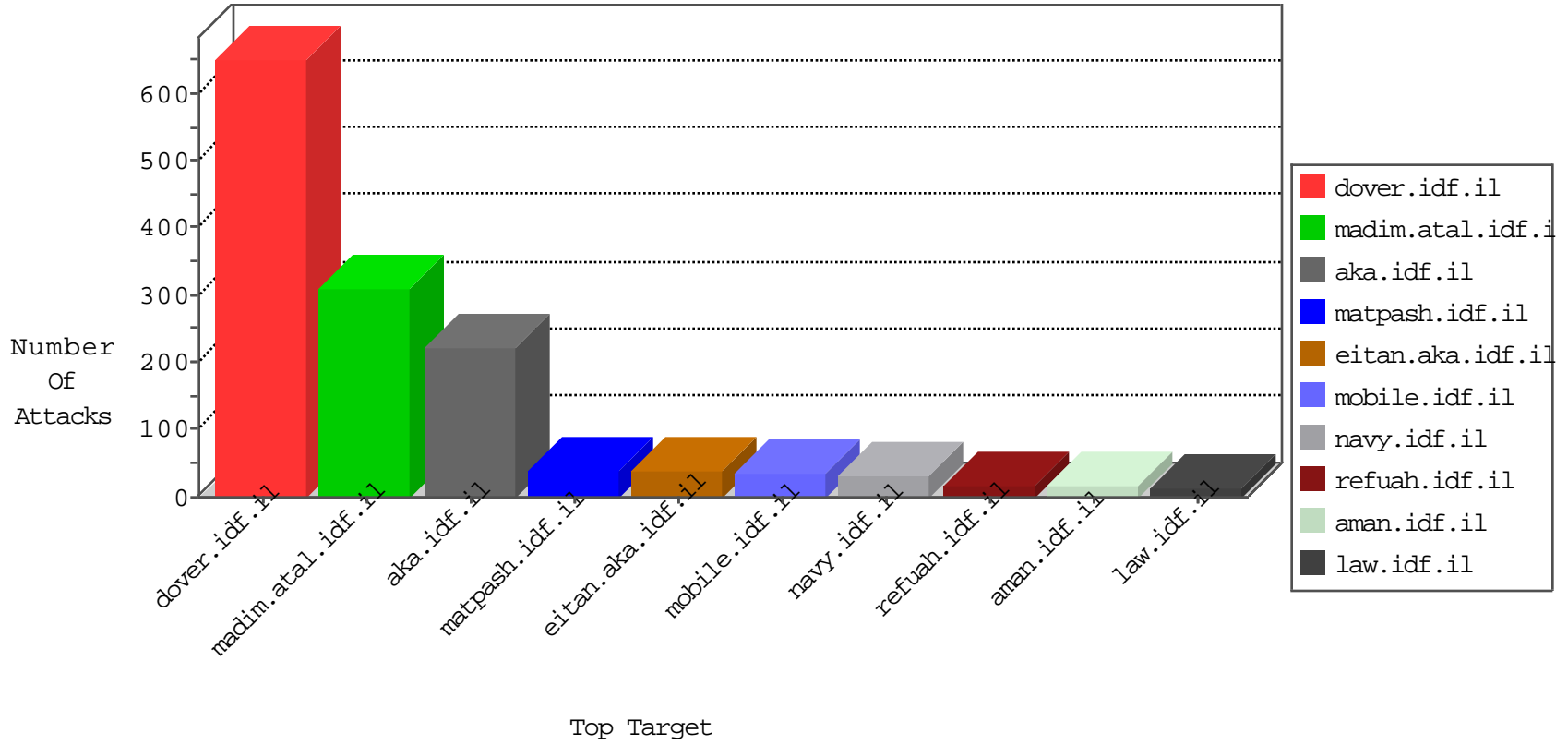


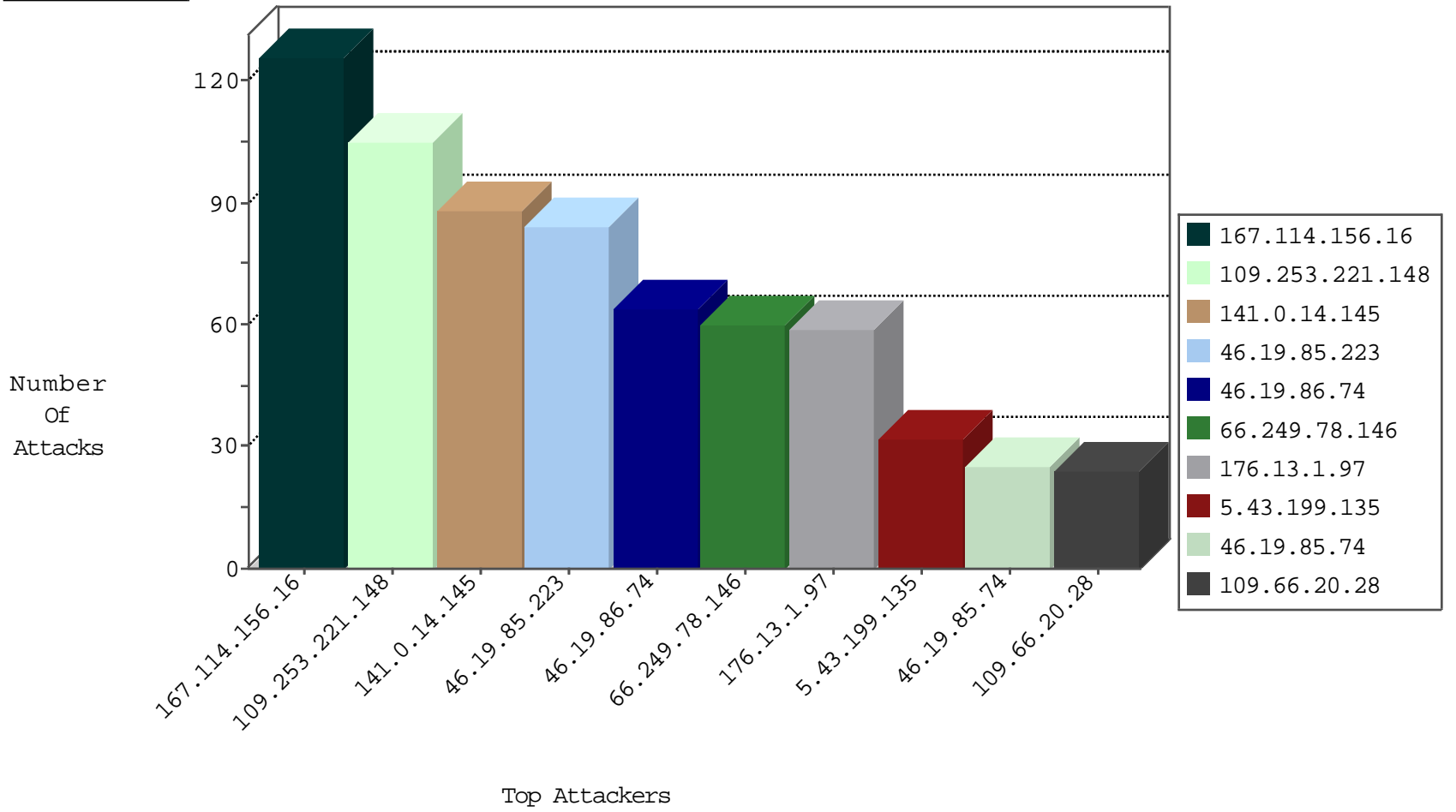
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4170
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1686
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	60
109.65.208.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	5
41.234.170.173	Egypt	147.237.77.216	dover.idf.il	HTTP-MISC-Havij-User-Agent	dest-reset	2
94.102.52.10	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

04-25-2016-16:04:03 to 04-25-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
78.185.229.218	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.14.145	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
109.66.20.28	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.13.1.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.67.101.213	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
84.185.140.194	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
188.161.67.142	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.234.170.173	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.116.184.161	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
5.43.199.135	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.43.199.135	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
204.169.24.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.110.48.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.74	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.146.6.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.5.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.74	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
156.196.57.254	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.18.18.166	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.176.211.95	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.39.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
189.84.218.237	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.43.199.135	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.224.143	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.43.199.135	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.255	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.43.199.135	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.221.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
46.19.86.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.13.1.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.26.149.187	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 37.26.149.187	Block	10
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
78.185.229.218	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
2.55.35.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
78.185.229.218	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.185.229.218	Block	5
78.185.229.218	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 78.185.229.218	Block	4
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
151.31.8.223	Italy	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 151.31.8.223	Block	3
46.18.18.166	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	3
2.53.176.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.13.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.194.222	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.108.18.212	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.70.49.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.147	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.19.85.141	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
81.218.66.107	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
194.153.113.13	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1956-he/cogat.aspx	Block	1
46.121.109.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
78.185.229.218	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
82.221.105.6	Iceland	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
46.121.122.189	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
151.80.31.171	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/faq.asp,	Block	1
177.159.120.162	Brazil	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
131.253.25.203	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
213.55.105.82	Ethiopia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
157.55.39.167	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
185.100.85.236	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
2.53.143.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.228.213.40	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
78.185.229.218	Turkey	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.66.160	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1