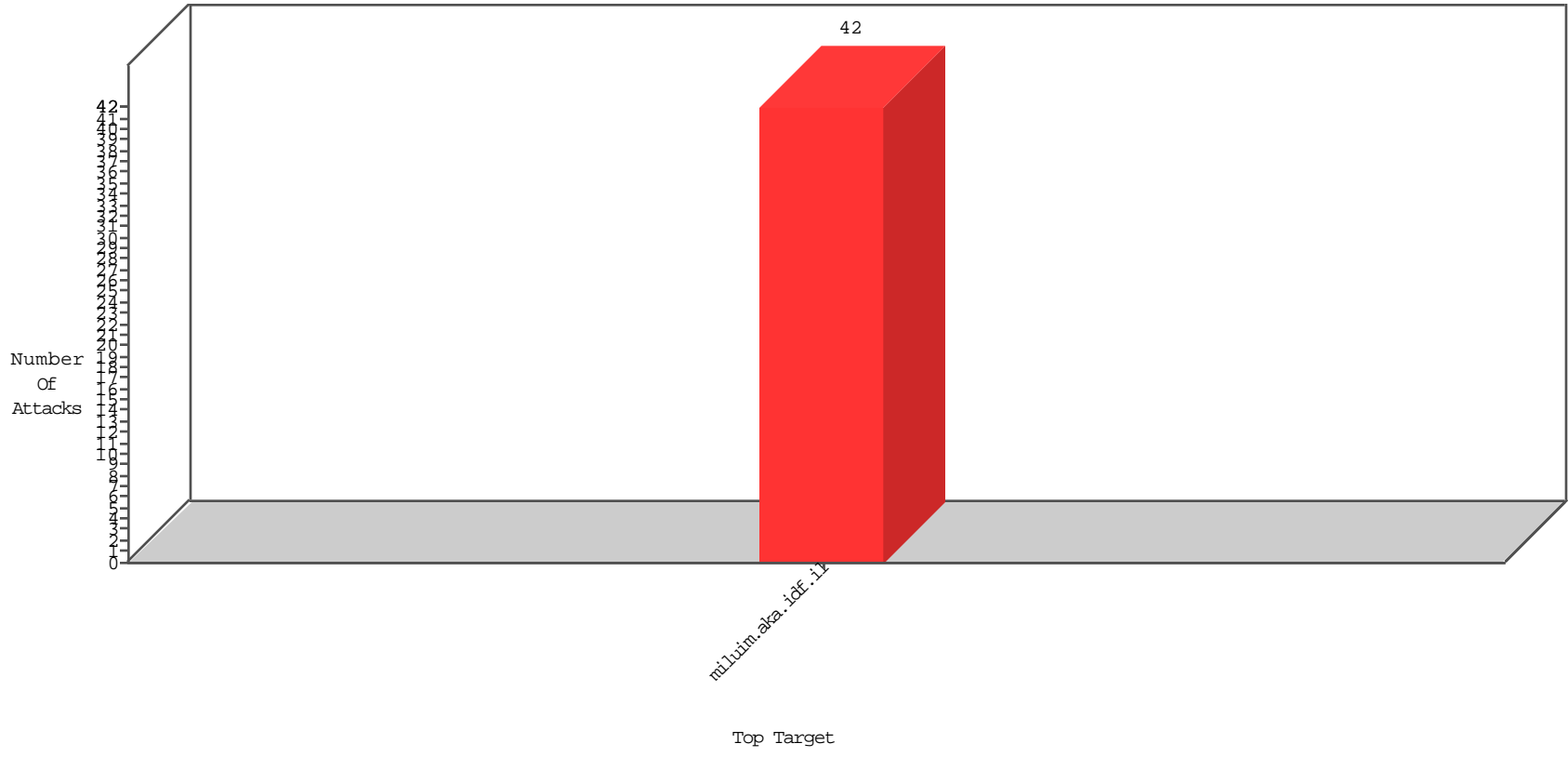


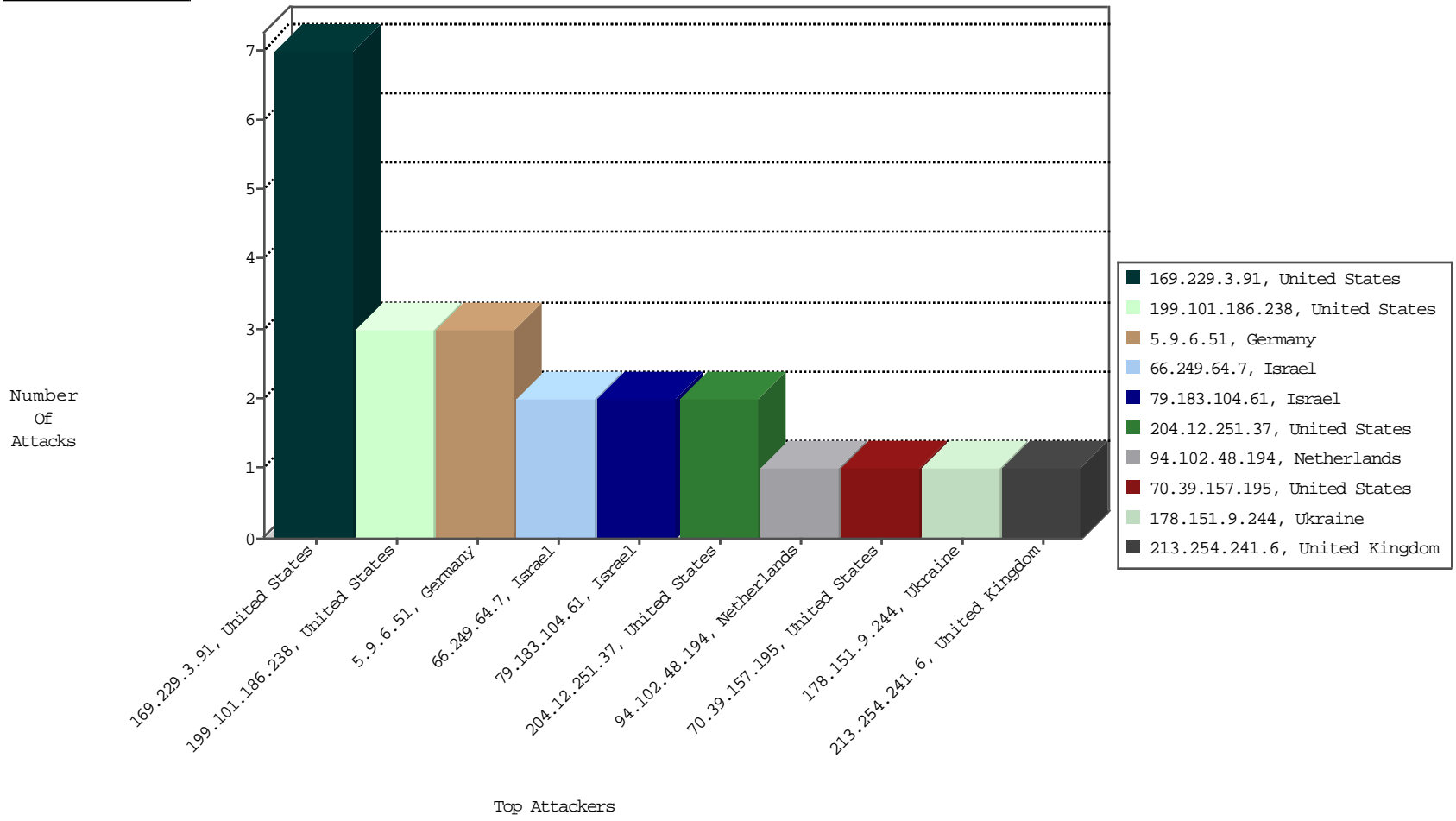
Focused IP Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
58.176.240.120	Hong Kong	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
74.82.47.61	United States	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
178.151.9.244	Ukraine	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1
184.105.139.68	United States	147.237.0.120	miluim.aka.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
204.42.253.132	United States	147.237.0.120	miluim.aka.idf.il	Block_Udp_All_Nets	drop	NetV-London	1

03-12-2016 to 03-13-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
151.80.31.124	Italy	147.237.0.120	miluim.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
188.165.15.223	France	147.237.0.120	miluim.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
199.101.186.238	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -f -sS	1
199.101.186.238	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.113	Ukraine	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
192.3.9.122	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.238	United States	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
218.57.11.7	China	147.237.0.120	miluim.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	Netherlands	147.237.0.120	miluim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
79.180.171.105	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2313
2.54.3.111	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2304
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
2.54.41.29	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2034
2.54.50.7	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1008
79.181.30.118	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	936
109.65.15.224	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	792
79.178.57.167	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	648
109.64.187.116	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
79.183.51.131	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	504
2.54.254.131	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
79.177.99.251	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	253
79.177.99.251	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	253
79.179.131.27	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	181
2.54.178.192	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
87.71.49.56	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
117.222.116.122	India	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	170
79.177.216.114	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
5.28.171.254	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
87.71.23.125	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
79.182.136.36	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
2.54.5.159	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
185.120.125.21		147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
87.71.13.59	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
84.109.50.139	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	137
2.52.60.107	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	100
79.178.242.210	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
79.177.133.151	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
46.19.86.124	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
37.26.147.158	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	64
204.12.251.37	United States	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
212.179.222.86	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
46.120.106.210	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
79.177.163.107	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.129.2	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.142.118.230	Israel	147.237.0.120	miluim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.178.187.149	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
37.26.146.156	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.120.145.128	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
79.179.9.105	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
85.250.4.0	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.85.92	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	25
31.168.91.10	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	20
89.138.72.143	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
87.69.35.214	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
84.229.37.95	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
93.173.113.32	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.121.103.245	Israel	147.237.0.120	miluim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
89.138.72.143	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
149.88.92.164	Israel	147.237.0.120	miluim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
5.9.6.51	Germany	147.237.0.120	miluim.aka.idf.i	Multiple Unauthorized URL Access from 5.9.6.51	Block	2
204.12.251.37	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	2
46.19.85.100	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/1459-he/miluim.aspx	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Unknown HTTP Request Method [[#22]]i"..."é[[#16]]kzþ)[[#11]]-ùð[[#26]]CÙØÝq in URL n [[#15]]æ	Block	1
141.212.122.160	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to 147.237.0.120/	Block	1
66.249.64.15	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/mobile/	Block	1
213.254.241.6	United Kingdom	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter &y	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in URL n [[#15]]æ: [[#6]] [[#28]] , (ÝÉ[[#3]] µ° [[#14]] @ Ÿ	Block	1
70.39.157.197	United States	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter &y	Block	1
66.249.64.1	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/general/general.aspx	Block	1
199.16.156.124	United States	147.237.0.120	miluim.aka.idf.i	Unknown Parameter platform in www.miluim.aka.idf.il/894-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
68.180.228.58	United States	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
213.254.241.7	United Kingdom	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/894-he/mailto:moked_miluim@mail.idf.il	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal HTTP Version Ýi[[#27]]§[[#3]] [[#6]]	Block	1
79.183.104.61	Israel	147.237.0.120	miluim.aka.idf.i	PHP Attempt	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/homepage/homepage.aspx	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Illegal Byte Code Character in Header Name	Block	1
70.39.157.194	United States	147.237.0.120	miluim.aka.idf.i	Distributed Unauthorized URL Access on www.miluim.aka.idf.il/894-he/mailto:moked_miluim@mail.idf.il	Block	1
5.9.6.51	Germany	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.120	miluim.aka.idf.i	Malformed URL n [[#15]]æ: [[#6]] [[#28]] , (ÝÉ[[#3]] µ° [[#14]]f< Ÿ®	Block	1
79.183.104.61	Israel	147.237.0.120	miluim.aka.idf.i	Unauthorized URL Access to www.miluim.aka.idf.il/xmlrpc.php	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
213.254.241.4	United Kingdom	147.237.0.120	miluim.aka.idf.i	Unknown Parameter &y 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	Illegal Byte Code Character in Method [[#22]]i"..."é[[#16]]kzþ)[[#11]]-ùð[[#26]]CÙØÝq	Block	1
70.39.157.195	United States	147.237.0.120	miluim.aka.idf.i	Distributed Unknown Parameter on www.miluim.aka.idf.il/templates/sendtofriend/sendtofriend.aspx parameter &y	Block	1