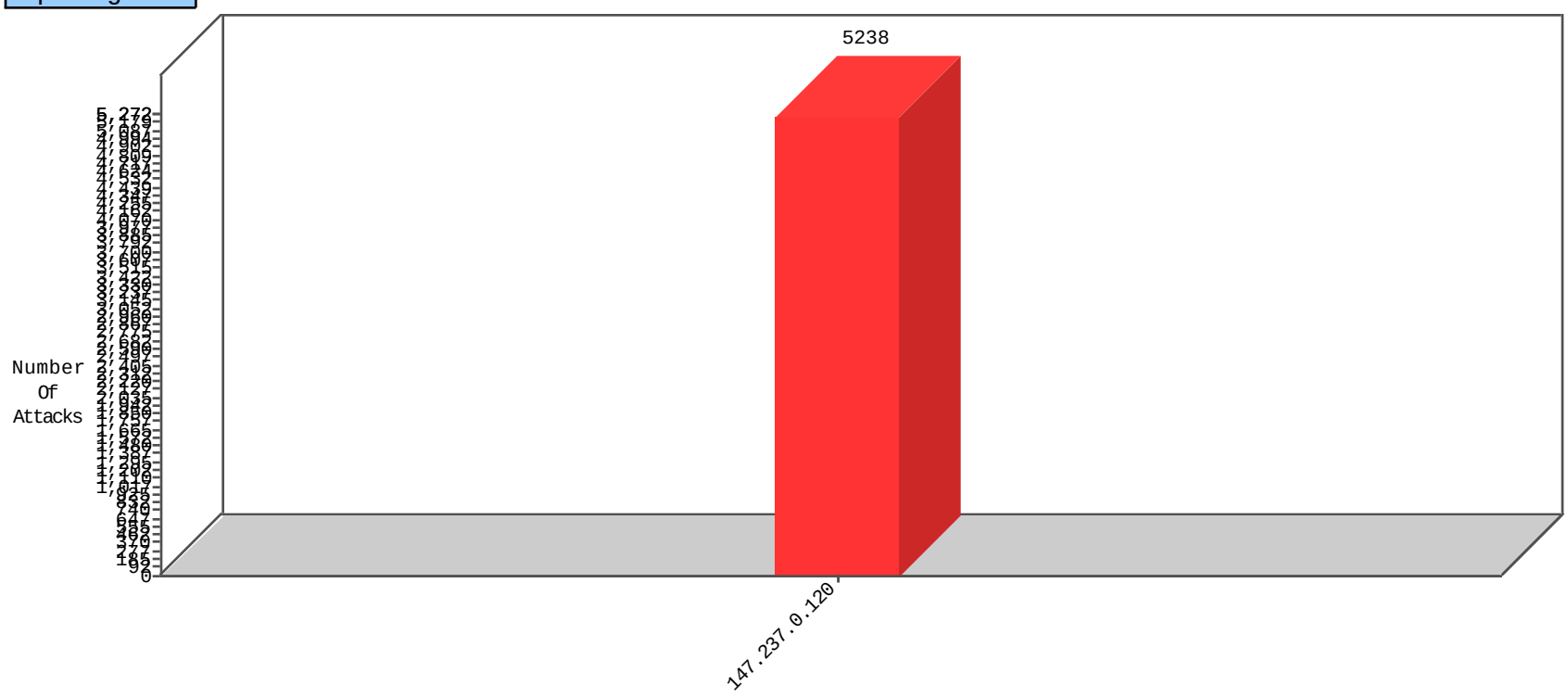
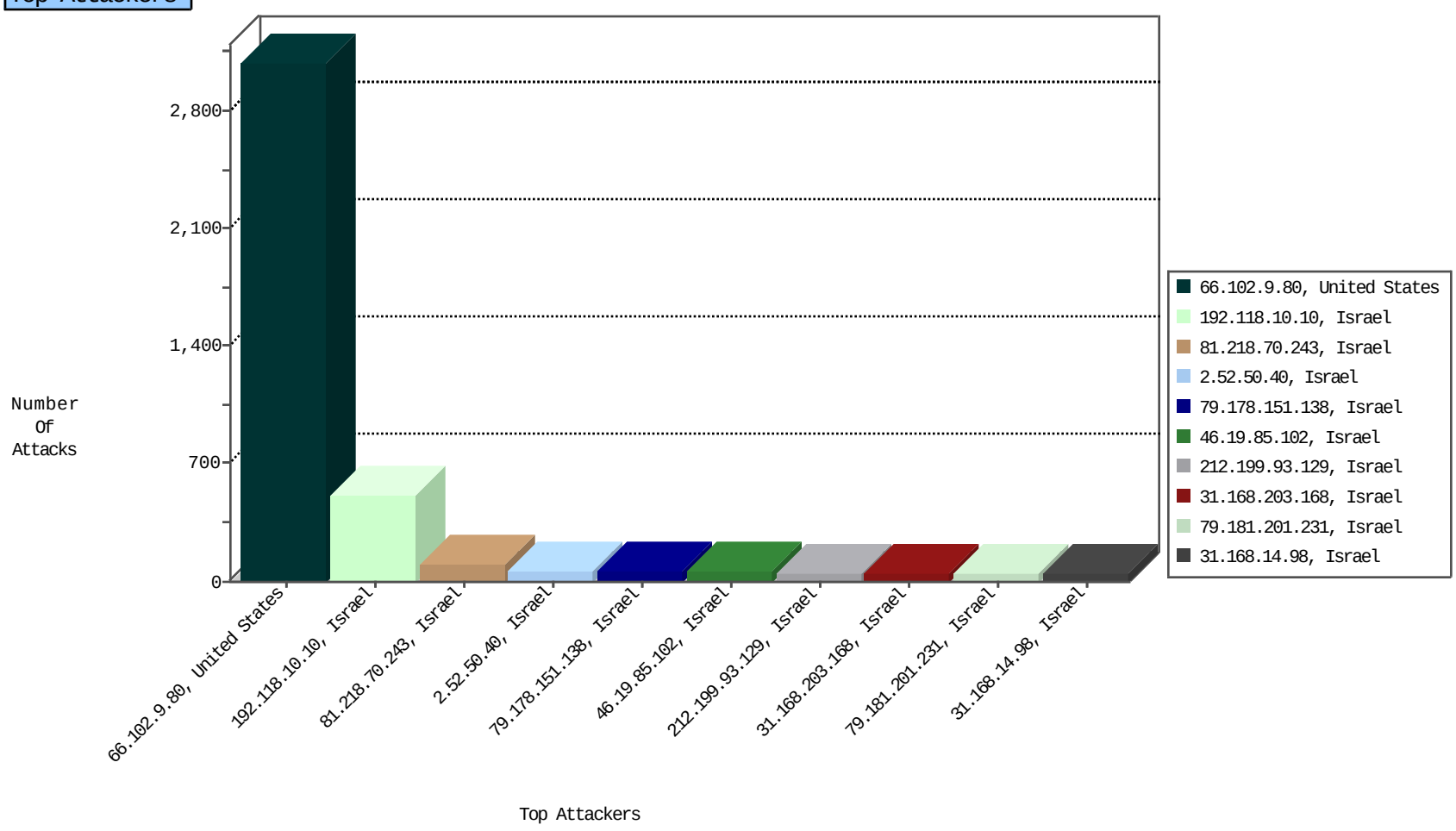
10-21-2015 to 10-22-2015

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015 to 10-22-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
66.102.9.80	United States	147.237.0.120		TCP handshake violation, first packet not syn	drop	BBL-Frankfurt	3091
62.219.254.22	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	15
81.218.206.82	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	3
192.118.132.185	Israel	147.237.0.120		Block_Udp_All_Nets	drop	BBL-Israel	3

10-21-2015 to 10-22-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
212.199.93.129	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	52
79.177.187.43	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	10
194.90.15.61	Israel	147.237.0.120		C1000004: HTTP: options method (Microsoft)	Block	2

10-21-2015 to 10-22-2015

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
172.8.58.186	United States	147.237.0.120		ET SCAN NMAP -sS window 3072	1
172.8.58.186	United States	147.237.0.120		ET SCAN NMAP -sS window 2048	1
222.186.21.48	China	147.237.0.120		ET SCAN Potential VNC Scan 5900-5920	1
172.8.58.186	United States	147.237.0.120		ET SCAN NMAP -f -sS	1

10-21-2015 to 10-22-2015

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.102.9.90	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	422862
66.102.9.100	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	406421
66.102.9.80	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	389662
66.249.93.203	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	385996
66.249.93.199	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	364297
66.249.93.207	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	361426
141.0.14.75	Europe	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	180119
79.161.20.58	Norway	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	6012
149.78.36.156	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	5553
168.63.200.167	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	3785
108.171.128.166	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	2458
79.180.56.79	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.178.143.71	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
108.171.133.166	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1949
2.52.138.161	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1296
108.171.129.189	Germany	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1213
79.183.219.169	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1154
46.19.86.155	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1152
46.19.86.111	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1152
128.30.52.73	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	1074
142.4.211.40	Canada	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	961
149.88.67.16	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	819
66.249.75.227	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	719
31.186.228.29	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	687
149.88.41.38	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	664
107.6.142.106	Netherlands	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	650
149.88.206.229	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	630
66.249.75.235	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	610
149.78.26.58	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	609
66.249.75.219	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	604
168.63.139.43	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	578
46.19.86.126	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
46.19.85.55	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
46.19.86.17	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
17.78.96.212	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	566
31.186.228.60	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	525
31.217.112.140	Croatia	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	518
31.186.228.30	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	503
31.186.228.58	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	481
68.180.229.121	United States	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	447
46.19.86.6	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
149.78.74.183	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	430
149.78.176.86	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	425
66.249.93.199	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	386
149.78.60.229	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	381
66.249.93.207	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	376
31.186.228.32	United Kingdom	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	357
66.249.93.203	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	331
149.88.14.11	Israel	147.237.0.120		Geo-location enforcement	Geo-location inbound enforcement	drop	324
46.19.85.102	Israel	147.237.0.120		Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	324

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
192.118.10.10	Israel	147.237.0.120		Multiple Unauthorized URL Access from 192.118.10.10	Block	364
192.118.10.10	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	156
81.218.70.243	Israel	147.237.0.120		Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	65
79.178.151.138	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	56
79.181.201.231	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	52
31.168.203.168	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	52
79.179.203.118	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	42
87.69.215.155	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	40
79.180.131.231	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	39
37.26.148.155	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	39
213.8.72.182	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	39
46.19.85.243	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	39
2.52.50.40	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	39
2.52.50.40	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	28
80.246.130.216	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	28
46.19.85.77	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	28
46.19.85.83	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	28
79.183.54.129	Israel	147.237.0.120		Multiple Unauthorized URL Access from 79.183.54.129	Block	28
2.54.32.112	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	28
46.120.34.241	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	28
31.168.14.98	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	28
46.19.86.85	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	28
46.19.85.116	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	27
109.67.50.60	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	26
46.19.85.90	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	26
81.218.70.243	Israel	147.237.0.120		Multiple Unauthorized URL Access from 81.218.70.243	Block	26
46.19.85.84	Israel	147.237.0.120		Unknown HTTP Request Method ofile: in URL www.htcmms.com.tw/android/common/fl0fd1acey/ua-profile.xml	Block	14
80.246.130.5	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
213.151.38.112	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.apx	Block	14
46.19.86.98	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
46.19.85.139	Israel	147.237.0.120		Distributed Malformed URL	Block	14
46.19.85.78	Israel	147.237.0.120		Unknown HTTP Request Method n;q=0.8,he;q=0.6 in URL	Block	14
79.182.180.229	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
46.19.85.102	Israel	147.237.0.120		Illegal HTTP Version __atuvc=0%7C38%2C0%7C39%2C0%7C40%2C0%7C41%2C1%7C42; __atuvs=56279ce2fe37de85000	Block	14
85.250.4.126	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
194.90.15.61	Israel	147.237.0.120		Unauthorized HTTP Method	Block	14
46.19.85.139	Israel	147.237.0.120		Distributed Unknown HTTP Request Method	Block	14
168.235.198.221	United States	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/shared/clientscripts/ui/	Block	14
46.19.85.102	Israel	147.237.0.120		Abnormally Long Request request version	Block	14
31.168.181.109	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he	Block	14
46.19.85.78	Israel	147.237.0.120		Abnormally Long Request method	Block	14
79.182.134.185	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
194.90.15.61	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	14
46.19.85.199	Israel	147.237.0.120		Distributed Unknown HTTP Request Method	Block	14
84.109.152.52	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
46.19.85.102	Israel	147.237.0.120		Distributed Malformed URL	Block	14
46.19.85.84	Israel	147.237.0.120		Illegal HTTP Version	Block	14
213.57.225.62	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
2.54.63.255	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
46.19.85.139	Israel	147.237.0.120		Distributed Abnormally Long Request	Block	14
46.19.85.78	Israel	147.237.0.120		Malformed URL	Block	14
31.168.14.98	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
46.19.85.199	Israel	147.237.0.120		Malformed URL	Block	14
85.65.172.245	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	14
46.19.85.102	Israel	147.237.0.120		Distributed Unknown HTTP Request Method	Block	14
2.54.149.140	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
46.19.85.96	Israel	147.237.0.120		Unknown HTTP Request Method NET_SessionId=u15ejd3nij5i5gjno0vq5gi1 in URL	Block	13
79.177.189.75	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
31.168.27.84	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1325-he/miluim.aspxâ€?â€Ž	Block	13
176.13.9.45	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/8/1968.pdf.	Block	13
5.22.129.76	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
46.19.86.115	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
82.166.22.81	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il./1355-he/miluim.aspx	Block	13
213.57.104.165	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
176.13.22.250	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
46.19.86.75	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
46.19.85.96	Israel	147.237.0.120		Abnormally Long Request method	Block	13
176.12.136.234	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
80.178.139.2	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
89.139.31.153	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/894-he/miluim.aspx/	Block	13
81.218.70.243	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/images/shared/hp/right_link.png	Block	13
46.19.85.96	Israel	147.237.0.120		Malformed URL	Block	13
79.182.162.104	Israel	147.237.0.120		Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/www.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	13
79.176.220.145	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
195.95.183.254	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13
176.12.138.76	Israel	147.237.0.120		Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1355-he/miluim.aspxâ€?â€Ž	Block	13