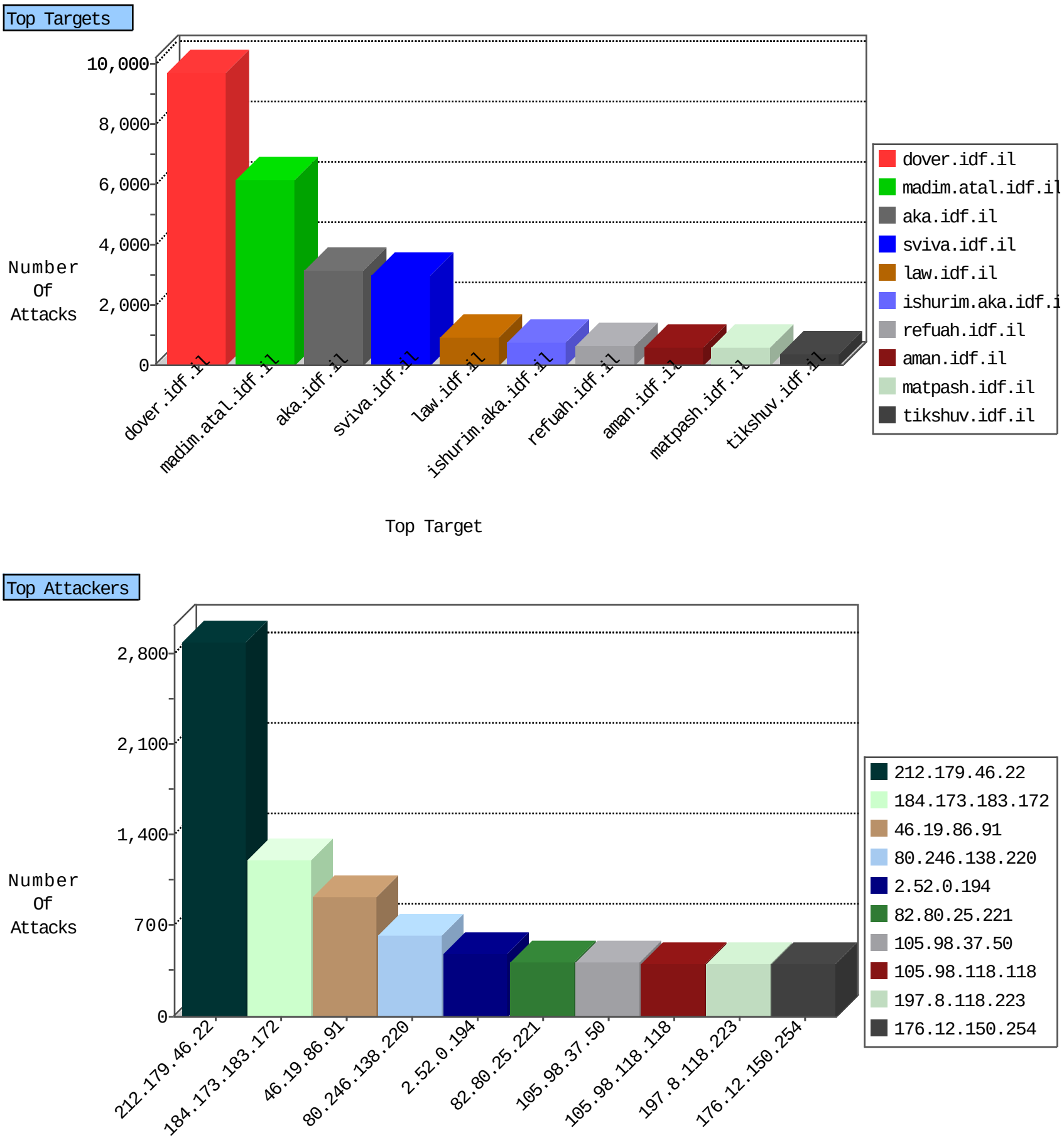
03-25-2015-00:00:08 to 03-26-2015-00:00:08

IDF Under Attack Daily Report



03-25-2015-00:00:08 to 03-26-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
5.102.224.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1546
109.160.243.146	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1121
79.177.113.114	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	790
197.8.118.223	Tunisia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	682
109.67.38.212	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	661
197.8.118.223	Tunisia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	582
147.235.236.1	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	581
93.173.171.180	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	556
77.126.252.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	513
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	331
93.172.171.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	280
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	262
109.67.155.127	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	228
87.68.36.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
109.65.72.249	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
37.46.36.165	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	171
87.68.157.8	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	168
79.180.119.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
162.243.220.250	United States	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	153
79.178.0.145	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	136
31.44.128.28	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
84.108.11.147	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
93.172.186.110	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
77.125.2.79	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
62.90.122.230	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	115
5.102.220.4	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
176.12.160.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
81.218.101.146	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	106
5.102.233.83	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
70.39.187.36	Satellite Provider	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	100
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
5.28.191.46	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	90
2.54.25.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
46.19.86.91	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
185.32.178.183	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	86
79.176.58.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	85
46.19.85.174	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
77.126.238.71	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	82
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
82.166.102.99	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	78
2.54.60.126	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
46.19.86.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	75
109.65.97.199	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
46.19.86.63	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
5.29.9.238	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
91.231.192.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
78.24.50.205	Moldova, Republic of	147.237.8.14	e.orchot.idf.il	TCP Scan (vertical)	drop	72
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	72

03-25-2015-00:00:08 to 03-26-2015-00:00:08

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	542
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	410
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	259
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	214
199.180.114.150	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	66
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	25
85.133.4.238	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
85.133.4.238	United Kingdom	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
94.102.153.58	United Kingdom	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
94.102.153.58	United Kingdom	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
96.31.33.55	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
96.31.33.55	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	15
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	15
116.0.23.222	Australia	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	15
94.23.24.76	France	147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
94.23.24.76	France	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
212.143.231.101	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
212.29.237.71	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
84.108.121.54	Israel	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	7
80.74.104.71	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
45.217.172.58		147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	6
212.143.186.38	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.179.140.133	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
88.150.187.210	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
46.121.199.10	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
2.54.16.201	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
82.80.135.182	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
105.98.37.50	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
149.78.149.53	United States	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.79	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
37.239.0.2	Iraq	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	4
46.19.85.40	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.143.231.101	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
193.201.224.176	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
122.107.249.146	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.90.255.56	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
37.59.123.142	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
79.181.182.68	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.108.12.23	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
93.120.27.62	Romania	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	3
96.44.189.102	United States	147.237.77.216	dover.idf.il	EgovRep_B-N_70-99	Block	3
93.120.27.62	Romania	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	3
193.201.224.176	Ukraine	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
84.163.197.94	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
93.120.27.62	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
152.233.23.225		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
216.17.138.97	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
41.105.100.51	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
93.120.27.62	Romania	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	3

03-25-2015-00:00:08 to 03-26-2015-00:00:08

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	366
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	113
77.126.137.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	17
5.22.129.178	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	15
208.80.155.147	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	14
94.102.153.58	United Kingdom	147.237.72.166	aka.idf.il	SQL Injection - Select From	13
85.133.4.238	United Kingdom	147.237.77.74	law.idf.il	SQL Injection - Select From	12
85.133.4.238	United Kingdom	147.237.77.74	law.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	12
85.133.4.238	United Kingdom	147.237.77.74	law.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	12
46.19.86.120	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	9
176.12.137.146	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
202.4.112.74	Bangladesh	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
46.116.153.109	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
66.249.73.233	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	3
218.77.79.43	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.159	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
2.54.148.189	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.95.212.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.81	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
80.179.13.39	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.191.141	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.157	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.157	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
85.250.104.202	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.29	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
77.127.250.169	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
195.238.181.159	Ukraine	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
95.86.91.137	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.157	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
128.199.183.72	Singapore	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
43.255.191.141	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.141	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
79.180.149.201	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.120.97	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
41.227.239.204	Tunisia	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
94.23.24.76	France	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
195.238.181.159	Ukraine	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
132.72.100.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.141	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.157	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.136	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.162	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.157	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.41	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2

03-25-2015-00:00:08 to 03-26-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.46.22	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	2888
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	322
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	284
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	238
197.8.118.223	Tunisia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	181
105.98.37.50	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	130
87.69.161.206	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	124
105.98.120.95	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	95
5.22.129.178	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	85
212.179.61.127	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	76
200.181.105.219	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
77.169.241.140	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
66.249.93.216	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
88.161.211.177	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
5.22.129.178	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	46
176.12.136.8	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
66.249.93.219	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
190.202.27.8	Venezuela	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
85.130.226.9	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	38
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.135.3	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.141.140	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.143.243	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.150.123	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.147.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
85.64.214.10	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	29
31.210.187.243	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	29
81.218.77.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
84.95.251.243	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
212.29.214.138	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	25
176.12.149.44	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.137.219	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.140.183	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
80.246.130.152	Israel	147.237.0.34	tikshuv.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	24
5.22.129.178	Israel	147.237.72.167	ishurim.aka.idf.il		Bad TCP sequence	monitor	24
176.12.140.76	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.143.84	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
5.22.129.178	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	24
213.244.81.60	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	24
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
77.93.39.13	Ukraine	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	23
41.227.250.131	Tunisia	147.237.0.15	kosher-kravi.idf.i	SAM rule	drop	drop	22
105.98.37.50	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
178.252.189.44	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	21
85.130.226.9	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	21
46.19.86.6	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
176.12.142.12	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
46.19.85.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
109.253.140.238	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20

03-25-2015-00:00:08 to 03-26-2015-00:00:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	913
80.246.138.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	627
2.52.0.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	471
176.12.150.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	408
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	377
80.246.140.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	317
2.54.51.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	310
185.32.178.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	282
2.54.171.183	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.171.183	Block	258
176.12.151.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	246
80.246.136.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
176.12.139.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	196
105.98.118.118	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	185
176.12.151.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
105.98.118.118	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.118.118	Block	175
109.253.141.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	168
109.253.136.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	146
105.98.37.50	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	131
176.12.147.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	127
105.98.37.50	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.37.50	Block	115
197.9.7.169	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	111
197.9.7.169	Tunisia	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 197.9.7.169	Block	110
197.9.7.169	Tunisia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	109
197.8.118.223	Tunisia	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 197.8.118.223	Block	104
176.12.142.148	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.142.148	Block	102
176.12.149.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	99
197.8.118.223	Tunisia	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	97
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	86
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	59
176.12.139.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	59
37.26.147.204	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.204	Block	56
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.21	Block	54
66.249.79.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	47
66.249.79.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	46
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	46
109.253.159.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
109.253.130.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
46.210.95.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	39
109.186.236.24	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	39
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	38
176.12.136.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	35
176.12.151.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
81.218.116.129	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	29
46.19.85.231	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.231	Block	28
84.111.7.136	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.111.7.136	Block	24
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	21
31.44.128.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	19
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	19
77.66.121.237	Denmark	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.66.121.237	Block	19

03-25-2015-00:00:08 to 03-26-2015-00:00:08