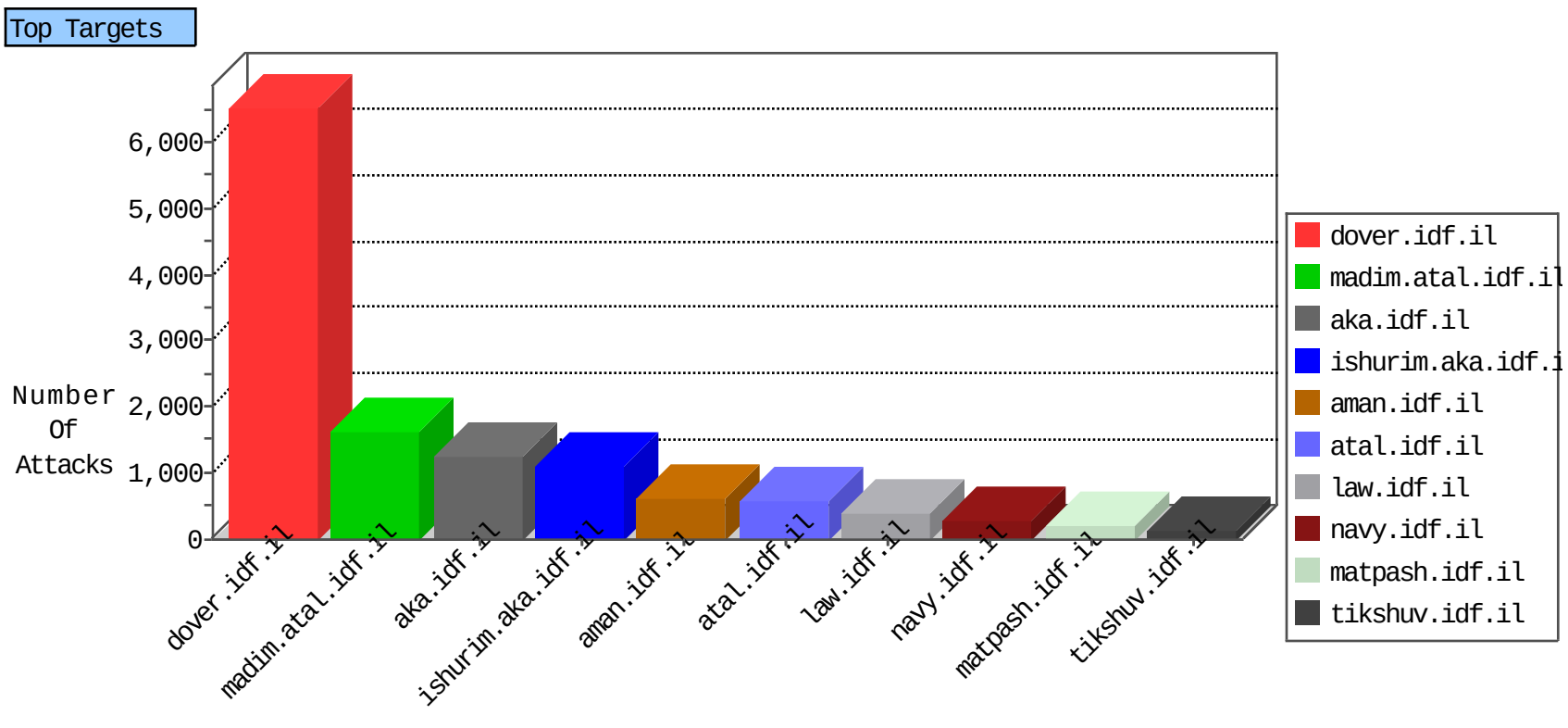
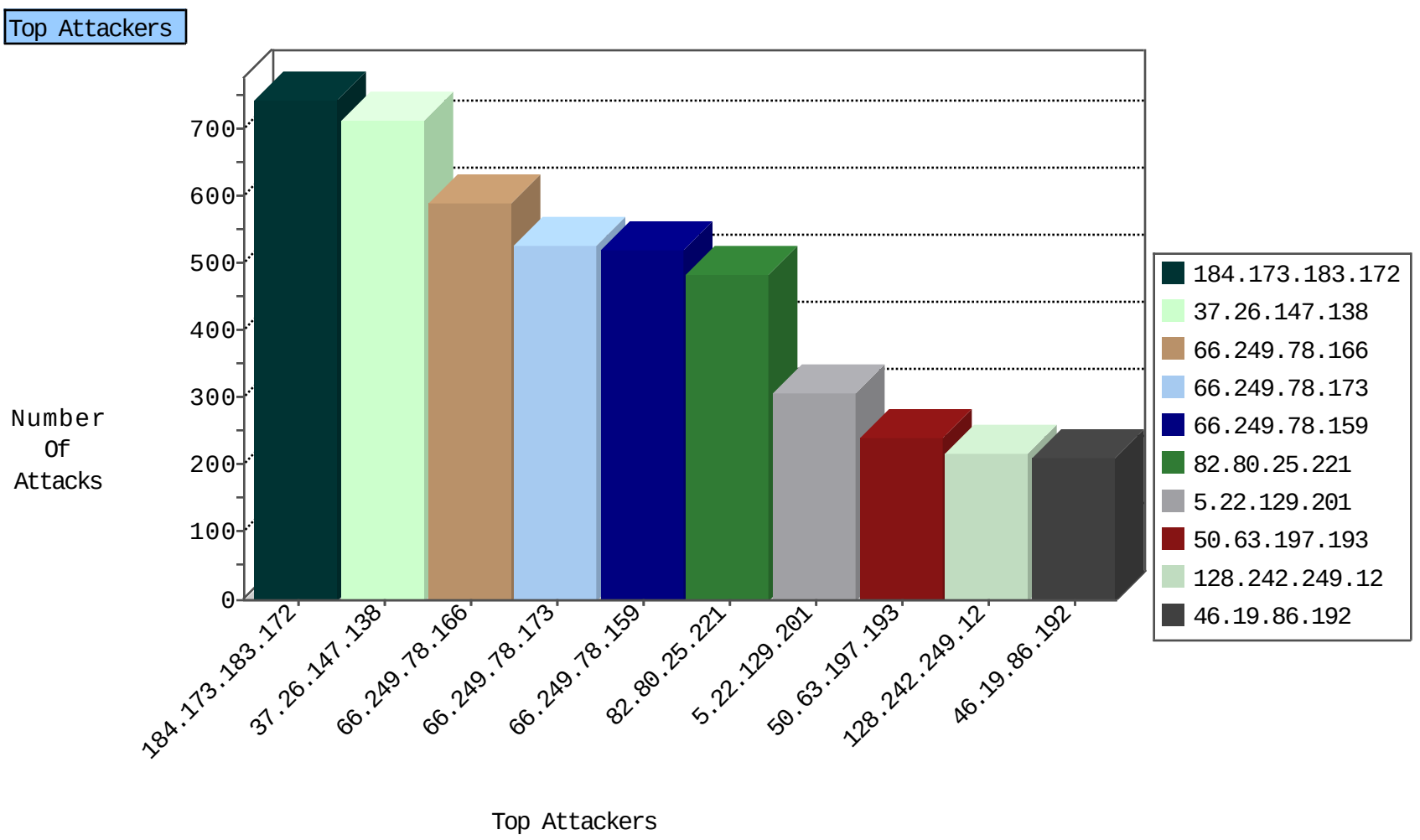
03-06-2015-00:00:08 to 03-07-2015-00:00:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-06-2015-00:00:08 to 03-07-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
109.111.118.20	Andorra	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2073
85.250.225.115	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	474
87.69.222.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	398
109.66.120.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	372
84.110.86.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	342
2.54.184.249	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	307
213.57.182.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	302
80.246.139.227	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	284
109.186.154.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	275
109.67.148.66	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	270
213.57.57.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	259
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	244
46.121.89.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
85.64.5.199	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
149.88.13.87	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
46.19.86.199	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	116
80.246.139.227	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
46.19.85.169	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
93.173.227.230	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
2.54.176.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
185.32.179.200	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
85.64.207.11	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
109.65.19.157	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	77
2.54.173.180	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
5.102.254.244	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
2.52.39.118	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
89.138.58.152	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
109.253.158.100	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
37.26.148.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
109.65.19.157	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
46.121.89.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	49
185.32.179.200	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	13
109.253.158.100	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	11
46.19.85.20	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	11
41.248.147.70	Morocco	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
79.177.186.150	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
37.26.147.201	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	5
82.229.253.176	France	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	4
94.71.150.213	Greece	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	3
101.109.0.163	Thailand	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	3
123.231.124.176	Sri Lanka	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	3
79.182.191.33	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
64.74.133.83	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
183.178.61.97	Hong Kong	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
119.64.2.14	Korea, Republic of	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2

03-06-2015-00:00:08 to 03-07-2015-00:00:08

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	410
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	217
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	192
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	142
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	91
178.5.64.72	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	75
46.116.255.228	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	54
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	45
188.143.235.17	Russian Federation	147.237.77.74	law.idf.il	C032: HTTP: Access to - web.config	Block	7
77.127.242.87	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
105.235.133.42	Algeria	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
88.254.120.177	Turkey	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
92.43.69.103	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.i	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.i	DVRep_B-N_60_100	Block	4
188.165.232.185	France	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
41.235.44.85	Egypt	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
175.44.47.233	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
212.117.143.250	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	3
197.248.73.58	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.36	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.177.186.150	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	3
109.253.96.68	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.i	DVRep_B-N_60_100	Block	3
89.138.78.201	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.250.177.124	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
93.120.27.62	Romania	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	3
79.180.18.208	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
87.69.112.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	3
89.138.78.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.111.174.19	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	3
80.246.136.207	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
176.67.121.170	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.43.94	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	2
65.115.104.226	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.141	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	2
93.120.27.62	Romania	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	2

03-06-2015-00:00:08 to 03-07-2015-00:00:08

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	485
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	135
37.26.147.201	Israel	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	120
50.63.197.193	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	48
50.63.197.193	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	48
94.230.86.152	Israel	147.237.72.167	ishurim.aka.idf.il	INDICATOR-SCAN myscan	8
188.165.232.185	France	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	8
94.230.86.152	Israel	147.237.72.167	ishurim.aka.idf.il	GPL SCAN myscan	8
2.6.139.252	France	147.237.72.166	aka.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	5
90.50.36.232	France	147.237.72.166	aka.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	5
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
213.204.127.33	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
2.6.139.252	France	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	4
185.32.179.19	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
209.166.166.199	United States	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	3
54.247.122.220	Ireland	147.237.72.166	aka.idf.il	ET WEB_SERVER PHP Crawler	2
115.231.218.147	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.199	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
85.250.212.100	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
2.52.141.96	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.121.242.169	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
195.238.181.159	Ukraine	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.75.13	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
209.166.166.199	United States	147.237.77.178	e.matpash.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
122.228.207.199	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.199	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
84.95.199.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.103.51	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.178.37.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.138.101	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	2
77.127.196.71	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.186.20.58	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
81.218.77.162	Israel	147.237.76.86	navy.idf.il	GPL SCAN nmap TCP	2
109.66.126.204	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.127.85.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
115.231.218.23	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
222.186.134.7	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
195.238.181.159	Ukraine	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
122.228.207.199	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
209.166.166.199	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	Germany	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	2
115.231.218.147	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
87.69.194.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
2.54.184.129	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

03-06-2015-00:00:08 to 03-07-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	382
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	364
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	344
5.22.129.201	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	306
46.188.81.158	Russian Federation	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	140
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	126
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	84
23.249.163.16	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	83
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
109.253.129.76	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
109.67.3.241	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
85.65.74.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
188.161.11.25	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
128.59.247.102	United States	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
203.215.32.163	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	35
176.12.141.46	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
46.244.67.78	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	30
188.73.128.158	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.150.223	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.138.218	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.139.4	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.143.130	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
207.46.13.118	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.129.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
41.43.56.224	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
93.172.130.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
109.75.66.60	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
63.240.52.147	United States	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	25
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.128.13	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
79.182.63.168	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.137.109	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
84.111.48.73	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
197.151.129.51	Egypt	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	23
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	23
109.64.204.81	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
2.52.143.143	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
157.55.39.119	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
157.55.39.12	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
77.125.123.161	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
37.26.147.142	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
187.4.152.93	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
2.52.7.133	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
94.59.166.169	United Arab Emirates	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.26	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	20
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
79.179.136.44	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.147.138	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.138	Block	712
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	197
185.32.179.19	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.19	Block	193
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	174
2.54.162.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.162.211	Block	138
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	102
134.17.31.249	Belarus	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 134.17.31.249	Block	98
185.32.179.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
109.253.139.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
109.253.157.187	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.157.187	Block	68
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	50
50.63.197.193	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	48
50.63.197.193	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	48
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
109.67.193.30	Israel	147.237.77.176	matpash.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
50.63.197.193	United States	147.237.77.74	law.idf.il	Multiple Admin Blocking from 50.63.197.193	Block	23
50.63.197.193	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 50.63.197.193	Block	23
66.249.64.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	14
66.249.64.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	11
46.19.86.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	11
93.172.28.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
66.249.69.159	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.69.159	Block	7
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	7
2.54.190.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
217.132.83.27	Israel	147.237.0.16	my-kosher-kravi.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 217.132.83.27	None	7
79.179.10.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	6
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.201	Block	6
88.254.120.177	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 88.254.120.177	Block	6
173.233.85.183	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
66.249.64.150	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.150	Block	5
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	5
95.86.73.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
109.65.28.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	5
46.116.179.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
46.19.86.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
5.22.130.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
79.180.7.209	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.180.7.209	Block	5
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
149.88.116.239	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1565	Block	4
109.65.28.195	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.28.195	Block	4
17.142.152.127	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
77.125.214.254	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il//categorytemplates/listchilddocuments/2042	Block	4
66.249.78.4	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	4
188.165.232.185	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
193.40.193.11	Estonia	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	4
23.254.129.17	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
64.74.215.44	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.74.215.44	Block	4
84.228.111.106	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/resource/userfollowresource/create/	Block	4
66.249.69.191	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//main/giyus/giyus/general.aspx	Block	4