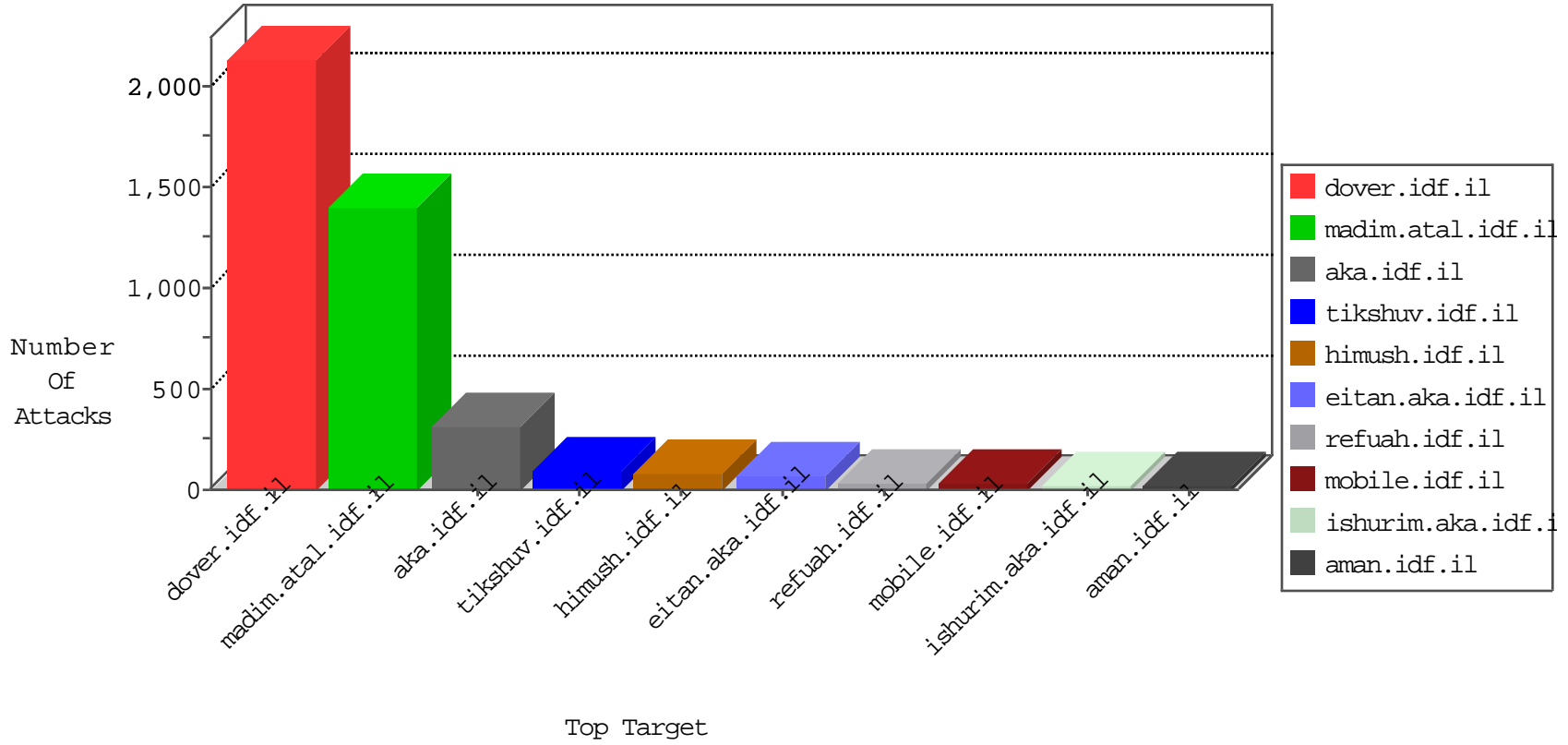


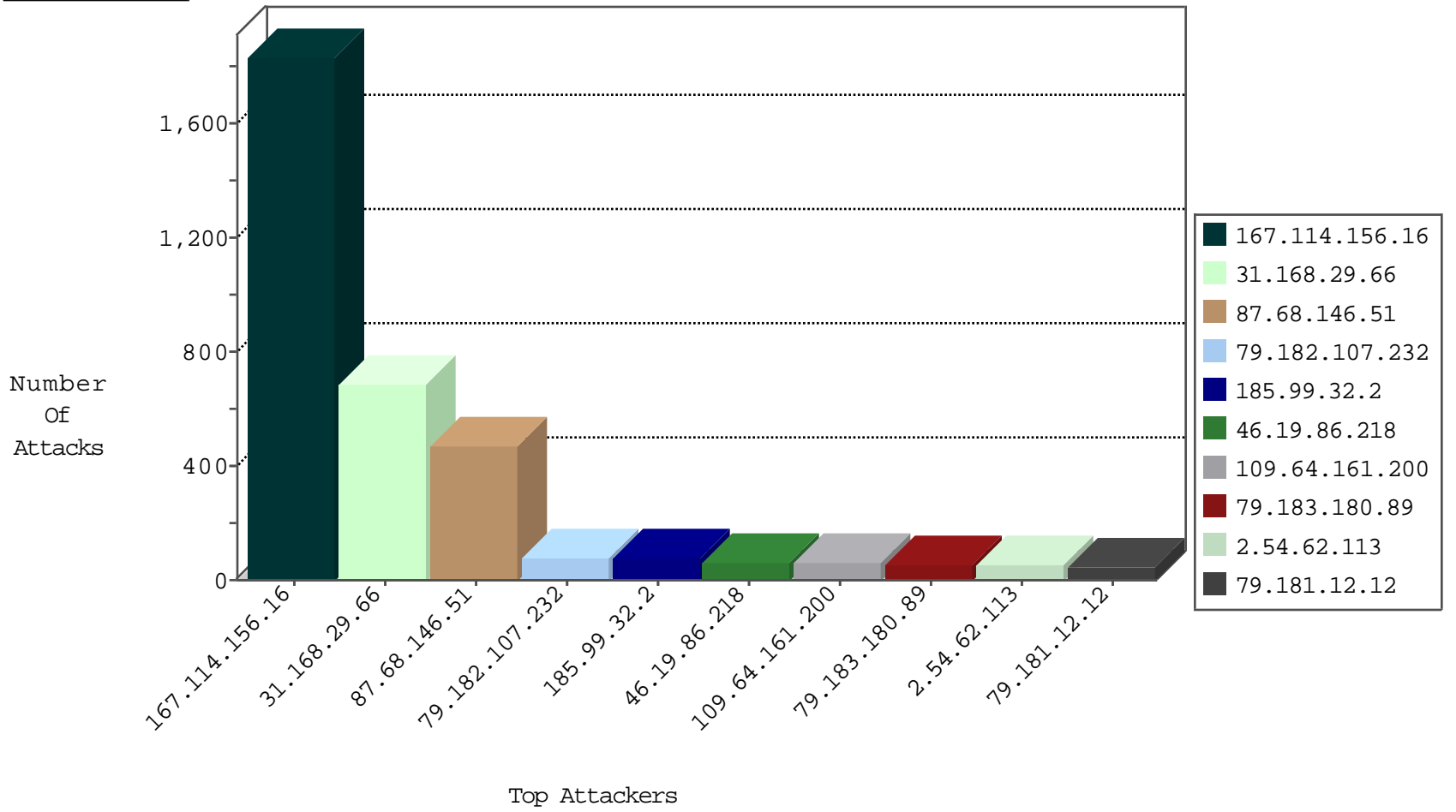
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3053
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	66
79.176.0.16	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.94.153.178	United States	147.237.76.42	refuah.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
61.135.189.97	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
98.119.105.221	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.163.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.180.89	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
185.99.32.2		147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
88.71.239.67	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
185.99.32.2		147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	34
80.246.130.85	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
46.133.101.87	Ukraine	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.62.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
203.133.169.168	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.62.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
212.179.9.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.62.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
2.54.62.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.54.62.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.176.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.133.101.87	Ukraine	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
109.64.161.200	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.54.160.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.64.161.200	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.6.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.205.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.111.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.44.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.15.178	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
156.109.18.122	Europe	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
109.67.31.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.161.200	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	6
93.172.166.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.8.204.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.218.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.183.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.26.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.183.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
92.109.213.179	Netherlands	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
213.8.204.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.130.253.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.161.200	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.180.204	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
93.172.155.34	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.185.253	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
203.133.169.166	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.29.66	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 31.168.29.66	Block	357
87.68.146.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	246
31.168.29.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	179
31.168.29.66	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 31.168.29.66	Block	150
87.68.146.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	115
87.68.146.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
79.182.107.232	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
79.181.12.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
109.64.161.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
2.54.29.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
109.253.144.106	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
2.52.7.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
92.109.213.179	Netherlands	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.14.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.183.217.245	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	3
109.253.214.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.69.172.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.171.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.180.168.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.183.26.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.108.49.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.64.161.200	Israel	147.237.0.19	madim.atal.idf.i	Multiple Untraceable SSL Sessions from 109.64.161.200 (Open Mode)	None	2
85.65.8.94	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
46.121.13.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.242.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.246.130.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
79.177.179.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.102.253.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18551-he/dover.aspx	Block	1
173.252.89.56	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.8.94	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to ww.nakhal.idf.il/sip_storage/files/8/	Block	1
84.108.169.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.117.42.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.208.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.128.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.55.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.54.128.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.69.88	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/error.htm	Block	1
68.180.230.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
176.13.23.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
46.121.203.118	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
109.253.214.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.176.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1