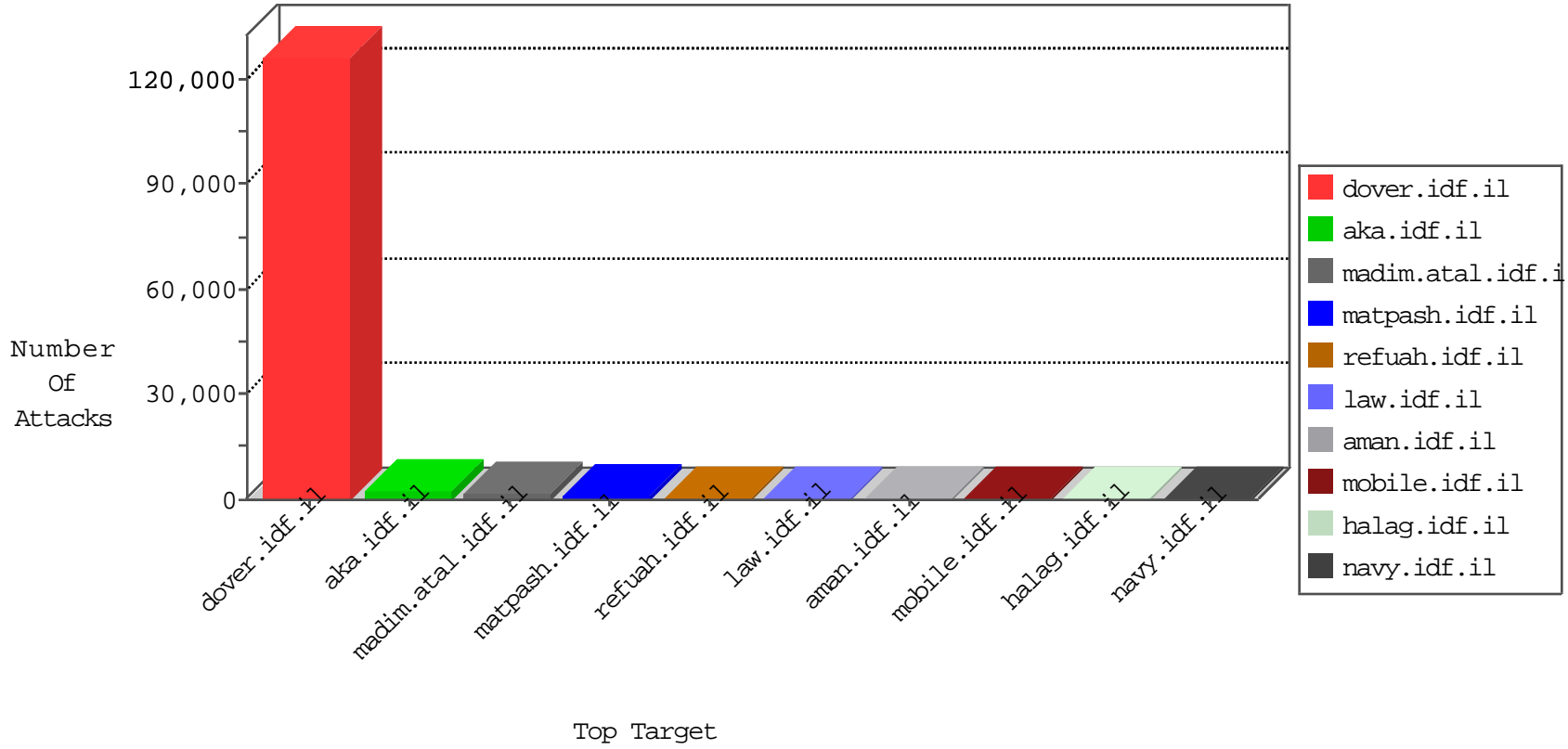


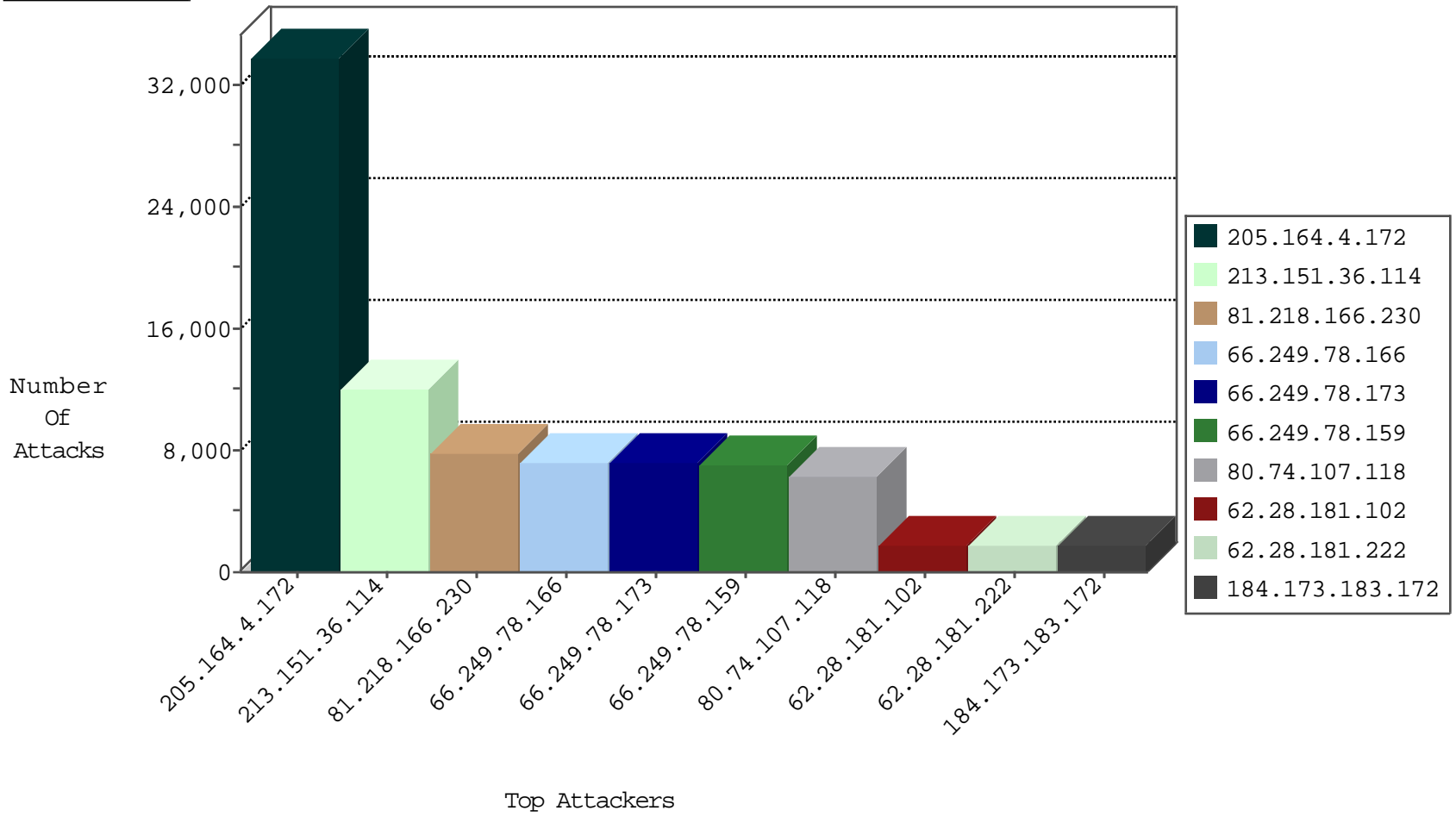
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	13859
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8856
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5324
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4720
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1673
220.181.108.81	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1225
220.181.108.76	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1092
220.181.108.79	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	771
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	689
79.176.20.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	611
220.181.108.101	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	606
149.78.81.63	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	480
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	466
46.121.120.180	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	409
220.181.108.75	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	251
79.177.171.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
77.125.135.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	226
46.121.110.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	203
79.182.150.42	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
109.186.181.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
220.181.108.123	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	174
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	170
79.180.37.136	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	167
205.164.4.172	United States	147.237.77.216	dover.idf.il	DOS-HOIC-TCP-80-gbo	forward	164
84.109.14.123	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	160
85.64.224.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
89.138.242.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
5.28.190.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
79.182.118.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	148
85.64.103.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
220.181.108.171	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	141
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
80.178.15.156	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
46.120.80.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
205.164.4.172	United States	147.237.77.216	dover.idf.il	DOS-WEB-HOIC-HTTP-80-snc	dest-reset	112
149.88.104.174	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
109.253.131.104	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
80.246.141.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	101
37.142.138.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	89
149.88.83.251	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
79.177.170.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
5.29.159.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
87.69.86.98	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	79
109.253.128.240	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	75
109.65.31.152	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
84.228.92.135	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
84.228.18.151	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
46.121.110.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	56

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	788
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	255
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	214
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	193
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	186
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	142
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	140
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	128
199.168.141.77	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	28
173.208.209.74	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	25
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
23.251.55.233	United States	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
5.50.204.72	France	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	10
89.138.30.159	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
109.64.32.66	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
213.8.129.138	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.116.102.21	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.116.202.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
98.31.12.102	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	6
94.230.86.174	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
94.222.208.98	Germany	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.8	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
93.172.40.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	4
193.37.128.117	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.42	refuah.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
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	3
5.102.254.207	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3

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	140
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	138
205.164.4.172	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	81
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	48
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	34
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP adminlogin access	30
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	22
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	14
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	14
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
205.164.4.172	United States	147.237.77.216	dover.idf.il	ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA	6
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
37.8.16.19	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
46.121.81.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	5
66.249.75.113	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	4
187.101.132.36	Brazil	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	4
134.191.232.68	Israel	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sA (2)	4
43.255.191.161	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	4
187.101.132.36	Brazil	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	4
66.249.75.44	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
187.101.132.36	Brazil	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	4
134.191.232.70	Israel	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sA (2)	4
43.255.191.161	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	3
43.255.191.161	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	3
43.255.191.161	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	3
43.255.191.161	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.66	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	3
43.255.191.161	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
80.230.66.252	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.75.60	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
80.178.9.232	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
222.168.65.122	China	147.237.0.17	m.my-kosher-kravi.idf.il	GPL SCAN nmap TCP	2
79.181.100.28	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.79.22	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
37.142.98.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
91.224.132.118	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
79.178.196.54	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.130.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.63.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
128.199.165.82	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
46.121.116.201	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
205.164.4.172	United States	147.237.77.216	dover.idf.i	SAM rule	drop	drop	33014
213.151.36.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12080
81.218.166.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7764
80.74.107.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6263
62.28.181.102	Portugal	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1807
62.28.181.222	Portugal	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1798
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1317
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1287
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1271
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1266
79.176.102.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1221
46.19.85.33	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1182
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1172
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1125
85.250.240.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1050
84.108.46.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	906
46.19.85.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	832
89.187.221.1	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	713
31.154.12.98	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	712
84.229.173.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	708
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	637
37.60.47.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	570
205.164.4.172	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	544
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	505
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	498
2.54.141.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	494
46.19.85.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	477
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	469
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	456
212.116.173.226	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	355
46.19.86.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	335
46.19.85.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	293
37.142.228.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	279
2.52.129.55	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	276
120.20.79.36	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	273
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	268
94.159.143.243	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	232
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	222
37.191.143.151	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	210
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	206
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	196
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	195
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	188
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	186
5.29.128.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	181
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	181
195.66.128.86	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	179
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	175
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	167
197.134.255.203	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	167

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3005
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2437
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2293
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	932
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	931
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	837
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	809
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	780
2.54.41.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	491
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	429
109.253.156.113	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.156.113	Block	280
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	279
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	252
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	237
2.54.0.8	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.0.8	Block	192
37.26.147.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	191
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.167	Block	188
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.8.57.95	Block	180
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	153
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	100
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	90
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	87
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	79
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	78
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 37.8.57.95	Block	71
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	70
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_imgtop.asp	Block	68
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	66
37.8.57.95	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	64
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	62
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/view_img.asp	Block	60
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	60
185.32.179.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
109.253.134.75	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.134.75	Block	53
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	52
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	51
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	PHP Attempt	Block	47
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	43
80.246.140.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
46.121.138.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	24
188.121.41.145	Netherlands	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 188.121.41.145	Block	23
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/print_text.asp	Block	19
5.102.215.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	19
95.86.75.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	19
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/print_text.asp	Block	17
157.55.39.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.138	Block	14
157.55.39.47	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.47	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12