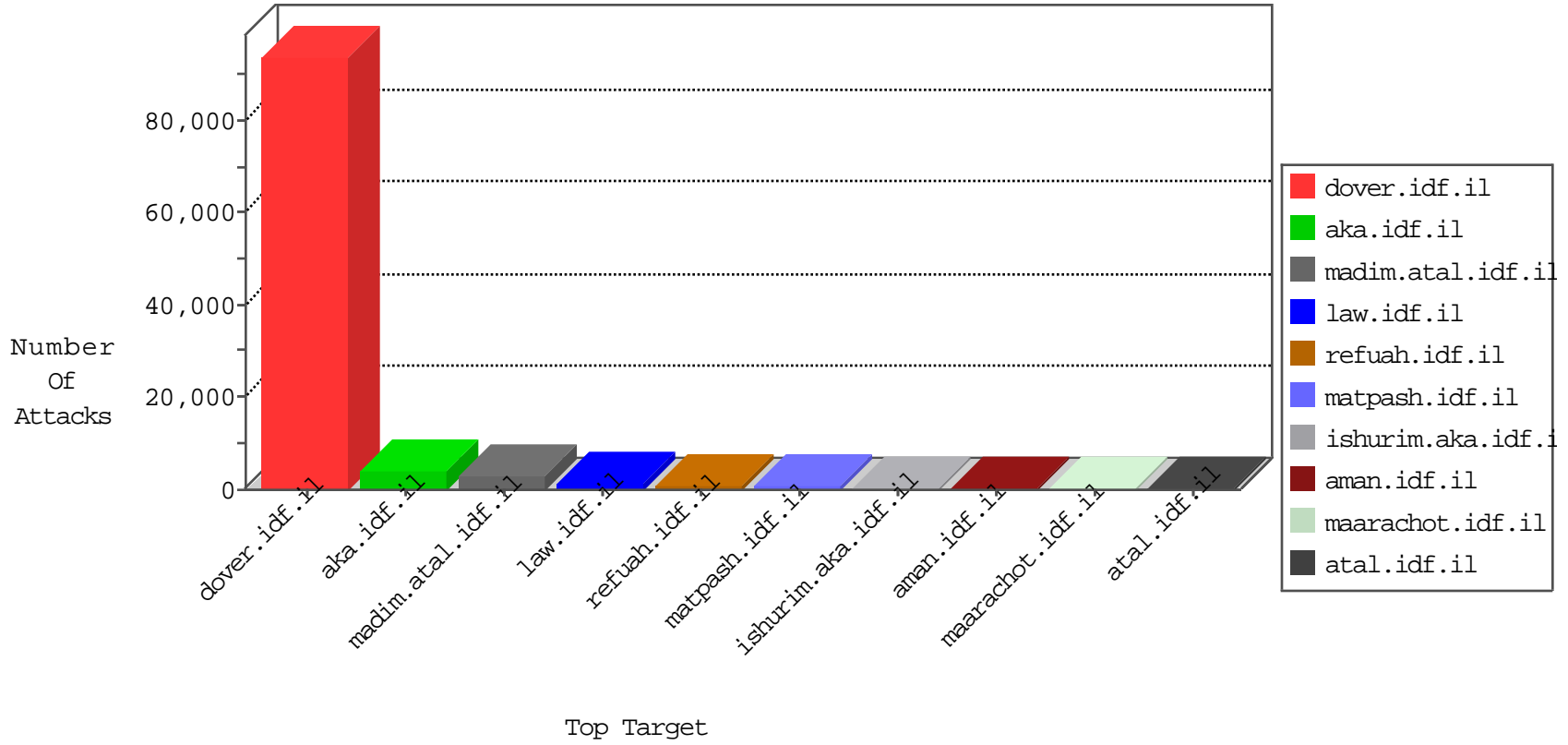


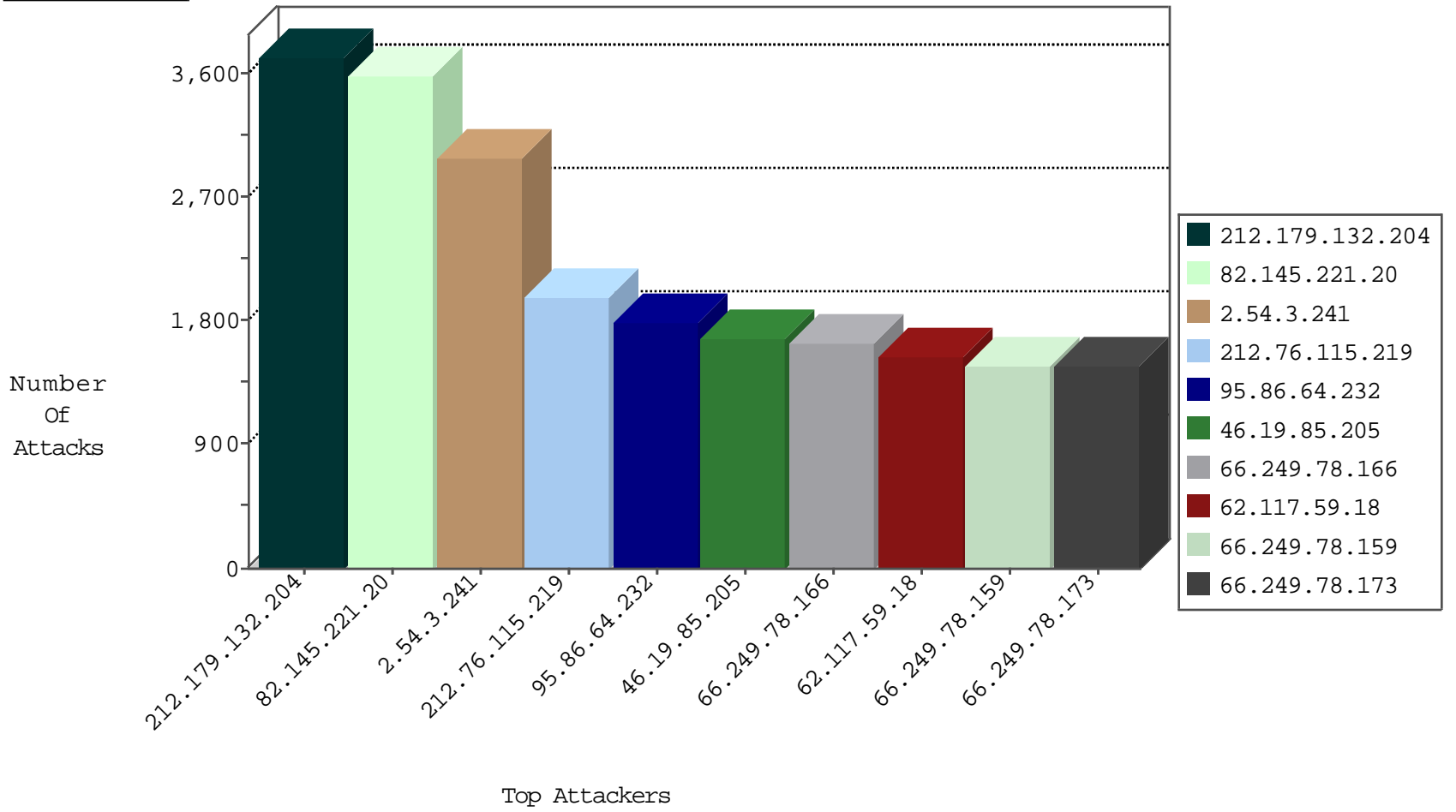
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	10978
212.179.212.227	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7317
66.249.65.41	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3868
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3710
176.12.150.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3077
66.249.65.39	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2966
79.183.151.104	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2877
212.179.61.127	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2638
77.126.61.39	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2628
66.249.79.13	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2534
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1455
66.249.79.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1368
220.181.108.161	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1132
66.249.73.217	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	963
79.179.116.165	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	911
79.176.144.5	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	689
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	581
66.249.73.209	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	561
85.250.145.114	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	537
176.228.16.128	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	467
84.211.16.251	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	413
220.181.108.158	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	399
81.218.83.34	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	389
220.181.108.113	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	373
220.181.108.166	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	368
84.108.66.66	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	342
85.250.222.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	321
46.116.179.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	315
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	301
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	278
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	255
85.250.40.141	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	232
84.228.138.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
66.249.79.157	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	214
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	198
213.57.42.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	197
95.86.98.161	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	160
220.181.108.84	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	159
181.167.106.66	Argentina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	148
2.54.134.180	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	133
91.231.192.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	122
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	111
46.117.18.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
81.218.48.37	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	108
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	107
85.65.60.200	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	105
149.78.230.210	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
2.54.153.11	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	96

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	465
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	456
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	172
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	130
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	82
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	45
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
207.176.85.13	United Kingdom	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	18
46.116.220.62	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
82.80.17.163	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
212.34.12.188	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
212.235.27.227	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
91.152.210.60	Finland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	11
194.90.134.253	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
74.71.49.139	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
83.45.156.37	Spain	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.177.181.120	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	6
84.228.231.150	Bulgaria	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.64.29.212	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	6
84.229.135.9	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
119.6.144.74	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
2.54.136.39	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.64.10.215	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.65.202.147	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.81	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.39	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
46.117.30.132	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
79.178.61.126	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.201	e.atal.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
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
81.218.48.37	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	4
103.224.250.23	Hong Kong	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	206
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	86
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	72
87.68.149.194	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	9
85.250.243.27	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	9
66.249.65.181	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	8
85.250.20.150	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	6
91.178.60.161	Belgium	147.237.76.34	yochalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
91.178.60.161	Belgium	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
91.178.60.161	Belgium	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
91.178.60.161	Belgium	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
66.249.81.184	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
91.178.60.161	Belgium	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
91.178.60.161	Belgium	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
66.249.65.173	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.41	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.1	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
91.178.60.161	Belgium	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
91.178.60.161	Belgium	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
91.178.60.161	Belgium	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
122.228.207.76	China	147.237.76.34	yochalan.idf.il	ET SCAN Potential SSH Scan	3
91.178.60.161	Belgium	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	3
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
122.228.207.77	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
84.94.16.109	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.178.60.161	Belgium	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
82.205.117.219	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.76	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
212.29.224.69	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.23	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.13	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
212.179.61.124	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.78.148	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
164.138.120.74	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.94.76.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.76	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
109.253.137.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.132.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3729
82.145.221.20	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3580
2.54.3.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2897
212.76.115.219	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1978
95.86.64.232	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1786
46.19.85.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1670
62.117.59.18	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1541
212.179.21.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1396
46.116.220.62	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1234
212.179.61.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1118
95.86.118.155	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1103
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	978
212.199.11.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	966
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	882
95.86.125.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	867
46.19.86.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	861
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	823
81.218.251.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	779
86.221.97.115	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	659
212.179.61.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	651
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	571
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	520
213.151.60.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	516
87.69.207.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	513
172.56.27.181	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	495
193.43.246.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	464
193.43.245.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	438
82.145.209.179	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	414
164.138.113.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	408
216.126.116.149	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	396
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	378
82.145.216.110	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	359
213.204.127.33	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	357
66.99.28.98	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	341
87.68.46.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	334
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	330
157.55.39.146	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	324
207.46.13.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	320
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	319
24.146.253.233	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	319
212.76.115.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	313
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	311
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	310
212.179.61.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	309
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	309
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	292
82.145.217.184	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	277
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	274
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	271
212.76.118.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	268

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
94.159.218.53	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 94.159.218.53	Block	671
46.19.86.83	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.83	Block	293
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	179
176.12.151.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	154
176.12.137.28	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.137.28	Block	144
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	140
176.12.143.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	133
185.32.177.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	125
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	120
185.32.177.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	94
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.84	Block	77
2.52.136.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	71
2.54.145.183	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.145.183	Block	68
83.130.101.117	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 83.130.101.117	Block	61
176.12.144.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	57
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	51
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	45
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	45
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
185.32.177.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
176.12.142.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	37
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	35
176.12.151.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
185.32.177.115	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.177.115	Block	32
77.125.132.32	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	32
79.183.180.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	29
85.64.29.212	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.29.212	Block	28
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	27
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	26
80.246.136.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
125.65.46.140	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.46.140	Block	21
84.108.94.127	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	19
89.139.168.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	19
46.19.85.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	19
46.19.86.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	18
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	13
95.86.119.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	13
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
46.120.137.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
81.218.155.22	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.155.22	Block	12
109.253.136.169	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.136.169	Block	10
157.55.39.206	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
2.54.174.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
207.46.13.133	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
212.143.99.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	10
109.253.149.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	10
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	9