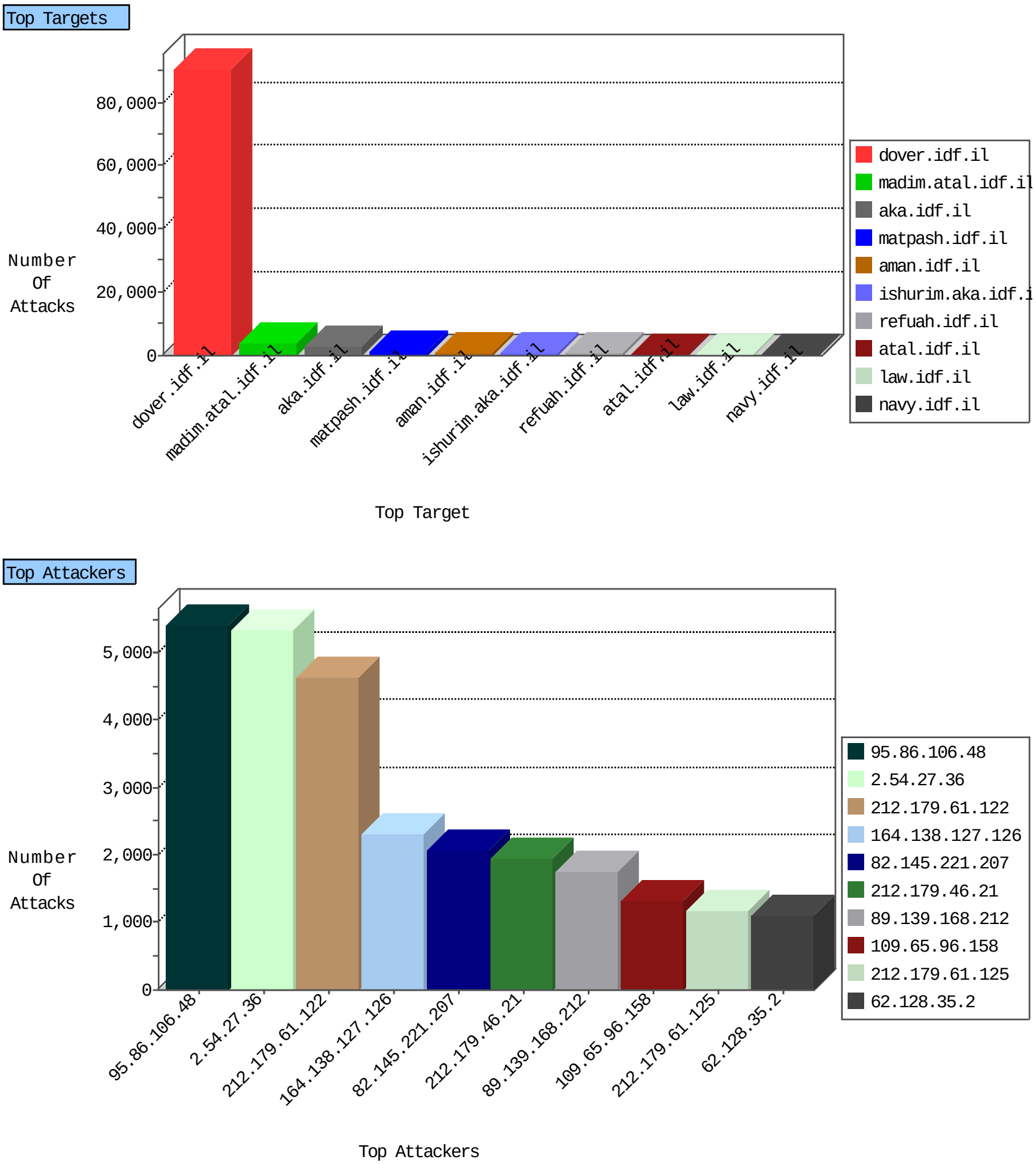
06-04-2015-00:00:09 to 06-05-2015-00:00:09

IDF Under Attack Daily Report



06-04-2015-00:00:09 to 06-05-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.83.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6239
45.96.88.11		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2781
89.139.168.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2661
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	577
77.127.215.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	553
220.181.108.160	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	509
109.186.173.206	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	504
79.179.68.186	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	458
79.182.119.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	452
80.179.78.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	448
5.28.189.243	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	445
87.69.2.174	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	412
79.176.38.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	399
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	363
46.121.248.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	356
213.57.97.73	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	290
37.142.80.183	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	285
84.108.149.41	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	241
5.29.96.95	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	222
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	199
213.8.71.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
87.68.147.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	190
132.64.24.106	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	185
84.108.35.55	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	184
213.57.153.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
212.235.8.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
5.29.223.249	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	177
220.181.108.84	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	173
77.127.147.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
37.142.82.190	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
220.181.108.178	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	170
80.12.63.111	France	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	168
80.179.141.237	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	167
220.181.108.119	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	165
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
85.65.17.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
213.57.139.166	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
84.94.83.137	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	152
85.250.175.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	142
5.28.181.104	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	136
91.231.193.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
84.228.16.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
109.64.202.91	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	129
46.120.23.31	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
109.64.115.235	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
84.111.201.132	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
37.142.15.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	115
109.253.130.24	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	107

06-04-2015-00:00:09 to 06-05-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.59.19.32	France	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	811
84.94.45.223	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	597
192.92.94.23	Europe	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	359
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	305
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	117
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	58
89.139.168.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	39
104.148.38.29		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
89.105.194.79	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	35
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
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
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
192.92.94.23	Europe	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	16
89.105.194.75	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	16
37.157.196.230	Czech Republic	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	14
176.67.104.177	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
70.32.85.52	United States	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
212.179.132.204	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
70.32.85.52	United States	147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
85.250.176.192	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
109.67.201.234	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
188.165.233.105	France	147.237.77.216	dover.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	8
99.91.152.60	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	8
79.179.139.42	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
212.117.143.250	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
46.116.142.236	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	6
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
203.151.234.15	Thailand	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	6
192.91.171.36	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	6
194.176.105.146	United Kingdom	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
84.228.78.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.57.250.79	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	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
176.228.200.25	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
212.76.113.209	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
212.143.226.107	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.183.29.103	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4

06-04-2015-00:00:09 to 06-05-2015-00:00:09

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	208
2.52.56.70	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	46
79.182.2.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	26
69.194.234.51	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	24
61.49.45.40	China	147.237.76.31	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
109.253.145.123	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
89.139.168.212	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	SERVER-WEBAPP .wwwacl access	4
66.249.69.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
61.183.128.6	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	3
66.249.64.193	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
176.12.137.214	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	GPL WEB_SERVER .htaccess access	2
61.240.144.65	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
85.64.38.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	SERVER-WEBAPP oracle web application server access	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	GPL EXPLOIT ISAPI .ida access	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	SERVER-WEBAPP /cgi-bin/ access	2
154.121.251.118		147.237.77.216	dover.idf.il	INDICATOR-SCAN sqlmap SQL injection scan attempt	2
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.28.145.218	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	GPL EXPLOIT .cnf access	2
84.108.106.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	SERVER-IIS webhits access	2
84.108.72.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	SERVER-IIS ISAPI .printer access	2
66.249.75.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	SERVER-IIS ISAPI .ida access	2
80.178.28.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	2
84.94.162.247	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.77	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	GPL WEB_SERVER ISAPI .printer access	2
79.182.174.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.132	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
37.26.148.188	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.49.45.43	China	147.237.77.226	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
70.32.85.52	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
61.183.128.6	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
157.55.39.177	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.160.237.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.246.4.158	Sweden	147.237.77.216	dover.idf.il	GPL EXPLOIT .htr access	2
93.173.156.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.187.75	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

06-04-2015-00:00:09 to 06-05-2015-00:00:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.106.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5414
2.54.27.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5332
212.179.61.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4576
164.138.127.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2318
82.145.221.207	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2076
212.179.46.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1919
89.139.168.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1697
109.65.96.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1328
212.179.61.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1142
62.128.35.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1097
82.145.221.48	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1025
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	918
82.145.216.210	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	908
213.151.55.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	886
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	782
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	773
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	751
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	749
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	728
188.120.143.249	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	636
101.87.235.180	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	618
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	578
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	560
95.86.119.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	556
84.111.114.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	550
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	514
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	487
37.237.140.47	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	442
66.249.83.188	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	430
66.249.83.182	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	424
78.108.169.23	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	412
46.164.128.106	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	392
204.93.58.187	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	391
66.249.83.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	381
2.54.151.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	380
212.25.102.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	375
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	365
212.179.132.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	348
66.87.66.83	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	335
82.205.11.7	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	330
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	301
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	300
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	299
84.94.32.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	280
213.57.143.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	277
66.249.75.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	270
66.249.75.66	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	270
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	269
157.55.39.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	266
166.137.252.23	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	260

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.178.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	750
46.19.86.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	499
176.12.140.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	435
213.57.243.152	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.243.152	Block	334
46.19.86.91	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.91	Block	304
37.26.150.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	284
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	272
79.180.61.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	244
77.125.165.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.165.99	Block	187
37.26.148.201	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.201	Block	166
109.253.133.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	136
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.74	Block	76
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	63
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	56
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	53
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	50
66.249.75.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	50
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.58	Block	36
69.194.234.51	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	24
37.26.148.180	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.180	Block	24
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	24
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	24
95.86.68.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	23
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	21
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	21
125.65.46.131	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.46.131	Block	20
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	18
89.138.22.74	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.22.74	Block	16
66.249.75.66	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	16
212.179.61.122	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	15
62.0.16.54	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
46.116.232.251	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	12
172.56.35.170	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	12
176.12.137.130	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	11
69.194.234.51	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 69.194.234.51	Block	11
94.159.174.28	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 94.159.174.28	Block	10
120.36.226.145	China	147.237.77.74	law.idf.il	Multiple signatures from 120.36.226.145	Block	9
149.78.54.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
94.153.9.220	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	9
120.36.226.145	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 120.36.226.145	Block	9
213.151.41.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
79.176.125.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
84.228.78.10	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	7
17.78.91.244	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
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	7
37.26.150.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
77.127.204.178	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	6
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	6
172.56.34.195	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6