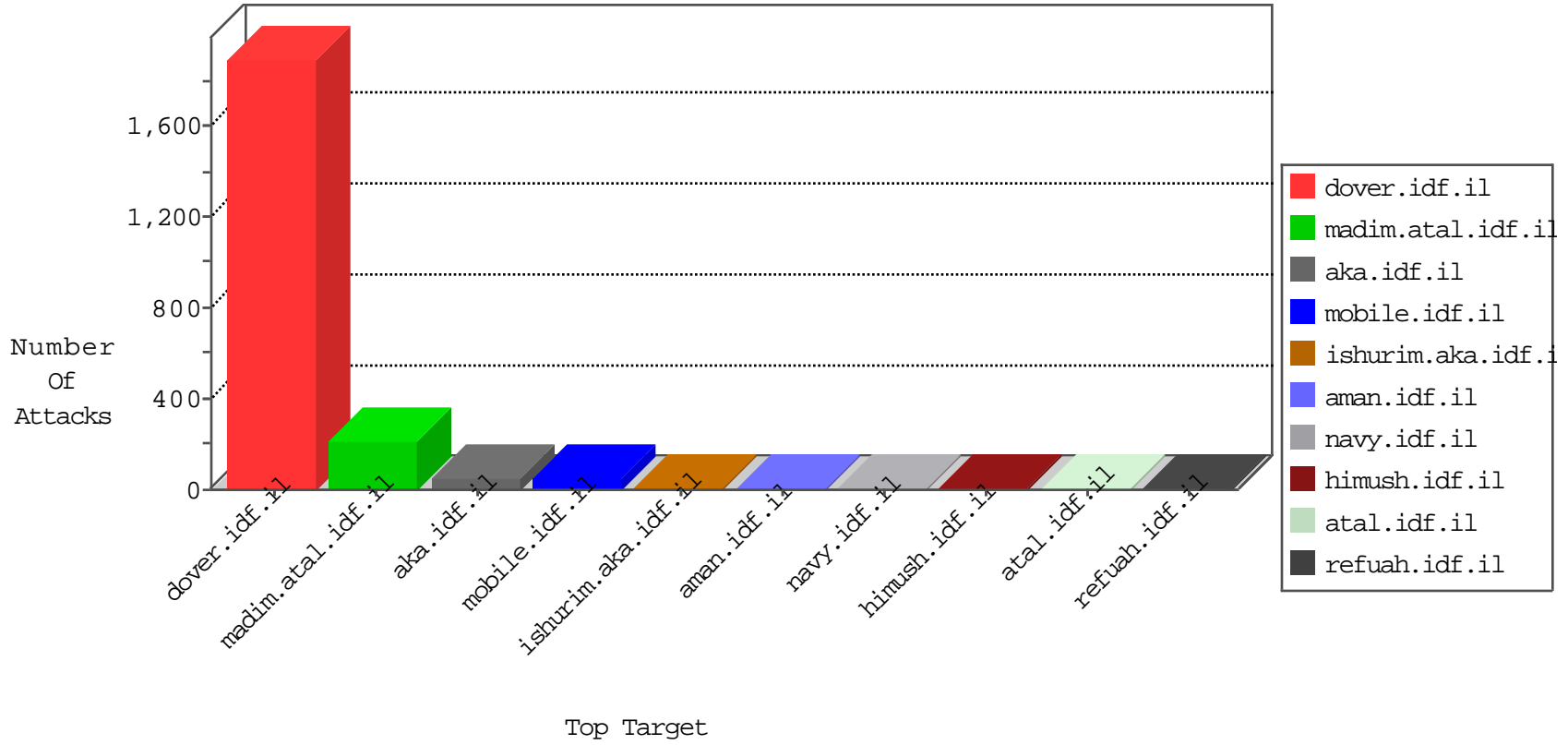


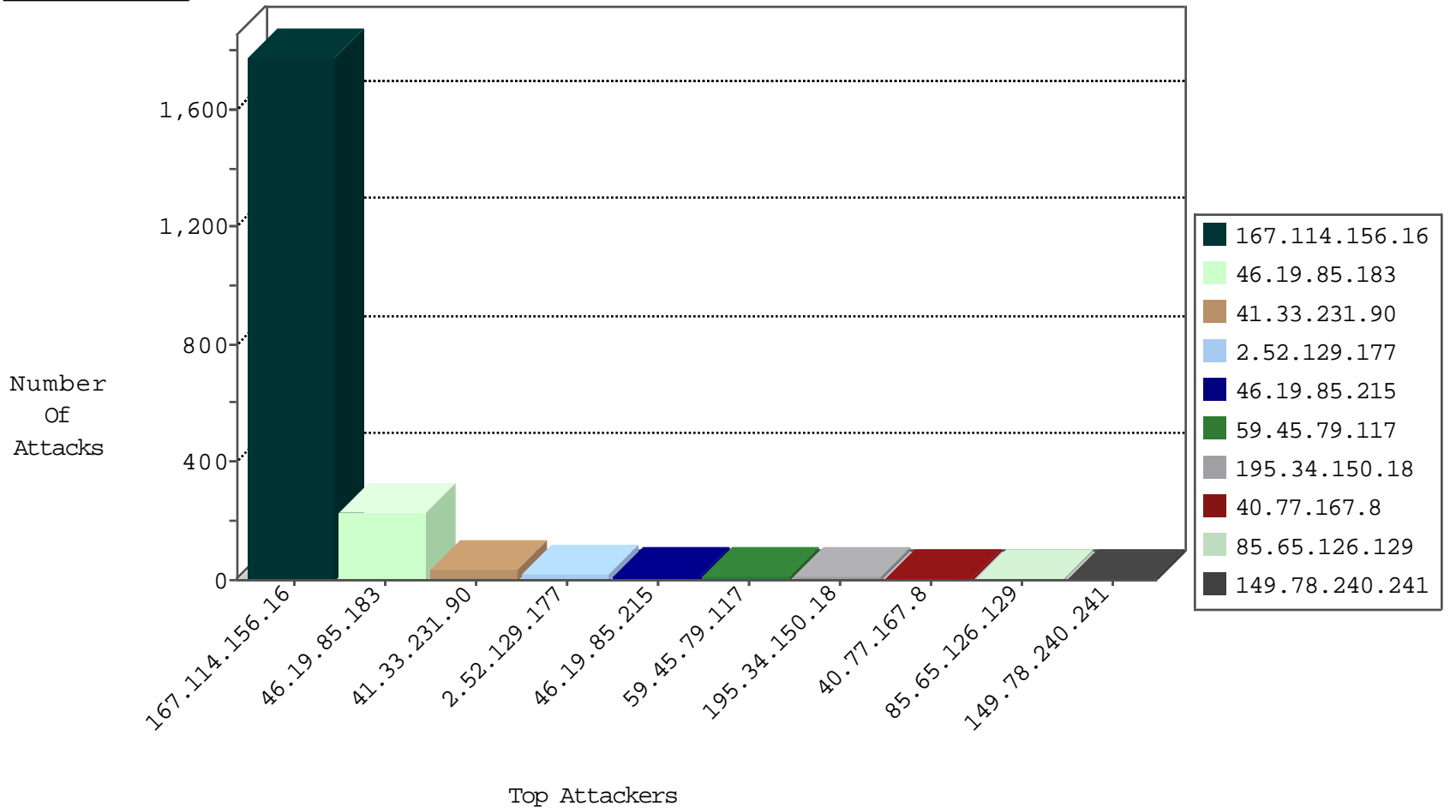
IDF Under Attack Daily Report



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	3042
142.54.160.210	United States	147.237.77.234	halag.idf.il	block-sp-trafl	drop	1
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
180.97.106.36	China	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.74	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	drop	1
211.179.6.103	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-08-2016-07:04:07 to 01-08-2016-08:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.202	e.halag.idf.il	13840: TLS: OpenSSL Heartbeat Packet	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	4
80.82.64.204	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
191.33.22.177	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
80.248.146.42	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
191.33.22.177	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
149.78.240.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.91.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
40.77.167.8	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.11.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.65.126.129	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.200.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.152.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.126.129	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.144.55.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.61.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
62.219.21.30	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.216.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.37	China	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
38.229.1.15	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
67.204.178.17	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
180.97.106.36	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
5.144.55.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.73	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.100	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.216.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.37	China	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
94.230.86.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.227.118	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
68.113.90.242	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.161	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
180.97.106.36	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
147.235.8.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.88	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.25.43.94	Germany	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.118	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.219.21.30	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.37	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
173.236.152.135	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
125.215.235.182	Hong Kong	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
198.20.69.74	United States	147.237.76.202	e.halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.161	China	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
180.97.106.36	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
147.235.8.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.144.55.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.183	Block	74
2.52.129.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.183	Block	6
80.178.201.104	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.178.201.104	Block	5
213.57.128.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.29.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.167.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
79.182.60.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.4.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.161.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.132.34.62	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an..	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
109.201.152.251	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
216.218.206.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.13.11.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.178.29	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18457-he/dover.aspx	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/se/util/setracker.cfm	Block	1
207.46.13.24	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
46.19.85.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19239-en/dover.aspx http://digg.com/submit	Block	1
5.28.190.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1512-he/refuah.aspx	Block	1
207.46.13.151	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
2.52.157.183	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
141.212.122.64	United States	147.237.76.86	navy.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
80.178.201.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
46.120.233.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
31.44.139.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
173.254.216.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.111.196.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19683-he/idfgdover.aspx	Block	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
37.8.81.239	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
109.186.130.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1