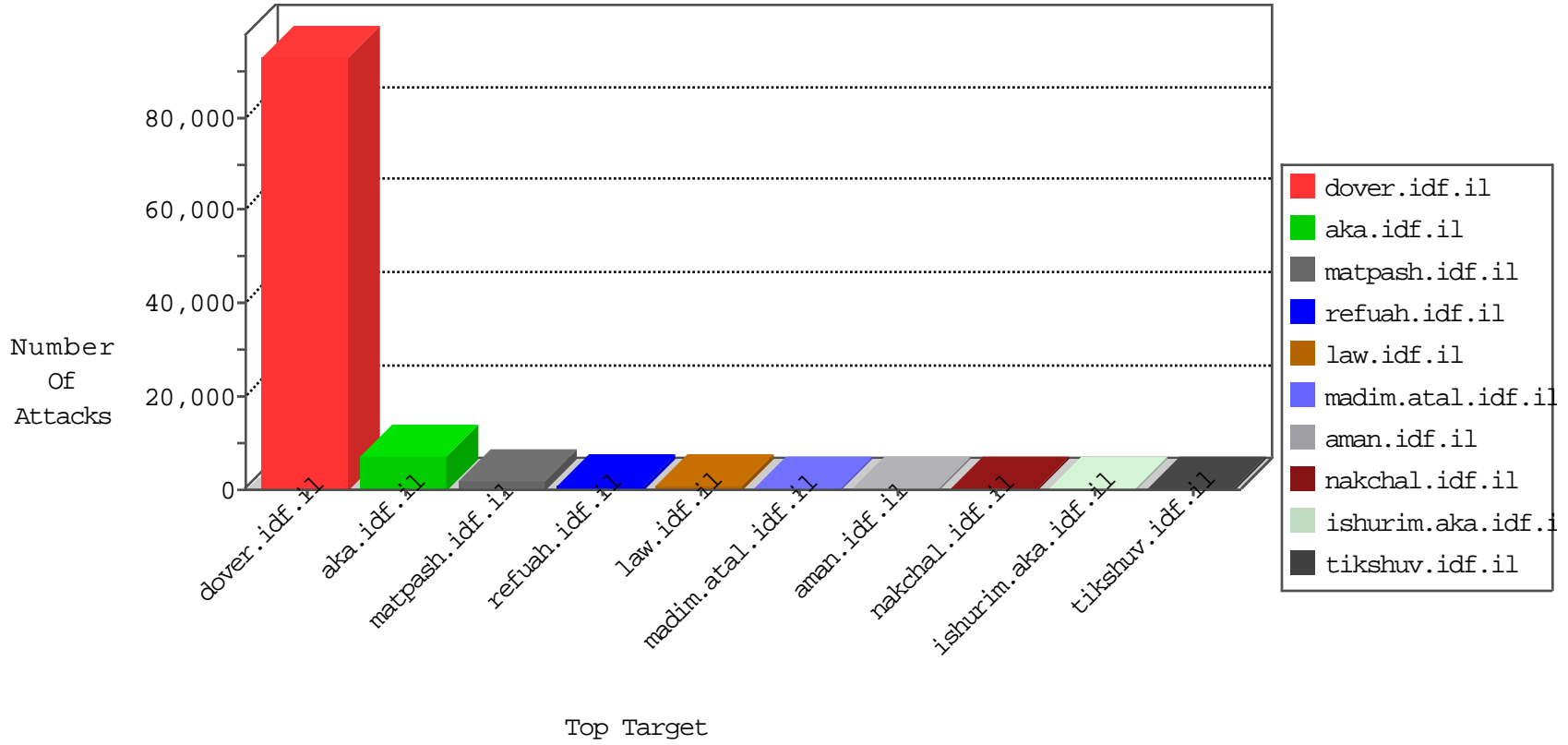


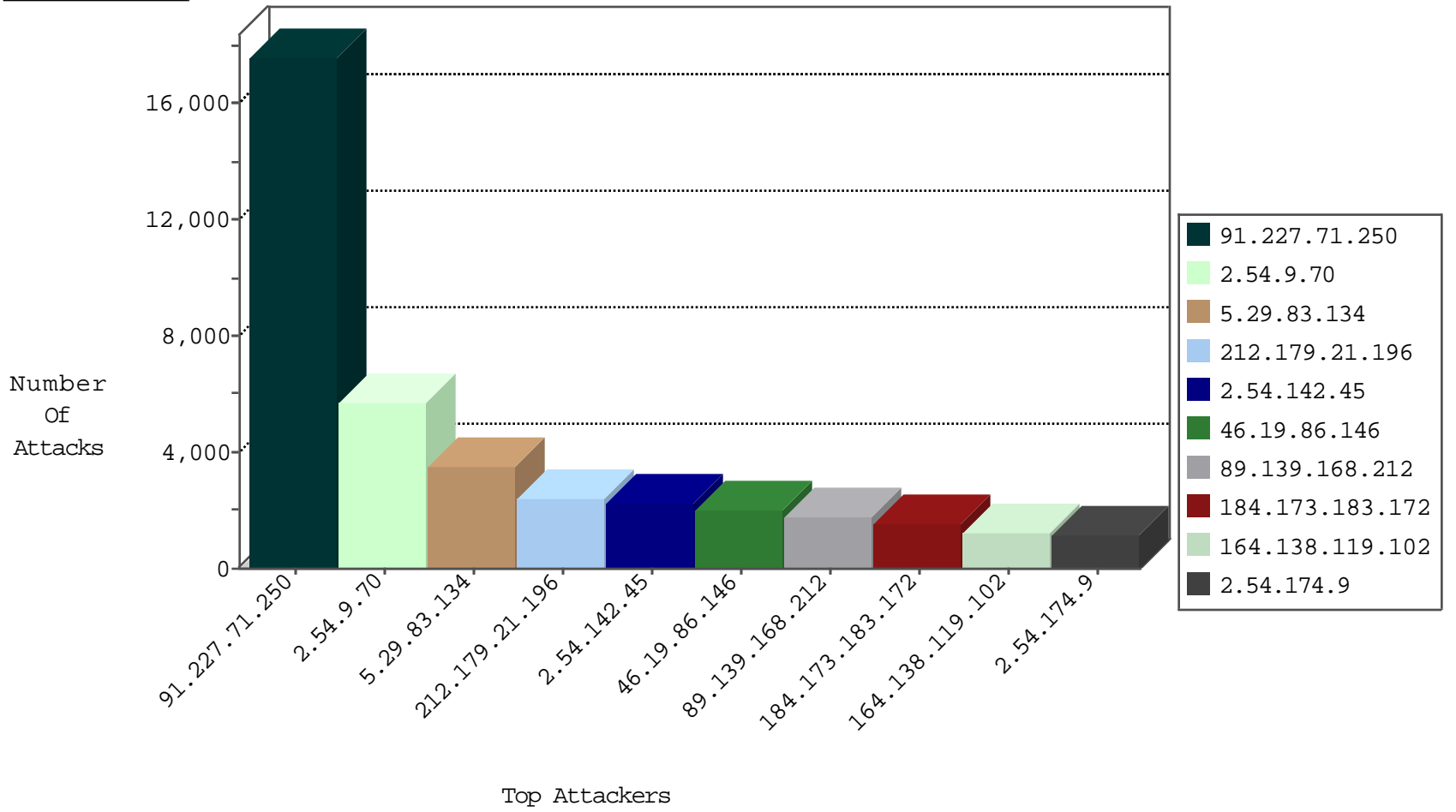
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	608229
37.26.148.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	133882
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36949
45.48.96.151		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19729
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16920
66.249.64.24	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6229
66.249.64.34	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4638
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	3371
66.249.78.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2949
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1884
82.196.42.196	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1366
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1053
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1041
220.181.108.161	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1011
66.249.93.239	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	970
220.181.108.185	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	810
213.57.111.235	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	747
79.176.12.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	556
212.179.21.196	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	490
109.64.15.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	476
81.218.44.13	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	400
213.57.183.157	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	358
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	328
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	296
213.57.34.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	247
46.116.177.115	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	246
84.228.144.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	237
109.67.19.4	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
220.181.108.158	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	216
188.120.142.244	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	203
220.181.108.123	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	191
77.125.73.189	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
84.110.60.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
46.120.158.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
220.181.108.107	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	167
220.181.108.180	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	156
109.253.158.101	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
2.54.41.129	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
94.159.151.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
79.182.124.94	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
5.29.63.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
109.65.173.11	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
82.166.117.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
5.29.244.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
220.181.108.143	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	120
5.102.217.192	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
37.142.105.141	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
212.179.21.195	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
46.121.42.168	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
176.12.136.184	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
62.118.222.184	Russian Federation	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	782
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	711
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	281
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	278
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	265
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	170
81.218.251.252	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	26
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
71.6.135.131	United States	147.237.76.177	noore.idf.il	DVRep_B-N_60_100	Block	8
89.139.190.37	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	7
84.108.17.104	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	6
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	6
46.19.85.119	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	6
84.111.6.228	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	6
212.179.162.246	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	6
192.114.91.214	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
31.210.187.235	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
188.120.148.255	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	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
82.80.26.64	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.117.41.190	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.93	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.136	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	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.249	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	4
212.179.21.197	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	4

Top Attackers In IDF

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	78
212.25.102.57	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	22
66.249.64.235	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	10
80.246.137.51	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
66.249.65.51	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.64.34	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5
66.249.64.16	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5
5.29.83.134	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	4
66.249.67.45	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	3
212.179.21.195	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
157.55.39.204	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
212.154.192.124	Kazakistan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	3
109.253.159.17	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	SQL Injection - Select From	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	SERVER-IIS cmd.exe access	3
41.46.53.28	Egypt	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	3
79.179.27.82	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
172.56.18.86	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
66.249.65.26	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
109.67.151.131	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.130.20	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.130	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
221.235.189.245	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
107.6.155.99	Netherlands	147.237.77.216	dover.idf.il	ET WEB_SERVER suhosin.simulation PHP config option in uri	2
212.179.42.226	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.8.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.3	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
107.6.155.99	Netherlands	147.237.77.216	dover.idf.il	ET WEB_SERVER open_basedir PHP config option in uri	2
43.255.188.130	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
93.173.153.200	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.3	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
107.6.155.99	Netherlands	147.237.77.216	dover.idf.il	ET WEB_SERVER auto_prepend_file PHP config option in uri	2
89.139.190.37	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
5.29.234.153	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.213.151	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.130	Japan	147.237.76.198	e.yochanan.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.245	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
31.168.132.131	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
91.227.71.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17555
2.54.9.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5684
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2338
2.54.142.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2274
46.19.86.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2018
89.139.168.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1785
164.138.119.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1182
2.54.174.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1149
82.166.183.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1069
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	838
151.151.16.13	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	820
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	753
70.39.185.164	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	685
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	658
212.76.110.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	657
193.16.147.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	651
89.139.190.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	634
107.6.155.99	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	604
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	575
79.179.0.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	520
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	512
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	492
92.250.139.217	Luxembourg	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	469
212.179.21.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	468
15.203.233.78	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	434
89.208.171.34	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	422
2.54.150.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	419
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	400
41.87.199.2	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	358
195.34.150.18	Austria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	357
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	355
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	346
109.65.52.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	341
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	332
70.39.186.189	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	316
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	316
77.126.54.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	311
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	297
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	297
212.179.46.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	290
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	281
149.88.205.189	United States	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	280
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	272
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	268
82.145.219.39	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	268
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	258
2.54.22.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	243
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	227
132.3.49.81	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	206
66.249.81.215	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	204

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.29.83.134	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.83.134	Block	3403
46.19.86.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.210	Block	238
79.178.120.144	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.120.144	Block	209
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	113
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	19
79.181.121.193	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.121.193	Block	18
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	16
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	14
109.65.98.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	13
185.32.177.12	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.177.12	Block	13
84.228.40.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
212.179.46.20	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	11
80.179.115.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.179.115.198	Block	11
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	10
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	10
46.229.164.114	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.114	Block	10
95.86.100.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
79.179.165.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
83.130.109.92	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 83.130.109.92	Block	9
37.26.148.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
109.253.139.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	7
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.106	Block	7
2.52.30.141	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	7
84.108.204.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	6
91.227.164.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
89.139.188.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
94.153.10.249	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	6
89.138.235.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	5
109.253.146.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	5
62.90.235.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	5
104.250.147.218		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.250.147.218	Block	5
212.143.99.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	5
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	5
46.19.85.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	5
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	5
185.23.60.4	United Kingdom	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
2.54.28.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
198.236.117.1	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 198.236.117.1	Block	4
81.218.50.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4
66.249.64.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
79.177.184.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
176.12.139.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4
66.249.64.60	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/m/main/giyus/general.aspx	Block	4
81.218.208.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
185.32.176.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.65.178.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	4
46.229.164.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	4
109.66.29.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4
46.229.164.113	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.113	Block	4
81.218.251.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	4