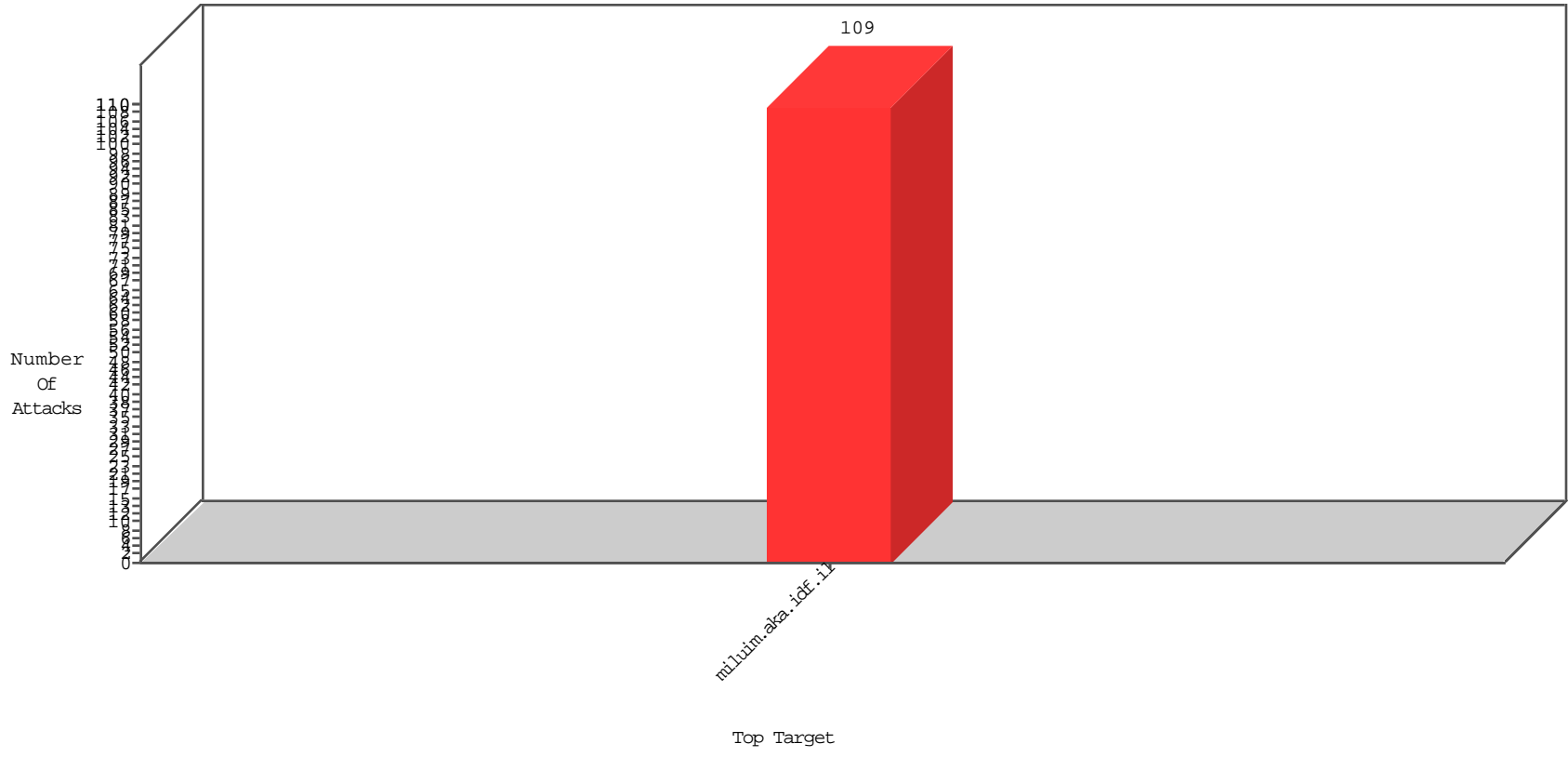


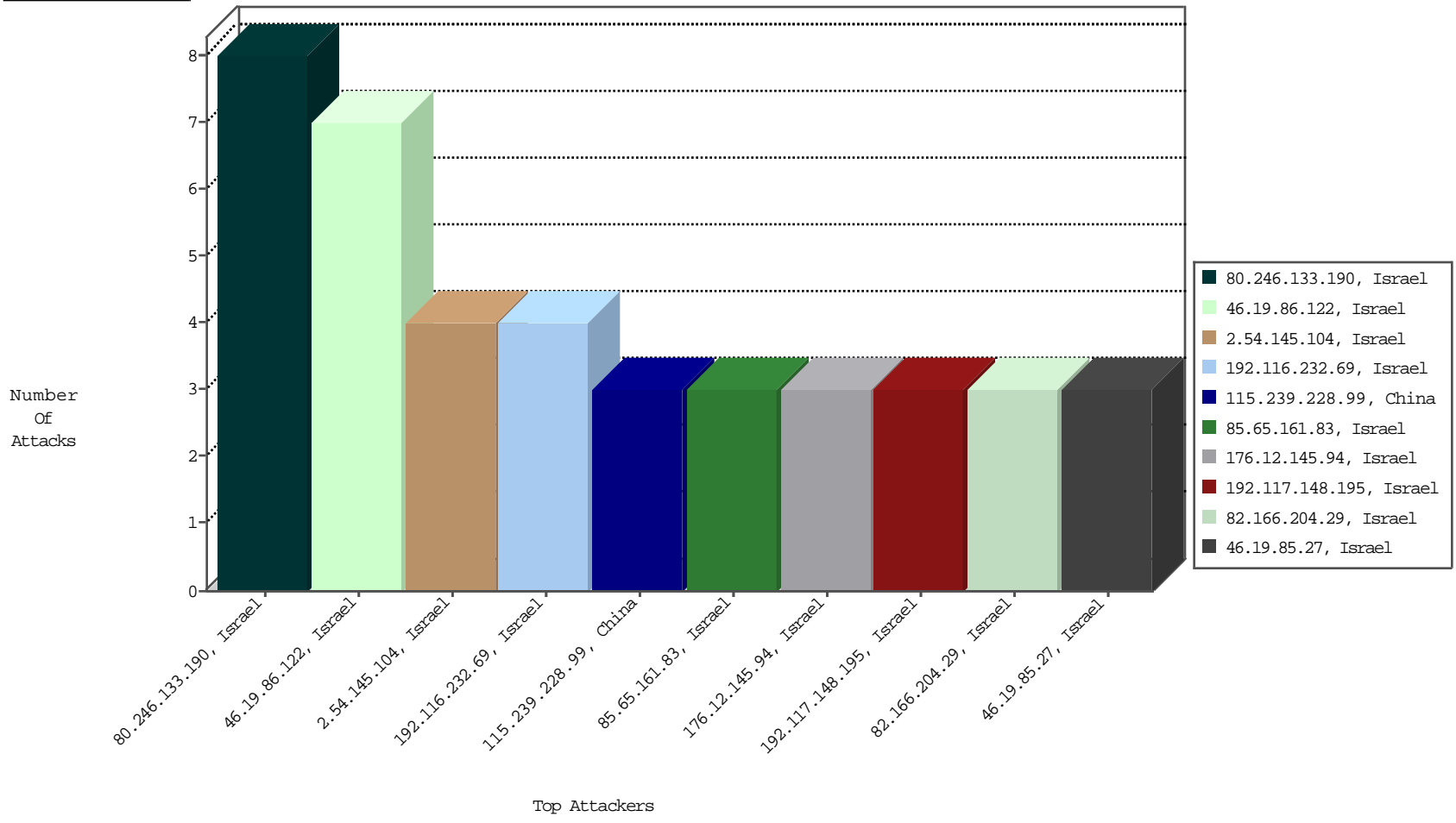
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



12-17-2015 to 12-18-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
115.239.228.99	China	147.237.0.120	miluim.aka.idf.il	Frk_Under_Attack_Con_Http	drop	BBL-Frankfurt	2
115.239.228.99	China	147.237.0.120	miluim.aka.idf.il	Frk_Purple_Con_Limit_Http	drop	BBL-Frankfurt	1

12-17-2015 to 12-18-2015

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
46.19.86.122	Israel	147.237.0.120	miluim.aka.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	2

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
46.19.86.122	Israel	147.237.0.120	miluim.aka.idf.il	SERVER-IIS asp-dot attempt	2
104.219.238.10		147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
182.140.131.147	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
66.249.93.209	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	20622
216.185.58.191	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	13056
66.249.93.215	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	11588
66.249.93.212	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	8895
149.88.111.168	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4956
66.249.81.224	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	3902
149.78.220.184	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	3004
66.249.81.230	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2759
46.19.85.205	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2510
37.26.147.176	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
149.88.241.71	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1907
149.88.185.109	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1651
66.249.81.217	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1450
149.78.24.75	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1421
192.232.81.1	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1333
82.166.6.248	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1314
108.171.128.172	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1256
68.180.229.121	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1017
200.121.203.203	Peru	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1015
195.222.249.130	Germany	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	958
149.88.39.221	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	920
149.78.243.58	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	888
52.0.238.61	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	837
149.78.160.204	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	819
168.63.137.102	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	610
2.54.38.61	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	522
149.88.20.66	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	516
181.176.37.5	Peru	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	500
157.55.39.142	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	494
149.88.9.182	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	462
108.171.128.169	United Kingdom	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	436
149.78.170.184	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	432
40.77.167.1	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	401
15.90.166.12	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	367
62.219.192.198	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	289
62.219.192.198	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	289
92.111.188.176	Netherlands	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	280
98.138.142.9	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	259
136.237.18.10	United States	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	254
79.181.52.223	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	252
46.19.85.36	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	243
109.64.121.120	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
140.242.217.2	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	216
134.191.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	213
149.88.177.137	Israel	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	207
190.238.66.92	Peru	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	186
46.19.85.49	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence		monitor	185
141.0.14.74	Europe	147.237.0.120	miluim.aka.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	182
81.218.161.72	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	178
46.19.85.189	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	169

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
80.246.133.190	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	4
85.65.161.83	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	3
46.19.85.27	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	3
82.166.204.29	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	3
192.117.148.195	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	3
80.246.133.190	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	3
2.54.145.104	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	3
5.102.254.10	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	2
84.108.129.64	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	2
2.54.39.227	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	2
176.12.145.94	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	2
80.246.133.252	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	2
109.253.213.206	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	2
84.109.114.41	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	2
2.54.151.213	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	2
2.54.51.16	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	2
46.19.86.122	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1393-he/miluim.asp.	Block	2
192.115.90.37	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	2
176.106.230.55	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	2
37.26.147.187	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	2
62.219.122.18	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	2
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
46.19.86.34	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	2
176.12.142.3	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	2
80.246.133.237	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	2
62.219.237.196	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	2
109.67.23.120	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
2.54.145.104	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx&?&ež	Block	1
213.8.204.9	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
80.246.133.190	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 80.246.133.190	Block	1
46.19.86.122	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
185.24.233.96	Ireland	147.237.0.120	miluim.aka.idf.i	eMail Hoarding	Block	1
37.26.147.235	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	1
2.54.166.208	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
2.54.61.70	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
79.181.145.191	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Unknown Parameter wb48617274 in www.miluim.aka.idf.il/scriptresource.axd	Block	1
176.13.12.166	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
46.19.85.251	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-heb/miluim.aspx	Block	1
31.168.14.94	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
176.12.145.94	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1393-	Block	1
2.54.167.163	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1393-	Block	1
109.65.49.187	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx&?&ež	Block	1
2.54.140.230	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
80.246.128.14	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/~1393	Block	1
46.19.86.16	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
132.64.205.32	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/homepage/undefined	Block	1
84.109.192.106	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
2.54.163.202	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
2.54.60.245	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
176.12.151.237	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 176.12.151.237	Block	1
46.19.85.89	Israel	147.237.0.120	miluim.aka.idf.i	Malformed URL	Block	1
5.29.181.164	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1355-he/miluim.aspx&?&ež	Block	1
109.67.23.120	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
84.95.134.8	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	1
212.143.63.31	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-	Block	1
80.246.133.186	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
185.24.233.96	Ireland	147.237.0.120	miluim.aka.idf.i	E-mail collector robots 14	Block	1
37.26.147.225	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
85.65.48.151	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx&?&ež	Block	1
2.54.164.32	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
2.54.61.70	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1394-he/miluim.aspx&?&ež	Block	1
192.116.232.69	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/4/2048.pdf	Block	1

12-17-2015 to 12-18-2015

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
176.13.11.155	Israel	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/1393-he/miluim.aspx?æž	Block	1
46.19.85.89	Israel	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method ,sdch in URL	Block	1

12-17-2015 to 12-18-2015