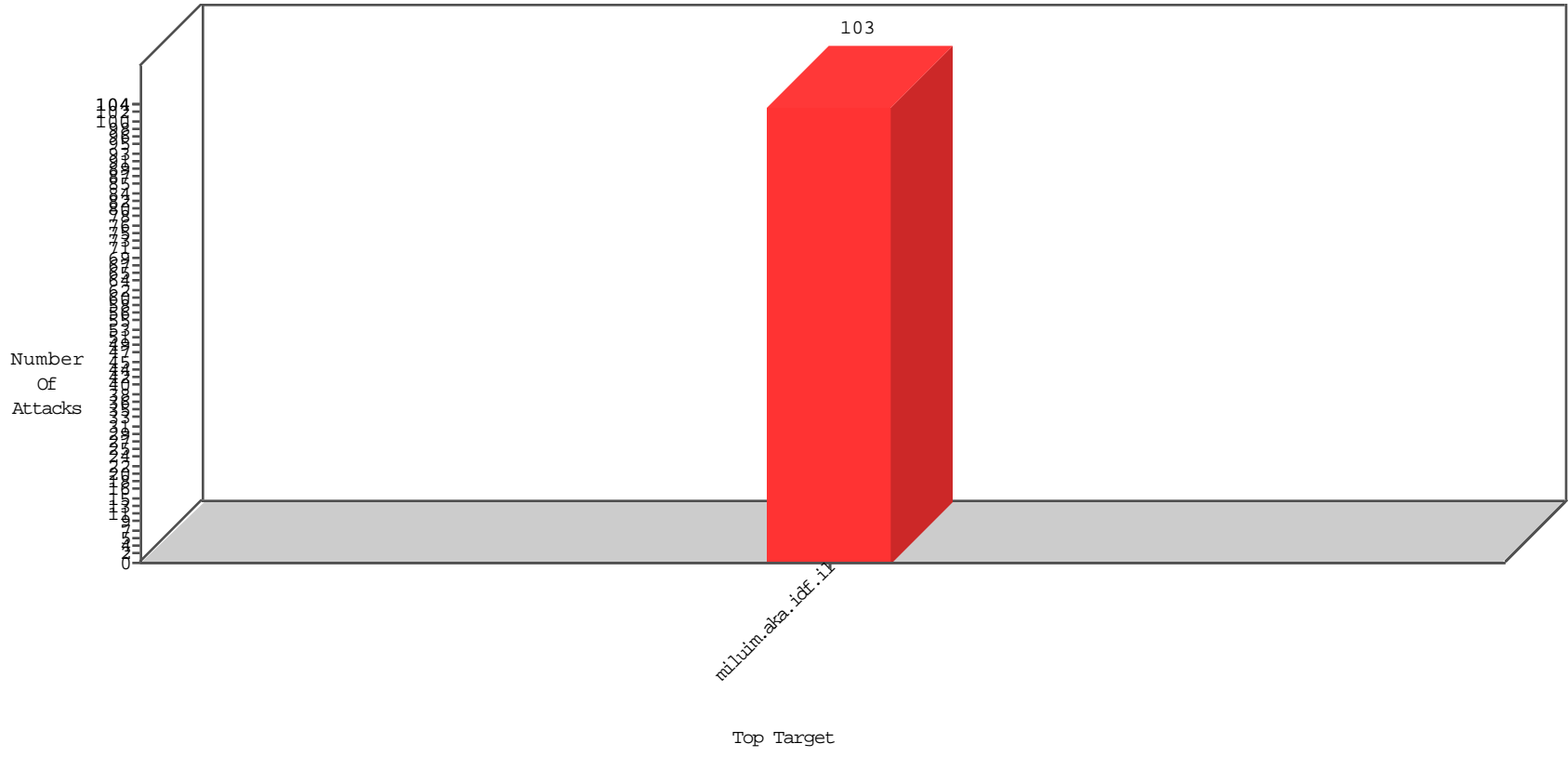


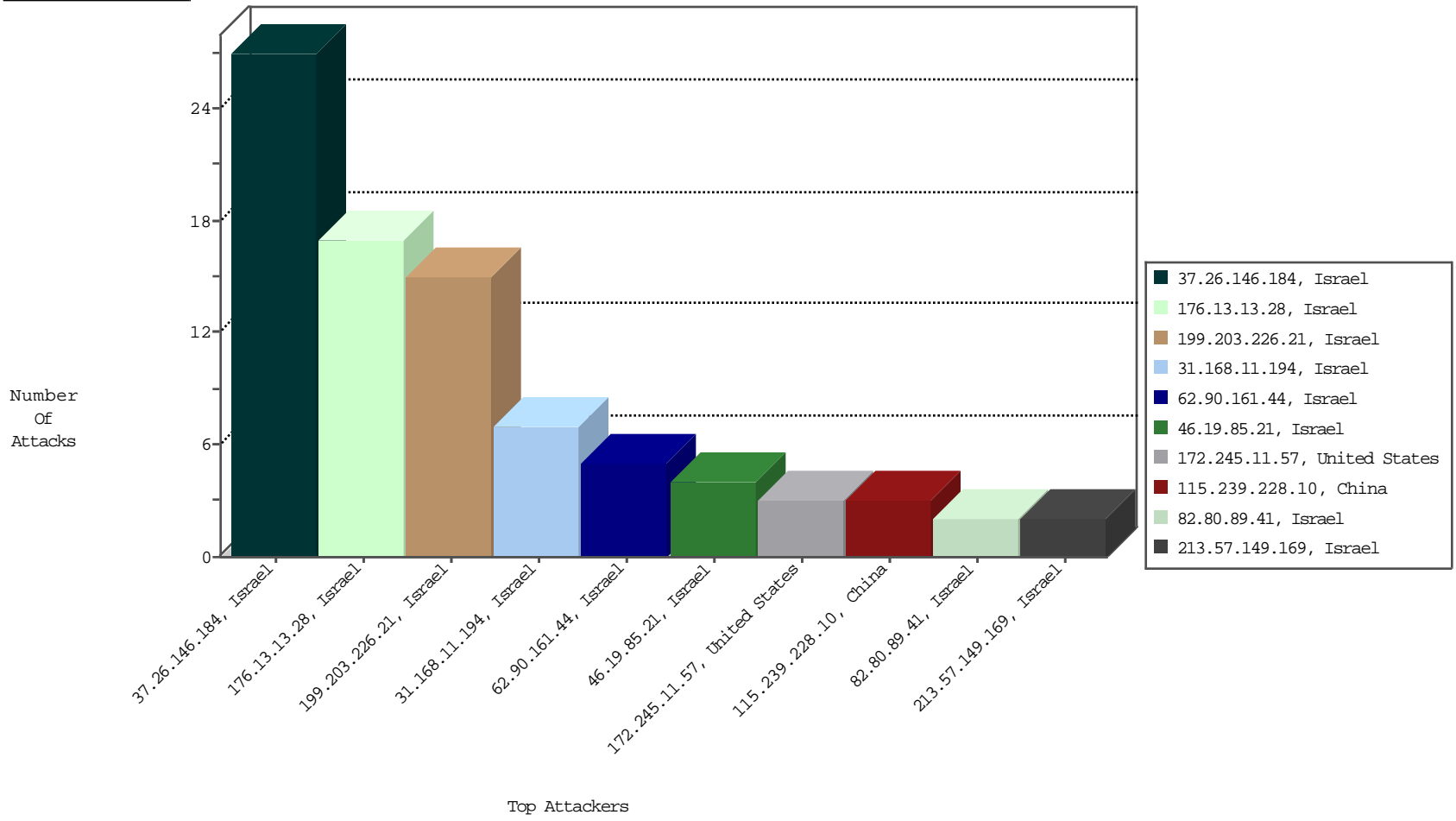
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
31.168.11.194	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	7
115.239.228.10	China	147.237.0.120	miluim.aka.idf.il	Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	2
115.239.228.10	China	147.237.0.120	miluim.aka.idf.il	Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

12-22-2015 to 12-23-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
82.80.89.41	Israel	147.237.0.120	miluim.aka.idf.il	GPL SCAN nmap TCP	2
188.120.135.12	Israel	147.237.0.120	miluim.aka.idf.il	GPL SCAN nmap TCP	2
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
155.94.224.206	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
172.245.11.57	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
196.47.173.21	Cote D'Ivoire	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.213.135	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
172.245.11.57	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
172.245.11.57	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	196854
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	99536
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	43730
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	38402
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	36991
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	30548
23.27.220.82	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	28733
77.127.61.246	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
8.37.234.232	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1444
149.88.233.73	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1417
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1077
213.207.157.117	Cyprus	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	813
149.78.174.246	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	779
81.218.167.106	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	765
149.78.250.48	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	681
207.46.13.162	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	584
149.88.80.46	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	471
149.88.207.54	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	433
149.78.248.29	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	339
95.142.17.12	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	338
167.220.196.25	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	331
66.102.9.90	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	323
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	295
66.249.93.215	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	265
66.249.93.212	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	264
157.55.39.79	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	225
66.102.9.80	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	225
149.78.31.71	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	194
149.88.104.114	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	189
207.46.13.151	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	178
149.78.49.182	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	168
149.88.83.69	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	166
149.78.239.180	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	154
198.208.27.69	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	150
109.67.132.28	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.66.29.112	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.64.125.96	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.63.148	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
66.249.81.224	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	136
149.78.23.22	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	135
66.249.81.230	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	132
85.115.52.201	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	125
149.78.40.112	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	124
173.33.242.56	Canada	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	123
149.78.45.239	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	120
149.88.28.123	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	120
149.78.240.170	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	119
108.171.129.189	Germany	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	114
66.102.9.100	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	111
66.249.81.227	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	111

12-22-2015 to 12-23-2015

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
37.26.146.184	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 37.26.146.184	Block	26
176.13.13.28	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 176.13.13.28	Block	17
199.203.226.21	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 199.203.226.21	Block	12
213.8.121.117	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1399-	Block	2
2.54.161.133	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1399-he/miluim.aspx?aeZ	Block	2
199.203.226.21	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	2
37.26.146.184	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/8/2048.p	Block	1
85.250.84.2	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx?aeZ	Block	1
46.19.85.21	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method User-Agent: in URL mozilla/5.0	Block	1
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.i	Multiple _vti_ from 62.90.161.44	Block	1
46.19.85.21	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request request version	Block	1
213.57.149.169	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 213.57.149.169	Block	1
107.178.38.209	United States	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1399-he/miluim.aspx?aeZ	Block	1
46.19.85.163	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/1393-he/	Block	1
199.203.226.21	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/7/1697.png	Block	1
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/_vti_bin/owssvr.dll	Block	1
46.19.85.21	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version (iPhone; CPU iPhone OS 9_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/13C75 Safari/601.1	Block	1
213.57.149.169	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/1398-he.miluim.aspx	Block	1
46.116.68.86	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1393-	Block	1
79.179.4.192	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1399-he/miluim.aspx?aeZ	Block	1
46.19.85.21	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL mozilla/5.0	Block	1
192.114.91.246	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/resource/userfollowresource/create/	Block	1
62.90.161.44	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 62.90.161.44	Block	1

12-22-2015 to 12-23-2015