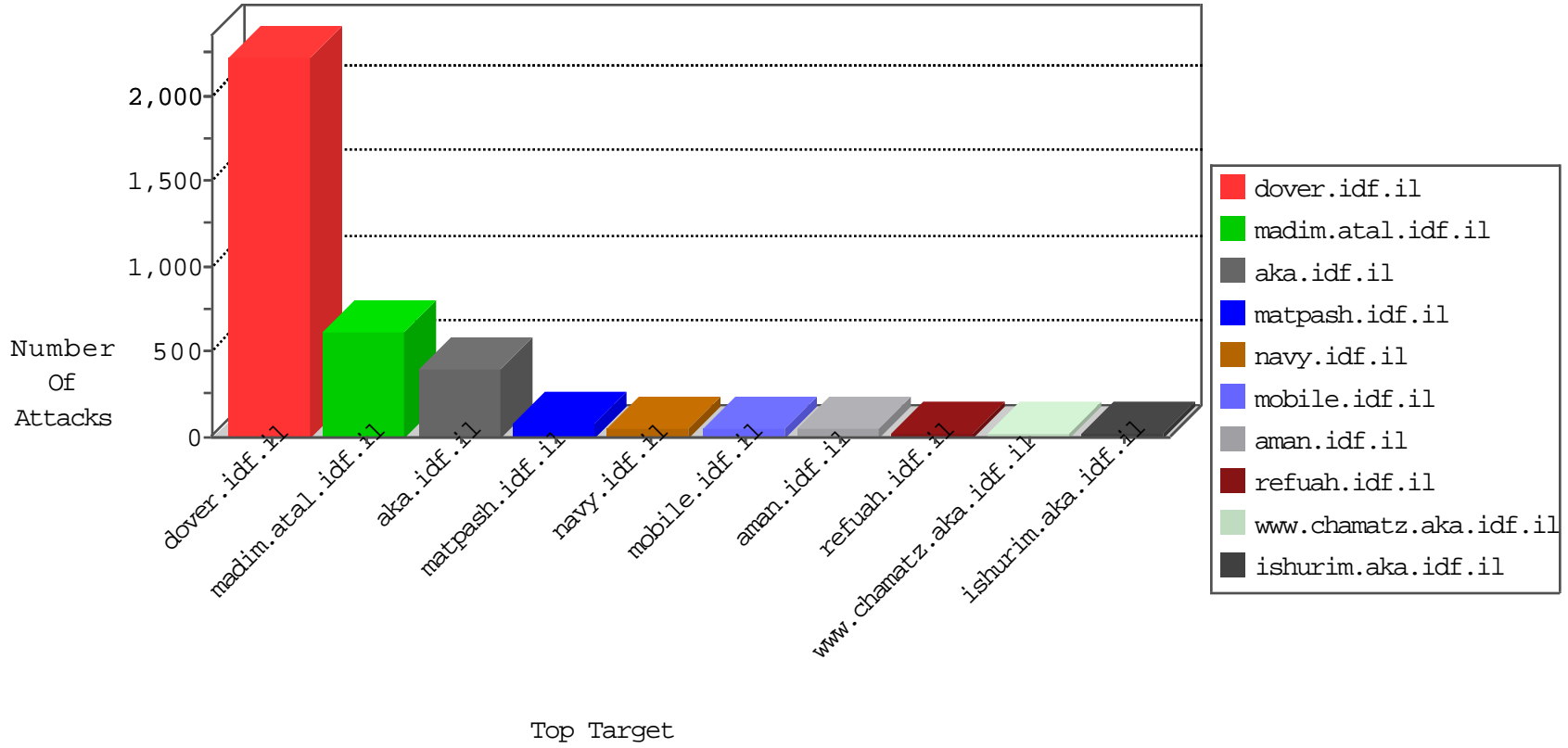


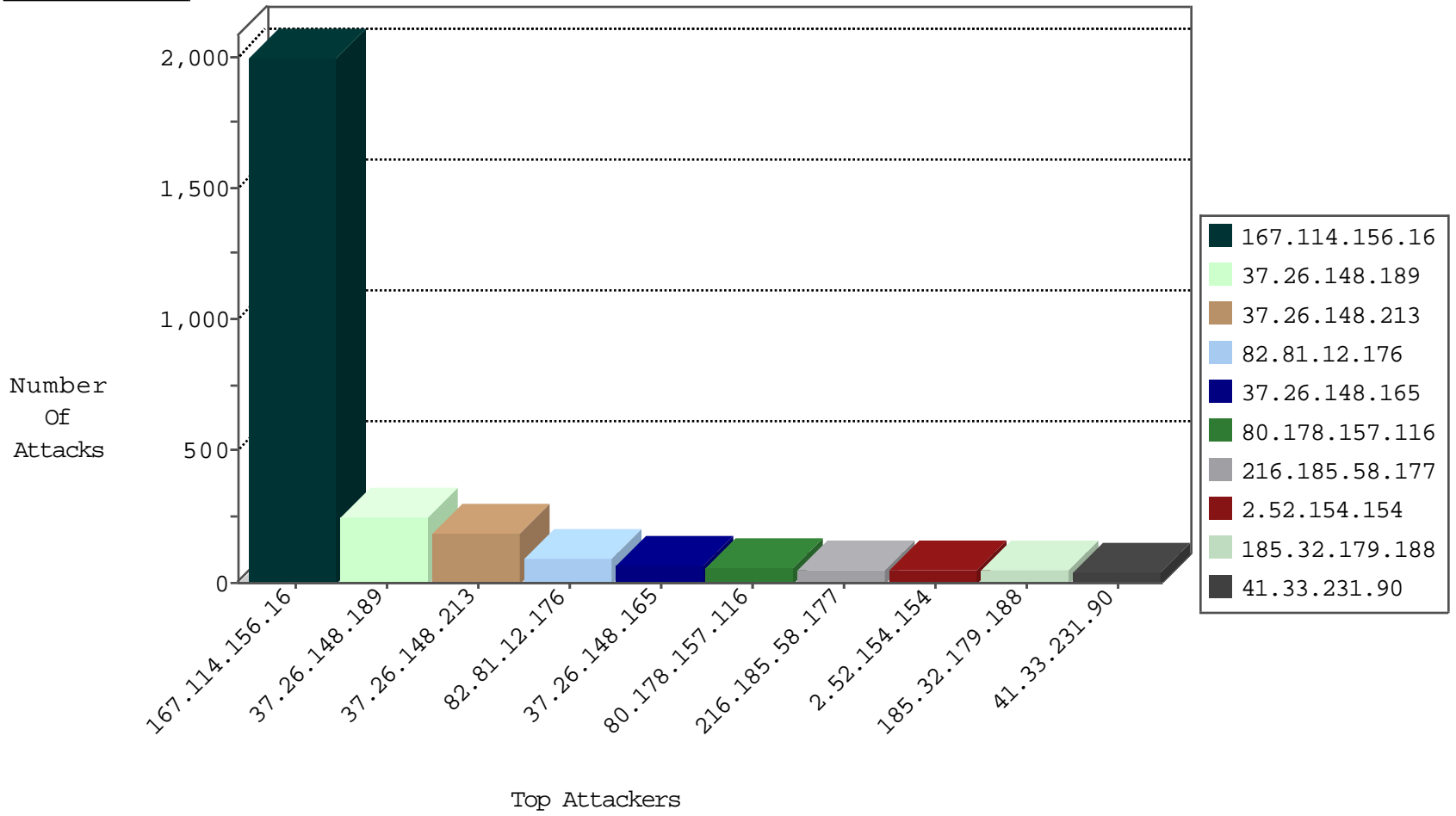
IDF Under Attack Daily Report



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	3003
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	96
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
2.54.138.73	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
14.99.58.94	India	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
145.225.60.5	Germany	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.165.186	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
42.200.37.18	Hong Kong	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
145.225.60.5	Germany	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
198.20.99.130	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
23.95.50.58	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.63.188.120	Russian Federation	147.237.76.86	navy.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
185.73.39.108		147.237.77.216	dover.idf.i	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.63.188.181	147.237.77.216	Italy	dover.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
216.185.58.177	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
46.19.86.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
62.219.236.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
145.225.60.5	Germany	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	15
185.32.179.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
185.32.179.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.154.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
5.22.129.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
158.169.150.6	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
79.180.232.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.120.126.89		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.92	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.32.179.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.65.4.14	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.178.134.47	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.154.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.137.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.154.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.160.143	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.143.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.154.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.52.46.48	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.192.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.108	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
145.225.60.5	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.154.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
176.13.7.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.167.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
176.13.7.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.167.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.167.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
147.236.38.168	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.167.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
172.56.38.223	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.167.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.210.180.192	France	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
158.169.150.9	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
147.236.232.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
81.218.55.253	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
80.178.157.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
147.236.232.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	135
37.26.148.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
37.26.148.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	118
37.26.148.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
80.178.157.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
185.32.179.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	14
176.13.7.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.26.148.189	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.148.189	Block	9
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
80.179.12.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.192.162	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
176.13.10.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.60.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.6.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.1.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.178.157.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.121.132.157	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.132.157	Block	1
176.13.2.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.12.186	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.179.12.186	Block	1
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	1
209.132.178.17	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 209.132.178.17 (Unsupported Cipher)	None	1
109.64.165.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.211.46.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.178.113.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.70.66.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.253.136.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/105570.pdf	Block	1
85.130.240.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/106340.pdf	Block	1
203.196.19.14	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
46.121.132.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus'	Block	1
80.179.12.186	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 2. in URL	Block	1
109.253.219.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.126.82.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	1
213.8.204.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.172.148	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
2.52.187.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/home/default.aspx	Block	1
81.218.172.184	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.210.180.192	France	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1
79.183.103.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1