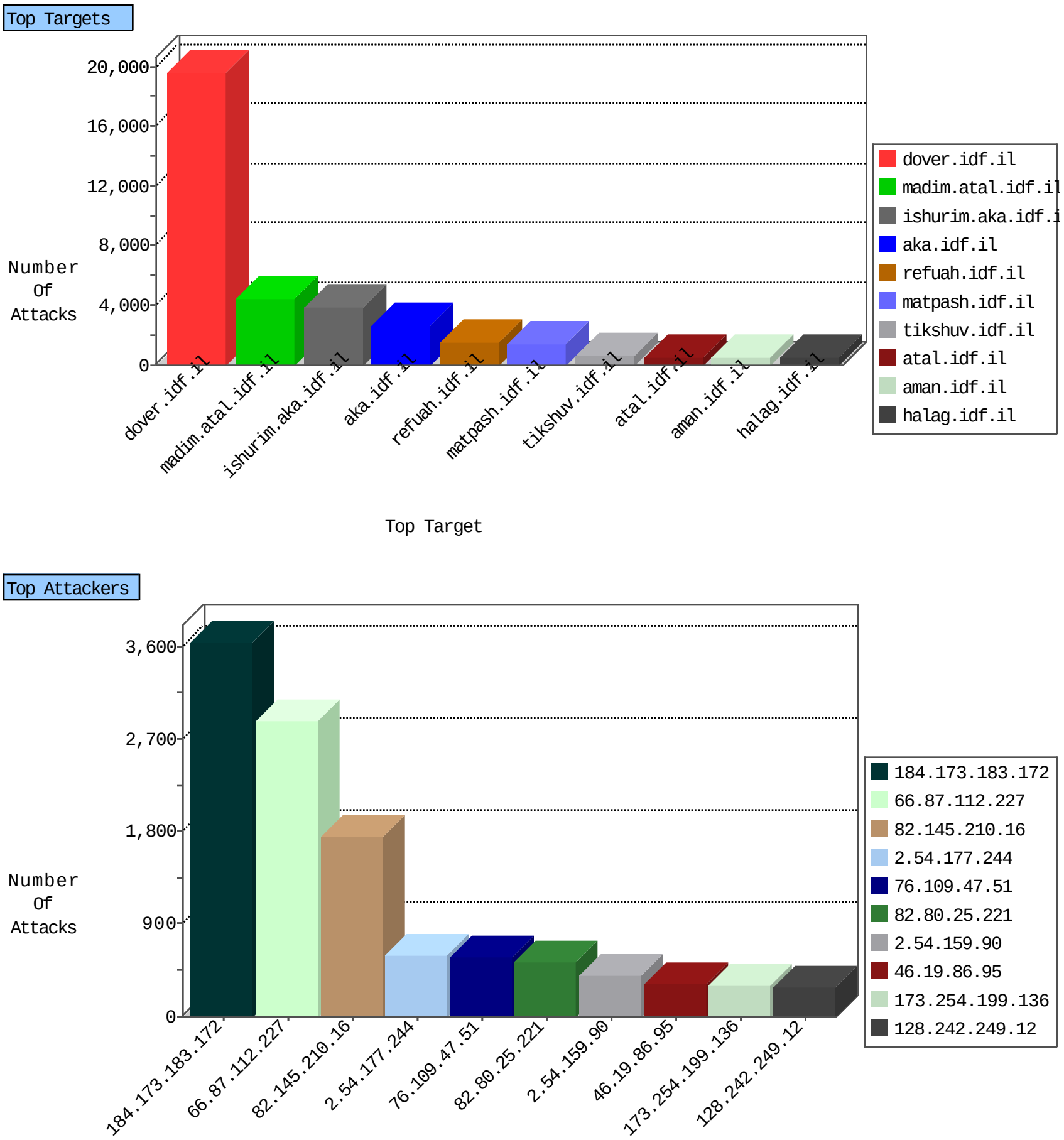
03-10-2015-00:00:05 to 03-11-2015-00:00:05

IDF Under Attack Daily Report



03-10-2015-00:00:05 to 03-11-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
84.229.189.216	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	678
87.69.200.234	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	438
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	430
83.130.111.1	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	329
5.28.182.245	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	275
109.66.12.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	272
197.29.167.21	Tunisia	147.237.0.17	m.my-kosher-kravi.idf.il	TCP Scan (vertical)	drop	259
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	253
109.67.8.64	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	243
94.159.132.75	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	222
212.179.21.198	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
77.125.84.151	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
37.142.46.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
79.179.107.6	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
84.110.86.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	181
46.121.110.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
197.29.167.21	Tunisia	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	165
46.19.85.128	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	162
46.121.142.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
212.117.157.74	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
46.117.62.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
84.109.90.39	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
197.29.167.21	Tunisia	147.237.0.19	madim.atal.idf.il	TCP Scan (vertical)	drop	139
46.116.84.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
93.173.63.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
46.117.124.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
46.19.86.169	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	102
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
46.19.85.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
213.57.183.223	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
79.179.34.170	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
85.65.232.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
46.120.146.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
109.186.144.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
93.172.17.24	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
109.65.170.168	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
217.132.247.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
2.54.44.146	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
5.28.182.245	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
46.19.86.149	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	70
2.54.161.215	Israel	147.237.77.216	dover.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	69
109.67.53.5	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
46.19.85.116	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
109.253.145.243	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
5.28.148.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
80.246.139.129	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	62

03-10-2015-00:00:05 to 03-11-2015-00:00:05

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
185.32.179.122	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	61

03-10-2015-00:00:05 to 03-11-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.87.112.227	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2884
82.145.210.16	Europe	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1756
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1200
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	1083
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	504
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	398
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	287
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	275
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	188
67.198.141.92	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	135
173.254.199.136	United States	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
173.254.199.136	United States	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
81.218.97.45	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	23
67.198.141.90	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_P-N_40-59	Permit	14
67.198.141.90	United States	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	14
67.198.141.90	United States	147.237.77.19	law-forum.idf.il	DVRep_P-N_40-59	Permit	14
46.137.186.92	Ireland	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
77.127.242.87	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
46.116.200.175	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
46.137.186.92	Ireland	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
212.199.130.90	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
190.188.55.179	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
130.43.88.111	Greece	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
46.116.211.186	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
81.22.0.93	Russian Federation	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
79.181.26.32	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
212.76.107.240	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
46.19.85.225	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.97.114	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
194.114.146.227	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
91.207.4.22	Ukraine	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	6
81.218.251.251	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.206	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.22	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
67.198.141.91	United States	147.237.77.205	prisha.idf.il	DVRep_P-N_40-59	Permit	5
79.182.15.27	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.148	ggcenter.aka.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
93.173.160.210	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	4

03-10-2015-00:00:05 to 03-11-2015-00:00:05

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	142
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	115
2.54.5.120	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	56
66.249.69.135	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	26
66.249.75.136	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
66.249.75.152	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
66.249.93.240	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	6
197.29.167.21	Tunisia	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	5
197.29.167.21	Tunisia	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
85.64.206.41	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
197.29.167.21	Tunisia	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	3
197.29.167.21	Tunisia	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
77.127.220.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
197.29.167.21	Tunisia	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
194.177.16.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
122.228.207.199	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	3
66.249.75.120	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
77.125.138.229	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
222.186.56.103	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
87.69.33.243	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
109.64.39.29	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.53.126.2	Turkey	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
109.66.35.154	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.140.179	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.172.162.136	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.21	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
109.65.202.4	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.105.131	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.117.199	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.146.147	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.228	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
80.230.76.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.47.70	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.158.215.206	Netherlands	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
149.78.192.178	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
95.86.80.102	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	2
197.29.167.21	Tunisia	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
176.12.151.125	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.119	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
197.29.167.21	Tunisia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.86.247	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.142.22	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
37.142.250.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.212	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
216.179.118.130	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2

03-10-2015-00:00:05 to 03-11-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
76.109.47.51	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	580
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	395
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	234
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	196
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	188
79.181.217.157	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	97
85.130.141.87	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	91
173.254.199.136	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	84
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	82
85.130.141.87	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	73
173.254.199.136	United States	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	73
5.29.112.80	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
109.253.137.106	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
90.5.56.104	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
173.254.199.136	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	60
118.123.11.45	China	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	60
92.90.21.25	France	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	54
168.187.27.22	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
176.12.147.87	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
176.12.146.228	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
176.12.149.173	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
168.63.137.102	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
168.63.139.43	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
31.186.228.57	United Kingdom	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	48
109.64.176.121	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	43
109.253.159.248	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.150.51	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
31.186.228.29	United Kingdom	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	42
31.154.232.155	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.253.157.92	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.253.140.16	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.64.9.88	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	41
46.120.66.24	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	40
128.223.223.243	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
197.33.225.231	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
31.186.228.65	United Kingdom	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	38
31.186.228.94	United Kingdom	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	37
31.186.228.31	United Kingdom	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	37
109.253.149.74	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.64.51.47	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	36
176.12.137.176	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.137.43	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.144.64	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.137.221	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.151.173	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.139.128	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.145.241	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.131.181	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.143.249	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.177.244	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.177.244	Block	594
2.54.159.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	394
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	324
2.52.156.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	280
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	247
79.179.107.6	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.179.107.6	Block	242
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.85	Block	236
176.12.138.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
83.130.113.220	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 83.130.113.220	Block	193
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
5.22.130.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	178
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.65	Block	126
2.52.57.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
176.12.146.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
93.173.150.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
109.253.142.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
2.54.128.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
46.19.86.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
176.12.137.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
46.19.86.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
84.108.60.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	54
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	50
176.12.149.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
109.253.156.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
185.32.176.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
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
5.102.223.64	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.102.223.64	Block	44
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	43
109.253.131.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
176.12.149.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
46.19.86.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
109.253.158.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
176.12.142.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
86.85.5.55	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	21
213.151.39.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	19
176.12.141.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
176.12.139.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
212.76.112.222	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	15
17.142.150.178	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.150.178	Block	14
84.95.133.185	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	14
176.12.139.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
79.178.21.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
62.219.172.178	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	12
17.142.152.38	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.38	Block	11
109.253.146.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
212.235.34.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.235.34.6	Block	11
17.142.151.188	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.188	Block	10