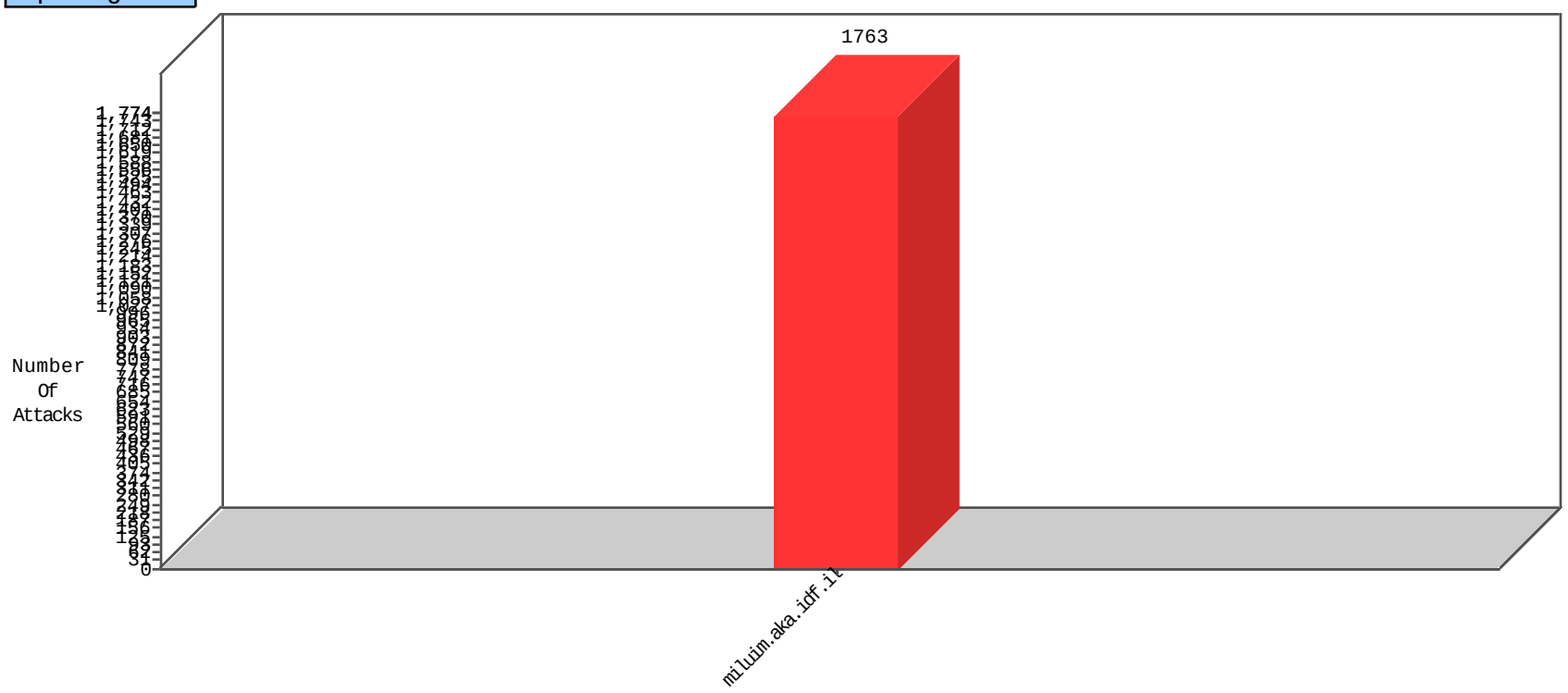
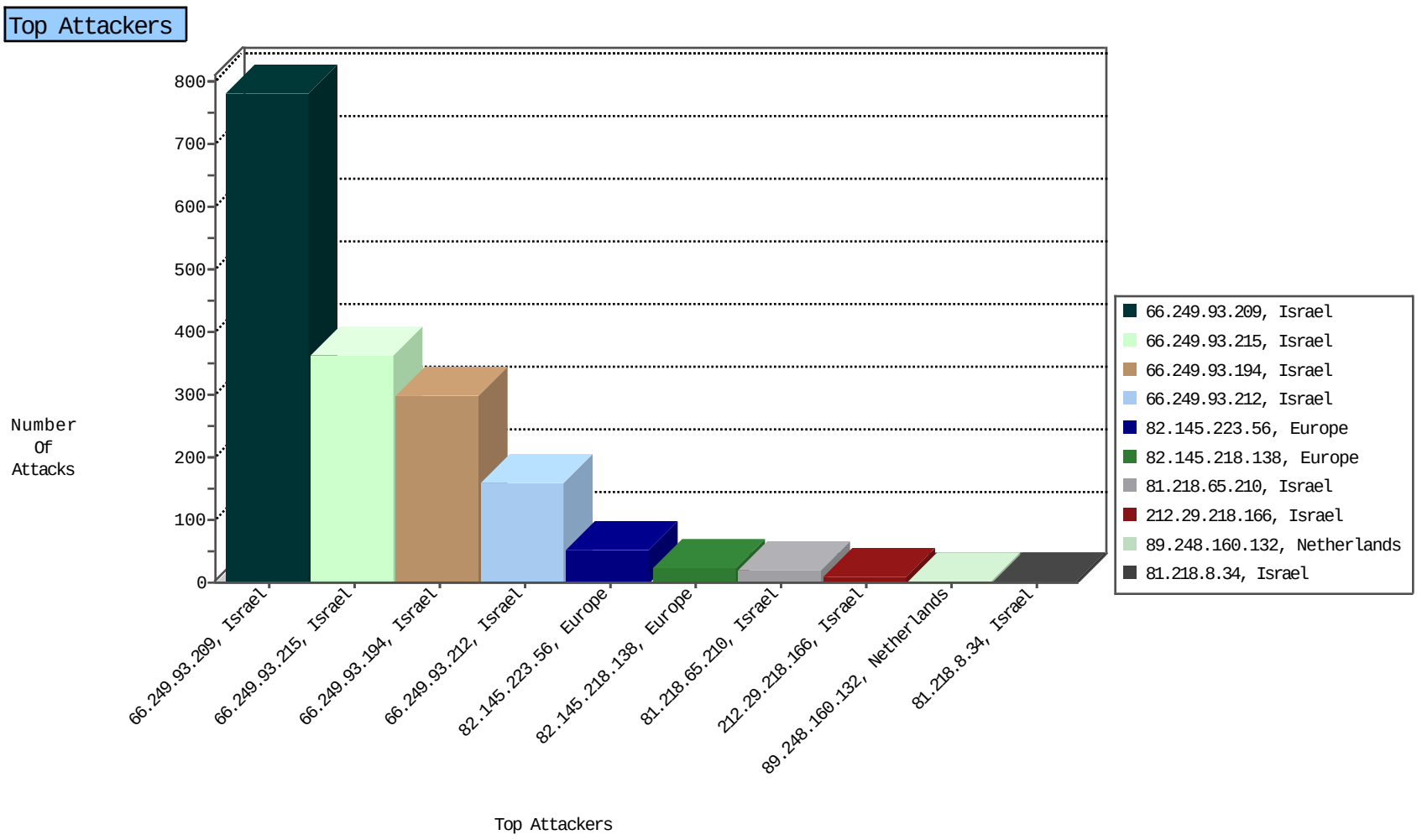
03-10-2016 to 03-11-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



03-10-2016 to 03-11-2016

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	BBL-Frankfurt	784
66.249.93.215	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	362
66.249.93.194	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	300
66.249.93.212	Israel	147.237.0.120	miluim.aka.idf.il	TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	160
82.145.223.56	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	53
82.145.218.138	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	23
81.218.65.210	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	21
81.218.8.34	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
89.248.160.132	Netherlands	147.237.0.120	miluim.aka.idf.il	block-sp-traf1	forward	DP-Tehila	1
89.248.160.132	Netherlands	147.237.0.120	miluim.aka.idf.il	block-sp-traf1	forward	NetV-London	1
89.248.172.207	Netherlands	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.247.222	United States	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
185.94.111.1		147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
216.218.206.71	United States	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1

03-10-2016 to 03-11-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count

03-10-2016 to 03-11-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sA (2)	2
31.148.219.200	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
122.114.117.177	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
190.216.146.151	Chile	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.84	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	Sweden	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.147	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1

03-10-2016 to 03-11-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
79.177.150.252	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2628
79.178.29.104	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
46.19.86.85	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.181.186.108	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.52.12.97	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1242
46.19.86.198	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	666
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	649
2.54.22.64	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
87.71.23.125	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	drop		drop	406
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
79.182.189.3	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
2.54.190.32	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.180.163.168	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
37.26.149.137	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	256
37.26.149.137	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	256
79.182.135.237	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
87.71.117.85	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
79.178.57.167	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
185.120.125.21		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	177
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	177
37.26.146.171	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	169
46.19.85.190	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	169
79.183.140.75	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
79.183.129.98	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.144.114	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
37.26.149.153	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	122
37.26.148.213	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
109.67.36.158	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
109.160.140.4	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
2.52.11.122	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	119
2.52.143.5	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
79.178.114.174	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
2.54.178.91	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
46.19.85.110	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	108
31.168.70.139	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	104
46.19.85.205	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	99
149.78.24.15	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	85
46.19.86.20	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
2.52.38.213	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	65
185.120.126.116		147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
193.47.165.251	Israel	147.237.0.120	miluim.aka.idf.i	drop	SAM rule	drop	64
46.19.85.75	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	61
37.26.149.132	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	58
2.52.152.33	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	54
2.52.154.39	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
149.88.166.87	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49

03-10-2016 to 03-11-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.29.218.166	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	4
212.29.218.166	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 212.29.218.166	Block	3
79.183.117.199	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/undefined	Block	2
2.54.143.6	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1459-he/miluim.aspx*	Block	2
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/scriptresource.axd parameter wb48617274	Block	2
2.54.181.177	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1459-he/miluim.aspx*	Block	2
212.179.4.49	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	2
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method	Block	1
66.249.93.212	Israel	147.237.0.120	miluim.aka.idf.i	URL is Above Root Directory www.miluim.aka.idf.il/../../images/shared/moreinfotitle.gif	Block	1
46.19.85.110	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method 59 in URL	Block	1
2.52.5.50	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1459-he/miluim.aspx*	Block	1
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/sip_storage/files/5/1935.gif	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
46.19.85.250	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1459-he/miluim.aspx*	Block	1
37.142.64.50	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	Block	1
178.239.82.65	United Kingdom	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
46.19.85.238	Israel	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version	Block	1
89.248.160.132	Netherlands	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.safeskyhacks.com/forums/forum.php	Block	1
46.116.15.74	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1459-he/miluim.aspx*	Block	1
37.142.64.50	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	Block	1
212.29.218.166	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1
185.25.151.159	Poland	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
80.246.130.208	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1459-he/miluim.aspx*	Block	1
46.19.85.238	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL sdch	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
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Abnormally Long Request method	Block	1
66.249.64.7	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/news/news.aspx	Block	1
46.19.85.110	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL	Block	1
192.99.8.19	Canada	147.237.0.120	miluim.aka.idf.i	Unknown Parameter platform in www.miluim.aka.idf.il/894-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
46.19.85.238	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method te, in URL sdch	Block	1
2.54.190.230	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1459-he/miluim.aspx*	Block	1

03-10-2016 to 03-11-2016