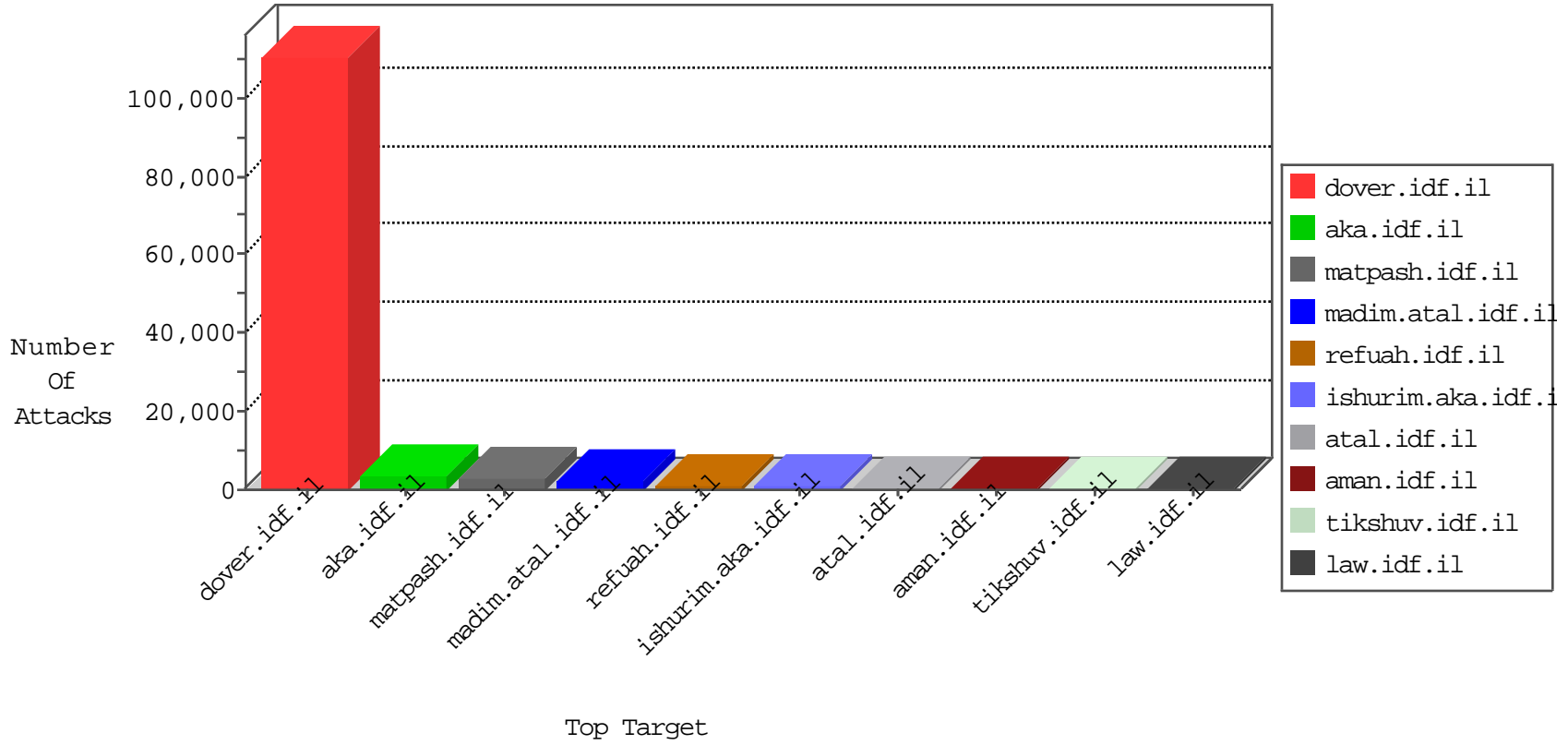


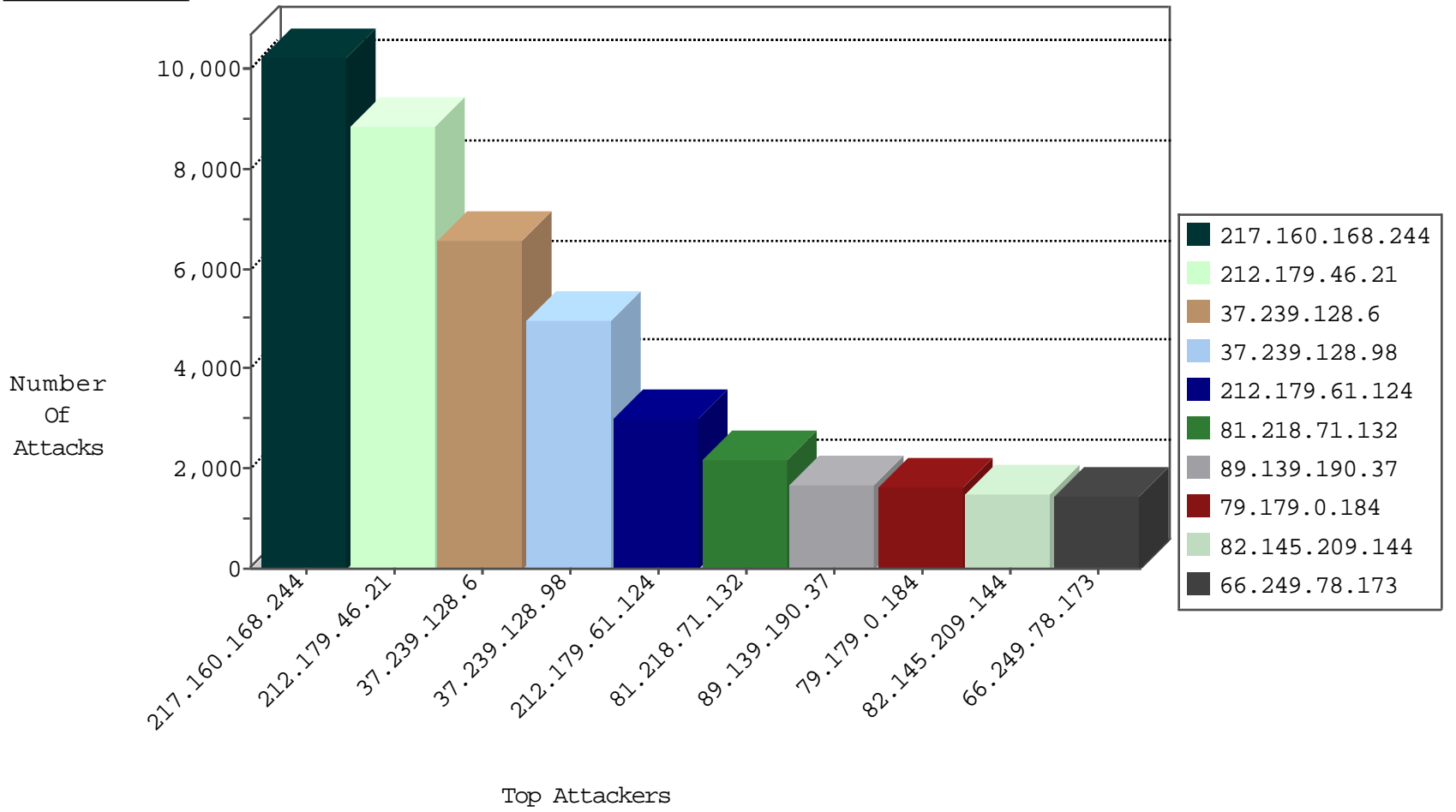
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
173.63.105.226	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6332
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5178
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3652
220.181.108.141	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2803
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1208
220.181.108.165	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	912
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	881
85.65.13.195	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	859
84.108.22.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	717
212.117.154.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	692
77.125.242.134	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	640
109.64.52.223	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	630
213.151.46.38	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	480
79.183.190.180	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	444
94.159.223.230	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	432
109.67.130.207	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	364
46.117.130.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	360
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	340
5.102.254.205	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	332
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	326
62.128.48.122	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	304
220.181.108.111	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	301
66.249.64.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	286
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	273
79.181.194.30	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
93.173.4.50	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	224
46.121.244.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
84.229.188.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	209
79.181.55.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
84.111.65.42	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
220.181.108.117	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	189
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	185
62.219.135.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	184
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	178
79.176.153.121	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	163
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
220.181.108.139	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	142
37.142.163.125	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
199.203.172.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
66.249.64.60	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	113
109.64.254.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
37.239.128.6	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	110
109.65.52.11	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
80.178.136.122	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
77.125.118.217	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
109.253.139.99	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
46.19.86.213	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
82.145.209.144	Europe	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	1481
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	215
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	137
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	125
81.218.251.250	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	96
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	87
138.134.192.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	36
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
89.139.190.37	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	17
89.139.182.255	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
109.66.202.179	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
46.19.85.148	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
93.120.27.62	Romania	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	5
77.125.89.174	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
178.175.128.50	Moldova, Republic of	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
80.246.138.2	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.181.21.180	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
81.136.203.19	United Kingdom	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
81.218.41.58	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	4
108.168.11.245	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
94.230.86.188	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	181
88.241.39.236	Turkey	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
89.139.182.255	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	5
43.255.188.131	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	4
95.110.228.68	Italy	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	4
89.139.190.37	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	4
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
43.255.188.131	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	3
105.109.195.89	Algeria	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	3
77.126.2.9	Israel	147.237.77.216	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	3
43.255.188.130	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	3
93.168.21.58	Romania	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
105.109.195.89	Algeria	147.237.77.216	dover.idf.il	SQL Injection - Select From	3
43.255.188.130	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	3
105.109.195.89	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	2
46.120.3.135	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
105.109.195.89	Algeria	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
66.249.67.206	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
85.65.195.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.133	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
109.66.102.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.131	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
37.8.124.7	Palestinian Territory, Occupied	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
105.109.195.89	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	2
61.240.144.65	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
105.109.195.89	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	2
46.19.86.68	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.131	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
109.65.52.11	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
93.173.133.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.133	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
31.210.177.198	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.130	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
5.231.205.182	Germany	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 4096	2
122.226.207.245	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.154	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
217.160.168.244	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10060
212.179.46.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8795
37.239.128.6	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6521
37.239.128.98	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4915
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2917
81.218.71.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2178
89.139.190.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1612
79.179.0.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1611
2.54.49.53	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1436
212.179.61.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1394
94.188.132.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1392
95.86.121.47	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1383
212.199.244.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1139
81.218.71.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	917
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	846
89.139.182.255	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	823
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	807
2.54.137.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	695
77.127.108.217	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	607
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	573
46.19.86.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	557
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	550
81.218.13.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	516
46.19.85.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	513
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	487
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	411
37.237.172.177	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	403
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	395
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	376
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	376
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	374
94.159.154.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	360
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	340
148.177.129.213	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	335
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	312
212.76.97.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	310
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	308
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	289
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	287
212.25.102.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	287
148.81.192.3	Poland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	284
50.118.172.124	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	283
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	278
213.151.35.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	261
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i		drop	drop	257
164.2.255.244	France	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	252
197.29.13.115	Tunisia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	250
212.179.46.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	248
84.94.32.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	246
109.64.157.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	244

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.99.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	545
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	510
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	507
37.26.147.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.214	Block	460
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	380
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.84	Block	250
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.127	Block	233
2.54.45.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	170
109.253.128.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	143
2.54.139.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.139.211	Block	138
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	134
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	133
46.19.85.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	76
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	68
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	67
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	66
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	63
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	63
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	57
46.19.86.125	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.125	Block	37
37.60.45.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	31
213.151.48.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	21
62.90.174.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	18
172.56.23.83	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	17
66.249.67.94	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.94	Block	17
84.173.122.7	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	14
183.60.244.44	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.60.244.44	Block	14
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	13
46.116.119.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
2.54.50.207	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.50.207	Block	12
84.94.194.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	12
164.138.126.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
37.26.146.213	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.146.213	Block	11
84.228.33.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
66.249.67.120	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.120	Block	11
176.12.146.55	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	10
95.86.110.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
109.64.100.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
79.176.38.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
178.125.243.74	Belarus	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	9
93.173.136.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
149.78.38.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	8
95.86.75.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
109.253.139.148	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
46.229.164.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	7
149.154.157.61	Italy	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 149.154.157.61	Block	7
66.249.67.107	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.107	Block	7
46.19.85.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7