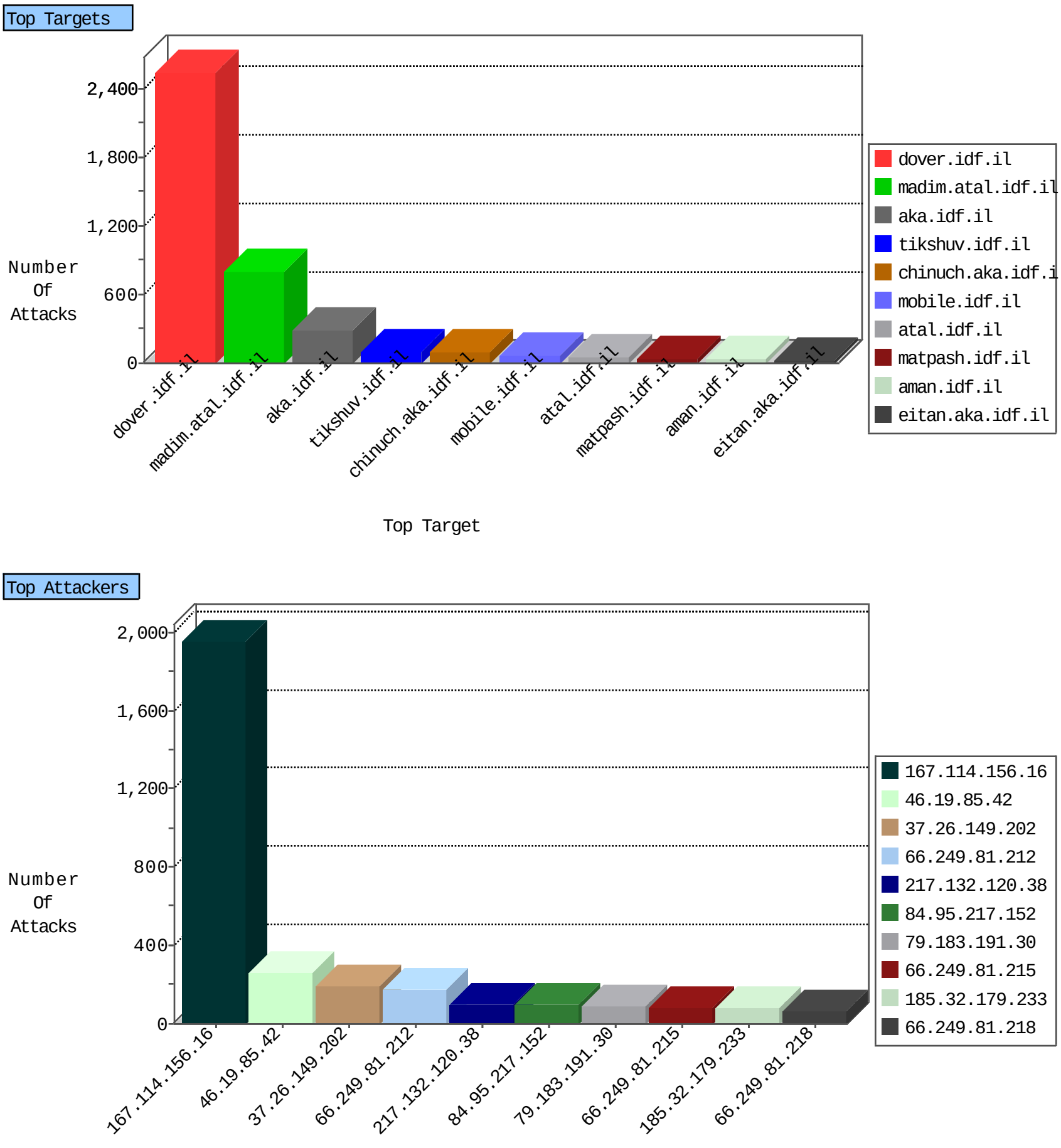
01-07-2016-21:04:03 to 01-07-2016-22:04:03

IDF Under Attack Daily Report



01-07-2016-21:04:03 to 01-07-2016-22:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4918
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3240
66.249.79.41	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2910
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
5.175.26.46	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.189.169.158	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

01-07-2016-21:04:03 to 01-07-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-07-2016-21:04:03 to 01-07-2016-22:04:03

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
106.79.129.35	147.237.0.34	India	tikshuv.idf.il	GPL SCAN nmap TCP	3
66.249.73.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
37.26.149.202	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
37.26.149.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.227.181	147.237.8.46	Israel	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.114	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.57.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
64.2.184.130	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.230.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
85.65.139.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.49.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.229.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.69.42	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

01-07-2016-21:04:03 to 01-07-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.217.152	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
89.139.187.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	31
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	25
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	25
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	22
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
176.13.10.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
37.142.68.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	16
46.19.85.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	12
79.183.180.89	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	11
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	10
94.230.86.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	10
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.8.204.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.78.60	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
76.21.157.243	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
37.142.68.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.37	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.218.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.65.149.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	6
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
93.172.232.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.67.52.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.194.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
46.19.85.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
217.132.120.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
79.183.191.30	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.183.191.30	Block	87
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
37.26.147.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
37.26.147.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.54.8.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.85.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	20
176.13.10.30	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.147.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
217.132.120.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
149.88.150.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.194.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.86.98.161	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.98.161	Block	2
46.19.85.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.149.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.150.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
69.171.231.226	United States	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	2
5.29.54.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.0.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
213.57.134.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
2.54.178.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.119	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
46.19.86.195	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.86.195	None	1
115.239.110.231	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1137-he/dover	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed URL is Above Root Directory	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
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
5.102.218.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.31.57.5	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.94.170.18	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.170.18	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.2	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.31.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.109.190	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
213.57.208.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.195.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainqsachar	Block	1
37.26.147.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1