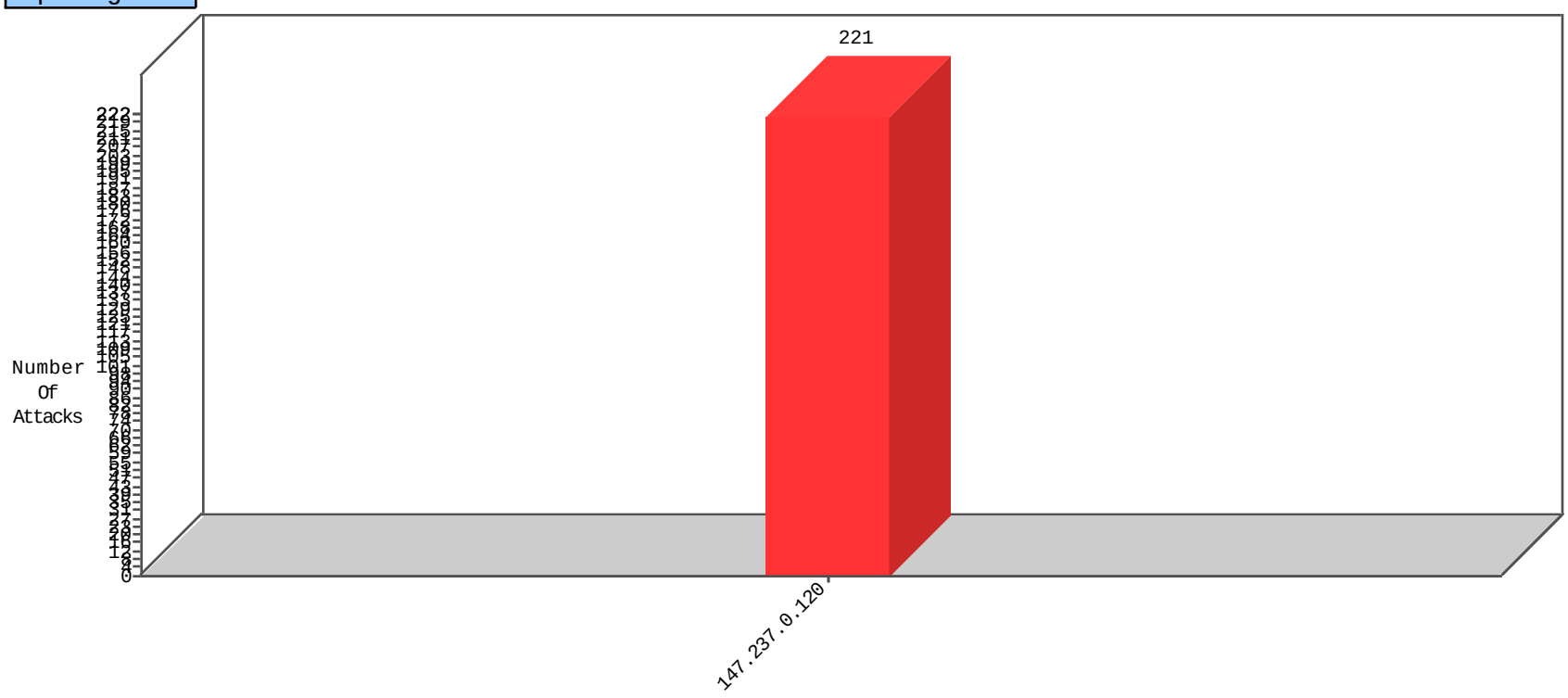
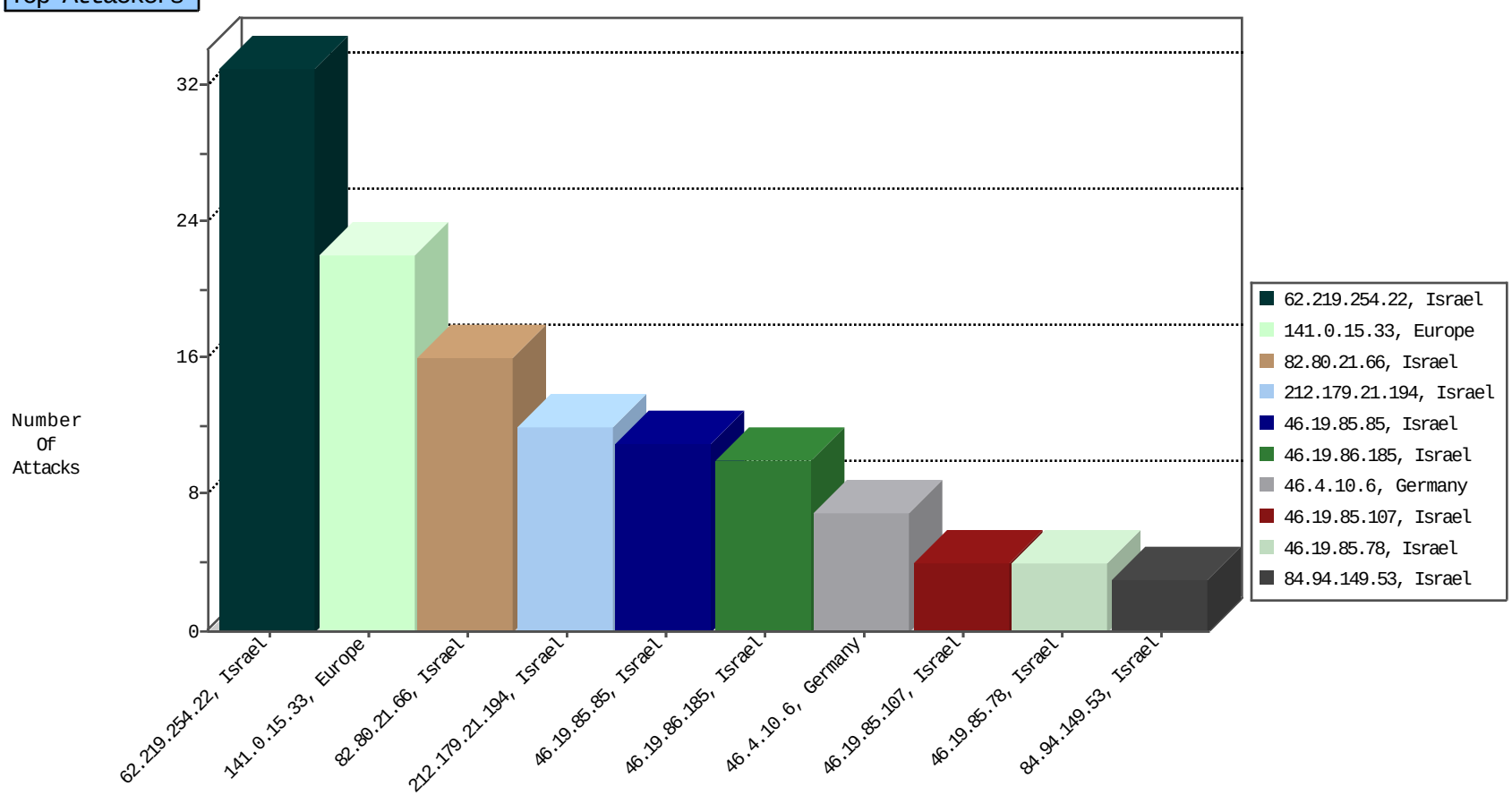
11-05-2015 to 11-06-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



11-05-2015 to 11-06-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
62.219.254.22	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	33
141.0.15.33	Europe	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	22
46.4.10.6	Germany	147.237.0.120		Invalid TCP Flags	drop	BBL-Frankfurt	7
81.218.56.125	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	2
149.88.55.69	Israel	147.237.0.120		Invalid TCP Flags	drop	BBL-Israel	1
37.26.148.217	Israel	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	1

11-05-2015 to 11-06-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	12
82.80.21.66	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	8

11-05-2015 to 11-06-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
46.19.86.185	Israel	147.237.0.120		ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	10
46.19.86.175	Israel	147.237.0.120		ET SCAN NMAP -sA (2)	2
187.18.103.129	Brazil	147.237.0.120		ET SCAN NMAP -f -sS	1
188.138.9.51	Germany	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
94.102.50.56	Netherlands	147.237.0.120		ET SCAN NMAP -sS window 1024	1
186.230.35.77	Brazil	147.237.0.120		ET SCAN Potential SSH Scan	1
187.18.103.129	Brazil	147.237.0.120		ET SCAN NMAP -sS window 2048	1
94.102.49.79	Netherlands	147.237.0.120		ET SCAN NMAP -sS window 1024	1
177.96.93.234	Brazil	147.237.0.120		ET SCAN NMAP -sS window 1024	1

11-05-2015 to 11-06-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	500306
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	484807
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	437835
141.0.15.33	Europe	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	197859
2.54.129.226	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4329
134.191.249.253	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2976
84.228.185.229	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
46.19.86.76	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
37.26.147.158	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.183.185.187	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.157.164	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
66.249.93.230	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2245
178.8.98.120	Germany	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2133
66.249.93.219	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2121
37.26.148.243	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1800
149.78.146.230	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1489
66.249.81.230	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1315
149.78.231.222	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1306
149.78.145.174	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1273
79.183.39.81	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1224
168.63.200.167	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1141
168.63.139.43	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1085
66.249.93.227	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1031
66.249.81.224	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	992
66.249.81.227	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	855
168.63.137.102	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	828
149.78.49.26	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	688
66.249.93.207	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	680
66.249.93.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	640
66.249.93.203	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	623
141.0.15.172	Norway	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	597
31.186.228.31	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	597
149.78.248.161	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	584
24.52.202.34	Canada	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	562
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	559
149.88.21.246	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	559
77.12.71.74	Germany	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	535
149.88.74.190	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	457
149.78.158.16	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	436
149.88.81.31	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	432
31.186.228.57	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	424
149.78.253.106	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	379
149.88.243.19	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	376
66.249.67.104	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	349
149.78.178.99	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	334
192.114.91.247	Israel	147.237.0.120		Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	332
149.88.184.110	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	316
194.9.253.238	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	312
149.88.31.11	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	303
149.88.231.123	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	300

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
82.80.21.66	Israel	147.237.0.120		Unauthorized HTTP Method	Block	4
2.54.5.203	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	3
46.19.85.85	Israel	147.237.0.120		Distributed Illegal HTTP Version	Block	3
82.80.21.66	Israel	147.237.0.120		Multiple Unauthorized URL Access from 82.80.21.66	Block	3
84.94.149.53	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	3
46.19.85.85	Israel	147.237.0.120		Distributed Malformed URL	Block	3
46.19.85.7	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	3
46.19.85.85	Israel	147.237.0.120		Distributed Unknown HTTP Request Method	Block	3
176.13.9.131	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
95.86.65.49	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
46.19.85.85	Israel	147.237.0.120		Distributed Abnormally Long Request	Block	2
2.54.130.135	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
82.80.173.170	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
79.182.195.205	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
192.117.16.96	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
46.117.239.220	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
2.54.3.184	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
62.219.99.130	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
2.54.4.235	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	2
80.246.130.100	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.78	Israel	147.237.0.120		Abnormally Long Request method	Block	1
213.57.62.195	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
37.46.39.254	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
79.176.81.222	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/replace_me_by_css	Block	1
46.19.85.184	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€¬	Block	1
2.54.29.71	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
2.54.0.8	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
82.80.21.66	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1
46.19.85.107	Israel	147.237.0.120		Distributed Unknown HTTP Request Method	Block	1
80.246.133.77	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
79.179.167.196	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.30	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
192.114.91.235	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim	Block	1
176.12.148.251	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€¬	Block	1
62.0.75.8	Israel	147.237.0.120		Unauthorized URL Access to miluim.aka.idf.il/1355-he/	Block	1
2.54.187.47	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
84.228.101.189	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.144	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€¬	Block	1
46.19.85.107	Israel	147.237.0.120		Distributed Abnormally Long Request	Block	1
81.218.140.112	Israel	147.237.0.120		eMail Hoarding	Block	1
80.246.130.175	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.78	Israel	147.237.0.120		Illegal HTTP Version	Block	1
213.57.108.65	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
37.142.64.83	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/giyus	Block	1
176.13.21.231	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
79.176.113.227	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.185	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
109.66.55.4	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
2.54.1.91	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.108	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
80.246.133.224	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.33	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
31.210.186.197	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/muluim.aspx	Block	1
176.12.149.4	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€¬	Block	1
62.219.98.197	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.161	Israel	147.237.0.120		Distributed Malformed URL	Block	1
2.54.16.206	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
84.228.194.105	Israel	147.237.0.120		Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 84.228.194.105	Block	1
46.19.85.107	Israel	147.237.0.120		Distributed Illegal HTTP Version	Block	1
80.246.130.226	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.78	Israel	147.237.0.120		Malformed URL _pk_ses.104.b624=*	Block	1
37.142.115.172	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
176.13.23.217	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
79.176.125.158	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
2.54.134.95	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
109.67.204.251	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.116	Israel	147.237.0.120		Distributed Malformed URL	Block	1
80.246.133.250	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
80.246.130.28	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.45	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
199.203.47.233	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
37.26.146.221	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
176.13.3.115	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.161	Israel	147.237.0.120		Distributed Unknown HTTP Request Method	Block	1
2.54.28.18	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
89.138.236.160	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim	Block	1
2.52.175.79	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.107	Israel	147.237.0.120		Distributed Malformed URL	Block	1
46.19.85.78	Israel	147.237.0.120		Unknown HTTP Request Method 746849.1446746849.; in URL _pk_ses.104.b624=*	Block	1
80.246.130.242	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/4	Block	1
192.114.23.208	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
79.179.151.106	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.121.192.138	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/13	Block	1
2.54.167.7	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
168.235.194.244	United States	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/×²Ö³Ö´	Block	1
84.95.255.130	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	1
46.19.85.116	Israel	147.237.0.120		Distributed Unknown HTTP Request Method	Block	1
81.218.140.112	Israel	147.237.0.120		E-mail collector robots 14	Block	1