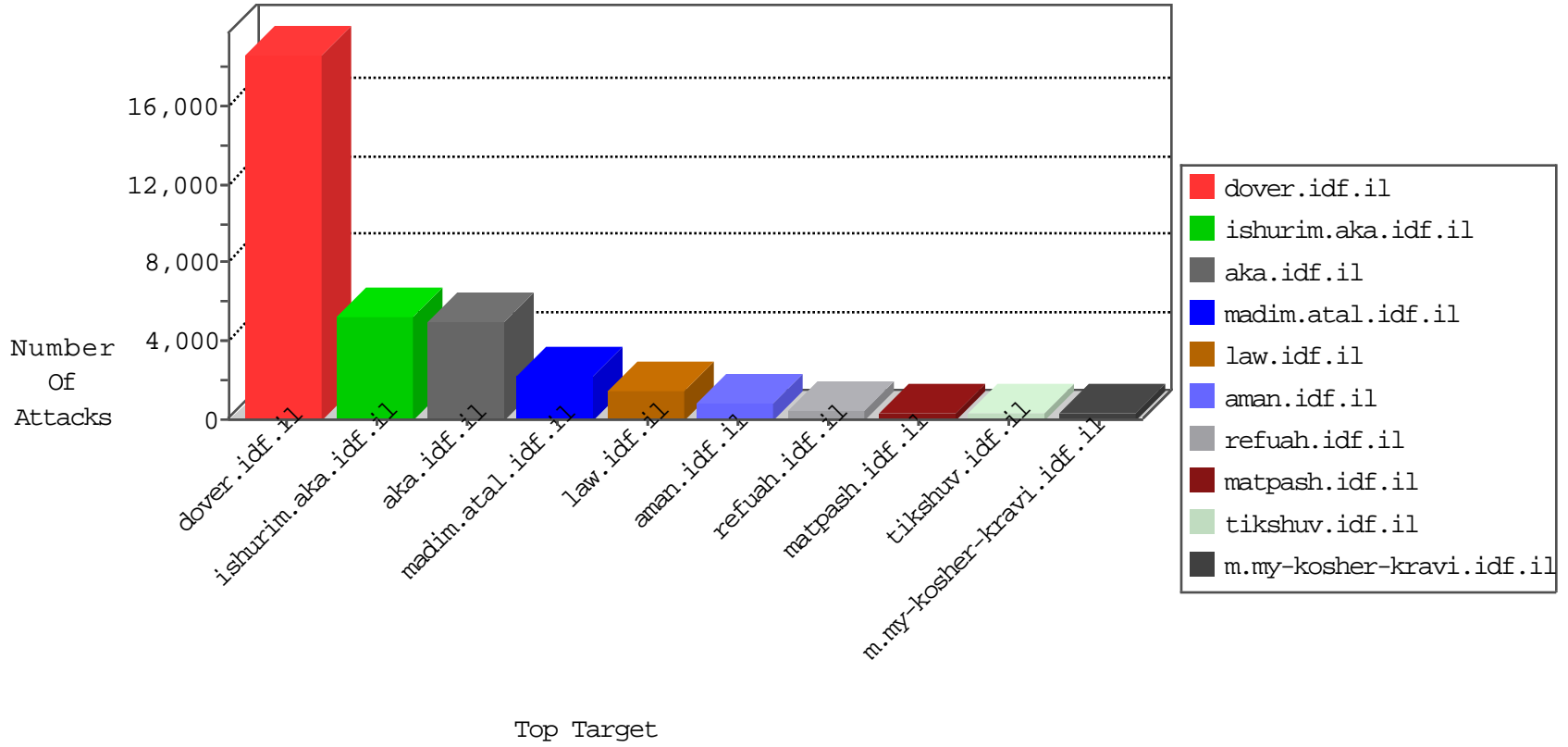


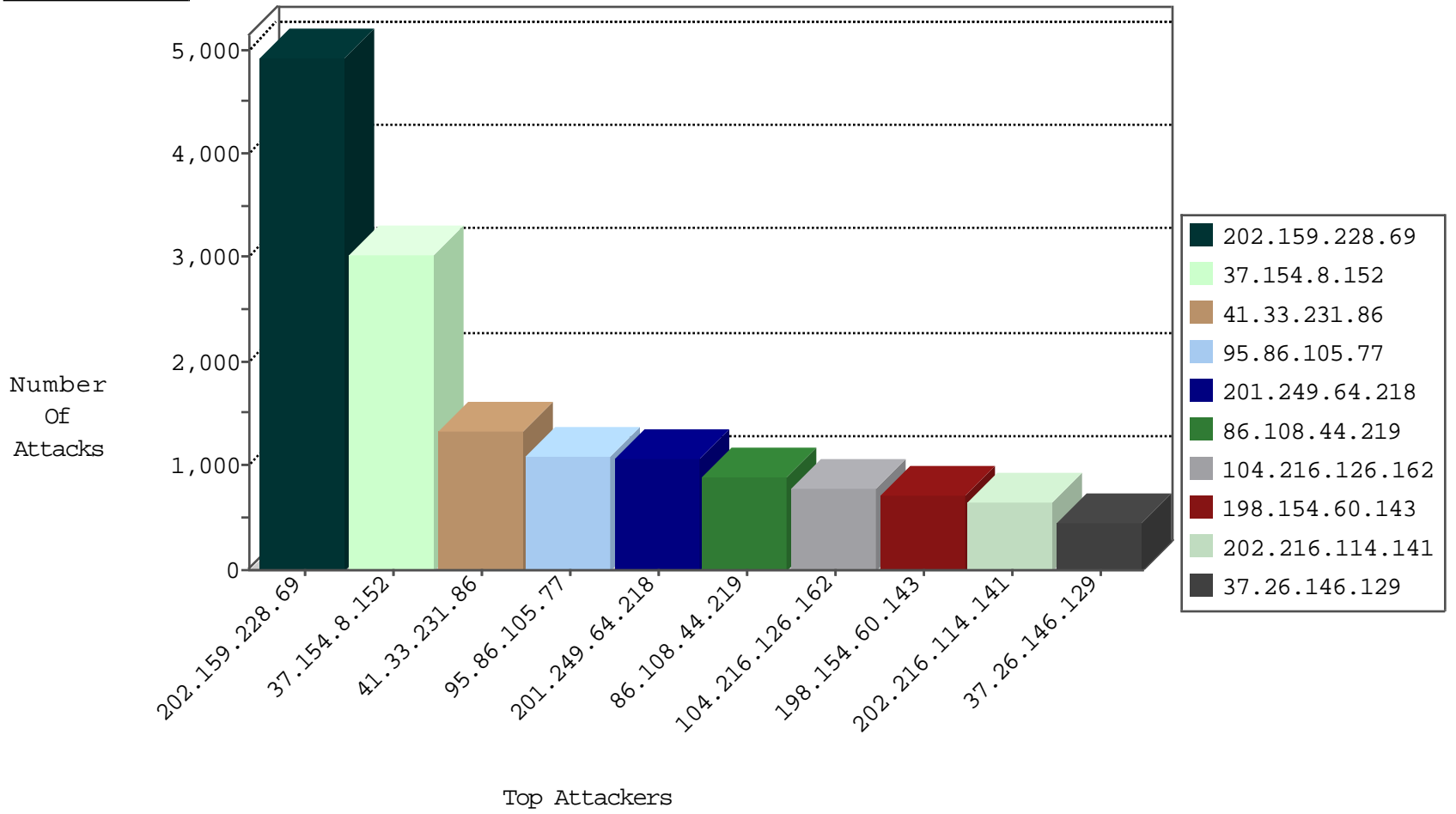
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
86.108.44.219	Jordan	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	4345
84.109.241.218	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1259
86.143.235.65	United Kingdom	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1231
109.67.187.185	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	712
86.143.235.65	United Kingdom	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Tcp	drop	597
5.29.66.232	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	forward	566
82.80.20.98	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	556
84.110.60.83	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	526
201.236.98.35	Chile	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	495
87.69.98.32	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	480
192.116.232.69	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	469
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	455
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	398
85.65.202.216	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	391
201.236.98.35	Chile	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	386
202.216.114.141	Japan	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	376
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	365
213.57.114.184	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	347
202.216.114.141	Japan	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	326
77.153.96.59	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	321
79.176.185.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	303
77.153.96.59	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	271
95.86.121.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	271
202.159.228.69	India	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	270
79.178.11.28	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	245
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	245
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
202.159.228.69	India	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	219
46.117.231.248	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	185
84.109.56.133	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	179
176.12.138.243	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
94.159.210.231	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	173
79.177.4.253	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
2.54.56.125	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
109.253.136.38	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	155
202.159.228.69	India	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Tcp	drop	152
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	145
149.88.120.18	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	141
85.65.86.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
193.46.64.93	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
202.159.228.69	India	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	119
87.69.85.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
79.181.177.239	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	118
109.186.164.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
82.102.141.222	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
2.54.130.246	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	113
85.64.57.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
46.19.85.38	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	105

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
218.77.79.43	China	147.237.76.197	e.himush.idf.il	Block_Level_70_100	Block	9
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	9
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	Block_Level_70_100	Block	9
218.77.79.43	China	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	9
218.77.79.43	China	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	9
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.i	Block_Level_70_100	Block	9
218.77.79.43	China	147.237.76.31	nakchal.idf.il	Block_Level_70_100	Block	8
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	Block_Level_70_100	Block	8
218.77.79.43	China	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	8
218.77.79.43	China	147.237.76.201	e.atal.idf.il	Block_Level_70_100	Block	8
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	Block_Level_70_100	Block	8
193.106.206.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	Block_Level_70_100	Block	8
93.173.26.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	Block_Level_70_100	Block	7
218.77.79.43	China	147.237.76.148	ggcenter.aka.idf.il	Block_Level_70_100	Block	6
208.92.211.22	United States	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
212.179.132.201	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
46.19.85.140	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
218.77.79.43	China	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	6
66.240.236.119	United States	147.237.0.33	idf.il	Block_Level_70_100	Block	5
46.19.85.80	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.76.34	yohalan.idf.il	Block_Level_70_100	Block	5
66.240.192.138	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.77.121	e.navy.idf.il	Block_Level_70_100	Block	5
149.88.116.220	United States	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
80.246.138.6	Israel	147.237.77.243	mobile.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.76.30	himush.idf.il	Block_Level_70_100	Block	4
66.240.236.119	United States	147.237.76.38	e.e.meitav.idf.il	Block_Level_70_100	Block	4
198.20.69.98	United States	147.237.77.216	dover.idf.il	Block_Level_70_100	Block	4
66.240.236.119	United States	147.237.77.121	e.navy.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	Block_Level_70_100	Block	4
188.161.16.36	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.95.255.154	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	4
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	Block_Level_70_100	Block	4
132.70.58.90	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
80.246.139.116	Israel	147.237.77.243	mobile.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
218.77.79.43	China	147.237.8.24	e.lifestyle.idf.il	Block_Level_70_100	Block	4
79.180.59.97	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	Block_Level_70_100	Block	4
66.240.236.119	United States	147.237.77.179	e.mazi.idf.il	Block_Level_70_100	Block	3
218.77.79.43	China	147.237.8.27	e.madim.atal.idf.il	Block_Level_70_100	Block	3
71.6.135.131	United States	147.237.0.35	akaws.idf.il	Block_Level_70_100	Block	3
66.240.236.119	United States	147.237.8.50	e.tikshuv.idf.il	Block_Level_70_100	Block	3
198.20.69.98	United States	147.237.72.156	aman.idf.il	Block_Level_70_100	Block	3
106.138.57.83	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.64.176	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	156
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	131
202.159.228.69	India	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	104
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	96
109.64.127.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	14
185.32.179.15	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
66.249.93.153	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	8
192.115.67.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
79.178.170.226	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	5
107.167.110.60	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	5
222.186.15.202	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	3
66.249.78.158	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
86.143.235.65	United Kingdom	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
77.126.219.120	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
222.186.15.202	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
84.111.82.82	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.139.26.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.60.85	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.64.102.163	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.228.28.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.93.176	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
193.46.64.93	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.209.129	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
149.78.128.196	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.74.101.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
201.236.98.35	Chile	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
37.26.148.185	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.65	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	2
87.69.29.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
222.186.15.202	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
77.153.96.59	France	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	2
84.229.227.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.5.130	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.147.56.190	Switzerland	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.137.55.5	Thailand	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
121.42.54.18	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
1.93.34.219	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
104.152.188.198		147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
70.209.138.35	United States	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
175.143.219.209	Malaysia	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
37.142.143.179	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.147.92	Israel	147.237.72.156	aman.idf.il	INDICATOR-SCAN mysan	1
117.21.191.228	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.188.125.13	Poland	147.237.76.147	chiruch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
216.229.0.202	United States	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
202.159.228.69	India	147.237.77.216	dover.idf.il		drop	drop	2403
202.159.228.69	India	147.237.77.216	dover.idf.il	SAM rule	drop	drop	2297
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1321
37.154.8.152	Turkey	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		908
37.154.8.152	Turkey	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	908
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il		drop	drop	907
202.216.114.141	Japan	147.237.77.216	dover.idf.il		drop	drop	614
104.216.126.162		147.237.77.216	dover.idf.il	SAM rule	drop	drop	509
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	445
201.236.98.35	Chile	147.237.77.216	dover.idf.il		drop	drop	277
177.85.60.202	Brazil	147.237.77.216	dover.idf.il		drop	drop	271
213.8.96.180	Israel	147.237.77.216	dover.idf.il		drop	drop	210
198.154.60.143	United States	147.237.0.19	madim.atal.idf.il	SAM rule	drop	drop	199
198.154.60.143	United States	147.237.0.15	kosher-kravi.idf.il	SAM rule	drop	drop	196
198.154.60.143	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SAM rule	drop	drop	192
104.216.126.162		147.237.77.216	dover.idf.il		drop	drop	136
77.153.96.59	France	147.237.77.216	dover.idf.il		drop	drop	131
79.176.182.249	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	94
137.95.1.11	United States	147.237.77.176	matpash.idf.il		drop	drop	92
81.218.44.254	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	76
79.177.115.217	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	73
8.37.227.253	Anonymous Proxy	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	73
77.153.96.59	France	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	71
130.226.222.202	Denmark	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	64
81.218.183.91	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	62
82.80.134.206	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	54
37.145.54.5	Russian Federation	147.237.77.233	atal.idf.il	Invalid sequence number	Bad TCP sequence	monitor	50
82.80.134.206	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
82.102.141.218	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence		46
82.102.141.218	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	46
82.102.141.218	Israel	147.237.0.34	tikshuv.idf.il	Invalid sequence number	Bad TCP sequence	monitor	46
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	SAM rule	drop	drop	37
31.177.39.101	Iraq	147.237.77.216	dover.idf.il		drop	drop	36
207.241.226.204	United States	147.237.77.74	law.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	36
37.26.147.222	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
81.218.208.114	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	35
46.19.86.19	Israel	147.237.72.167	ishurim.aka.idf.il		drop	drop	34
46.19.85.121	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
37.145.54.5	Russian Federation	147.237.77.233	atal.idf.il		drop	drop	34
37.26.146.171	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
79.176.81.78	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	32
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
62.219.224.172	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	32
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		32
192.115.248.2	Israel	147.237.72.156	anan.idf.il	Invalid sequence number	Bad TCP sequence	monitor	30
41.232.179.83	Egypt	147.237.77.216	dover.idf.il		drop	drop	30
80.246.133.62	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	29
84.229.10.95	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
41.43.128.184	Egypt	147.237.77.216	dover.idf.il		drop	drop	29
41.203.64.132	Nigeria	147.237.77.216	dover.idf.il		drop	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.154.8.152	Turkey	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning	Block	1205
95.86.105.77	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/contactform/undefined	Block	1101
37.26.146.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	451
2.54.36.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	274
79.178.11.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	261
89.139.37.166	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.37.166	Block	207
176.12.143.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	193
109.253.157.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
176.12.149.254	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.149.254	Block	169
207.241.226.204	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	157
37.236.8.241	Iraq	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	113
95.86.72.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	108
147.235.8.61	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 147.235.8.61	Block	63
162.248.48.39	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
79.176.9.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	56
84.94.180.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.94.180.210	Block	49
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
198.154.60.143	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 198.154.60.143	Block	38
198.154.60.143	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Unauthorized URL Access from 198.154.60.143	Block	38
198.154.60.143	United States	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 198.154.60.143	Block	38
164.138.126.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	37
213.57.30.15	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.57.30.15	Block	33
78.47.254.216	Germany	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 78.47.254.216	Block	33
77.125.0.158	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 77.125.0.158	Block	32
78.47.254.216	Germany	147.237.77.216	dover.idf.il	Multiple NULL Character in Method from 78.47.254.216	Block	31
46.19.86.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	31
95.86.72.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	30
46.19.85.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	25
46.117.121.52	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	24
213.57.133.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	23
212.25.83.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	23
164.138.127.106	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	23
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	22
31.168.133.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	21
82.166.53.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	19
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	18
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	18
80.246.130.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	18
80.246.133.132	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	18
80.179.222.238	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.179.222.238	Block	17
62.219.248.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	17
91.135.102.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	17
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	16
149.78.207.78	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	16
46.19.86.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	15
104.216.126.162		147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	15
192.115.64.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	15
37.26.148.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	15
109.253.157.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
46.234.206.190	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/home/home.asp	Block	14