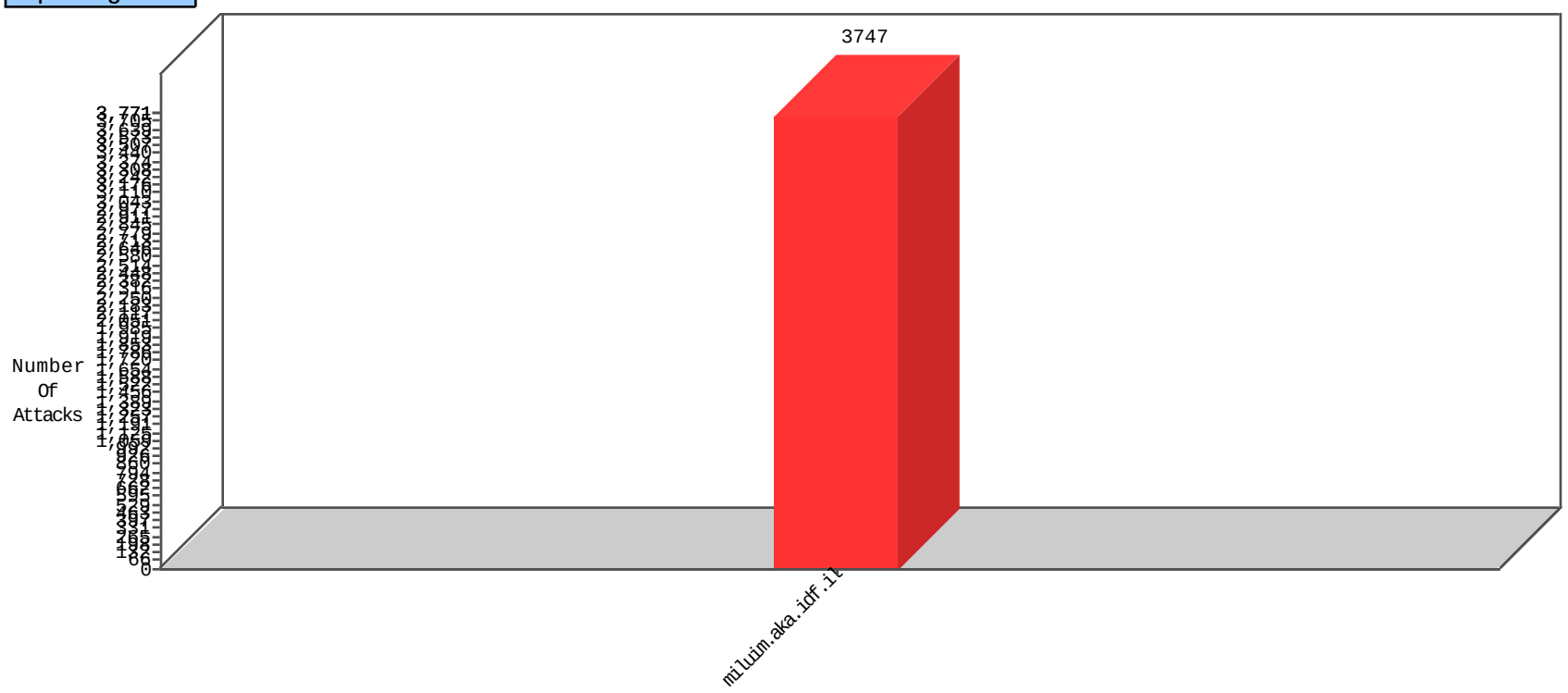
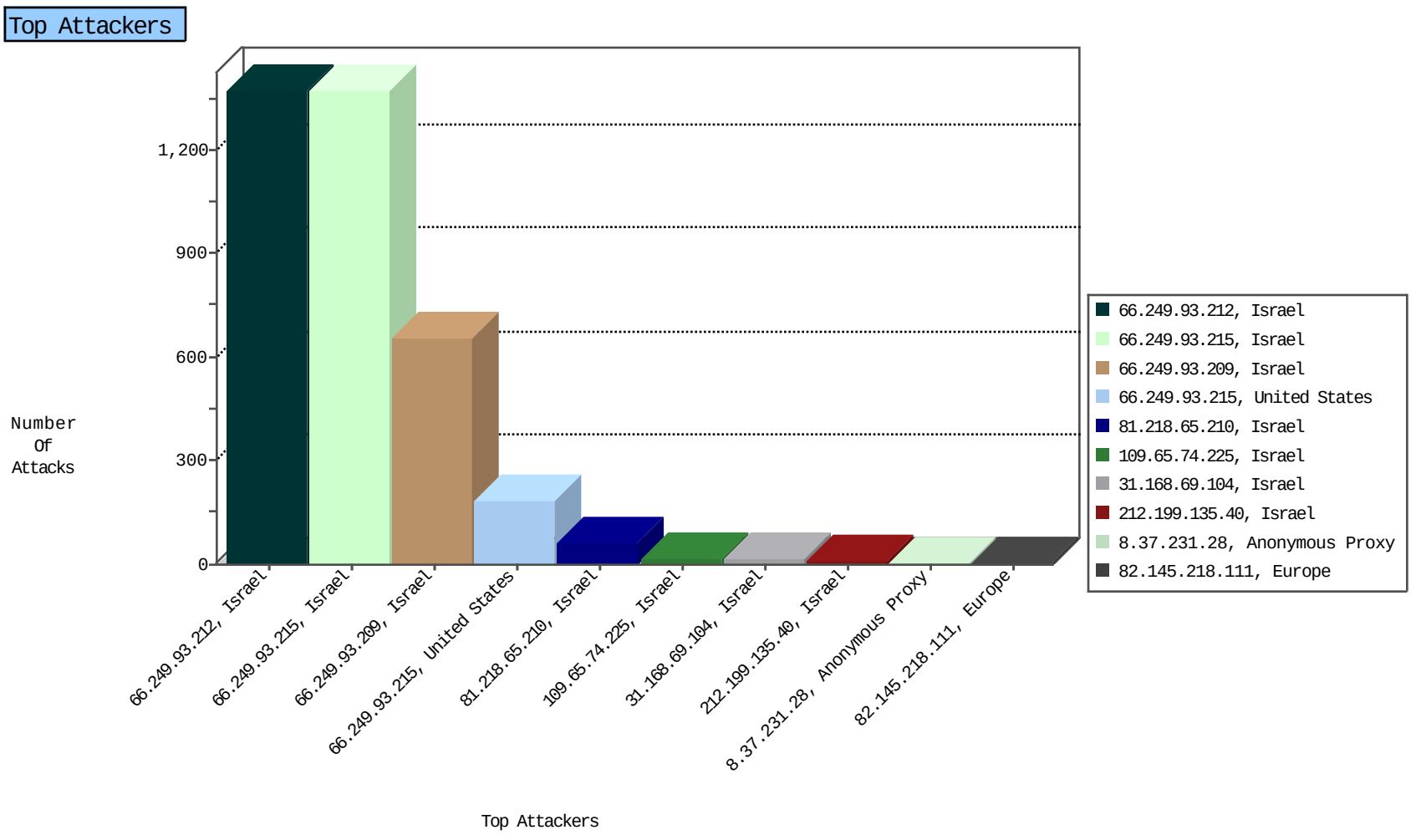
03-03-2016 to 03-04-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



03-03-2016 to 03-04-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.249.93.212	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1376
66.249.93.215	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1372
66.249.93.209	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	658
81.218.65.210	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	61
109.65.74.225	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	18
82.145.218.111	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	5
81.218.206.82	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
8.37.231.28	Anonymous Proxy	147.237.0.120	miluim.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	NetV-London	3
8.37.231.28	Anonymous Proxy	147.237.0.120	miluim.aka.idf.il	JLM_Under_Attack_Con_Http	drop	NetV-London	2
183.60.48.25	China	147.237.0.120	miluim.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	NetV-London	2
104.245.97.224		147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.96	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
71.6.167.142	United States	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1

03-03-2016 to 03-04-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

03-03-2016 to 03-04-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	181
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	2
193.201.227.62	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1

03-03-2016 to 03-04-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
109.65.36.161	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5832
5.29.159.24	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4608
109.65.148.32	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2331
77.126.40.251	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
5.28.174.107	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
82.166.145.234	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
8.37.231.28	Anonymous Proxy	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1225
2.54.172.127	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	720
79.180.163.168	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	522
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	490
109.65.93.11	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	441
80.178.187.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	369
107.16.88.108	United States	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	360
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324
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
2.52.162.90	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	268
46.19.86.169	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	261
109.65.88.127	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	261
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	248
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	248
46.19.85.102	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	243
2.52.7.43	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	drop	Unexpected post SYN packet - RST or SYN expected	drop	180
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	177
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	177
149.78.24.120	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
46.19.85.11	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	144
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
37.26.149.151	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.125.40		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.181.201.73	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
82.81.46.204	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.161.148	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.52.45.237	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	136
37.26.149.208	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
37.26.148.252	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
37.26.149.136	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
46.116.215.38	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
149.88.62.236	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
46.19.85.200	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	121
46.19.85.200	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	121
2.52.40.19	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
109.67.112.102	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
2.54.167.234	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	101
8.37.231.28	Anonymous Proxy	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	100
79.180.100.212	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
46.19.85.35	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
46.19.85.67	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	98
85.130.240.173	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	91

03-03-2016 to 03-04-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
31.168.69.104	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 31.168.69.104	Block	14
212.199.135.40	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.199.135.40	Block	7
37.26.147.213	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1455-	Block	3
194.90.155.74	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	2
37.26.147.213	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1455-	Block	2
213.151.60.43	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1273-he/miluim.aspx&sa=u&ved=0ahukewiwvpuq0ktlahve_ywkhfywdjqqfggpmai&usg=afqjcnh6ezsiewtdvlbw9c2mxnix2vfbpw	Block	2
212.25.106.78	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1455-	Block	2
95.86.106.247	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjwmkjdnkxlahuljnikhfqecjmqfggimaa&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	1
66.249.93.212	United States	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
46.19.85.142	Israel	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
89.139.136.131	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	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/general/www.behatsdaa.org.il	Block	1
31.168.69.104	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspx)	Block	1
212.76.96.251	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjvmrrgq6xlahwgj3ikhdswakgqfggimaa&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	1
157.55.39.148	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
69.197.169.202	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.142	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version _pk_ses.104.b624=*	Block	1
212.199.135.40	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/images/shared/hp/sub_bg.png"	Block	1
194.90.155.74	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/3/	Block	1
89.139.136.131	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.64.15	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/mobile/	Block	1
212.76.106.172	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjxivk5u6tlahxdknikhcoxaliqfggimaa&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	1
185.49.14.190	Poland	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
80.246.130.57	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/mobile/	Block	1
46.19.85.142	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL _pk_id.104.b624=1af0baf7fca25449.1457028358.1.1457028358.1457028358.;	Block	1
207.46.13.169	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
95.86.106.247	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 95.86.106.247	Block	1
66.249.64.15	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/general.aspx	Block	1
212.76.121.224	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/&sa=u&ved=0ahukewjx4prju6tlahufyxikhcuyasqqfggqmae&usg=afqjcne5p7m9pmcma58u2cjznfg7azoamw	Block	1
194.90.155.74	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 194.90.155.74	Block	1
89.139.136.131	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 89.139.136.131	Block	1
46.19.85.142	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method vs=56d87d0451058ab7000; in URL _pk_id.104.b624=1af0baf7fca25449.1457028358.1.1457028358.1457028358.	Block	1

03-03-2016 to 03-04-2016