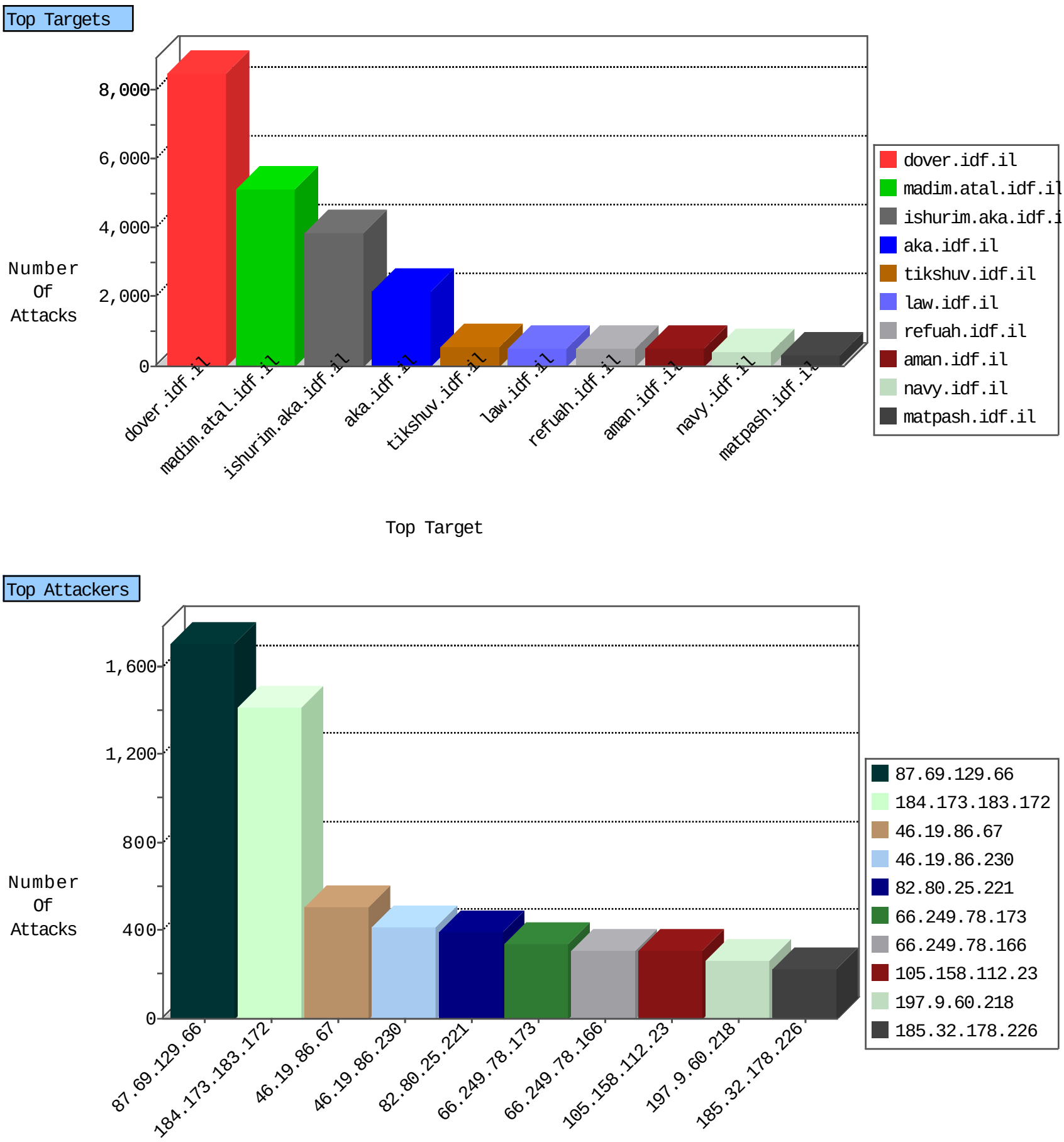
03-12-2015-00:00:07 to 03-13-2015-00:00:07

IDF Under Attack
Daily Report



03-12-2015-00:00:07 to 03-13-2015-00:00:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
105.158.112.23	Morocco	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2186
66.249.67.34	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	890
188.120.148.140	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	717
192.116.232.69	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	583
132.73.194.161	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	561
80.230.85.135	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	530
79.180.7.171	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	487
194.54.168.76	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	433
194.90.239.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	294
84.110.86.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	288
84.94.63.88	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	281
109.67.212.167	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	240
46.19.85.126	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	212
93.173.49.104	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	208
62.219.253.117	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
194.90.128.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
46.120.182.152	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	164
84.109.38.17	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
213.8.78.141	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
194.54.168.76	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
84.229.199.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
109.66.12.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
212.179.46.189	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
185.32.178.17	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	110
79.180.30.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
46.19.85.36	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	107
85.65.208.251	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
46.19.85.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
79.180.227.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
84.111.22.73	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
5.29.223.104	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
46.19.85.148	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	94
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
37.26.147.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
2.54.173.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
176.12.143.213	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
84.108.60.96	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
87.69.67.213	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
84.228.116.87	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
79.180.30.73	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
79.178.218.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
85.64.94.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
197.27.180.203	Tunisia	147.237.0.17	m.my-kosher-kravi.idf.il	TCP Scan (vertical)	drop	72
2.54.19.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
2.54.43.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
84.108.110.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
46.116.114.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65

03-12-2015-00:00:07 to 03-13-2015-00:00:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	757
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	305
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	193
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	163
180.76.5.193	China	147.237.77.216	dover.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	115
180.76.5.193	China	147.237.77.170	maarachot.idf.il	DVRep_P-N_40-59	Permit	58
115.219.24.86	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
77.126.33.170	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	27
212.143.3.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
72.167.249.79	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
212.97.133.140	Denmark	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
96.31.35.151	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
72.167.249.79	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
212.97.133.140	Denmark	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
46.116.251.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
108.168.219.174	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	14
212.34.12.166	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
197.9.60.218	Tunisia	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	13
104.155.209.47		147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
108.168.219.174	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
93.190.88.107	Germany	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	12
93.190.88.107	Germany	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
104.155.209.47		147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	11
46.19.85.39	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
109.64.212.119	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
115.219.24.86	China	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	7
37.130.227.133	United Kingdom	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	7
198.20.69.98	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	6
90.141.148.121	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
62.219.166.87	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	6
58.7.109.89	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
18.239.0.155	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
84.228.60.83	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
103.37.201.92		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.109.139.27	Switzerland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.179	e.mazi.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
80.230.98.170	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4

03-12-2015-00:00:07 to 03-13-2015-00:00:07

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	353
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	116
105.158.112.23	Morocco	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	17
197.242.151.91	South Africa	147.237.72.166	aka.idf.il	SQL Injection - Select From	11
41.42.186.234	Egypt	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	6
66.249.69.119	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
197.27.180.203	Tunisia	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
123.126.2.18	China	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
108.168.219.174	United States	147.237.77.74	law.idf.il	SQL Injection - Select From	4
197.9.60.218	Tunisia	147.237.77.216	dover.idf.il	SERVER-WEBAPP adminlogin access	4
108.168.219.174	United States	147.237.77.74	law.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	4
197.27.180.203	Tunisia	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
197.9.60.218	Tunisia	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	4
108.168.219.174	United States	147.237.77.74	law.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	4
192.35.222.17	United States	147.237.77.216	dover.idf.il	ET DOS SSL Bomb DoS Attempt	3
61.240.144.67	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	3
213.57.198.27	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
212.59.16.19	Lithuania	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
197.27.180.203	Tunisia	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
87.69.89.8	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.24.6	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.130.125	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.190	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
58.20.54.249	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
104.155.209.47		147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
122.228.207.193	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.190	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
84.108.75.170	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
79.178.113.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
178.19.107.114	Poland	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.193	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
84.94.96.120	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.230.155	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.150.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.176.219.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
87.68.37.221	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.204.117	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
149.78.150.59	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
208.80.155.147	United States	147.237.76.86	navy.idf.il	Tehila - Perl LWP with fake user agent	2
122.228.207.190	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
79.181.216.162	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

03-12-2015-00:00:07 to 03-13-2015-00:00:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	250
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	224
91.231.193.150	Israel	147.237.0.15	kosher-kravi.idf.il	First packet isn't SYN	drop	drop	180
62.207.60.231	Netherlands	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	162
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	138
84.95.84.211	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	109
197.27.180.203	Tunisia	147.237.0.15	kosher-kravi.idf.il	SAM rule	drop	drop	92
50.167.38.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	84
168.235.194.162		147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	76
66.249.75.154	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	76
168.235.194.162		147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	69
192.118.118.1	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	65
77.126.14.8	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	62
66.249.75.122	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
79.176.164.231	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
109.253.158.80	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
79.180.25.191	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	49
62.219.147.212	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	47
109.66.37.56	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	47
66.249.75.138	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
164.215.101.39	Azerbaijan	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.253.156.108	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
207.241.226.97	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	40
196.219.243.246	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
212.179.46.22	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
109.64.183.214	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.148.68	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
5.29.183.229	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.134.207	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
189.2.52.227	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
31.186.228.62	United Kingdom	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	34
109.66.121.54	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
185.32.179.160	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
195.93.246.47	Russian Federation	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	33
132.66.34.93	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
46.19.85.130	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
79.183.184.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
81.218.126.220	Israel	147.237.72.167	ishurim.aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	32
62.219.153.212	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
90.164.137.212	Spain	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.145.112	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
78.144.76.128	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
176.12.150.127	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
199.203.179.99	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	30
212.143.66.74	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.144.180	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.149.14	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.140.245	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.129.211	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.131.209	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.69.129.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1707
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.67	Block	510
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	416
80.246.136.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	197
109.160.240.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	197
185.32.176.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	193
197.9.60.218	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.9.60.218	Block	187
185.32.178.226	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.178.226	Block	179
109.253.145.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	159
46.116.159.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	153
185.32.179.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	134
176.12.149.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
2.54.137.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.114	Block	90
46.210.131.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
185.32.176.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
185.32.179.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	73
109.253.138.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
84.108.78.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	65
2.54.158.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
2.54.29.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
17.142.152.78	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.78	Block	53
17.142.152.60	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.60	Block	53
17.142.144.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.144.26	Block	52
17.142.151.198	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.198	Block	51
46.19.86.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
66.27.122.80	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	49
197.9.60.218	Tunisia	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 197.9.60.218	Block	49
185.32.178.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
109.253.156.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	41
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	41
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	41
109.253.136.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
176.12.145.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
2.52.164.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
185.32.178.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
66.249.78.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	34
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	34
185.32.177.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
69.164.193.21	United States	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
2.54.177.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
87.68.157.44	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.68.157.44	Block	22
66.249.75.154	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.154	Block	19
17.142.152.78	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
84.95.84.211	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	19
17.142.151.198	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18