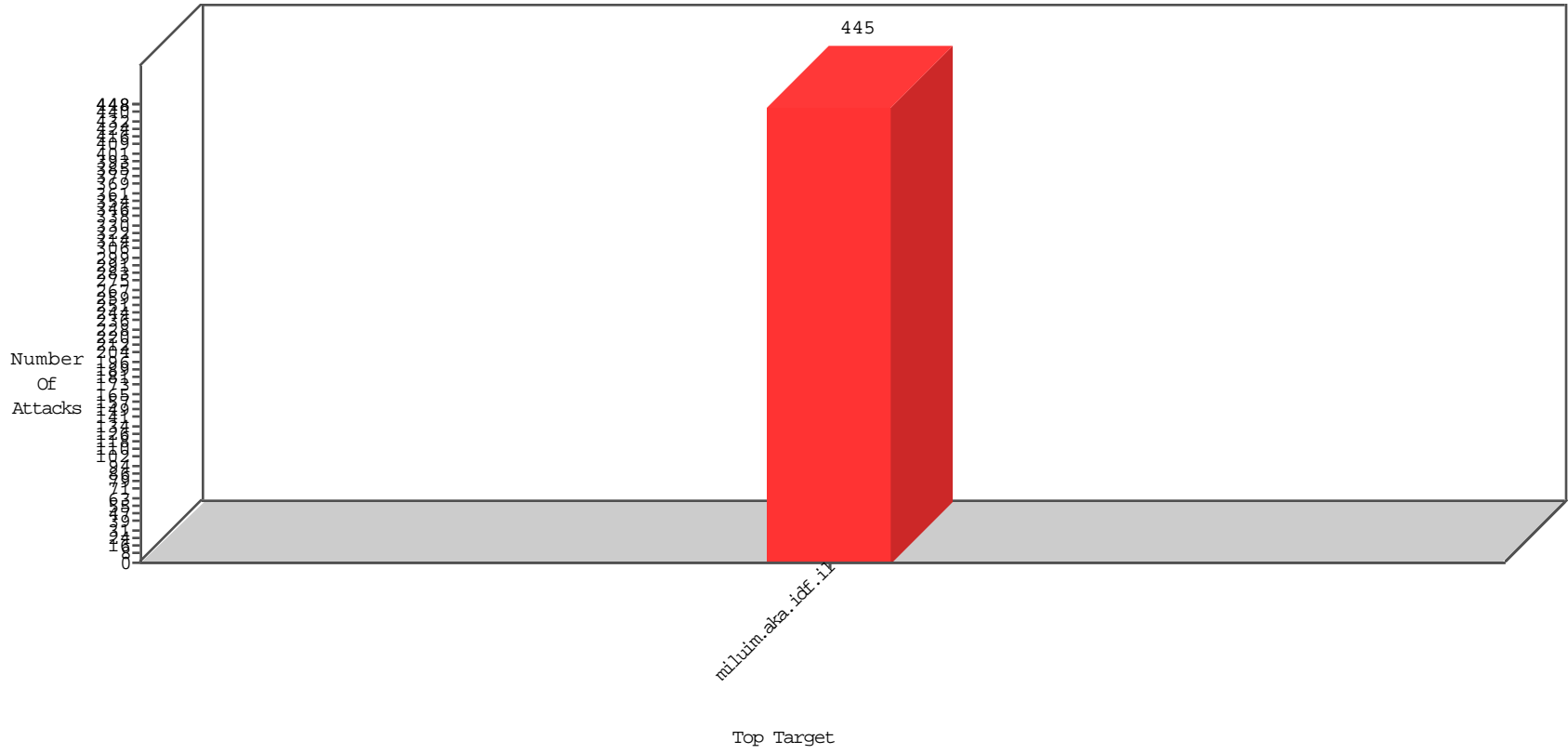


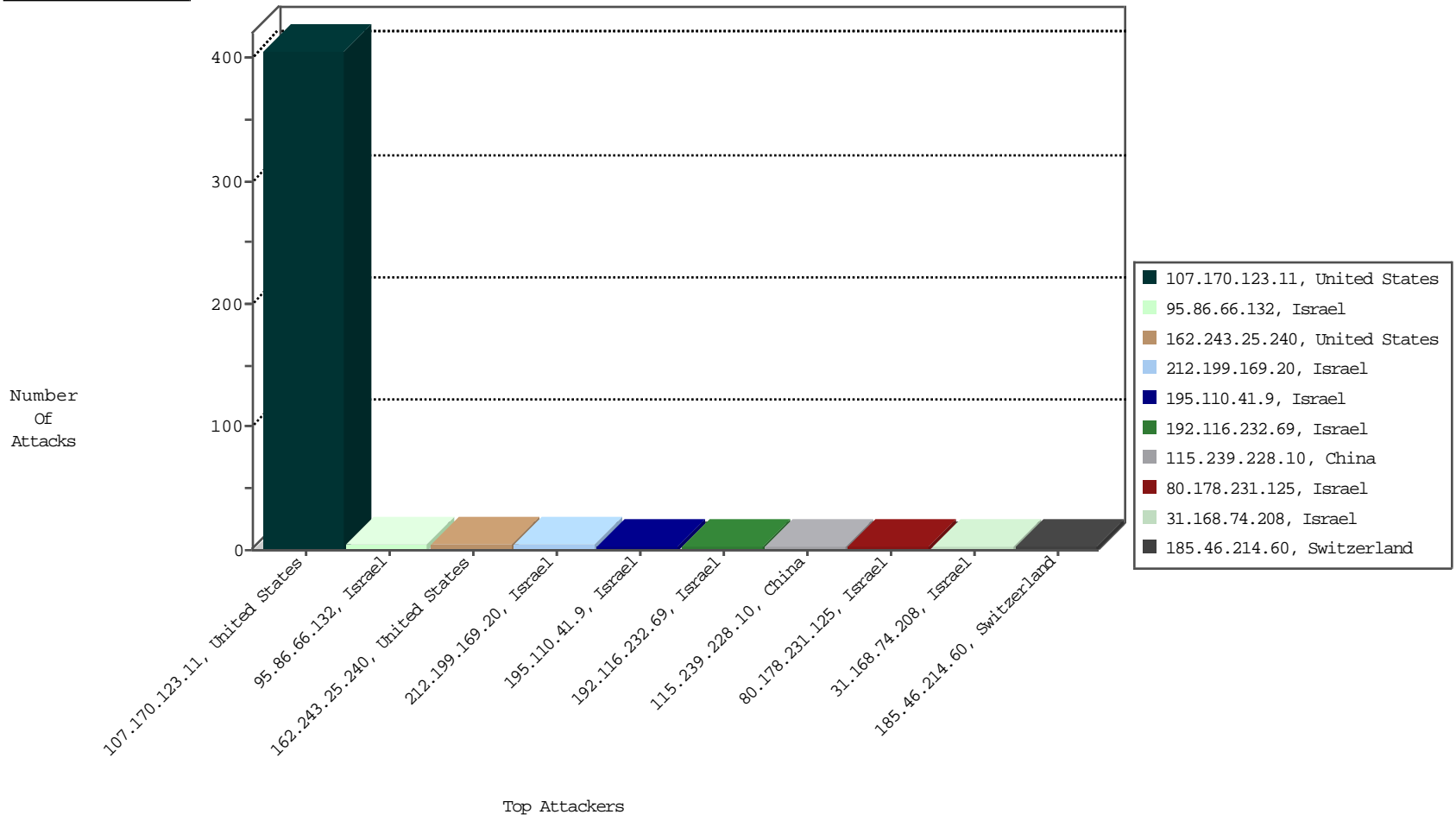
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



01-10-2016 to 01-11-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
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

01-10-2016 to 01-11-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
195.110.41.9	Israel	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	3
93.174.93.203	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.90.21	France	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
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	51947
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	18445
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	17079
8.37.234.25	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4007
169.0.184.111		147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	3272
79.179.208.203	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.21.161	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
82.80.180.229	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2253
81.218.40.194	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2025
2.54.130.44	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2025
168.63.139.43	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1275
64.79.85.205	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1022
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	794
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	741
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	736
149.78.84.19	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	394
149.78.251.210	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	351
79.177.202.241	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	319
79.177.202.241	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	317
149.78.106.169	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	280
149.78.234.208	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	200
109.246.2.234	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	193
149.78.235.227	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	185
15.90.166.11	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	181
66.102.9.80	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	180
149.78.238.85	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	180
149.88.116.187	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	173
149.78.194.209	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	168
81.255.155.162	France	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	166
149.78.18.166	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	160
149.88.7.242	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	151
109.64.220.191	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.180.149.181	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.177.107.113	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.24.21	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.178.126.2	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
149.88.229.240	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	132
149.78.240.103	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	127
149.78.226.247	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	124
66.249.66.52	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	122
149.78.41.140	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	121
37.46.45.41	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	121
37.46.45.41	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	121
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	119
199.127.226.150	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	118
89.76.56.170	Poland	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	113
134.191.232.71	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	112
59.152.202.68	Hong Kong	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	108
149.78.40.5	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	104

01-10-2016 to 01-11-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
107.170.123.11	United States	147.237.0.120	miluim.aka.idf.i	Too Many of the Same Response Code (404) in IP from 107.170.123.11	Block	407
95.86.66.132	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1325-he/miluim.aspx?â€Ž	Block	4
80.178.231.125	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspx).	Block	3
162.243.25.240	United States	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 162.243.25.240	Block	3
31.168.74.208	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/homepage.aspx	Block	2
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/1935.gif	Block	2
212.199.169.20	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	2
185.89.217.229		147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/./images/shared/hp/hp_icon.png	Block	1
212.199.169.20	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.199.169.20	Block	1
162.243.25.240	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
104.236.52.43		147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
2.52.36.22	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1325-he/miluim.aspx?â€Ž	Block	1
185.46.214.60	Switzerland	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 185.46.214.60	Block	1
37.26.146.145	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/8	Block	1
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
2.54.49.93	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1325-he/miluim.aspx?â€Ž	Block	1
212.199.169.20	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/3/	Block	1
185.46.214.60	Switzerland	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/login	Block	1
192.198.151.45	Europe	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/login	Block	1
10.104.60.1		147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1316	Block	1

01-10-2016 to 01-11-2016