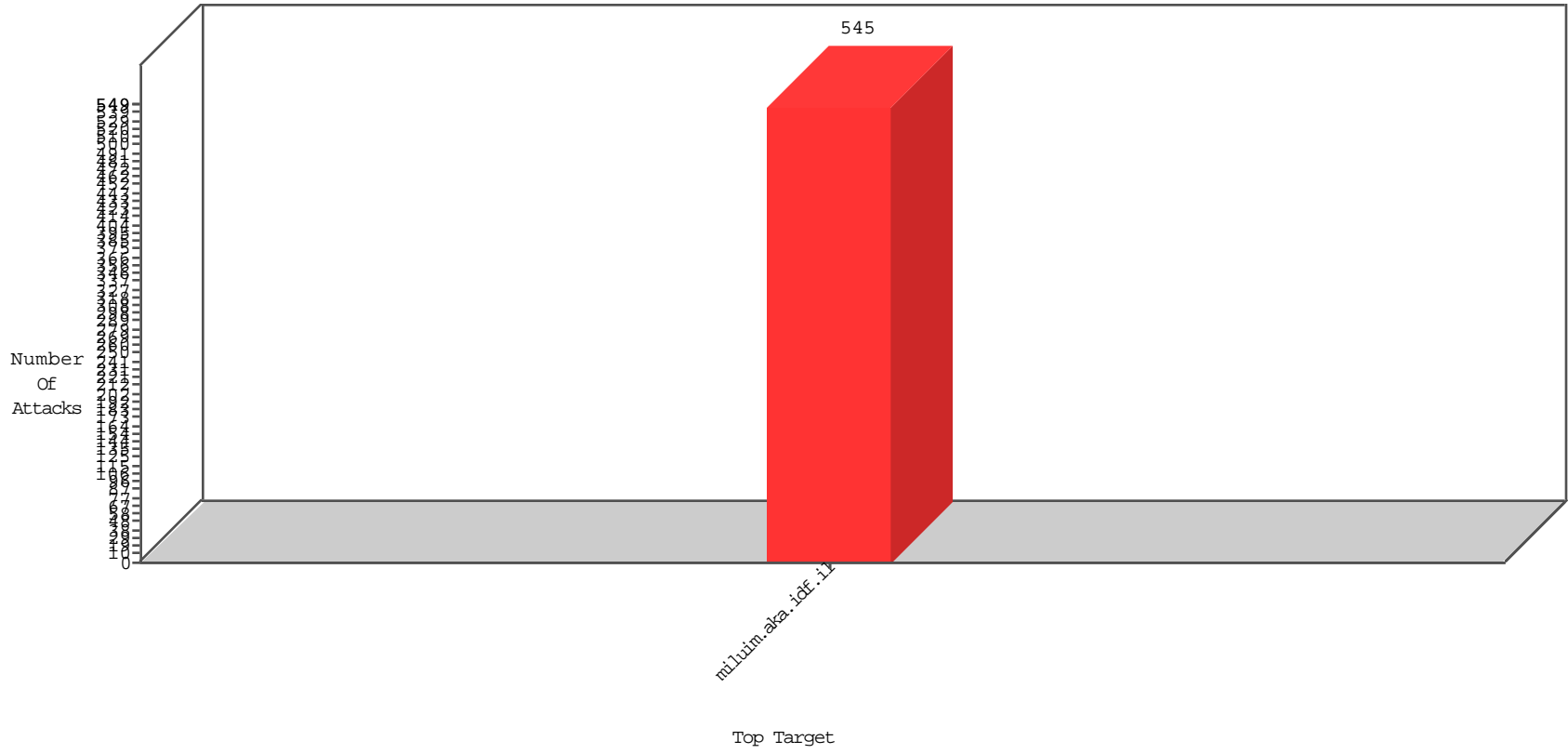


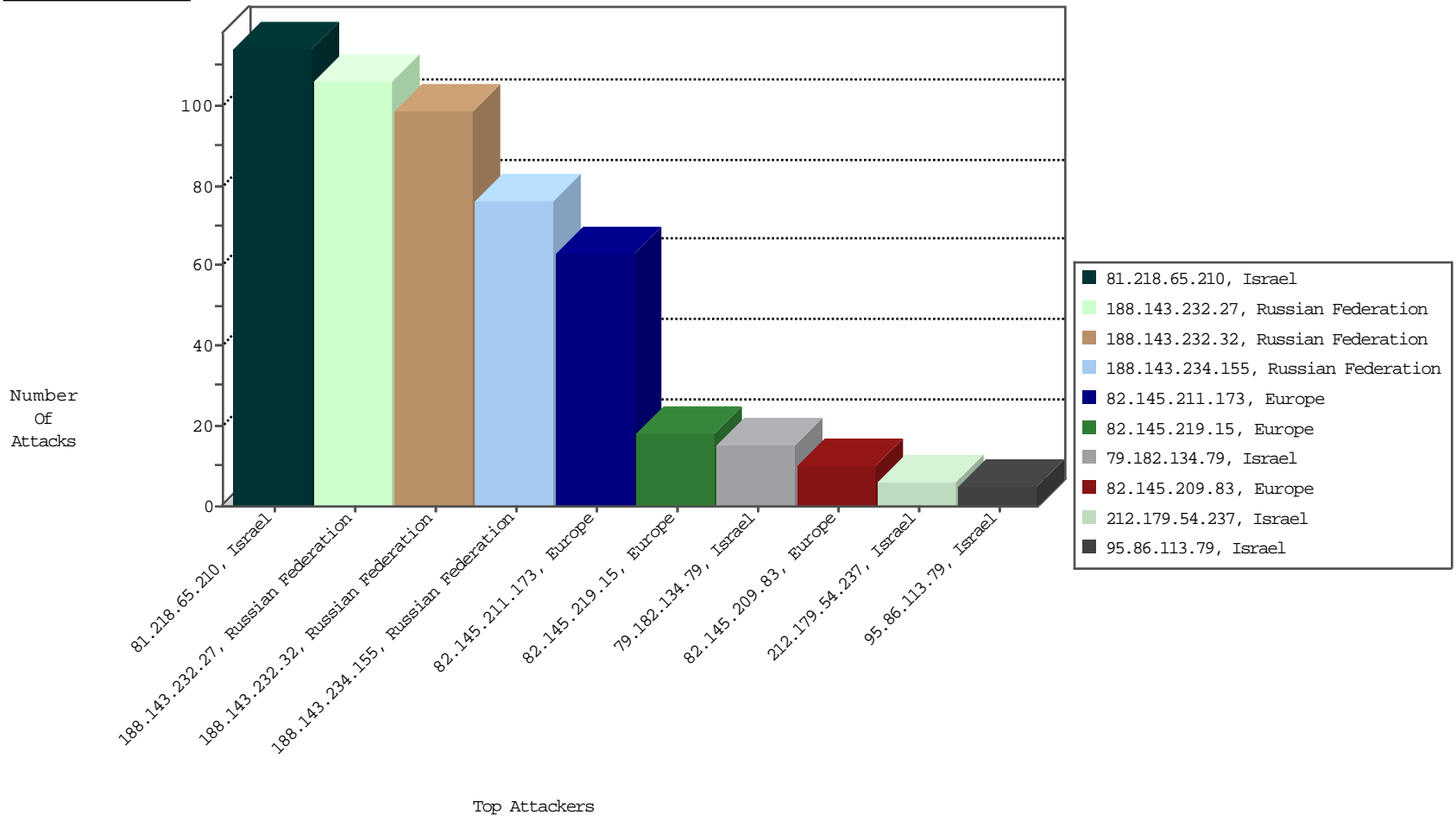
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
81.218.65.210	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	114
82.145.211.173	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	63
82.145.219.15	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	18
79.182.134.79	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	15
82.145.209.83	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	10
212.179.54.237	Israel	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	BEL-Israel	6
184.105.139.120	United States	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
187.210.32.17	Mexico	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
204.42.253.2	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
82.145.219.58	Europe	147.237.0.120	miluim.aka.idf.il	Block_Ip_Web_In	drop	NetV-London	1
146.185.239.100	Russian Federation	147.237.0.120	miluim.aka.idf.il	block-sp-trafl	drop	NetV-London	1

03-04-2016 to 03-05-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
------------------	--------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
193.36.35.241	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.144	Israel	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.215.142	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
217.10.46.148	Russian Federation	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
40.76.34.233	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.215.33	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
79.177.11.244	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
2.54.27.14	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
109.67.30.141	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
79.182.209.240	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	698
185.120.125.40		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
2.54.138.45	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	441
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
109.67.166.179	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
79.178.57.167	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
46.19.86.119	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	244
79.176.184.210	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
79.176.185.22	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	225
5.28.160.227	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
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
87.69.80.183	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	121
109.65.226.234	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
109.67.170.34	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
77.127.176.252	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
2.52.49.232	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
46.19.86.119	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	81
46.19.86.119	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	81
37.26.149.224	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
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	72
79.180.241.2	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
46.19.86.130	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
37.26.148.191	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.19.85.11	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
79.179.131.27	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
2.54.6.80	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.10	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	36
46.19.85.98	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.85.10	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
46.19.86.130	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
79.183.243.182	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.181.0.126	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
213.8.204.80	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
194.54.168.65	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
107.150.24.158	United States	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
46.19.86.164	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.86.202	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
77.125.4.55	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.86.208	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
149.78.239.136	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
2.52.57.145	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
2.52.54.244	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.85.72	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	25
149.78.239.136	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
46.19.85.72	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
2.52.56.79	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
81.218.40.10	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
188.143.232.27	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter btnSendToFriend	Block	59
188.143.232.32	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/sendtofriend	Block	48
188.143.232.27	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/sendtofriend	Block	46
188.143.232.32	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter btnSendToFriend	Block	45
188.143.234.155	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/sendtofriend	Block	39
188.143.234.155	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter btnSendToFriend	Block	33
188.143.232.32	Russian Federation	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/sendtofriend	Block	4
95.86.113.79	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 95.86.113.79	Block	4
84.108.184.130	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1455-	Block	2
188.143.232.32	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	2
87.69.239.159	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized HTTP Method	Block	2
188.143.234.155	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	2
66.249.64.15	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Header Value	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.ishurim.aka.idf.il/1044-he/ishurim.aspx	Block	1
185.89.217.227		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
74.208.10.248	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
188.143.234.155	Russian Federation	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Method '[#24]]ö[#23]]Kç	Block	1
87.69.239.159	Israel	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 87.69.239.159	Block	1
66.249.64.1	United States	147.237.0.120	miluim.aka.idf.i	Unknown Parameter fileld in www.miluim.aka.idf.il/console/core/doc_mgr/library/manage/resource/getfilecontent.hh.asp	Block	1
95.86.113.79	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1209-he/miluim.aspx&sa=u&ved=0ahukewinjck7ablahukxrqkhtiwbmuqfeggvmag&usg=afqjcnh0vpxxuc6_wmt6rig2q5ceeic81g	Block	1
80.246.130.235	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1397-he/miluim.aspx	Block	1
188.143.234.155	Russian Federation	147.237.0.120	miluim.aka.idf.i	Unknown Parameter btnSendToFriend in www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Malformed URL	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/headerupper/	Block	1
188.143.232.27	Russian Federation	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Header Name èlê/hú1[#7]]ú	Block	1
80.246.130.243	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1394-he/miluim.aspx	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/sip_storage/files/1/1911.pdf	Block	1
201.173.134.198	Mexico	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to /tmunblock.cgi	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method '[[#24]]ö[#23]]Kç in URL	Block	1
87.69.239.159	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/sip_storage/files/5/	Block	1