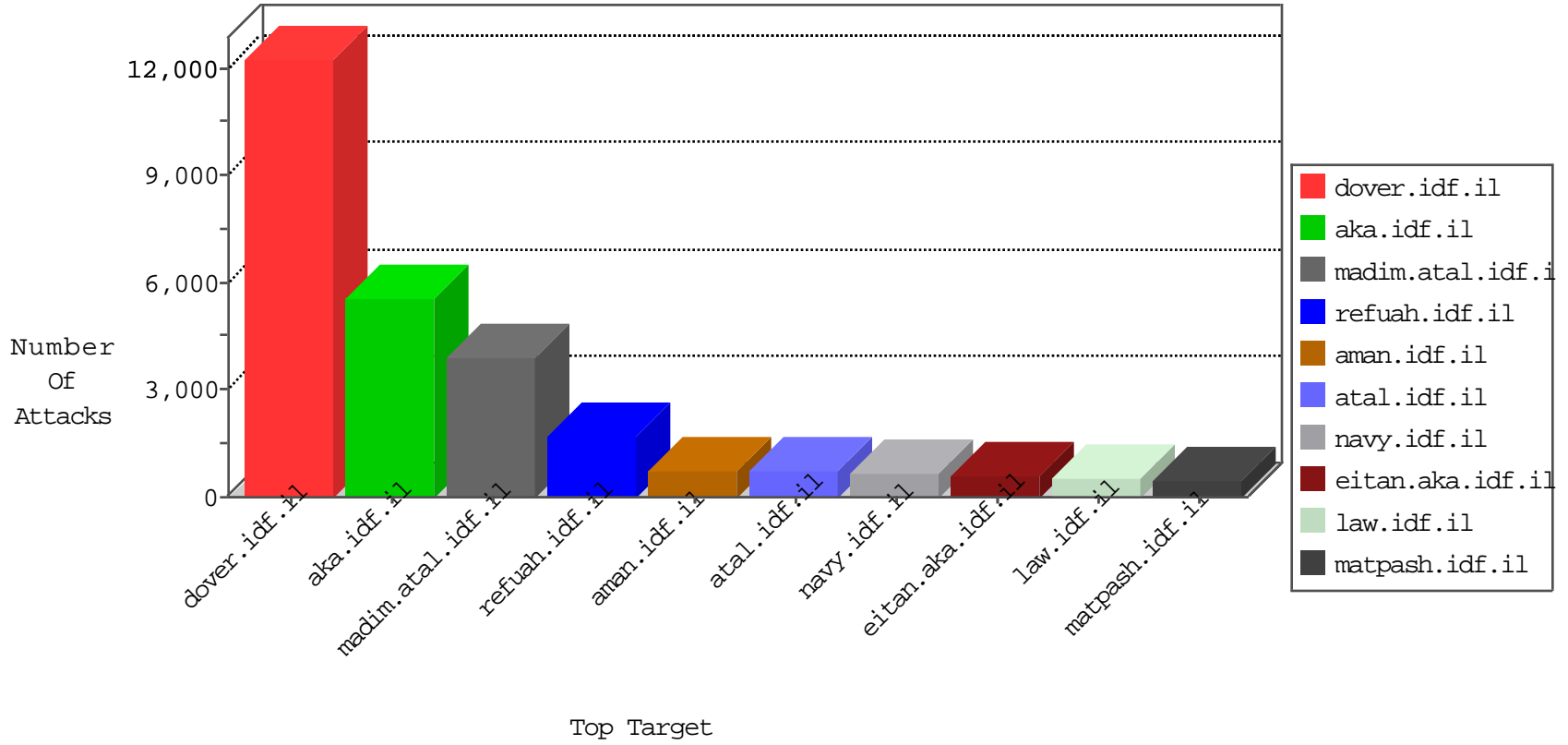


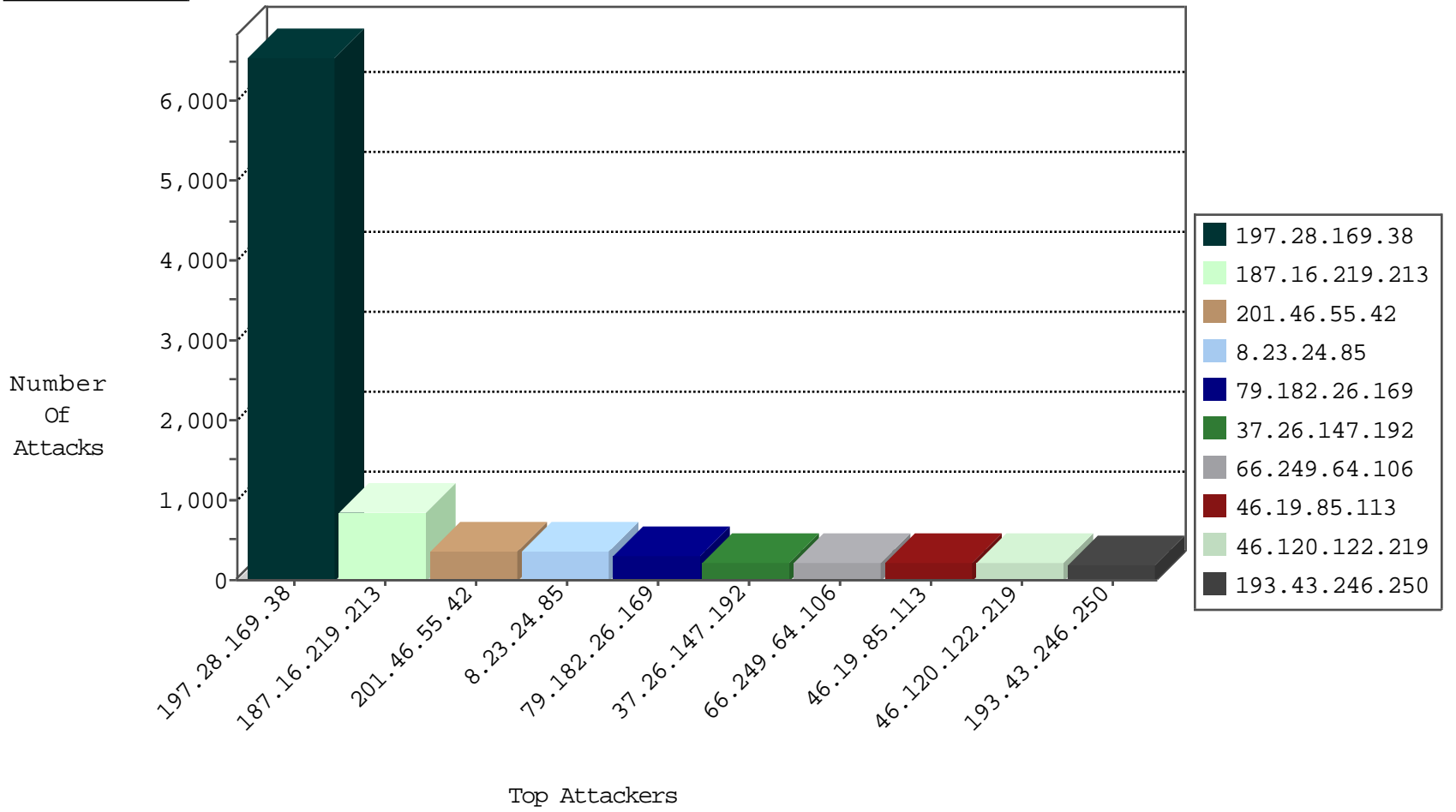
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.191.232.72	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	96
134.191.232.72	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	46
176.13.1.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	31
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	29
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	26
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	25
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	23
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	23
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	23
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	22
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	22
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	22
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	22
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	21
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	20
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	19
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	19
151.100.59.194	Italy	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	18
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	18
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	18
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	17
212.150.127.133	Israel	147.237.77.216	dover.idf.il	ICMP-Frag-Needed-Storm	drop	16
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	15
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	15
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	14
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	14
84.111.118.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
200.55.189.172	Cuba	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	13
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
2.53.55.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	12
88.65.147.114	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
5.102.220.105	Israel	147.237.72.166	aka.idf.il	Black List	drop	11
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	11
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	11
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
86.107.52.39	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
212.25.74.130	Israel	147.237.77.216	dover.idf.il	Black List	drop	9
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	65
51.255.51.250	France	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	53
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	53
50.77.136.81	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
168.1.80.134	Australia	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
77.67.47.7	France	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
92.222.142.219	France	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
177.12.172.43	Brazil	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
51.255.51.250	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	10
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
51.255.51.250	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
91.109.242.34	United Kingdom	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
202.124.109.87	New Zealand	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.42	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.95	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.230.195	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.1.80.134	Australia	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
205.144.171.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.51	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
184.168.27.81	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.242.112.45	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.246.49.11	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.166.190.139	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
77.67.47.7	France	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
205.144.171.34	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
23.91.70.51	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.104.215	United States	147.237.77.74	law.idf.il	C1000016: HTTP: administrator in URI	Permit	6
92.222.142.219	France	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
24.222.4.86	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.12.172.43	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
208.52.175.27	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.75	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
199.79.62.138	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.87.23.55	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
185.21.133.159	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.109.242.34	United Kingdom	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
74.208.218.66	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.1.80.134	Australia	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
67.199.10.25	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
51.255.51.250	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
91.109.242.34	United Kingdom	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
144.76.4.148	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
23.91.70.51	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
51.255.51.250	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	4
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
51.255.51.250	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	4
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.213.138	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
216.119.125.34	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.106	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	212
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	89
62.219.229.118	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	57
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	28
23.91.70.51	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	26
168.1.80.134	147.237.77.176	Australia	matpash.idf.il	SQL Injection - Select From	26
74.208.230.195	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	25
46.19.85.164	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
50.77.136.81	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	22
177.12.172.43	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	20
92.222.142.219	147.237.76.86	France	navy.idf.il	SQL Injection - Select From	20
91.109.242.34	147.237.76.86	United Kingdom	navy.idf.il	SQL Injection - Select From	20
77.67.47.7	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	20
74.208.218.66	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	18
24.222.4.86	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	18
199.79.62.138	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	17
46.120.122.219	147.237.76.31	Israel	nakchal.idf.il	Xenu Link Sleuth User Agent	17
205.144.171.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
67.199.10.25	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
79.182.32.127	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	10
79.182.32.127	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	10
194.114.146.227	147.237.76.42	Israel	refuah.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	10
202.124.109.87	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	8
213.246.49.11	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	8
72.167.131.75	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	8
185.21.133.159	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
23.91.70.95	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
108.166.190.139	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
64.87.23.55	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
23.91.70.42	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
216.119.125.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
87.242.112.45	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	8
184.168.27.81	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	8
208.52.175.27	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
79.177.227.200	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	6
87.70.25.125	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	5
46.120.122.219	147.237.76.42	Israel	refuah.idf.il	Xenu Link Sleuth User Agent	5
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	4
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	4
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	4
84.93.84.77	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	4
79.182.32.127	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	4
45.79.103.178	147.237.72.167	United States	ishurim.aka.idf.i	WEB-MISC Chunked-Encoding transfer attempt	4
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	4
91.224.160.106	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	3
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	3
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	3
58.218.200.137	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	3
31.168.172.136	147.237.72.156	Israel	aman.idf.il	ET SCAN Potential SSH Scan	3

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6182
79.182.26.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	291
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	165
31.154.17.106	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	150
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	129
203.117.143.129	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	107
168.235.197.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
109.253.144.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
109.66.31.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	84
87.69.32.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	83
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		monitor	78
87.69.32.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	71
84.229.33.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	70
107.167.112.193	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	69
84.111.216.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	68
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
168.235.197.242	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	57
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
46.19.86.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
141.0.14.73	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
89.139.29.68	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
79.180.29.8	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
187.16.219.213	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	46
185.120.126.5	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	44
212.179.21.194	Israel	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	44
187.16.219.213	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	43
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	43
187.16.219.213	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
187.16.219.213	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
85.130.242.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
85.130.242.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	42
187.16.219.213	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	41
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	41
187.16.219.213	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	40
84.108.224.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
187.16.219.213	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	40
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
187.16.219.213	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	40
187.16.219.213	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	40
187.16.219.213	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	40
197.28.169.38	Tunisia	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	40
193.43.246.250	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	39
187.16.219.213	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	39
77.124.61.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	210
37.26.147.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	207
176.13.228.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
77.139.42.238	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
77.125.89.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
79.177.53.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
77.139.74.12	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.53.190.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
109.253.201.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
141.226.218.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.197.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
2.53.56.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
2.55.182.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
2.53.161.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.53.166.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	60
46.19.85.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	48
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
109.253.143.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
176.13.227.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
31.168.8.110	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	41
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
80.246.136.106	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	40
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	39
37.26.146.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.53.159.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.53.162.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	35
95.35.144.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
31.168.8.110	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 31.168.8.110	Block	34
121.204.154.166	China	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 121.204.154.166	Block	34
109.253.156.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
80.246.136.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.249.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
109.253.210.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
109.253.140.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.55.138.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	29
79.177.233.232	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	27
79.177.233.232	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 79.177.233.232	Block	26