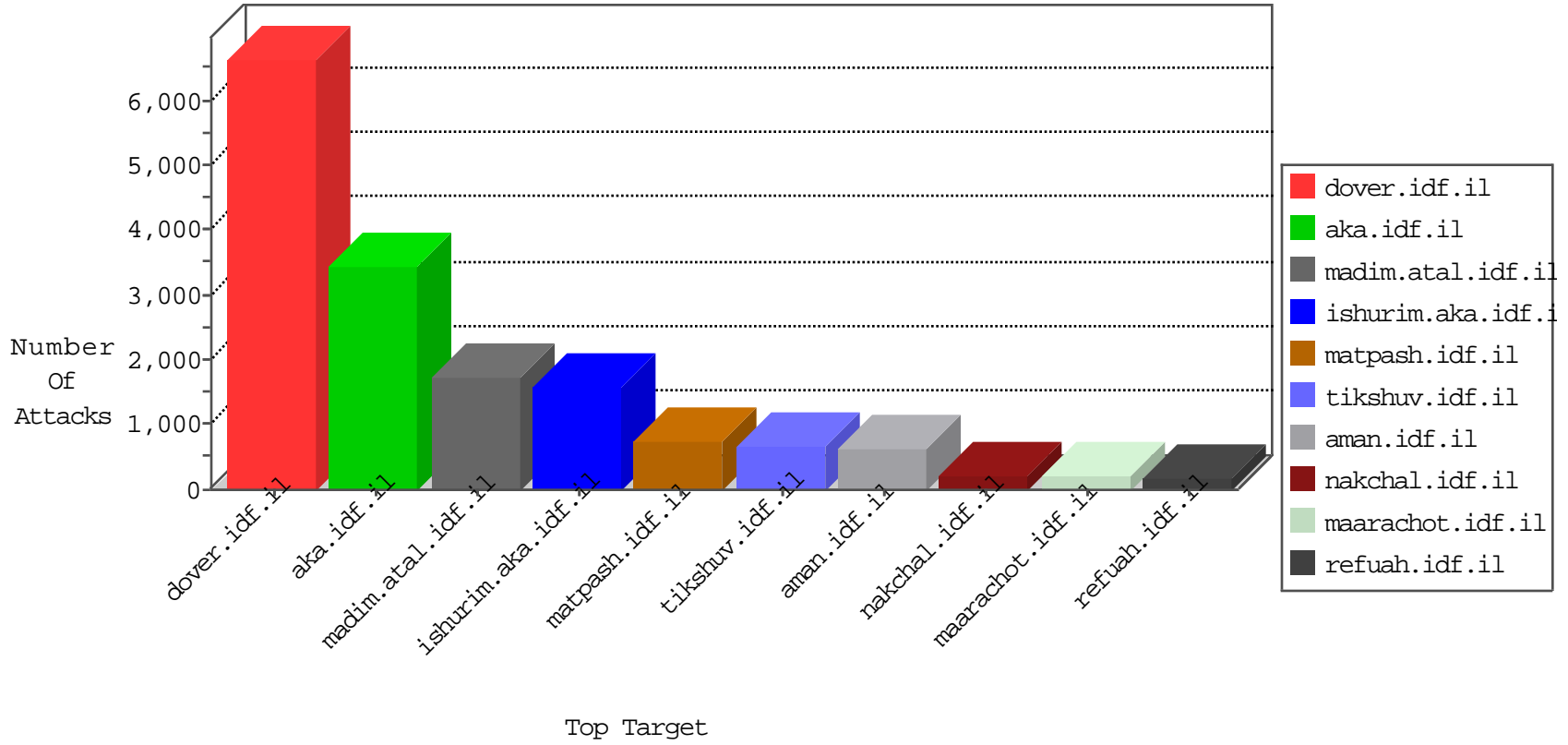


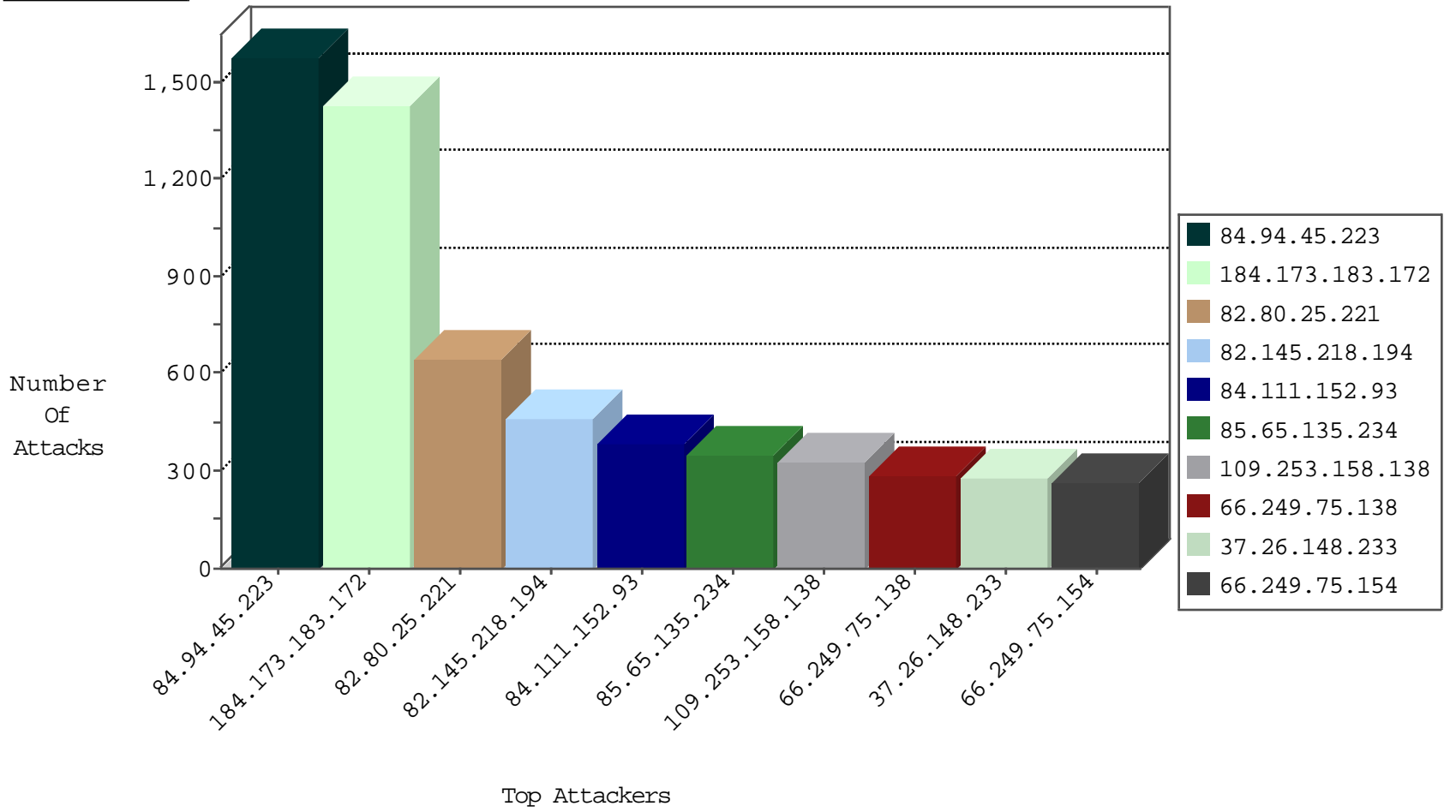
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.197	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3602
109.66.49.134	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	788
85.250.183.158	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	626
84.110.216.6	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	582
46.120.146.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	445
84.110.86.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	347
109.64.42.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	280
46.19.85.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	274
79.179.35.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	266
62.219.239.242	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	235
109.186.145.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	234
82.166.93.237	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	223
84.111.155.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
46.120.216.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
89.139.49.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
87.69.221.36	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
79.181.61.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
84.110.216.6	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	134
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	130
84.94.24.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
79.177.157.100	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
84.108.15.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
2.54.15.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
79.179.10.145	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
213.57.253.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
79.177.167.230	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
46.117.86.128	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
46.19.86.147	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	89
109.186.160.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
132.74.151.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
46.19.86.147	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
213.57.182.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
2.54.191.253	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
46.116.77.124	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
2.54.156.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
89.139.5.128	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
192.116.92.56	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	72
79.180.146.234	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
5.102.254.94	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
46.19.86.9	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	61
80.246.136.236	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	42
80.74.123.12	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	36
91.143.238.9	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	28
92.61.233.3	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	28
80.74.97.79	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	28
185.32.178.103	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	22
192.116.92.56	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	18
2.54.191.253	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	13
79.177.178.67	Israel	147.237.72.156	aman.idf.il	I4 Source or Dest Port Zero	drop	9

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.94.45.223	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1577
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	783
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	482
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	165
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	151
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	38
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	34
46.116.251.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	17
212.34.12.177	Jordan	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
188.241.155.30	Romania	147.237.77.216	dover.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
188.241.155.30	Romania	147.237.77.216	dover.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	10
212.34.12.138	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
212.34.12.177	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
77.126.33.170	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
154.72.166.245	Cameroon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
69.197.186.210	United States	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	8
212.143.3.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.181.227.177	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
130.211.168.76		147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	6
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	6
84.228.153.194	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
188.138.9.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	5
89.144.198.193	Austria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.177	ncore.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
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	4
2.54.27.77	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	3
146.185.56.214	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.70.114	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	3

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	515
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	143
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
209.88.157.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
85.64.94.191	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
79.177.195.104	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
109.186.173.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
182.50.130.48	Singapore	147.237.72.166	aka.idf.il	ETPRO WEB_SERVER PHP Possible Open Flash Direct Access to File Upload Directory	2
122.228.207.199	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
79.176.126.25	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.249.179	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.147	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
84.228.147.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
46.19.86.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.134.250	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.199	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
84.108.127.8	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.199	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
62.128.35.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.140.197	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.158	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
58.20.54.249	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.193	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	2
93.158.215.206	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
80.82.64.116	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
188.226.226.40	Netherlands	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.199	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.193	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
115.231.218.147	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.82.57	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
79.177.111.194	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.33.95	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.199	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
128.61.240.66	United States	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
46.121.74.52	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
182.50.130.48	Singapore	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.67	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
79.176.129.8	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.199	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
84.229.196.87	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
182.50.130.48	Singapore	147.237.72.166	aka.idf.il	ETPRO WEB_SERVER PHP Open Flash Charts File Upload Attempt	2
122.228.207.193	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
46.117.180.202	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.67.48.93	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
82.145.218.194	Europe	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	462
66.249.75.138	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	258
66.249.75.154	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	240
126.193.71.28	Japan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	234
66.249.75.122	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	206
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	152
46.19.85.4	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	140
85.64.121.79	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	136
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	124
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	116
46.19.85.228	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	98
107.199.206.71	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	86
186.17.165.203	Paraguay	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	74
46.19.85.175	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	61
201.92.184.242	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
109.253.145.72	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
176.12.142.214	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
31.186.228.58	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	39
31.186.228.89	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	38
176.12.136.100	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.139.182	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
95.220.97.167	Russian Federation	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	34
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.139.200	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.147.67	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
31.186.228.65	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	30
109.66.37.56	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	29
176.12.151.148	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
31.186.228.32	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	28
201.233.154.207	Colombia	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
109.253.137.38	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
31.186.228.93	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	28
202.66.60.166	Hong Kong	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
31.186.228.63	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	27
46.19.86.147	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	27
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
41.237.94.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
31.186.228.27	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	25
176.12.142.16	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.133.176	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.137.239	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.131.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.228.88	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
62.207.60.228	Netherlands	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	24
217.132.218.123	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.136.167	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.129.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.157.202	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
199.30.25.115	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.111.152.93	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.111.152.93	Block	382
85.65.135.234	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.65.135.234	Block	352
109.253.158.138	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.158.138	Block	324
37.26.148.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	275
46.19.85.146	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.146	Block	97
109.253.141.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	91
185.32.176.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	56
17.142.148.12	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.148.12	Block	53
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	49
109.253.146.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
17.142.152.70	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.70	Block	35
46.120.166.28	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.166.28	Block	33
66.249.75.122	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.122	Block	26
66.249.75.154	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.154	Block	21
17.142.148.12	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	19
66.249.75.138	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.138	Block	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	17
37.59.29.19	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	17
109.253.141.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	17
149.78.153.50	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	16
109.253.131.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	15
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
187.17.106.135	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1589- en/dover.aspx	Block	14
109.253.143.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
185.32.176.104	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.176.104	Block	11
109.186.173.9	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/resource/userfollowresource/create/	Block	11
17.142.152.70	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
84.228.149.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
84.228.152.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
109.253.130.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
2.54.16.0	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	8
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	8
213.57.146.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
87.69.219.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	8
79.179.143.170	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.179.143.170	Block	7
37.140.188.30	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.140.188.30	Block	7
80.179.96.90	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 80.179.96.90	Block	7
46.19.86.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7
46.117.27.213	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 46.117.27.213	Block	7
162.246.18.116		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
77.125.147.201	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
94.23.30.222	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
207.46.13.121	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.121	Block	6
85.250.16.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
109.253.142.224	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	6
95.86.120.254	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.120.254	Block	6
194.50.102.2	Netherlands	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.50.102.2	Block	6
176.12.138.122	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	5