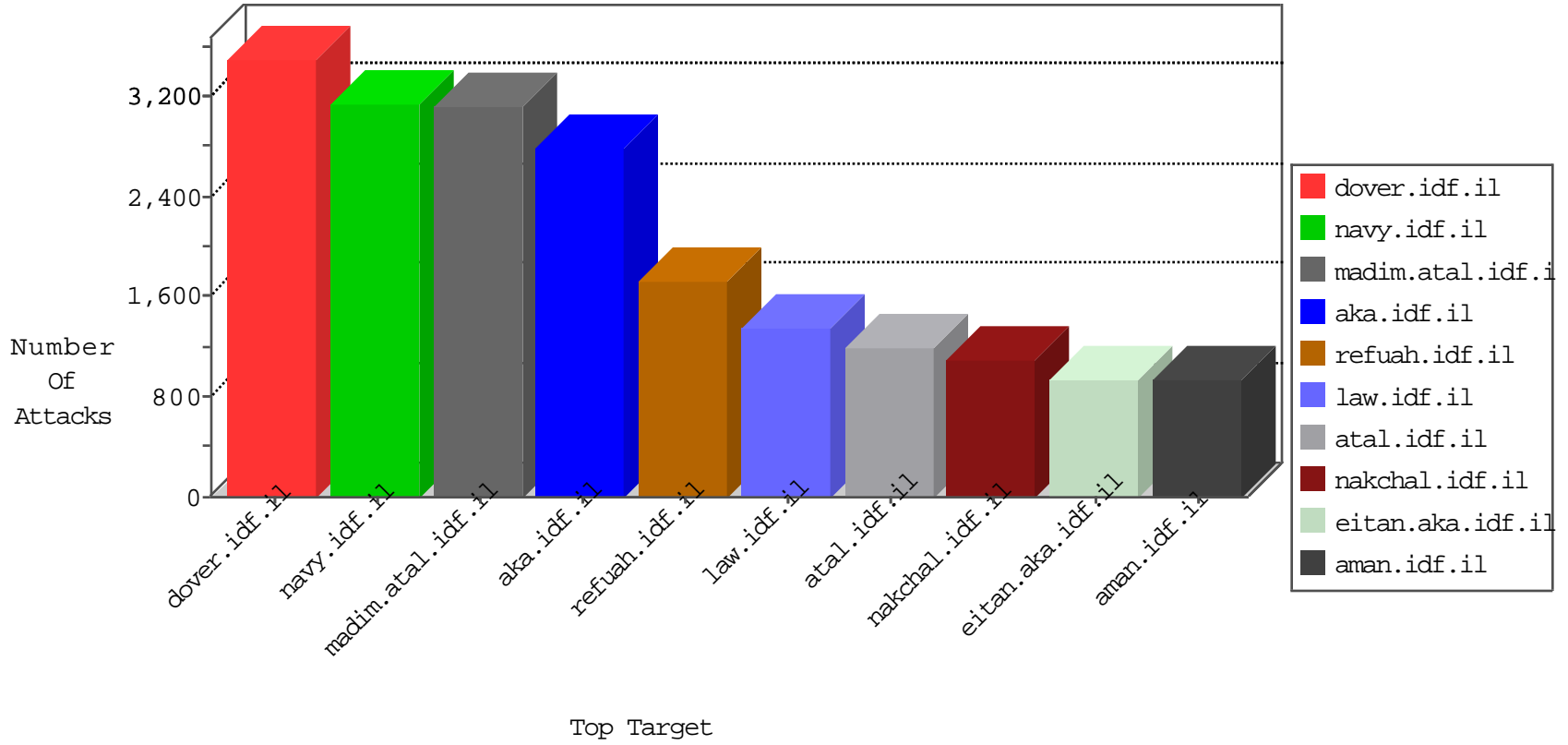


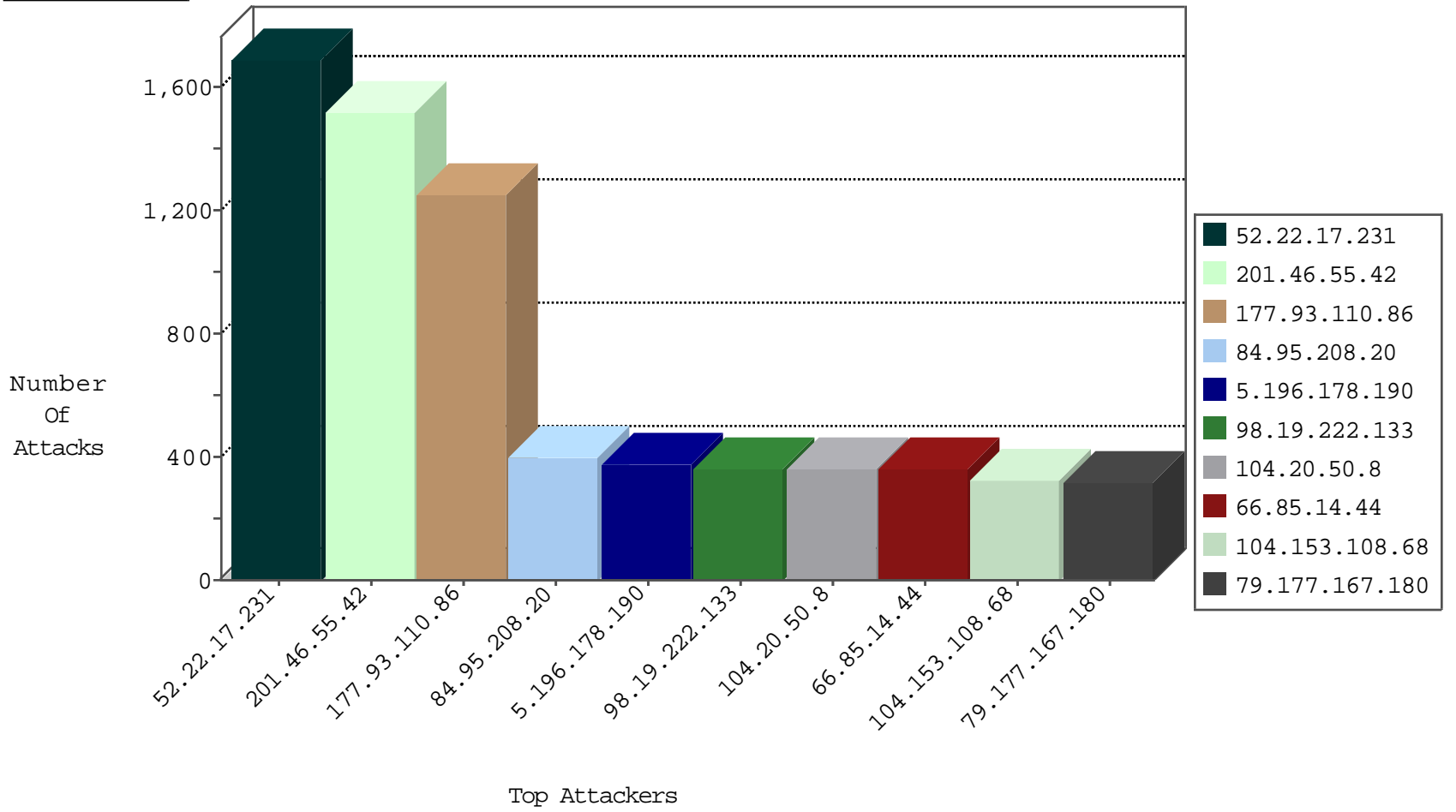
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.47	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	497
176.13.20.136	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
8.37.225.189	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10
2.53.170.165	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
46.19.86.97	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
82.145.221.82	Europe	147.237.76.42	refuah.idf.il	Black List	drop	5
120.132.50.135	China	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	forward	4
58.218.200.137	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	4
109.253.198.205	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
2.53.145.189	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
8.37.225.189	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
185.89.217.232	Netherlands	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3
8.37.225.189	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
8.37.225.88	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	2
179.99.200.39	Brazil	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	forward	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Black List	drop	2
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
120.132.50.135	China	147.237.72.156	aman.idf.il	block-sp-trafl	forward	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
207.46.13.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Black List	drop	2
109.253.206.207	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.34	yochalan.idf.il	Black List	drop	2
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	2
185.89.217.226	Netherlands	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	2
139.19.117.8	Germany	147.237.76.30	himush.idf.il	Black List	drop	2
79.176.105.139	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.198	e.yochalan.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Black List	drop	2
2.53.138.185	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Black List	drop	2
134.147.203.115	Germany	147.237.76.198	e.yochalan.idf.il	Black List	drop	2
218.93.206.21	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
163.172.49.61	United Kingdom	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	92
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	64
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	54
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	49
163.172.49.61	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	44
98.19.222.133	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	36
61.220.26.201	Taiwan	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	24
98.19.222.133	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	18
98.19.222.133	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	18
98.19.222.133	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	18
87.242.112.35	Russian Federation	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
38.110.11.92	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
87.117.203.30	United Kingdom	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
49.236.200.182	Malaysia	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
103.21.58.191	India	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
97.74.215.165	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
50.63.197.7	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
91.219.122.2	Poland	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
87.242.112.45	Russian Federation	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
204.93.196.218	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
216.26.128.28	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
61.220.26.201	Taiwan	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
177.185.194.45	Brazil	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
87.242.112.35	Russian Federation	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
37.228.93.70	Russian Federation	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
23.91.70.77	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
87.106.184.160	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
61.220.26.201	Taiwan	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
91.219.122.4	Poland	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
88.208.252.129	United Kingdom	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
213.174.55.11	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
71.171.93.66	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
50.63.197.7	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
210.169.203.81	Japan	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
87.242.112.45	Russian Federation	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
71.171.93.66	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
52.91.49.78	United States	147.237.77.74	law.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	10
54.86.105.62	United States	147.237.77.74	law.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	10
137.117.8.203	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	10
188.163.109.21	Ukraine	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	8
216.119.125.173	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
71.171.93.66	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
50.63.197.140	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
64.34.186.9	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
103.21.58.191	India	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.246.49.11	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
97.74.215.165	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
188.165.250.173	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
71.227.28.52	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	192
103.21.58.191	147.237.76.42	India	refuah.idf.il	SQL Injection - Select From	72
37.228.93.70	147.237.76.86	Russian Federation	navy.idf.il	SQL Injection - Select From	54
74.84.136.105	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	54
62.210.226.9	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	54
61.220.26.201	147.237.76.42	Taiwan	refuah.idf.il	SQL Injection - Select From	50
98.19.222.133	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	48
87.106.184.160	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	36
87.242.112.35	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	31
185.96.92.54	147.237.76.31	United Kingdom	nakchal.idf.il	SQL Injection - Select From	28
91.219.122.2	147.237.77.233	Poland	atal.idf.il	SQL Injection - Select From	26
87.242.112.45	147.237.77.176	Russian Federation	matpash.idf.il	SQL Injection - Select From	26
23.91.70.77	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	26
87.242.112.35	147.237.76.42	Russian Federation	refuah.idf.il	SQL Injection - Select From	20
66.29.216.40	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	20
50.63.197.140	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	20
65.39.128.237	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
50.63.197.7	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	20
49.236.200.182	147.237.77.216	Malaysia	dover.idf.il	SQL Injection - Select From	20
216.26.128.28	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
97.74.215.165	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	20
210.169.203.81	147.237.76.42	Japan	refuah.idf.il	SQL Injection - Select From	20
87.117.203.30	147.237.0.34	United Kingdom	tikshuv.idf.il	SQL Injection - Select From	20
71.171.93.66	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
38.110.11.92	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	20
177.185.194.45	147.237.77.226	Brazil	www.chamatz.aka.idf.il	SQL Injection - Select From	20
91.219.122.4	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	20
67.199.10.25	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
50.63.197.7	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
88.208.252.129	147.237.77.216	United Kingdom	dover.idf.il	SQL Injection - Select From	20
216.26.128.28	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	20
95.110.142.198	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	18
199.79.62.138	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
177.185.194.130	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
177.185.192.86	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
185.96.92.54	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	18
216.119.112.144	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	18
81.223.238.42	147.237.77.74	Austria	law.idf.il	SQL Injection - Select From	18
62.210.226.9	147.237.77.74	France	law.idf.il	SQL Injection - Select From	18
23.91.70.119	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
96.251.45.13	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
71.227.28.52	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
95.110.142.198	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	18
209.208.126.125	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
137.117.8.203	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
207.54.144.207	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
184.172.106.100	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
97.88.198.223	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	18
87.242.112.45	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	18
200.59.199.229	147.237.77.233	Argentina	atal.idf.il	SQL Injection - Select From	18

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.167.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	312
141.0.15.34	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	194
52.22.17.231	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	162
52.22.17.231	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	161
52.22.17.231	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	161
52.22.17.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	161
52.22.17.231	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	159
52.22.17.231	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	157
52.22.17.231	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	157
52.22.17.231	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	156
188.165.22.182	Poland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	153
24.182.177.175	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	127
8.37.225.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	101
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	100
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	98
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	96
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	96
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	95
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	95
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	94
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	93
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	82
79.179.103.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	80
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	79
177.93.110.86	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	78
177.93.110.86	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	78
177.93.110.86	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	77
177.93.110.86	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	75
177.93.110.86	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	74
177.93.110.86	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	73
177.93.110.86	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	73
177.93.110.86	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	72
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
104.153.108.68	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	68
104.153.108.68	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	67
104.153.108.68	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	67
8.37.225.88	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	64
46.19.85.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
104.153.108.68	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	62
66.85.14.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	59
104.153.108.68	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	55
8.37.225.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
8.37.225.189	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	48
177.93.110.86	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	48
5.196.178.190	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
5.196.178.190	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
5.196.178.190	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
5.196.178.190	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47

09-09-2016 to 09-10-2016

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.21.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	299
85.65.71.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	292
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	233
80.246.137.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	205
82.81.10.32	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	175
46.19.86.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	157
37.26.146.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	137
2.55.186.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
176.13.5.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
185.32.179.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.253.207.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	98
46.117.135.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
176.13.23.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
2.53.151.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
85.130.241.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
109.253.241.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
2.53.181.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
109.253.158.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.210.140.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
121.9.142.113	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 121.9.142.113	Block	34
46.19.86.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
37.26.147.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	26
109.66.126.123	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	21
2.53.19.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
36.5.249.243	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.5.249.243	Block	17
218.18.171.7	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.18.171.7	Block	17
110.89.17.48	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 110.89.17.48	Block	17
183.11.4.25	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 183.11.4.25	Block	17
5.102.192.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
27.154.34.210	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 27.154.34.210	Block	15
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	13
121.9.142.113	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	12
79.179.50.204	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.40	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	10
46.19.85.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.55.21.168	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.55.21.168	Block	8
37.26.146.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	7
130.60.168.5	Switzerland	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	7
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	7

09-09-2016 to 09-10-2016