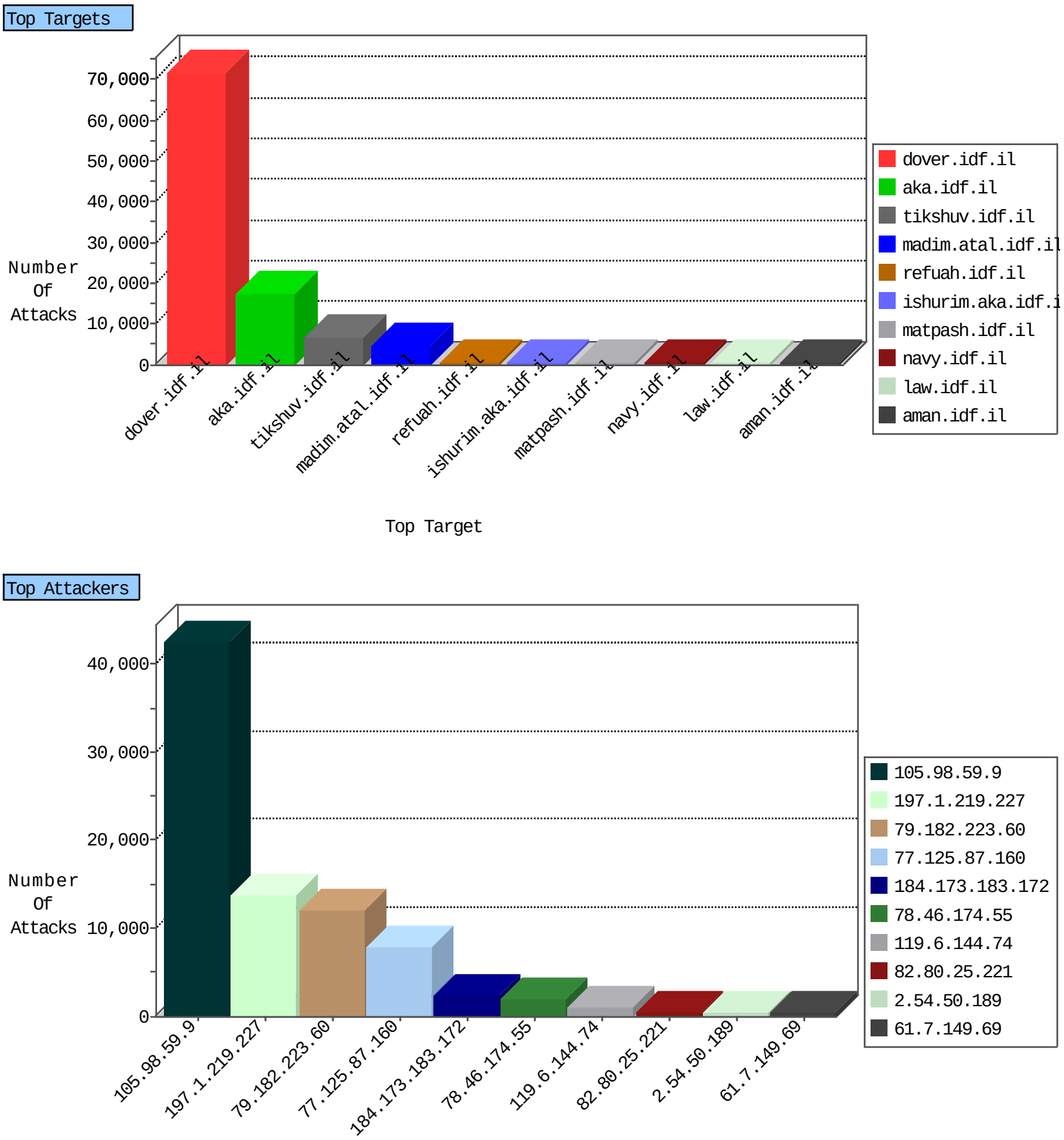
03-24-2015-00:00:05 to 03-25-2015-00:00:05

IDF Under Attack Daily Report



03-24-2015-00:00:05 to 03-25-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	5372
5.29.174.188	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1432
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1350
109.66.12.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1322
84.228.30.86	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1230
82.81.240.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	980
213.57.114.160	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	533
79.178.0.145	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	455
61.7.149.69	Thailand	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	448
220.248.41.106	China	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	443
77.126.128.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	314
109.66.30.181	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	297
192.114.182.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	294
213.8.71.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	292
37.46.37.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	282
190.52.175.76	Paraguay	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	278
188.120.148.136	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	214
46.121.110.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
185.32.178.189	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
80.178.219.199	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	161
93.173.18.97	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
79.176.197.93	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
192.115.116.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	140
109.67.98.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
37.142.29.119	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
132.67.170.131	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	133
31.168.144.13	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	129
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	121
93.172.219.15	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
46.117.215.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
186.92.45.185	Venezuela	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	107
78.46.174.55	Germany	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	104
2.54.24.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	97
212.143.181.110	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	97
200.84.227.189	Venezuela	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	95
82.81.240.91	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	86
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
2.54.57.209	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	83
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	82
46.19.85.185	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
2.52.190.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
84.94.72.189	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
46.19.85.188	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	72
46.19.85.121	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
220.181.108.167	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	71
2.52.155.47	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
212.143.222.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
79.179.190.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69

03-24-2015-00:00:05 to 03-25-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.87.160	Israel	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	6484
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1223
119.6.144.74	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1103
77.125.87.160	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	988
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	503
77.125.87.160	Israel	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	331
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	282
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	257
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	172
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	145
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	136
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	124
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	109
83.246.164.188	Russian Federation	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	40
138.134.192.10	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
62.241.24.18	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	23
180.76.5.193	China	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	15
62.241.24.41	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
196.202.206.227	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
62.219.21.30	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
132.72.138.1	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
93.172.28.147	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
95.94.100.43	Portugal	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
68.229.211.18	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.190.243.137	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.138	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.72.36.124	Netherlands	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	5
46.19.85.164	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.125.87.87	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
123.30.75.115	Vietnam	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
210.7.0.202	Fiji	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.107.142.131	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
201.5.143.198	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
27.159.113.116	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
93.120.27.62	Romania	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	4
2.54.171.194	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.89.134.98	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
105.156.219.132	Morocco	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
197.9.53.136	Tunisia	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	4
120.149.177.79	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.187.129.166	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	3
91.233.116.68	Finland	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.31	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
178.217.187.39	Poland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
204.85.191.30	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
23.242.179.205	United States	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.182.123.143	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.197	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

03-24-2015-00:00:05 to 03-25-2015-00:00:05

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	432
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	114
66.249.93.179	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	8
5.29.28.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
46.19.85.206	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
109.66.140.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
79.181.17.26	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
85.65.60.23	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
87.69.194.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
43.255.191.161	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
122.228.207.77	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	3
43.255.191.141	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
78.46.174.55	Germany	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	2
77.127.152.53	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.158	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
132.66.62.239	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.69.194	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.141	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
128.139.197.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.211.150	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
41.227.239.204	Tunisia	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.77	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
109.186.163.177	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
43.255.191.161	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
46.117.231.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.88.102.25	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.244.188	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.141	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
79.177.50.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.172	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
109.253.139.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.158.215.206	Netherlands	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
109.66.116.110	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
66.249.73.129	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
109.65.126.120	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.27.193	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.118.186	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.35.154	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.127.205.208	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
77.127.84.198	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 Potential SSH Scan	2
122.228.207.77	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
115.231.218.147	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
46.19.86.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
79.182.197.134	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

03-24-2015-00:00:05 to 03-25-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
105.98.59.9	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	40779
197.1.219.227	Tunisia	147.237.77.216	dover.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	13310
79.182.223.60	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2313
78.46.174.55	Germany	147.237.72.166	aka.idf.il	SAM rule	drop	drop	1120
105.98.59.9	Algeria	147.237.77.216	dover.idf.il		drop	drop	1073
105.98.59.9	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	356
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	312
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	312
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	290
212.179.46.19	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	214
190.203.41.8	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	144
197.1.219.227	Tunisia	147.237.77.216	dover.idf.il	SAM rule	drop	drop	139
190.207.57.213	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
190.38.206.13	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	120
212.179.46.20	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	87
67.58.38.246	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	86
201.249.1.232	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
190.38.61.42	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
190.75.166.189	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
190.37.154.223	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
213.1.221.206	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
190.200.244.222	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
190.201.217.208	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
201.249.21.151	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
190.37.100.158	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
217.25.209.34	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
200.84.227.189	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
212.179.21.195	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	47
62.241.24.18	Italy	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
186.94.24.147	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
213.47.14.93	Austria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
85.106.135.33	Turkey	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
109.64.125.76	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	43
213.55.112.241	Ethiopia	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	41
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
176.12.140.88	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
212.252.164.134	Turkey	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	34
163.177.79.4	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
121.199.30.110	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.253.128.43	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.159.47	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
121.41.84.140	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
201.242.1.96	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
37.8.5.152	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.142.98	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.145.77	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
186.84.127.78	Colombia	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
201.211.152.235	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.223.60	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	7034
79.182.223.60	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	2432
2.54.50.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	527
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	439
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	364
5.29.190.222	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.190.222	Block	343
2.54.56.115	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.56.115	Block	333
79.182.223.60	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.223.60	Block	288
2.54.96.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	271
37.237.148.6	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	271
2.52.167.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	234
109.253.158.160	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.158.160	Block	232
37.26.146.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	217
105.98.59.9	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.59.9	Block	192
105.98.59.9	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	191
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.227	Block	182
109.253.132.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	165
79.176.197.93	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.176.197.93	Block	163
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	156
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	156
176.12.140.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	133
41.98.106.107	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.98.106.107	Block	119
41.98.106.107	Algeria	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	118
109.253.130.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	112
2.54.144.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	106
197.1.219.227	Tunisia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 197.1.219.227	Block	104
197.1.219.227	Tunisia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 197.1.219.227	Block	104
176.12.151.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	103
176.12.150.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	101
197.1.219.227	Tunisia	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 197.1.219.227	Block	99
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	86
109.253.139.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	84
2.54.27.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	82
2.54.166.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	82
109.253.146.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	81
109.253.137.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
109.253.139.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	56
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	56
109.253.129.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	54
109.253.159.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	49
66.249.79.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	49
109.253.138.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	44
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	44
66.249.79.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	43
149.88.70.164	United States	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	42
109.253.157.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
109.253.138.172	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.138.172	Block	39
176.12.149.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
62.44.134.70	Denmark	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	32