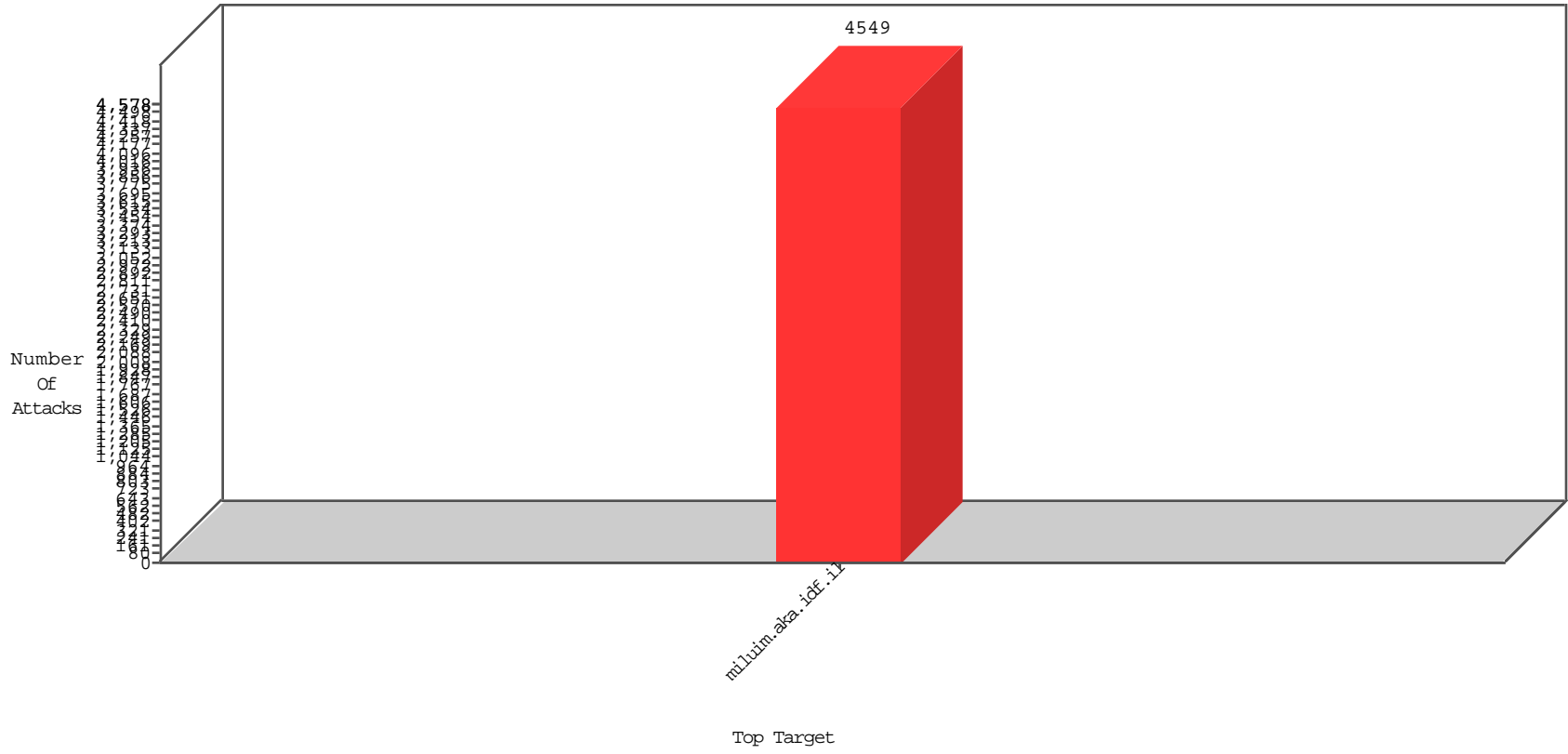


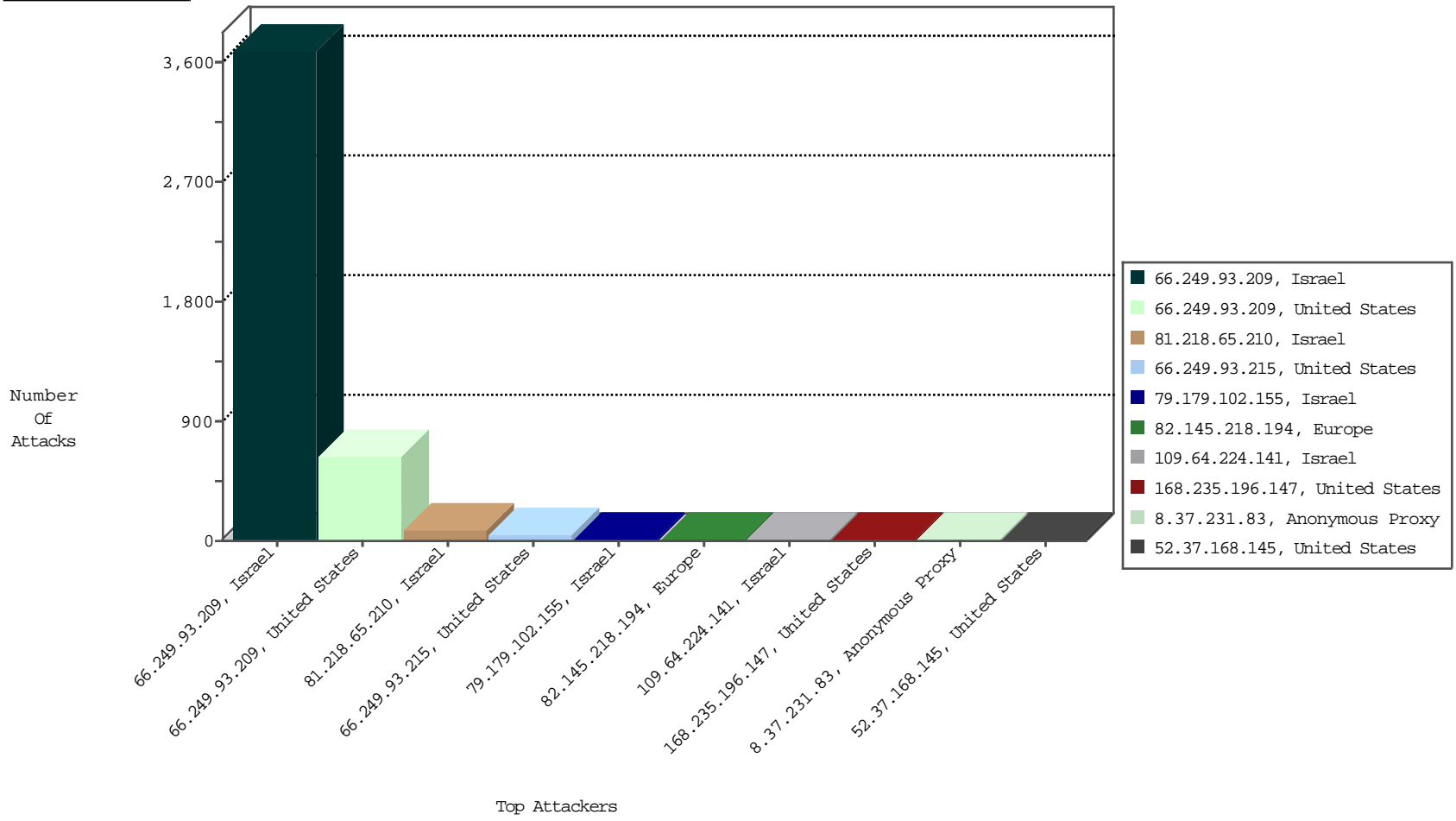
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BEL-Frankfurt	3689
81.218.65.210	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	86
82.145.218.194	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	7
109.64.224.141	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	6
81.218.206.82	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3
82.81.54.21	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3
8.37.231.83	Anonymous Proxy	147.237.0.120	miluim.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	NetV-London	3
212.179.54.237	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	3
168.235.196.147	United States	147.237.0.120	miluim.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	NetV-London	3
168.235.196.147	United States	147.237.0.120	miluim.aka.idf.il	JLM_Under_Attack_Con_Http	drop	NetV-London	2
8.37.231.83	Anonymous Proxy	147.237.0.120	miluim.aka.idf.il	JLM_Under_Attack_Con_Http	drop	NetV-London	2
81.218.56.125	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	1
184.105.139.86	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
193.242.218.6	Switzerland	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
209.126.105.33	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
89.248.174.4	Netherlands	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
71.6.216.45	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1

03-07-2016 to 03-08-2016

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
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	627
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	45
221.226.31.210	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
114.207.112.188	Korea, Republic of	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
125.88.181.35	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.6.32.82	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
221.226.31.210	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
118.112.185.236	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
208.109.53.250	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
221.6.32.82	China	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
31.210.178.99	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6146
79.176.143.159	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5697
168.235.196.147	United States	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4525
168.235.196.147	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4525
79.176.119.8	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4100
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	3953
79.176.194.49	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2628
31.210.187.163	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2313
79.176.175.104	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2313
87.71.12.228	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.179.114.242	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
192.116.245.209	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.16.97	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	1953
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1903
87.71.13.59	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1386
2.54.163.43	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1089
46.19.86.207	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1089
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	830
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	drop	Unexpected post SYN packet - RST or SYN expected	drop	760
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	585
79.178.57.167	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
79.182.108.253	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	449
46.19.85.107	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	441
2.54.161.63	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
62.219.48.54	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	414
192.115.30.42	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	382
192.115.30.42	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	344
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	318
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	315
79.181.165.33	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	297
79.179.28.208	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
82.166.57.226	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	274
109.64.195.75	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	261
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	261
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	254
2.54.166.182	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
2.52.27.35	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
79.180.151.206	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
2.54.5.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
46.19.85.15	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
8.37.231.83	Anonymous Proxy	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	196
2.54.11.77	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	189
2.54.156.140	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	189
2.54.2.232	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.160.178	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.181.58.195	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
62.0.104.6	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
87.70.8.68	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
79.179.102.155	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 79.179.102.155	Block	13
79.183.184.234	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	3
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	3
52.37.168.145	United States	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	2
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.179.21.194	Block	2
212.179.21.194	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	2
212.25.93.246	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/mefakdim.htmhttp:/	Block	2
194.114.146.227	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
46.19.85.39	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method 57001436.2.1457341892.1457341610.; in URL _pk_ses.104.b624=*	Block	1
95.86.114.4	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 95.86.114.4	Block	1
46.19.85.128	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method 4e4024ea1.1448895439.1.1448895445.1448895439.; in URL asp.net_sessionid=0jcypx45ean2ut554f303hrx	Block	1
217.132.37.61	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1451-he/miluim.asp	Block	1
46.19.85.39	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	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/footer/1230-he/miluim.aspx	Block	1
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	1
52.37.168.145	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to miluim.aka.idf.il/wp-login.php	Block	1
46.19.85.128	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
95.86.114.4	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjd3-cc_q7lahxh1a4khzvha2qqfggimaa&usg=afqjcne5p7m9pmcma58u2cjzfnfg7azoamw	Block	1
79.179.190.47	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
46.19.85.236	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1422-he/	Block	1
46.19.85.39	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
204.12.251.37	United States	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/./shared/usercontrols/footer/1230-he/miluim.aspx	Block	1
66.249.73.235	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
46.19.85.128	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
213.151.45.75	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 213.151.45.75	Block	1
45.55.32.117		147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 45.55.32.117	Block	1
185.82.200.91		147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
79.179.190.47	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
52.37.168.145	United States	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 52.37.168.145	Block	1
46.19.85.39	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL _pk_ses.104.b624=*	Block	1
87.69.86.197	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/	Block	1
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Distributed URL is Above Root Directory	Block	1
46.19.85.128	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL asp.net_sessionid=0jcypx45ean2ut554f303hrx	Block	1
217.132.37.61	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 217.132.37.61	Block	1
45.55.32.117		147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/magento_version	Block	1