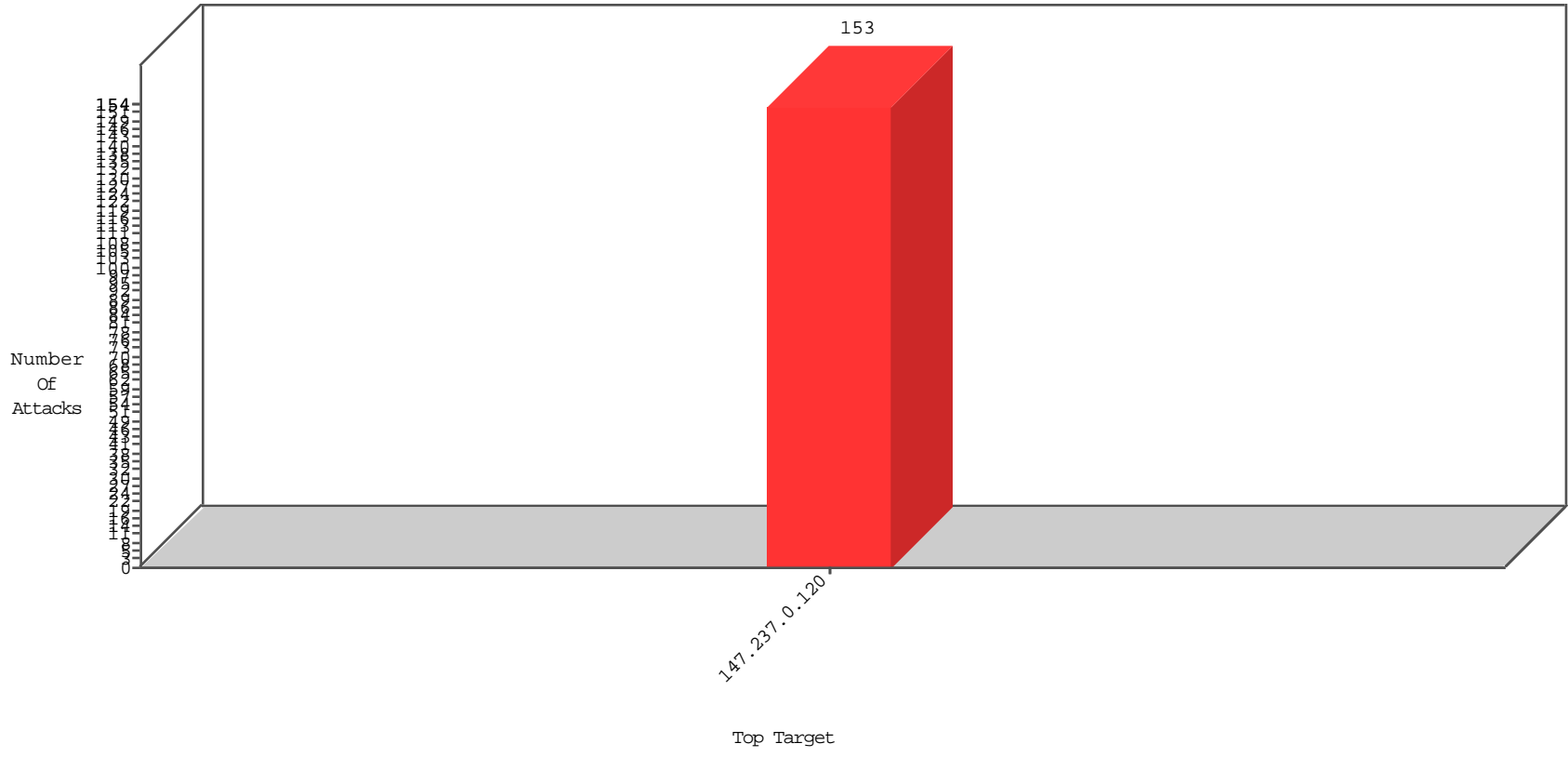


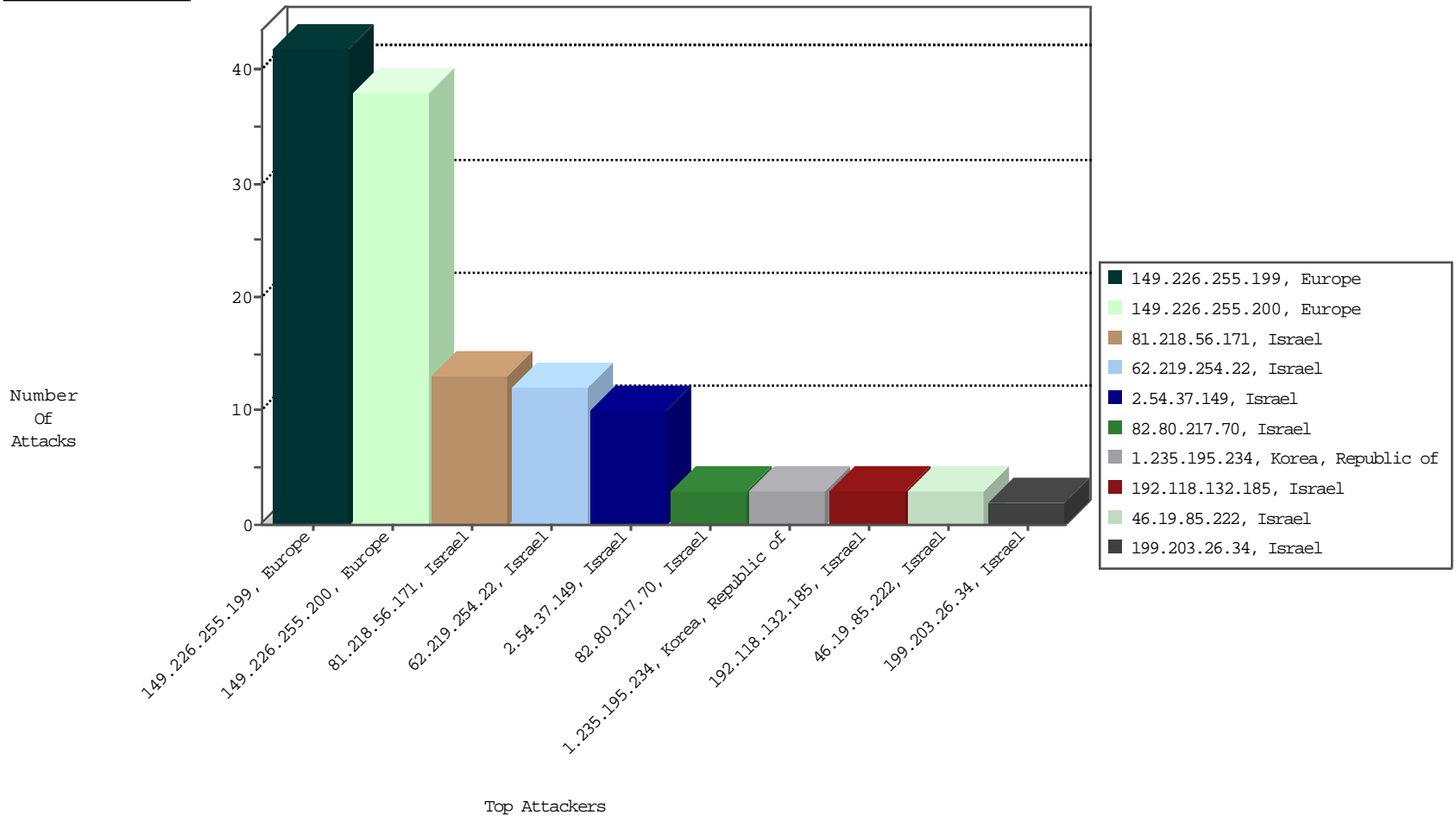
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
62.219.254.22	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BEL-Israel	12
82.80.217.70	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BEL-Israel	3
192.118.132.185	Israel	147.237.0.120		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
149.226.255.199	Europe	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	42
149.226.255.200	Europe	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	38

11-15-2015 to 11-16-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
1.235.195.234	Korea, Republic of	147.237.0.120		ET SCAN NMAP -sS window 2048	1
112.225.163.197	China	147.237.0.120		ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.235.195.234	Korea, Republic of	147.237.0.120		ET SCAN NMAP -sS window 1024	1
68.168.137.2	Canada	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
161.202.147.196	Netherlands	147.237.0.120		ET SCAN Potential SSH Scan	1
1.235.195.234	Korea, Republic of	147.237.0.120		ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	4222
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	4162
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	3759
2.54.60.5	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3278
149.78.245.119	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2860
2.54.12.110	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
109.66.43.216	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
77.126.51.38	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
62.219.161.217	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
62.219.82.51	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1521
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1054
37.26.146.216	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	729
149.78.225.176	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	539
149.88.220.65	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	504
192.146.6.2	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	498
78.53.72.183	Germany	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	485
157.55.39.1	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	419
207.46.13.82	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	407
66.249.73.212	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	393
149.78.247.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	390
66.249.73.228	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	382
149.88.107.84	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	360
82.166.73.216	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
66.249.73.220	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	291
207.38.145.2	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	279
84.131.77.241	Germany	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	259
207.46.13.83	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	250
66.249.75.235	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	238
157.55.39.224	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	236
66.249.93.203	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	217
66.249.75.219	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	214
149.78.50.57	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	210
66.249.93.207	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	205
157.55.39.253	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	204
66.249.75.227	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	203
207.46.13.151	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	196
207.46.13.152	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	184
149.78.60.229	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	181
66.249.73.228	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	172
66.249.93.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	170
194.9.253.238	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	169
2.54.164.167	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
185.82.52.225		147.237.0.120		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	152
149.78.160.250	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	152
66.249.81.224	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	146
109.64.159.87	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.161.20.58	Norway	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	144
157.55.39.225	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	142
64.236.4.31	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	140
157.55.39.114	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	134

11-15-2015 to 11-16-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
81.218.56.171	Israel	147.237.0.120		Multiple Unauthorized URL Access from 81.218.56.171	Block	11
2.54.37.149	Israel	147.237.0.120		Unauthorized HTTP Method	Block	4
2.54.37.149	Israel	147.237.0.120		Multiple Unauthorized URL Access from 2.54.37.149	Block	3
81.218.56.171	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	2
2.54.37.149	Israel	147.237.0.120		PHP Attempt	Block	2
31.168.64.65	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1359-he/miluim.aspx?â€Ž	Block	2
199.203.26.34	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-en/miluim.aspx	Block	2
46.19.85.165	Israel	147.237.0.120		Distributed Unknown HTTP Request Method	Block	1
2.54.165.67	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1359-he/miluim.aspx?â€Ž	Block	1
213.57.194.24	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1358-he/miluim.aspx?â€Ž	Block	1
109.66.154.66	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1359-he/miluim.aspx?â€Ž	Block	1
46.117.249.236	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
31.168.103.115	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
192.117.130.146	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1359-he/miluim.aspx?â€Ž	Block	1
81.218.241.26	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/894-he/miluim.aspx	Block	1
46.19.85.222	Israel	147.237.0.120		Abnormally Long Request method	Block	1
5.29.33.216	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
176.12.141.145	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
79.178.18.151	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1359-he	Block	1
37.26.149.175	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
193.169.70.108	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim	Block	1
94.159.168.94	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
46.19.85.222	Israel	147.237.0.120		Malformed URL	Block	1
176.13.18.96	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1359-he/miluim.aspx?â€Ž	Block	1
46.19.85.165	Israel	147.237.0.120		Distributed Malformed URL	Block	1
2.54.37.149	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/chat/presence_icon.php	Block	1
109.65.154.116	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?â€Ž	Block	1
46.19.85.222	Israel	147.237.0.120		Unknown HTTP Request Method 447538567.1447538544. in URL	Block	1
31.168.103.115	Israel	147.237.0.120		Multiple Unauthorized URL Access from 31.168.103.115	Block	1
185.82.52.225		147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/valtam	Block	1

11-15-2015 to 11-16-2015