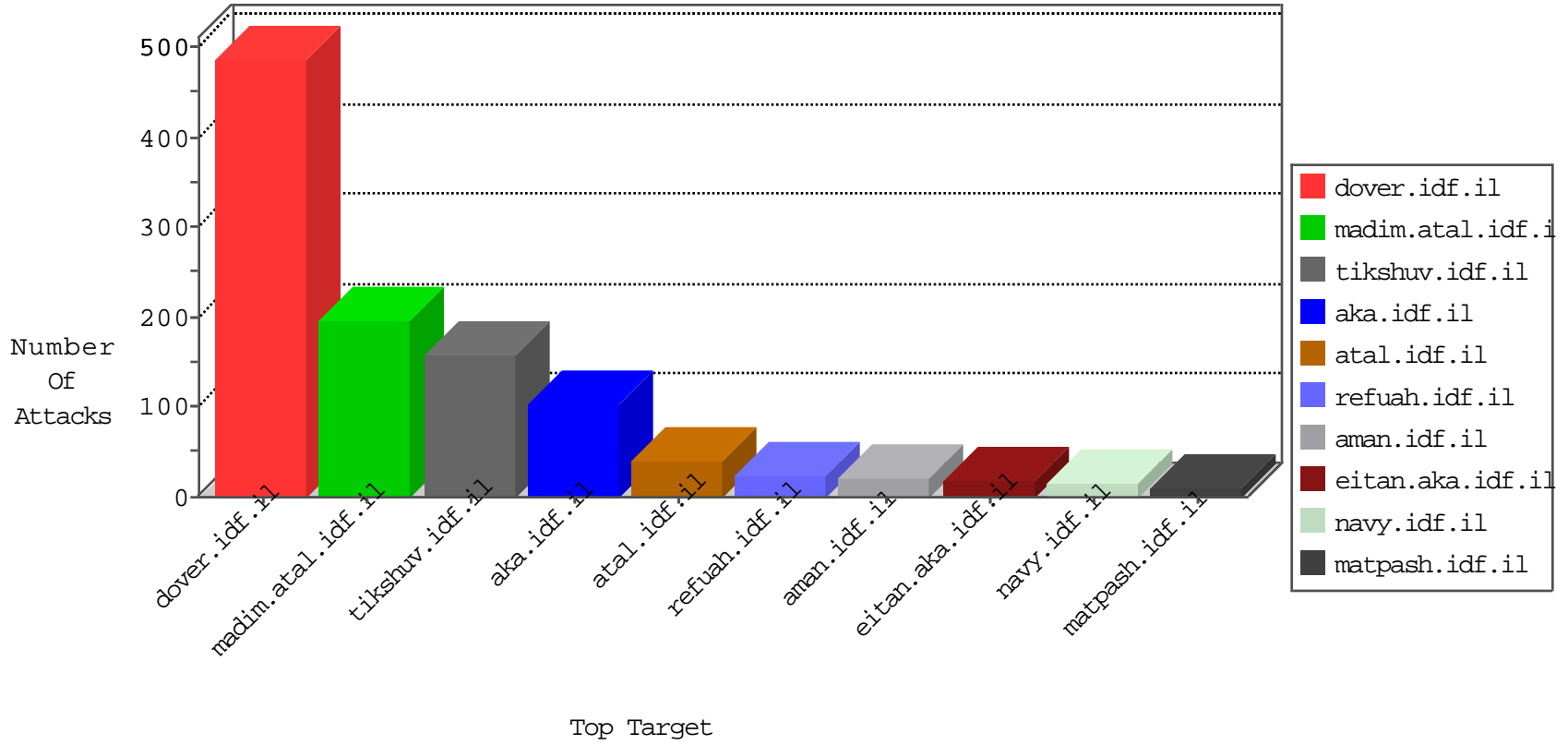


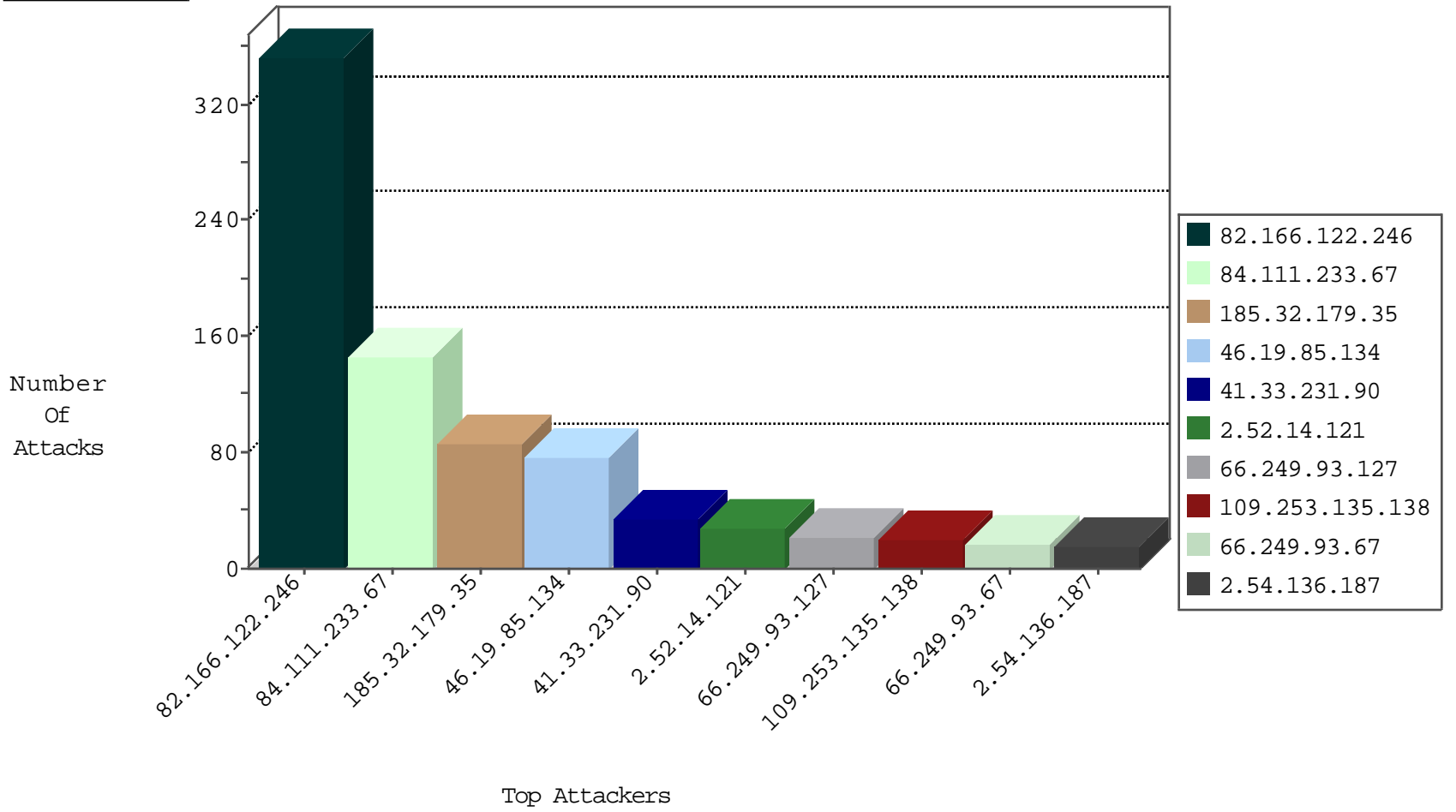
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3

02-15-2016-00:04:04 to 02-15-2016-01:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.76.39	mobile.meitav.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	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
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
201.232.25.160	147.237.72.156	Colombia	aman.idf.il	ET SCAN NMAP -sS window 4096	1
94.176.78.49	147.237.76.31	Moldova, Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.77.233	Turkey	atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.70	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
221.226.31.210	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
221.6.32.82	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
201.232.25.160	147.237.72.156	Colombia	aman.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.105	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.51.30	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.70	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
221.226.31.210	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
221.6.32.82	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	340
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
109.253.135.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	16
217.132.121.233	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.102.222.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.22.130.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
94.230.86.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
2.54.28.204	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.191.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.49.166	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
71.168.187.90	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.126	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.39.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.127	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.102.9.49	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.127	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.181.54.135	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.93.127	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.126	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.93.127	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.136.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.228.78.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.173.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.136.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.204.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.195.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.136.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
185.120.126.62		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.250.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.132.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
74.6.254.118	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
5.102.242.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.228.179.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.233.67	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 84.111.233.67	Block	145
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
185.32.179.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	57
2.52.14.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
185.32.179.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00\$ContentPlaceholder1\$ucArticleLobbyControl\$datepicker1 in www.idf.il/1781-he/dover.aspx	Block	11
185.32.179.35	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 185.32.179.35	Block	8
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	5
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	3
185.120.125.52		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.117.60.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.170.23	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
31.210.189.195	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
85.65.26.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.121.219.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
89.138.185.137	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
79.181.9.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
141.212.122.112	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /x	Block	1
50.62.208.82	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
31.210.189.195	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	1
208.115.111.73	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
84.111.108.40	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_source in www.aka.idf.il/main/rabanut/general.aspx	None	1
157.55.39.147	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
128.72.24.220	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1397-en/dover.aspx	Block	1
84.228.11.203	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
79.182.16.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
185.120.126.39		147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
149.88.76.218	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to ww.aman.idf.il/https://www.aman.idf.il/	Block	1
64.71.32.26	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
84.111.110.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
72.34.33.170	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
46.121.152.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
128.72.24.220	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1397-en/dover.aspx	Block	1
198.20.87.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
82.166.122.246	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00\$ContentPlaceholder1\$ucArticleLobbyControl\$datepicker in www.idf.il/1781-he/dover.aspx	Block	1
149.88.113.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
40.77.167.63	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to ww.aman.idf.il/...	Block	1
109.253.135.138	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.111.180.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
79.177.6.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
128.194.135.65	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
2.52.134.158	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
199.30.25.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.2.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16552-en/dover.aspx-title=for	Block	1
109.253.138.210	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.111.233.67	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
79.179.121.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1