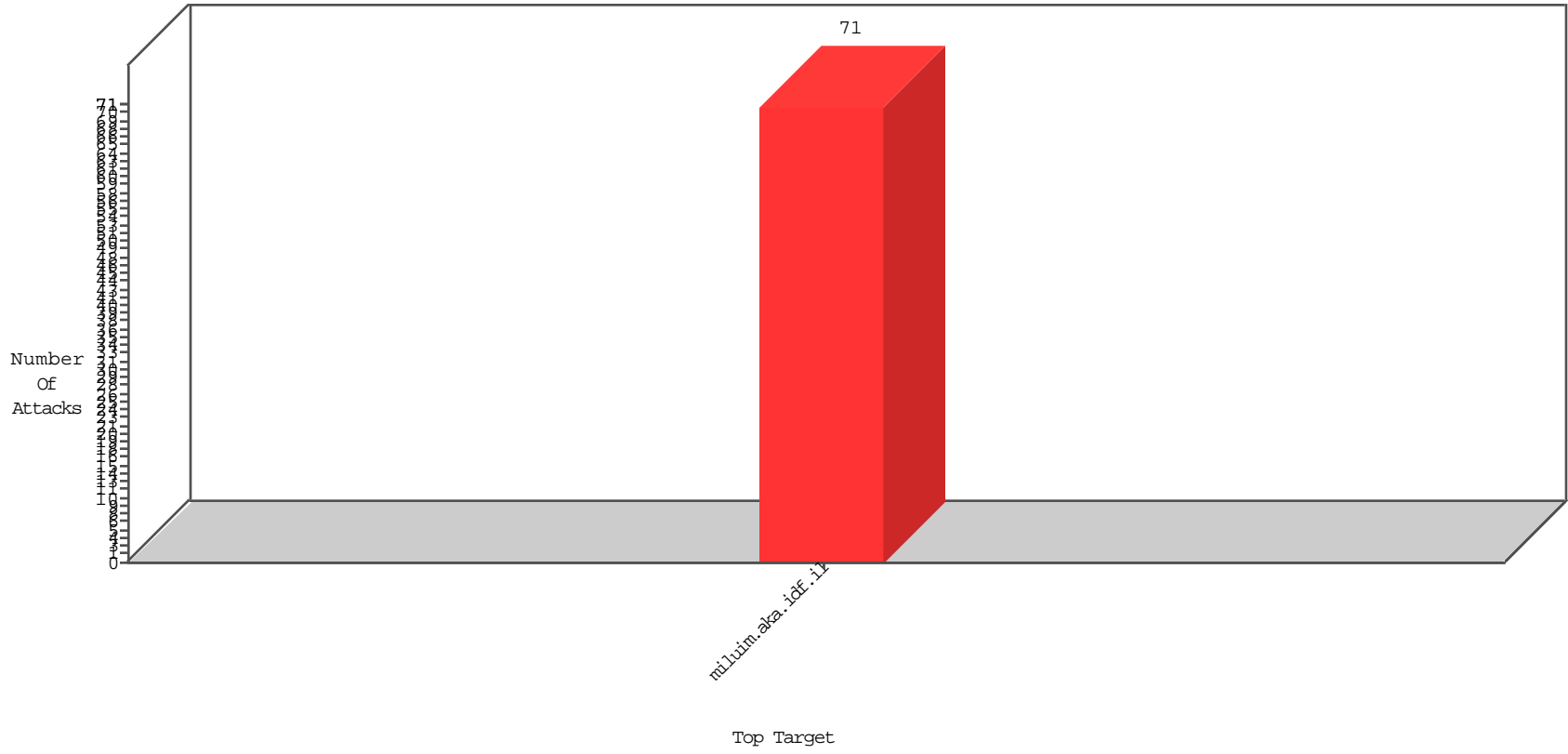


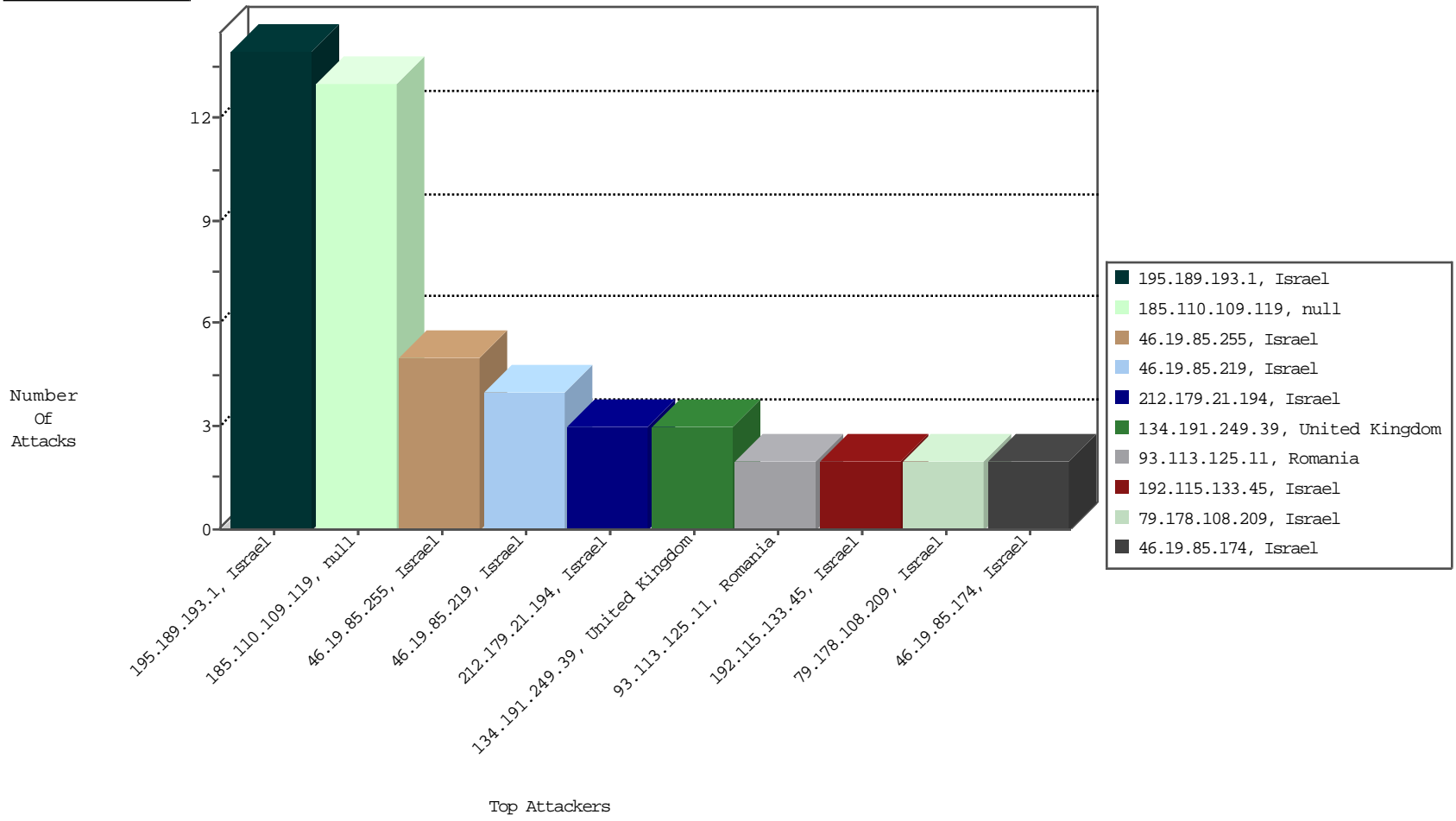
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



Top Attackers In DDoS-Defence

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

## Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
195.189.193.1	Israel	147.237.0.120	miluim.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	14
192.115.133.45	Israel	147.237.0.120	miluim.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.120.204.172	Israel	147.237.0.120	miluim.aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
93.113.125.11	Romania	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.23.112.119	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.209.6	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
109.66.183.140	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4608
91.148.217.199	Netherlands	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1602
2.54.36.151	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	693
82.81.88.98	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
87.68.41.74	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
109.64.98.166	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
109.64.4.42	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
2.54.161.52	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
2.52.168.169	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	150
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
62.219.238.10	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.187.203	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	129
2.54.0.96	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	116
2.54.0.96	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	116
185.27.105.154	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
79.181.118.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
84.228.111.120	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
207.232.21.105	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	78
46.19.86.125	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
79.182.180.175	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
149.78.165.30	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
2.52.1.72	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.85.223	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
31.168.194.98	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
37.26.146.245	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.183.122.207	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.12	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.181.137.11	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.85.63	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.181.179.57	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.130	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	32
109.253.222.136	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
37.46.39.87	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.100	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
46.19.85.189	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
185.3.144.111	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.66.157.154	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
148.177.129.213	Europe	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.198.151.36	Europe	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
31.210.186.10	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
37.26.147.218	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.179.227.201	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
212.143.240.134	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
80.179.201.104	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
213.57.215.42	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
2.54.3.76	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.194	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
176.13.3.227	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
87.69.238.94	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.55	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
185.110.109.119		147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 185.110.109.119	Block	11
174.129.237.157	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	2
134.191.249.39	United Kingdom	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspxhttp:/	Block	2
79.182.174.30	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/xmlrpc.php	Block	1
46.19.85.255	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unknown HTTP Request Method from 46.19.85.255	Block	1
46.19.85.219	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
104.128.144.131	Canada	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
79.178.108.209	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
46.19.85.255	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
185.110.109.119		147.237.0.120	miluim.aka.idf.i	Unknown Parameter vir in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
134.191.249.39	United Kingdom	147.237.0.120	miluim.aka.idf.i	Suspicious Response Code	Block	1
81.218.56.171	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
46.19.85.255	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	1
46.19.85.219	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL keep-alive	Block	1
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
185.89.217.225		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
128.232.110.28	United Kingdom	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
79.178.108.209	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
46.19.85.255	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
199.255.138.45	United States	147.237.0.120	miluim.aka.idf.i	eMail Hoarding	Block	1
46.19.85.174	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
81.218.241.26	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/	Block	1
46.116.40.91	Israel	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method	Block	1
46.19.85.219	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	1
213.151.47.152	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 213.151.47.152	Block	1
133.130.49.166	Japan	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 133.130.49.166	Block	1
79.182.174.30	Israel	147.237.0.120	miluim.aka.idf.i	Distributed PHP Attempt	Block	1
46.19.85.255	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Malformed URL from 46.19.85.255	Block	1
46.19.85.174	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Distributed Illegal Byte Code Character in Method	Block	1
93.113.125.11	Romania	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /	Block	1
46.116.40.91	Israel	147.237.0.120	miluim.aka.idf.i	NULL Character in Method	Block	1
46.19.85.219	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method Connection: in URL keep-alive	Block	1
213.151.47.152	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewij3fwi44dlahvhfhokhym-axeqfggimaa&usq=afqjncne5p7m9pmcma58u2cjznfg7azoamw	Block	1
185.110.109.119		147.237.0.120	miluim.aka.idf.i	Unknown Parameter vi in www.miluim.aka.idf.il/1422-he/miluim.aspx	Block	1
133.130.49.166	Japan	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.behatsdaa.org.il	Block	1