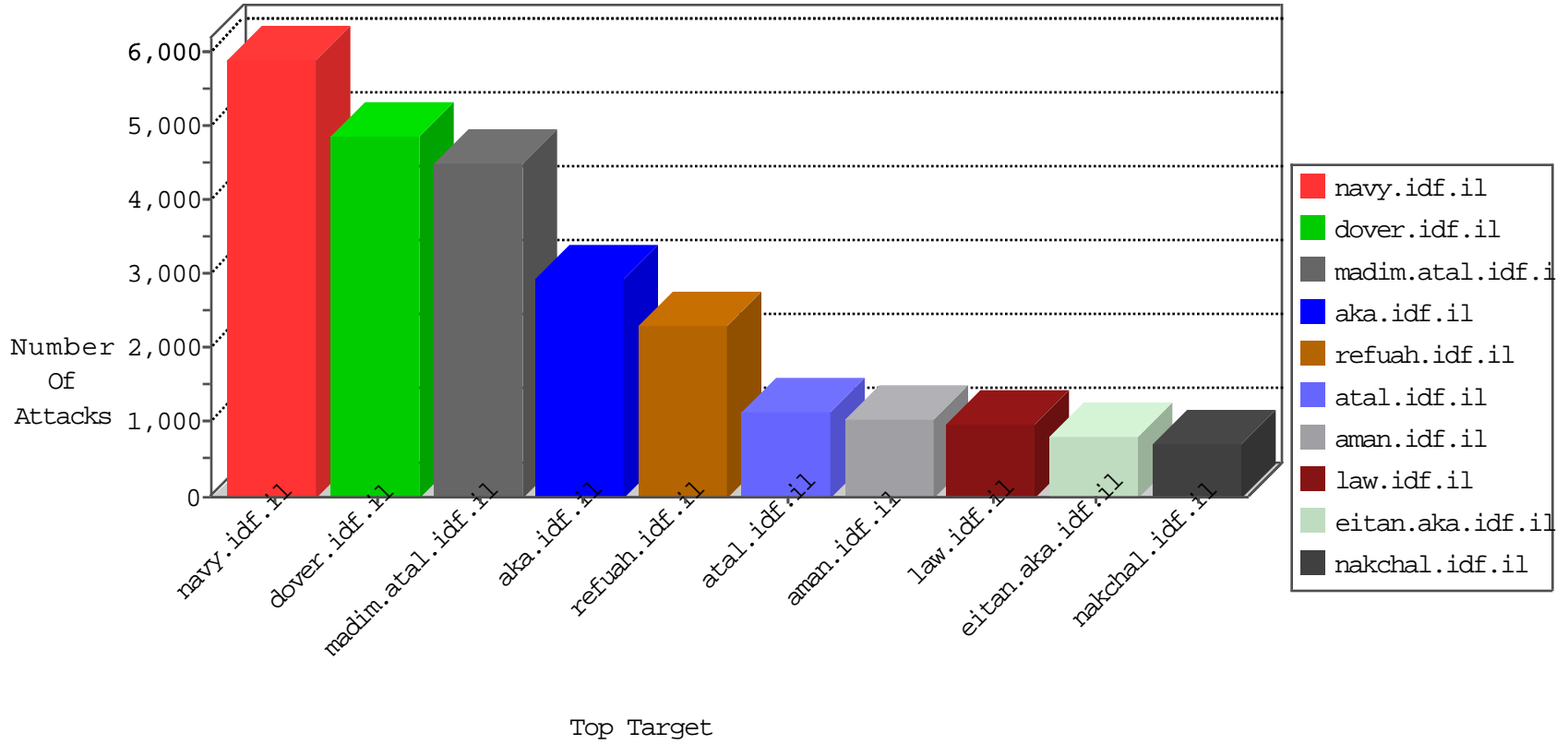


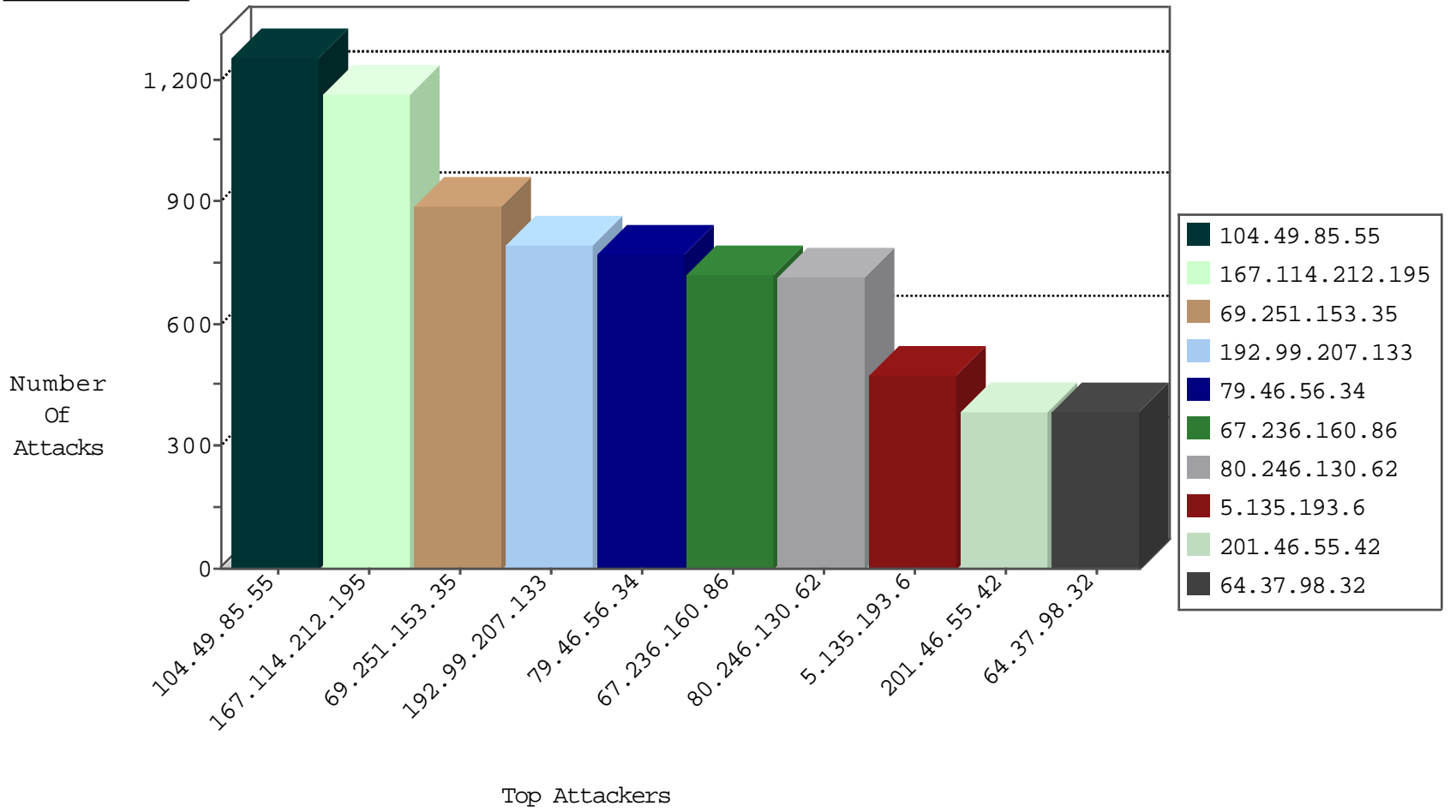
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.180.6	United States	147.237.77.74	law.idf.il	TCP Scan (vertical)	drop	323
204.93.154.220	United States	147.237.77.74	law.idf.il	TCP Scan (vertical)	drop	175
204.93.154.212	United States	147.237.77.74	law.idf.il	TCP Scan (vertical)	drop	155
176.13.234.124	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
46.19.85.112	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	31
37.46.38.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
79.182.11.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
109.253.213.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
46.19.86.26	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
66.102.9.147	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
2.53.18.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
212.179.44.34	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
176.13.243.48	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	8
46.120.98.48	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
95.35.37.223	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
157.55.39.150	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.229.61.20	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
2.53.190.101	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	forward	4
109.205.114.106	Iraq	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
176.13.224.13	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
89.139.177.158	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.181.224.100	Israel	147.237.72.156	aman.idf.il	I4 Source or Dest Port Zero	drop	4
2.53.47.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
68.180.230.47	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Black List	drop	3
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	3
109.228.19.67	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Black List	drop	3
2.53.133.207	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
27.254.150.65	Thailand	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Top	drop	3
79.182.117.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.25.74.130	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
209.126.136.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
209.126.136.2	United States	147.237.76.30	himush.idf.il	Black List	drop	2
46.19.85.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
162.213.30.36	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Top	drop	2
139.162.13.205	Singapore	147.237.77.226	www.chamatz.aka.idf.il	block-sp-trafl	forward	2
156.34.46.193	Canada	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
120.59.83.3	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
217.23.9.123	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	2
17.78.149.98	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
209.126.136.2	United States	147.237.76.42	refuah.idf.il	Black List	drop	2
141.143.212.228	Belgium	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.228.19.67	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
209.126.136.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	2
120.132.50.135	China	147.237.76.30	himush.idf.il	block-sp-trafl	forward	2
58.186.25.153	Vietnam	147.237.77.170	maarachot.idf.il	Frk_Under_Attack_Con_Top	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.8.132	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	100
51.254.215.143	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	27
51.254.215.143	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	23
188.165.250.173	France	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
74.208.218.66	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
216.119.125.159	United States	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
92.222.142.219	France	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
173.0.129.149	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
62.210.143.245	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	12
193.28.95.4	Italy	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
121.40.25.174	China	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
204.93.196.218	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
208.52.175.27	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
188.165.18.232	Poland	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	8
208.52.175.27	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
204.93.196.218	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
177.12.161.72	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
121.40.25.174	China	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
23.91.70.119	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.154.73.125	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	6
92.222.142.219	France	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.57	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.117.203.23	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
193.28.95.4	Italy	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
184.168.152.45	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
81.88.48.113	Italy	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.173	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
49.236.200.182	Malaysia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.57	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
208.52.175.27	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
193.28.95.4	Italy	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.45	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.147.60.96	Switzerland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.35	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.75	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.159	United States	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
121.40.25.174	China	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.109.242.34	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
5.196.22.55	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.45	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
213.203.204.143	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.34.186.9	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
188.165.250.173	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.218.66	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.159	United States	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.8.208.130	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.43	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.193.48	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
216.119.125.159	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	72
216.119.125.57	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	54
74.208.218.66	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	54
188.165.250.173	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	26
173.0.129.149	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	26
23.91.70.119	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	24
193.28.95.4	147.237.76.31	Italy	nakchal.idf.il	SQL Injection - Select From	23
121.40.25.174	147.237.77.216	China	dover.idf.il	SQL Injection - Select From	20
92.222.142.219	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	20
208.52.175.27	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
204.93.196.218	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
184.168.152.45	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	20
66.102.9.153	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	19
23.91.70.43	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
177.12.161.72	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
184.168.193.48	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	15
91.109.242.34	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	14
151.80.41.178	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	12
208.52.175.27	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	11
37.8.65.231	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	11
213.203.204.143	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	9
87.117.203.23	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
212.147.60.96	147.237.77.74	Switzerland	law.idf.il	SQL Injection - Select From	8
72.167.131.75	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
50.63.196.35	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	8
195.245.205.76	147.237.77.205	Russian Federation	prisha.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
195.8.208.130	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	8
121.40.25.174	147.237.77.74	China	law.idf.il	SQL Injection - Select From	8
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
50.77.136.81	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
49.236.200.182	147.237.77.74	Malaysia	law.idf.il	SQL Injection - Select From	8
64.34.186.9	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
212.179.223.120	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	8
5.196.22.55	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	8
91.121.222.79	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.245.205.76	147.237.77.61	Russian Federation	e.cogat.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
195.245.205.76	147.237.76.31	Russian Federation	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
84.93.84.77	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	6
81.88.48.113	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	6
216.119.125.173	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
195.245.205.76	147.237.76.39	Russian Federation	mobile.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
187.17.109.54	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
45.79.71.122	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	6
195.245.205.76	147.237.77.121	Russian Federation	e.navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
195.245.205.76	147.237.8.14	Russian Federation	e.orchot.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
195.245.205.76	147.237.72.217	Russian Federation	e.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
195.245.205.76	147.237.72.156	Russian Federation	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
217.132.239.169	147.237.76.31	Israel	nakchal.idf.il	ET SCAN NMAP -sA (2)	5
195.245.205.76	147.237.76.42	Russian Federation	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
195.245.205.76	147.237.76.38	Russian Federation	e.e.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.49.85.55	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1256
69.251.153.35	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	891
79.46.56.34	Italy	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	770
67.236.160.86	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	719
80.246.130.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	711
1.201.102.11	Korea, Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	245
185.34.104.124	Ireland	147.237.76.86	navy.idf.il	SYN Attack		monitor	221
69.158.58.23	Canada	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	216
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	210
80.246.133.124	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	195
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	161
46.19.85.90	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	155
185.34.104.124	Ireland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	94
24.154.151.146	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	92
141.0.13.214	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	78
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	77
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	76
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	75
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	74
167.114.212.195	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	74
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	74
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	73
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	73
167.114.212.195	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	72
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	71
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	71
78.246.51.246	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
167.114.212.195	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	67
109.253.221.15	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
109.253.197.67	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
167.114.212.195	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	65
167.114.212.195	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	65
167.114.212.195	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	64
167.114.212.195	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	63
162.243.113.129	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	62
85.64.39.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
37.75.210.193	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	51
109.65.38.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
185.24.207.100	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	48
176.13.246.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
195.248.234.85	Ukraine	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
141.226.147.179	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
167.114.212.195	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	46
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	46
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	45
62.0.197.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
91.195.162.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44



## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.7.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	286
80.246.139.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	280
2.53.173.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	221
109.253.221.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
109.253.243.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
176.13.19.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
109.253.201.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
5.28.161.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
176.13.243.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
109.67.39.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
2.53.129.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
46.19.86.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
185.32.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
2.53.29.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
37.26.146.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
109.253.147.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
109.253.146.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
109.253.201.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
217.132.105.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
109.253.231.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
176.13.3.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
46.19.86.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.53.160.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.53.146.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
109.253.221.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
37.26.146.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
2.53.156.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
109.253.210.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.224.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.116.127.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
109.253.219.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
2.53.15.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
109.253.157.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
79.180.97.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.242.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
176.13.241.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
212.143.187.162	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	30
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
80.246.137.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.53.62.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.53.186.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
176.13.18.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
109.253.143.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
84.111.152.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26