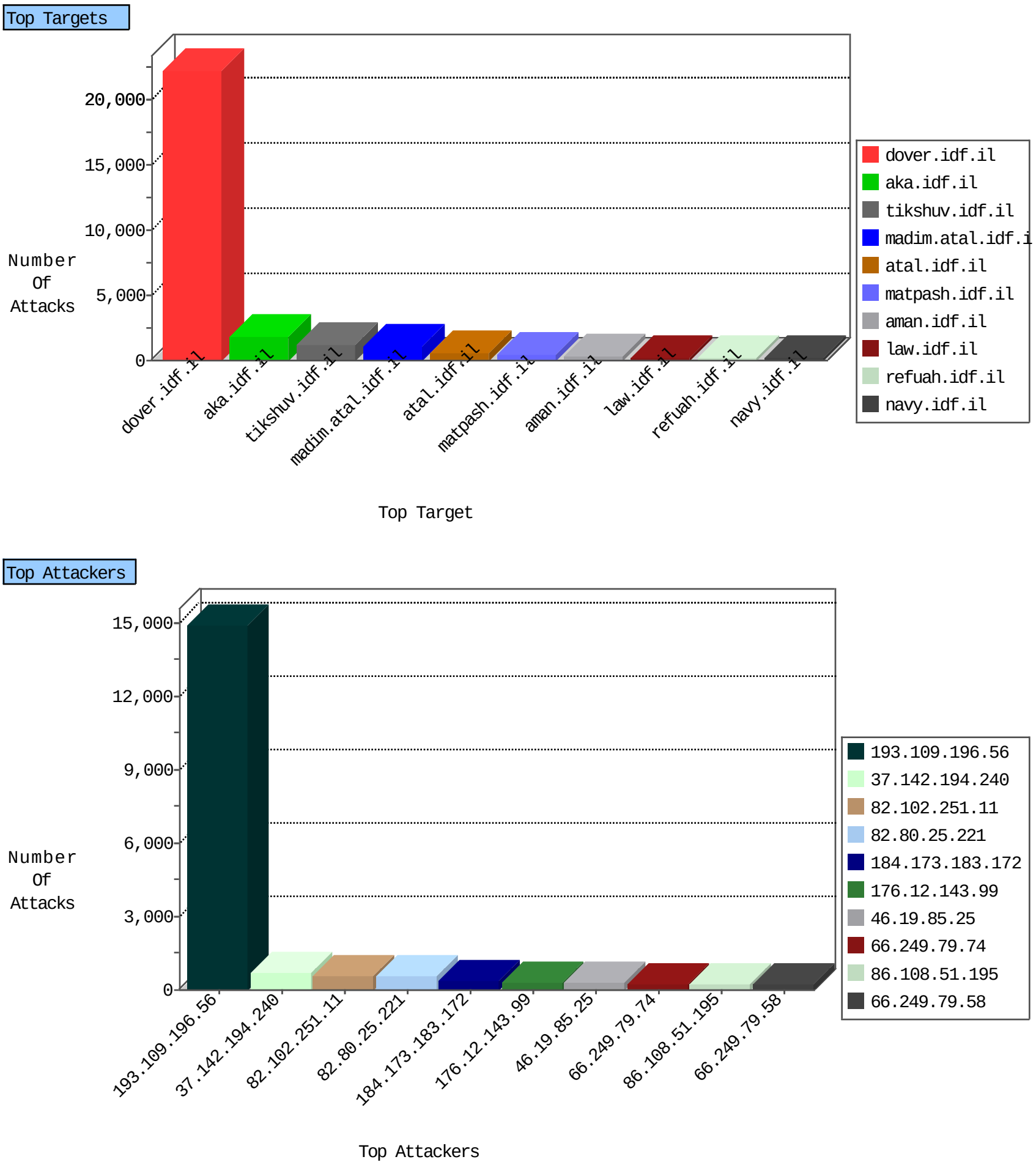
03-27-2015-00:00:08 to 03-28-2015-00:00:08

IDF Under Attack Daily Report



03-27-2015-00:00:08 to 03-28-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	472
46.120.242.32	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	327
5.43.202.144	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	252
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
86.108.51.195	Jordan	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	195
79.176.158.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
84.228.255.251	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
2.54.136.35	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
79.183.177.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	141
84.111.109.105	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
85.64.245.182	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
109.67.116.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
46.120.226.52	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
80.178.160.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
78.24.50.205	Moldova, Republic of	147.237.0.17	m.my-kosher-kravi.idf.il	TCP Scan (vertical)	drop	91
84.228.71.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
37.26.147.236	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
84.94.54.126	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	78
2.52.172.57	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
86.185.204.200	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	73
52.16.5.197	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	72
109.253.144.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	71
5.29.196.141	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
84.229.39.252	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	68
157.55.39.6	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	64
54.72.0.55	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	62
188.165.15.148	France	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	60
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	58
157.55.39.137	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	56
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	55
82.145.208.68	Europe	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	55
50.87.144.145	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	50
195.34.150.18	Austria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	50
54.72.73.168	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	45
41.129.32.247	Egypt	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	43
157.55.39.42	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	43
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	39
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	38
66.249.73.140	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	33
5.255.253.99	Russian Federation	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	33
66.249.73.244	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	32
204.237.22.235	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	29
66.249.73.132	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	29
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	29
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	26
92.99.252.174	United Arab Emirates	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	24
207.46.13.79	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	20
77.114.86.84	Poland	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	20

03-27-2015-00:00:08 to 03-28-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	127
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	126
184.173.183.172	United States	147.237.76.30	himush.idf.il	DVRep_P-N_40-59	Permit	113
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	79
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	48
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	30
94.126.171.132	Portugal	147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	24
85.159.206.101	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	22
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	12
81.218.251.252	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
175.44.25.203	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	8
212.34.12.150	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.190	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
176.58.77.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
41.97.37.118	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
103.246.112.221	Malaysia	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
85.250.189.52	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.22	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
99.237.226.211	Canada	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.182.226	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
72.252.37.204	Jamaica	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
94.159.152.135	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.35	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
18.239.0.155	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
79.178.11.114	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.180.144.185	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
217.243.198.68	Germany	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	2
46.117.235.53	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.141.172.14	Finland	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
175.44.7.8	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
85.25.43.94	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
216.145.95.127	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.121.128.156	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
190.18.140.167	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.106	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
89.138.233.141	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
175.44.8.190	China	147.237.77.74	law.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
67.228.95.186	United States	147.237.0.34	tikshuv.idf.il	C003: HTTP: phpMyAdmin access	Block	1
109.65.41.56	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
2.52.141.110	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.226	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
207.201.223.195	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1

03-27-2015-00:00:08 to 03-28-2015-00:00:08

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	542
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	136
79.178.120.37	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
77.126.137.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.200	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
192.116.162.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
203.115.148.214	Philippines	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	3
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
122.228.207.76	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
115.231.218.147	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
109.253.143.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
115.231.218.147	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
37.162.241.23	France	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.66.19.68	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.85.84	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
222.69.94.13	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	2
37.26.147.222	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
105.109.233.30	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	2
2.54.162.71	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
2.52.1.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.216	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.7.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.99.38	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.53	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.238.251	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
84.229.0.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
122.228.207.77	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
79.176.192.205	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.213.168	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.13	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
61.240.144.65	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	2
93.188.208.162	Russian Federation	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
115.231.218.147	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
109.253.158.201	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.187	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
109.186.5.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.14	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
37.142.74.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.218.202	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

03-27-2015-00:00:08 to 03-28-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	232
37.142.194.240	Israel	147.237.0.34	tikshuv.idf.il	Response out of state	Block HTTP Non Compliant	monitor	219
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	200
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	174
213.16.86.179	Hungary	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	89
142.105.62.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	82
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
189.32.88.90	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	62
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
84.108.27.61	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
176.12.143.24	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
90.174.2.39	Spain	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.141.94	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.129.88	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
176.12.151.167	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
199.30.25.233	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
77.171.50.176	Netherlands	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
79.181.154.11	Israel	147.237.77.243	mobile.idf.il	First packet isn't SYN	drop	drop	27
172.19.1.200		147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	27
31.186.228.95	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	26
109.253.149.153	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
204.12.251.37	United States	147.237.0.15	kosher-kravi.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	25
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.141.38	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.186.228.92	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	24
87.69.247.232	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
109.64.28.228	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
58.8.209.148	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
31.186.228.58	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	22
31.186.228.26	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	22
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
31.186.228.28	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	22
177.41.11.82	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
31.186.228.87	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	20
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
31.186.228.89	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.91	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	19
178.214.67.196	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	19
109.253.156.163	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.138.1	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.150.95	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
31.186.228.57	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	18
14.207.176.107	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.138.114	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.149.125	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.157.73	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.149.40	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
192.118.78.198	Israel	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
193.109.196.56	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to hss/	Block	14935
37.142.194.240	Israel	147.237.0.34	tikshuv.idf.il	Multiple Abnormally Long Request from 37.142.194.240	Block	436
176.12.143.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	324
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.25	Block	301
176.12.146.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
2.54.33.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
176.12.146.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
109.66.168.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/priv.dog.settings/getstatistics	Block	71
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	45
46.117.77.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	36
31.154.25.14	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 31.154.25.14	Block	31
86.108.51.195	Jordan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 86.108.51.195	Block	29
66.249.67.128	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.128	Block	22
66.249.67.120	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.120	Block	21
5.29.35.36	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	19
213.251.182.10	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	18
66.249.67.136	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.136	Block	17
66.249.79.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	17
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.102.251.11	Block	15
175.44.8.190	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 175.44.8.190	Block	15
66.249.79.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	13
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	13
175.44.8.190	China	147.237.77.74	law.idf.il	PHP Attempt	Block	11
85.64.0.107	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 85.64.0.107	Block	10
37.142.194.240	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 37.142.194.240	Block	10
213.151.48.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
2.54.162.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
84.95.198.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
85.65.221.186	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	8
46.117.217.192	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	8
178.214.67.214	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 178.214.67.214	Block	8
2.54.182.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.182.90	Block	8
37.142.207.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
79.178.22.200	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.178.22.200	Block	7
58.206.126.28	China	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 58.206.126.28	Block	7
164.138.124.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
5.29.211.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
192.151.154.82	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	6
79.182.130.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
84.228.10.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
207.46.13.102	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.102	Block	6
68.180.228.45	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	6
37.142.182.226	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 37.142.182.226	Block	6
207.46.13.30	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.30	Block	5
85.64.105.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	5
17.142.149.128	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.149.128	Block	5
217.132.111.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	5
105.109.233.30	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.109.233.30	Block	5

03-27-2015-00:00:08 to 03-28-2015-00:00:08