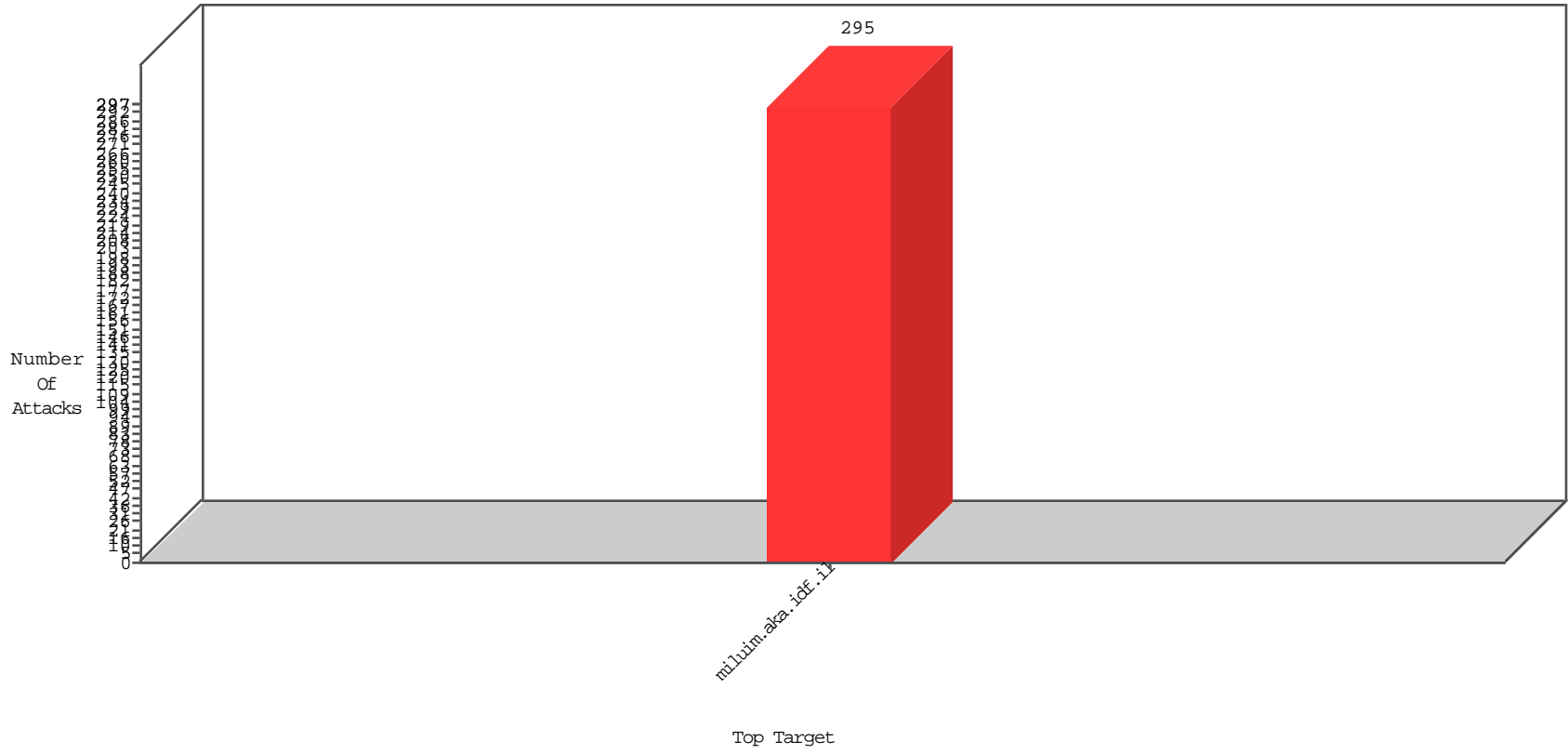


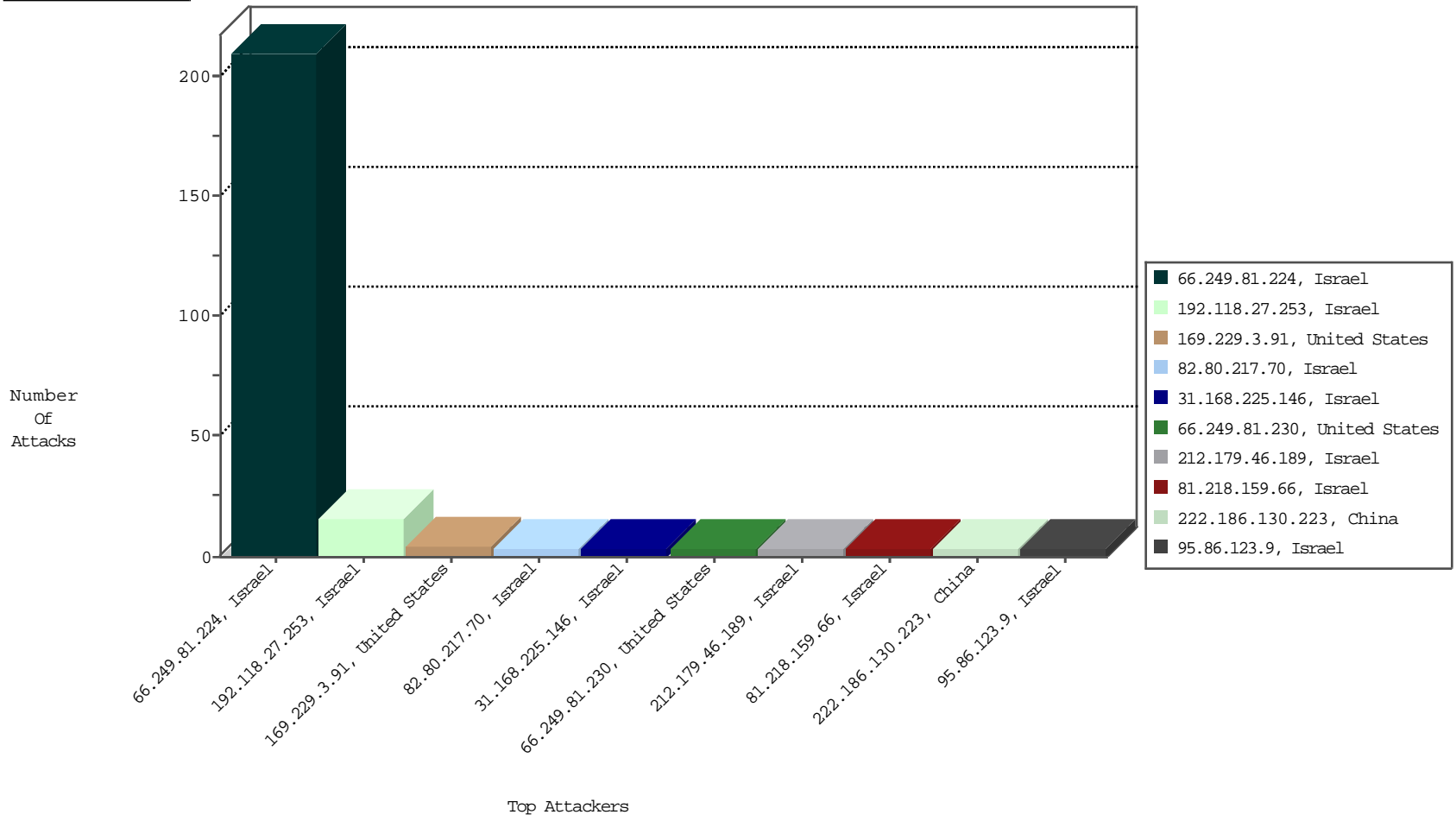
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.81.224	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	210
31.168.225.146	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Isreal	3
82.80.217.70	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Isreal	3
212.179.46.189	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Isreal	3
222.186.130.223	China	147.237.0.120	miluim.aka.idf.il	Frk_Under_Attack_Con_Http	drop	BEL-Frankfurt	2
222.186.130.223	China	147.237.0.120	miluim.aka.idf.il	Frk_Purple_Con_Limit_Http	drop	BEL-Frankfurt	1
81.218.56.125	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Isreal	1
109.66.0.130	Israel	147.237.0.120	miluim.aka.idf.il	L4 Source or Dest Port Zero	drop	BEL-Isreal	1

02-14-2016 to 02-15-2016

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
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	3
40.76.48.99	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
123.220.251.190	Japan	147.237.0.120	miluim.aka.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
2.52.15.149	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3033
79.180.154.208	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.59.119	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
62.219.151.187	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
82.102.184.211	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1332
79.181.118.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
2.54.167.23	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	414
2.54.63.185	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	369
46.19.86.116	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack		reject	289
79.181.145.160	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.180.127.208	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
2.54.175.7	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
81.218.204.248	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	188
46.19.85.34	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.125.24		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.17.160	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
46.19.86.116	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	121
37.46.39.44	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	121
81.218.204.248	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	111
81.218.204.248	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	106
79.176.232.187	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	103
2.54.60.225	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
149.78.43.80	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.86.116	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	82
79.180.210.230	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
37.46.38.224	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	81
2.52.18.112	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
2.52.40.22	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	65
149.88.246.189	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
46.19.85.140	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
81.218.68.234	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
109.64.163.90	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence		monitor	52
46.19.86.176	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	51
2.52.139.57	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
79.179.116.183	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.86.163	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
82.81.13.170	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
46.19.86.75	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	38
46.19.86.116	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	37
87.69.219.104	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.69	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
77.125.13.200	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.21	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.85.69	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
77.125.108.214	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
89.139.150.64	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
109.67.34.29	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
2.54.144.47	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.75	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.118.27.253	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 192.118.27.253	Block	8
192.118.27.253	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	7
46.19.86.25	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1438	Block	3
81.218.159.66	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1439he/miluim.aspx	Block	3
95.86.123.9	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 95.86.123.9	Block	3
192.116.166.6	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1438	Block	2
87.69.130.233	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
80.178.190.178	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1439-he/miluim.aspx&?&eZ	Block	1
212.143.173.198	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	1
2.54.158.67	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspx.	Block	1
141.212.122.112	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /x	Block	1
109.66.151.125	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1439-he/miluim.aspx&?&eZ	Block	1
82.80.192.100	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/1439-he	Block	1
217.132.129.157	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1439-he/miluim.aspx&?&eZ	Block	1
198.204.249.34	United States	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/./shared/usercontrols/headerupper/	Block	1
46.19.86.7	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1438	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method @yÄ,Ä;Ä;Ä†;ÄeÄ²Ä^Ä?Ä@([#4])J0ÄŠ IÄo([#24])	Block	1
123.220.251.190	Japan	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/manager/html	Block	1
93.172.58.137	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1439he/miluim.aspx	Block	1
80.178.190.178	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1439-he/miluim.aspx&?&eZ	Block	1
212.143.173.198	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
31.168.185.0	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1439-he/miluim.aspx	Block	1
149.78.26.82	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1435-he/miluim.aspx&?&eZ	Block	1
109.67.15.75	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1439-he/miluim.aspx&?&eZ	Block	1
82.166.233.145	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1325-hemiluim.aspx	Block	1
212.143.90.173	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	1
2.54.50.155	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1439-he/miluim.aspx&?&eZ	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in URL	Block	1
139.181.48.2	United States	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 139.181.48.2	Block	1
95.86.116.26	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1438he/miluim.aspx	Block	1
213.8.71.26	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	1
37.26.148.243	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1439-he/miluim.aspx&?&eZ	Block	1
157.55.39.229	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
122.201.19.100	Mongolia	147.237.0.120	miluim.aka.idf.i	E-mail collector robots 14	Block	1
87.69.130.233	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
61.135.190.69	China	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
212.143.90.173	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
2.54.135.130	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1439-he/miluim.aspx&?&eZ	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method @yÄ,Ä;Ä;Ä†;ÄeÄ²Ä^Ä?Ä@([#4])J0ÄŠ IÄo([#24]) in URL	Block	1
139.181.48.2	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/0	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
213.8.71.26	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
192.118.27.253	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1
46.19.85.59	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1438-he/miluim.aspx&?&eZ	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
122.201.19.100	Mongolia	147.237.0.120	miluim.aka.idf.i	eMail Hoarding	Block	1