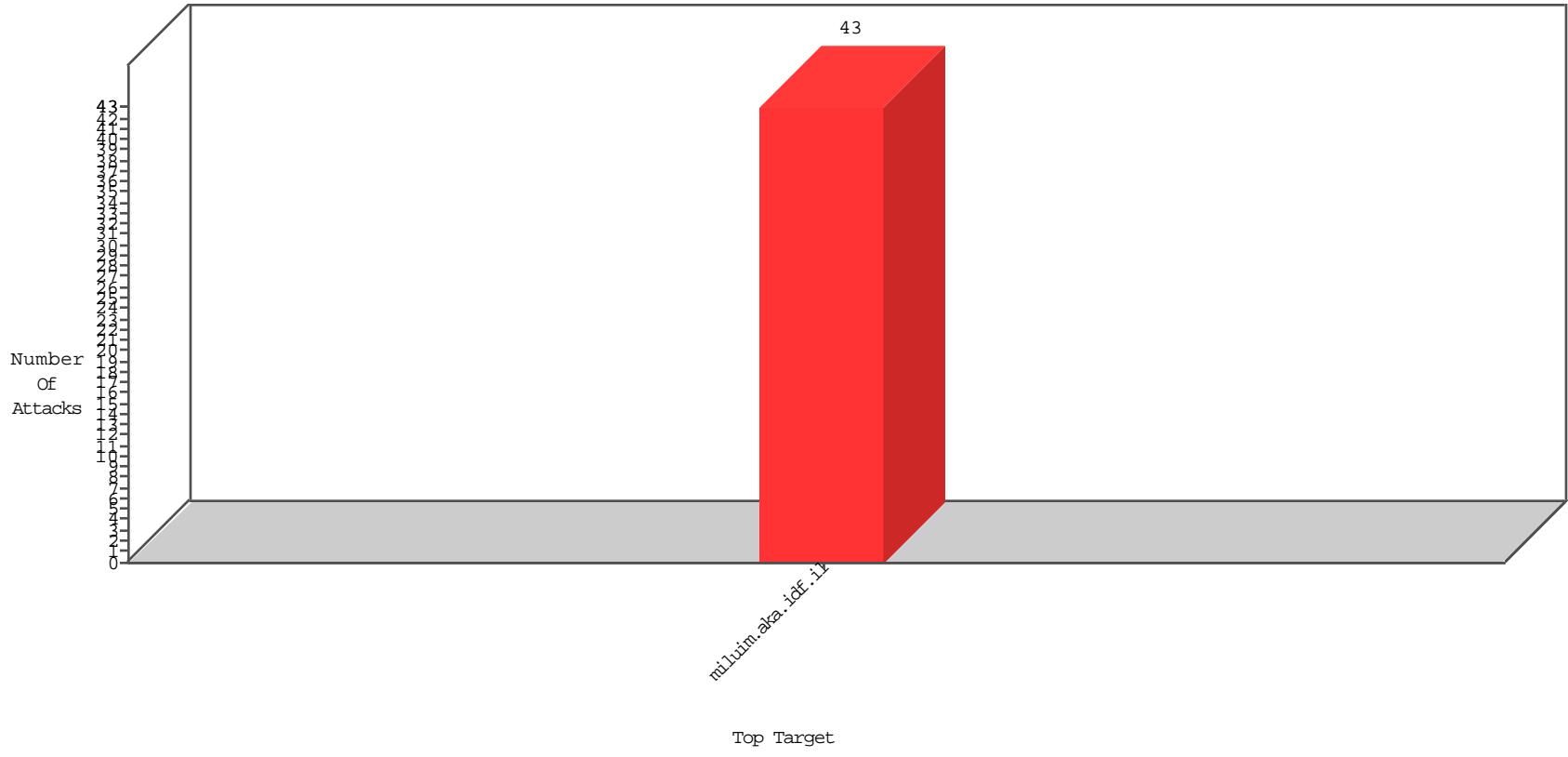


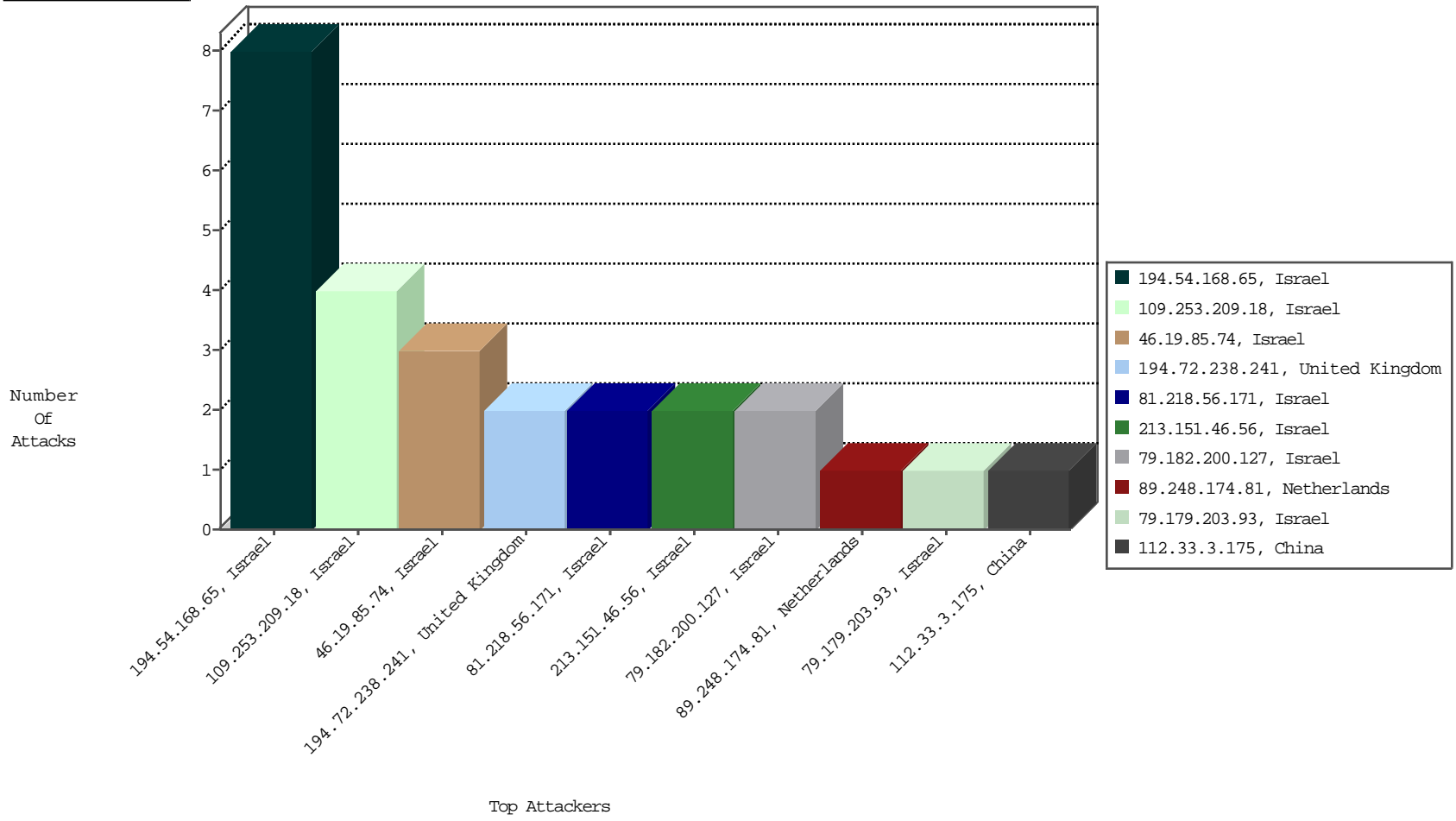
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



02-03-2016 to 02-04-2016

Top Attackers In DDoS-Defence

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

02-03-2016 to 02-04-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
194.54.168.65	Israel	147.237.0.120	miluim.aka.idf.il	C122: HTTP: Access to - .exe or .dll	Permit	2
188.165.15.132	France	147.237.0.120	miluim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
89.248.174.81	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	Canada	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
193.201.227.84	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
91.142.174.82	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
112.33.3.175	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	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
109.66.36.35	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4608
2.52.157.191	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2745
79.179.203.93	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2313
195.200.205.2	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
109.66.113.43	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
84.228.252.153	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.177.119.247	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
87.68.157.102	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
176.12.155.173	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
46.19.86.123	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2120
84.95.130.81	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	882
5.22.134.189	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	674
79.183.181.120	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	513
79.179.28.185	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	360
87.68.23.97	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
84.228.202.188	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
85.65.62.71	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.126.62		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
176.12.154.137	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.176.63.76	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
109.64.163.109	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
77.127.161.100	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	122
79.179.8.53	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
77.127.241.103	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	82
46.19.86.106	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
2.52.185.227	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
199.203.151.209	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
37.26.148.232	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
79.179.51.191	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.86.96	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
84.111.20.148	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
149.78.32.224	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
46.19.85.131	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.117	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
77.126.62.81	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
82.81.55.167	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.131	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
37.26.149.210	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
149.78.32.224	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
46.19.85.129	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	29
2.52.33.49	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
109.65.11.173	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
212.143.240.134	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
212.143.240.134	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
46.121.128.98	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
217.132.103.134	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
62.219.44.190	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	drop	Unexpected post SYN packet - RST or SYN expected	drop	20
66.249.81.227	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	20

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
109.253.209.18	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 109.253.209.18	Block	4
194.54.168.65	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 194.54.168.65	Block	3
81.218.56.171	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
194.54.168.65	Israel	147.237.0.120	miluim.aka.idf.i	Multiple _vti_ from 194.54.168.65	Block	2
79.182.200.127	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	1
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
208.115.113.89	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/te	Block	1
79.177.193.156	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	1
46.19.85.74	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method 4bl; in URL idf_cellular_redirect=toosite	Block	1
194.54.168.65	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/_vti_bin/owssvr.dll	Block	1
80.178.121.228	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 80.178.121.228	Block	1
70.39.157.192	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/mailto:moked_miluim@mail.idf.il	Block	1
213.151.46.56	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 213.151.46.56	Block	1
175.158.0.1	Korea, Republic of	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/994-8344-he/miluim.aspx.	Block	1
79.179.203.93	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter ei in www.miluim.aka.idf.il/console/core/doc_mgr/library/manage/resource/getfilecontent.hh.asp	Block	1
61.135.190.197	China	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
194.72.238.241	United Kingdom	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /	Block	1
70.39.157.196	United States	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter &y	Block	1
46.19.85.74	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
213.151.46.56	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewibnevok9zkahvjvbjkbnexaqfegg1mae&usq=afqjcne5p7m9pmcma58u2cjzfnfg7azoamw	Block	1
79.182.200.127	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 79.182.200.127	Block	1
66.249.81.230	Israel	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/../../images/shared/hp/nav_bg.png	Block	1
194.72.238.241	United Kingdom	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/xyzzzy	Block	1
89.248.174.4	Netherlands	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
70.39.157.199	United States	147.237.0.120	miluim.aka.idf.i	Unknown Parameter &y in www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.85.74	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL idf_cellular_redirect=toosite	Block	1