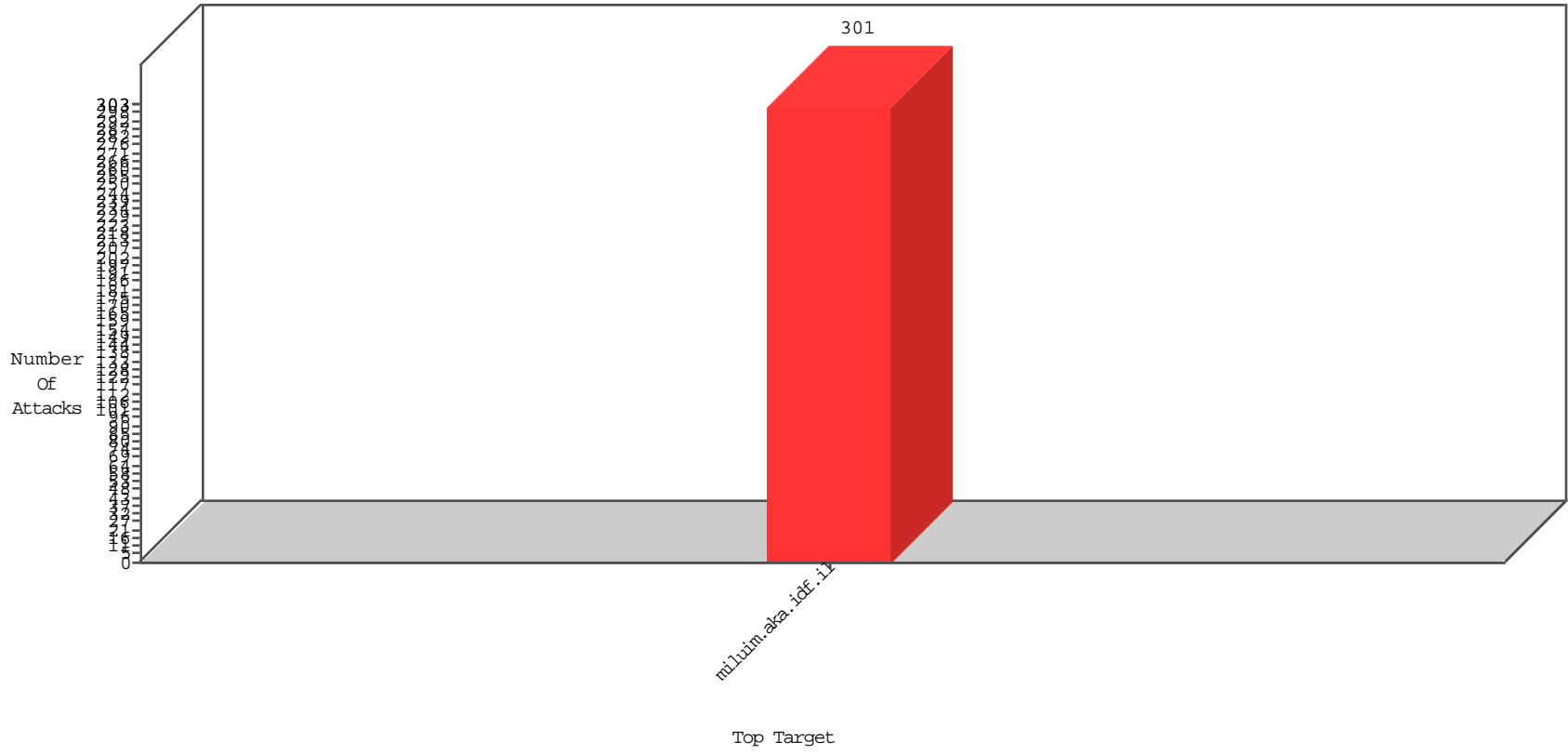


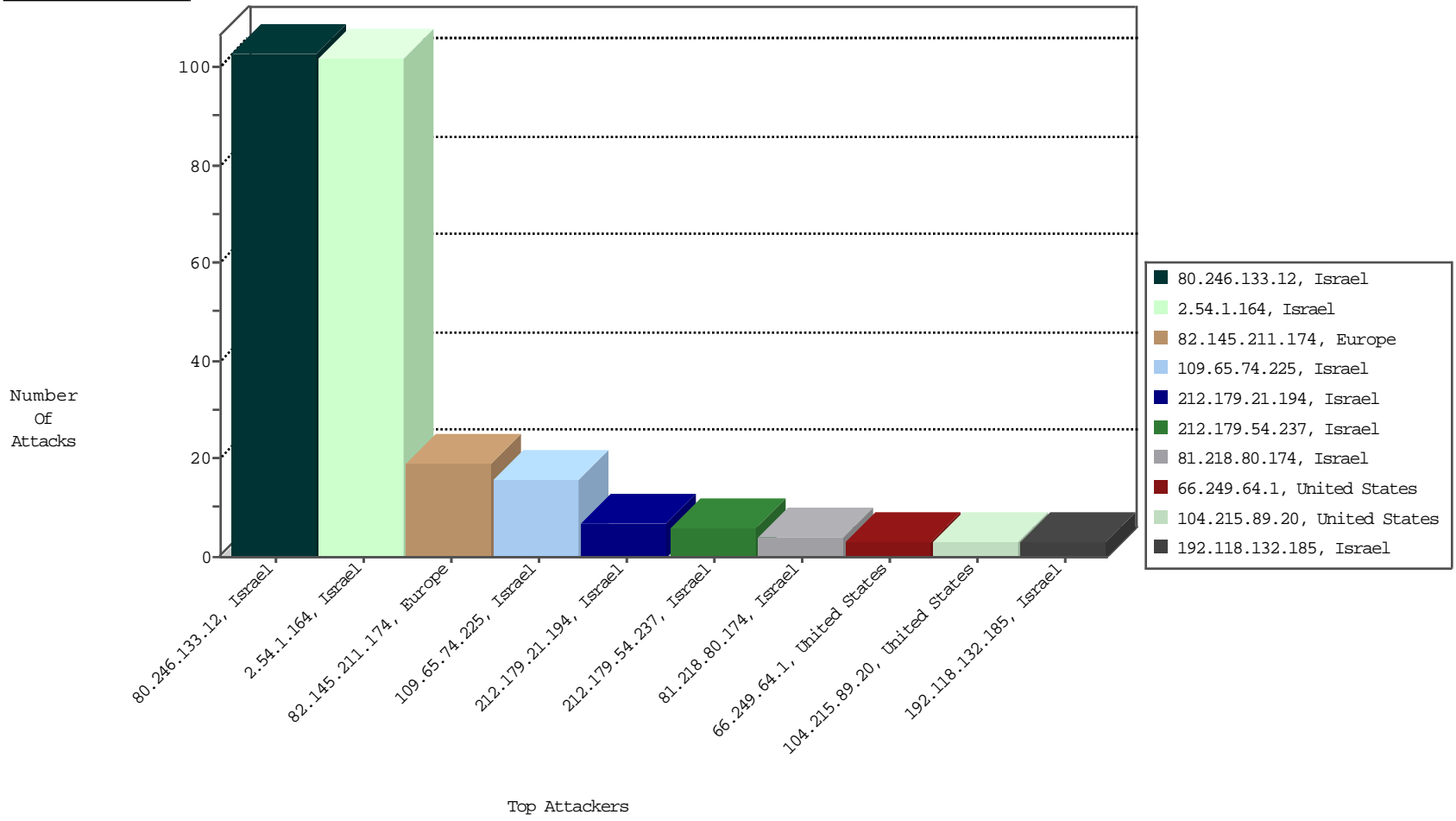
# Focused IP Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
82.145.211.174	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	19
109.65.74.225	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	16
212.179.54.237	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	6
192.118.132.185	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
120.25.238.95	China	147.237.0.120	miluim.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	BBL-Israel	1
162.216.114.158	United States	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
184.105.139.70	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.247.247	United States	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
198.84.107.122	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1

## Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
80.246.133.12	Israel	147.237.0.120	miluim.aka.idf.i	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	103
2.54.1.164	Israel	147.237.0.120	miluim.aka.idf.i	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	102
80.246.133.220	Israel	147.237.0.120	miluim.aka.idf.i	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	3

## Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
94.102.49.151	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.215.89.20	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.249		147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
212.227.89.173	Germany	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
87.101.205.108	Saudi Arabia	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.215.89.20	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
104.215.89.20	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
193.201.227.52	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
79.179.117.148	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
46.19.85.83	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
46.19.86.231	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1296
31.168.246.165	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	900
79.180.210.18	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	441
79.179.230.193	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
109.67.166.179	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
37.26.147.163	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	256
2.54.186.33	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
109.64.122.2	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	162
46.19.85.54	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	146
109.65.152.207	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
77.127.2.70	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.125.34		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
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
185.120.126.12		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.125.26		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.179.32.84	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	125
2.54.172.149	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
197.27.33.77	Tunisia	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.85.146	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
2.52.140.113	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
46.19.85.21	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
37.26.148.157	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
46.19.85.247	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.86.47	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
37.26.146.206	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
79.183.129.98	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.86.49	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.177.112.23	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.141	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	32
212.68.132.218	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
93.173.166.142	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
46.19.85.177	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
46.19.85.150	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
84.111.170.161	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
84.111.170.161	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
110.77.251.64	Thailand	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.86.180	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
37.26.149.193	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
149.88.184.132	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
87.71.68.151	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
37.46.41.49	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
212.150.255.134	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.49	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.189	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
87.71.68.151	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.85.50	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
194.56.215.218	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	13

## Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	3
81.218.80.174	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	2
197.27.33.77	Tunisia	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/1/1911.pdf'	Block	2
95.86.66.165	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 95.86.66.165	Block	2
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Distributed PHP Attempt	Block	2
82.166.58.226	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/newpassword/firstlogin	Block	1
66.249.64.7	United States	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
46.120.78.168	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	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
149.78.38.68	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/x	Block	1
66.249.64.1	United States	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 66.249.64.1	Block	1
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Distributed URL is Above Root Directory	Block	1
46.120.78.168	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter in www.miluim.aka.idf.il/1316-he/miluim.aspx	Block	1
157.55.39.58	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
81.218.80.174	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1
66.249.64.1	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/navmenu/	Block	1
37.26.146.195	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspx.	Block	1
132.64.205.32	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/undefined	Block	1
79.179.131.215	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/login	Block	1
62.219.110.1	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1325-he	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method	Block	1
81.218.241.25	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/1231-he/miluim.aspx	Block	1
66.249.64.1	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/sitemap/sitemap.aspx	Block	1
46.120.78.168	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 46.120.78.168	Block	1
132.68.9.80	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter fileld in www.miluim.aka.idf.il/console/core/doc_mgr/library/manage/resource/getfilecontent.hh.asp	Block	1
81.218.80.174	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 81.218.80.174	Block	1
62.219.110.1	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1325-he/	Block	1
185.112.248.32		147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1