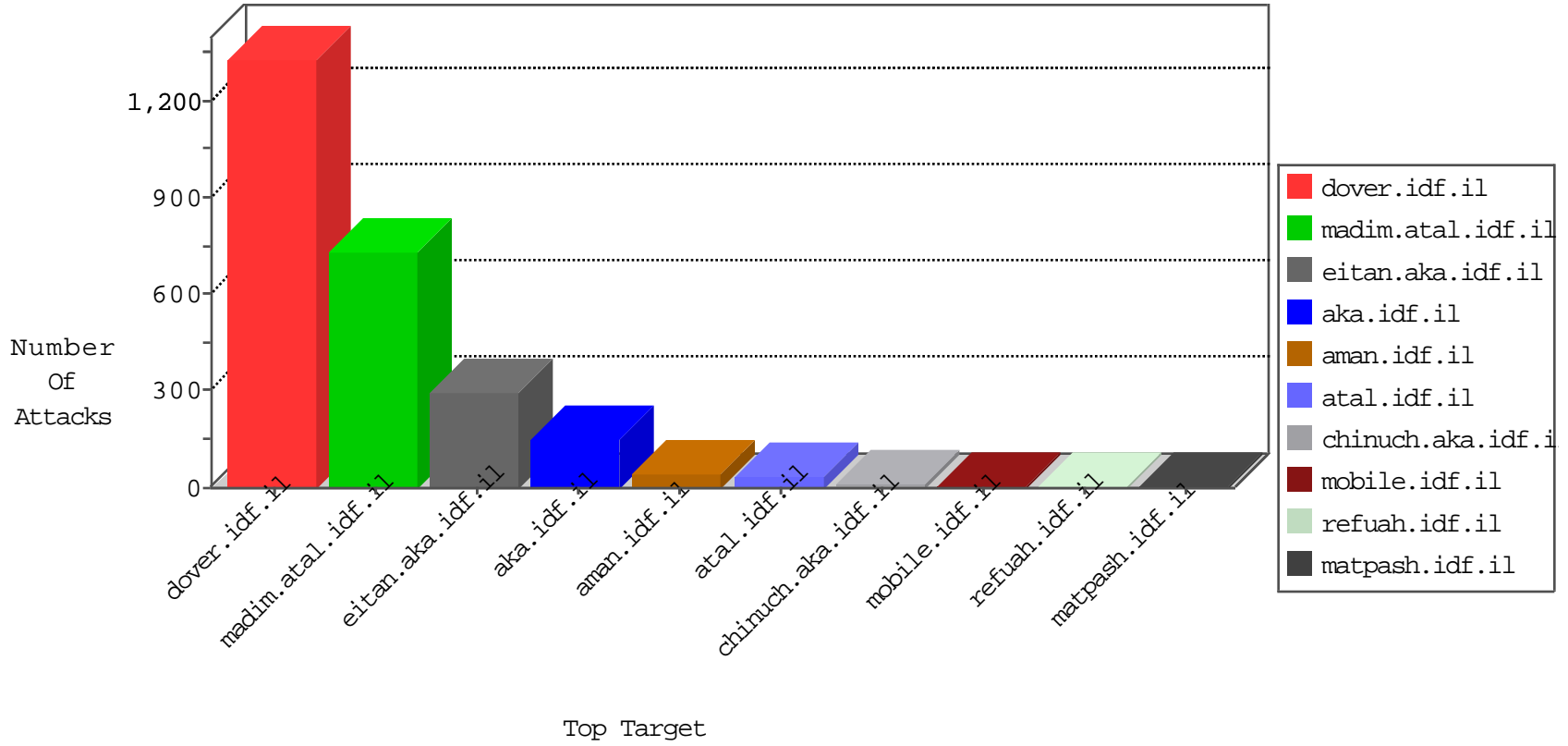


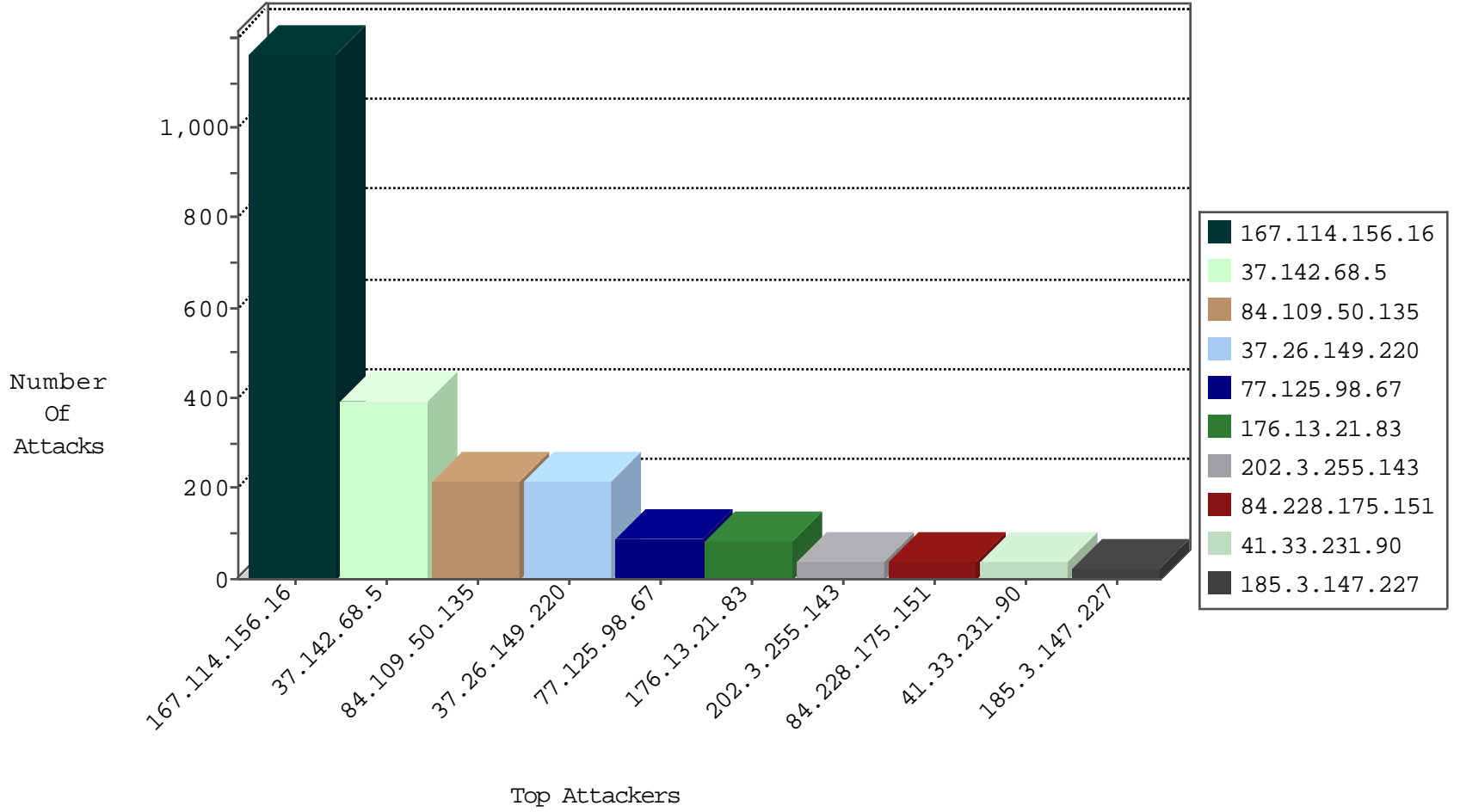
# IDF Under Attack Daily Report



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	3235
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	362
104.131.221.134	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.130.5.224		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	204
77.125.98.67	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.3.147.227	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
89.206.52.99	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
31.168.217.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
207.241.231.229	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	10
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.20.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.120.126.37		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.125.98.67	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.64.28.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.130.127	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.65.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.144.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
199.30.16.167	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.135.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
212.179.212.25	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.154.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.143.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
212.179.212.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.48.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.212.25	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	3
79.176.58.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.219.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.57.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.212.25	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.181.36.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.162.16.100	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.26.148.161	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
54.162.16.100	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
94.230.86.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.125.98.67	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
185.3.147.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.7.213.42	Czech Republic	147.237.76.31	nakchal.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
149.78.198.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.253.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.113.93	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.146.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.117.132.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.68.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	250
37.142.68.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
84.109.50.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
84.109.50.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
176.13.21.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
84.228.175.151	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	38
37.142.68.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	21
176.13.21.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
84.109.50.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	8
109.64.19.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.145.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.64.19.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	4
46.19.86.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.143.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.141.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.36.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.86.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.239.8.105	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
5.29.234.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
109.64.19.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
109.64.19.218	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
84.109.154.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.25	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
5.28.144.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.204.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.149.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.3.147.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.253.219.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.79.17	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
176.13.16.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.166.94	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/1133-22461-he/dover.aspx.	Block	1
136.243.48.86	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
40.77.167.7	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.26.148.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
69.30.244.53	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
176.13.21.83	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ***** ***** *****, Observed ***** ***** ***** ****	None	1
46.117.183.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.81.50.82	Denmark	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
2.52.150.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	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
79.181.175.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
40.77.167.12	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1