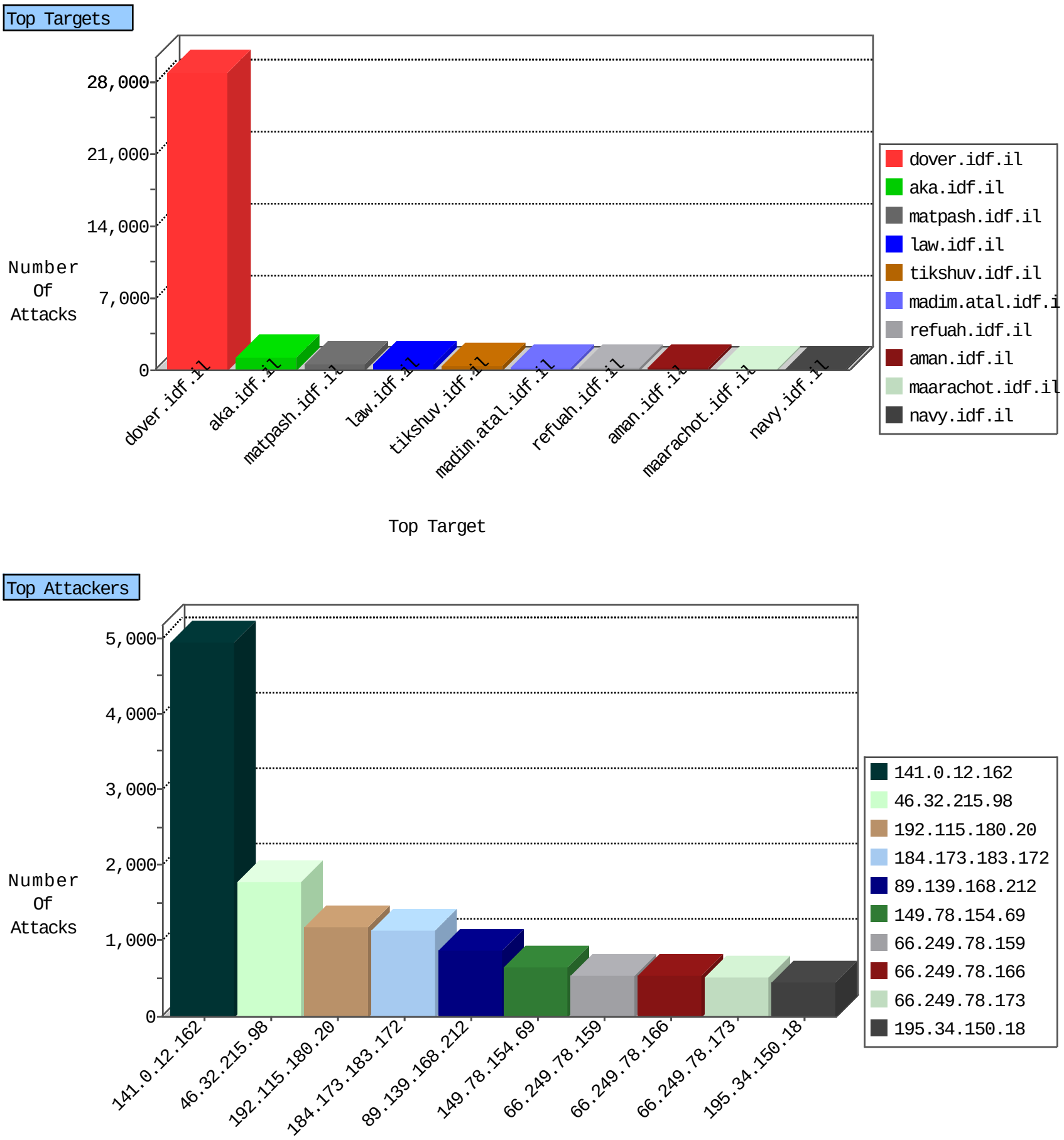
06-06-2015-00:00:04 to 06-07-2015-00:00:04

IDF Under Attack Daily Report



06-06-2015-00:00:04 to 06-07-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
197.162.53.189	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6131
220.181.108.108	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	4270
220.181.108.159	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2716
109.67.58.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	365
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	318
82.3.4.25	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	229
220.181.108.139	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	181
220.181.108.119	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	179
220.181.108.178	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	177
220.181.108.90	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	170
84.110.86.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
5.29.63.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	160
2.54.144.235	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
84.228.195.100	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
87.68.145.144	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
2.52.154.94	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	101
46.117.237.53	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	88
192.168.10.117		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	84
109.253.134.236	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	82
149.78.245.51	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
46.31.100.225	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	78
220.181.108.102	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	78
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
93.172.14.197	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
93.173.171.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
2.54.1.108	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
79.180.149.73	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
62.90.235.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
37.26.150.222	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
85.65.171.132	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
5.102.254.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	52
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	42
220.181.108.149	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	34
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
50.46.110.217	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22
213.57.112.127	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
2.54.176.201	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
89.139.168.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
192.115.180.20	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
109.253.146.72	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
149.78.32.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
46.19.85.156	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
105.103.115.235	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
64.233.172.162	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
85.65.199.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
89.139.168.212	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
114.79.29.100	Indonesia	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6

06-06-2015-00:00:04 to 06-07-2015-00:00:04

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	488
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	306
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	216
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	173
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	140
94.230.92.16	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	114
89.139.168.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	43
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	27
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	21
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	8
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	8
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	8
210.54.197.66	New Zealand	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
84.109.200.241	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	7
71.98.168.180	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
79.136.42.226	Sweden	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
46.117.166.41	Israel	147.237.0.16	my-kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	6
89.139.4.188	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	5
5.102.212.131	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
211.20.239.55	Taiwan	147.237.76.147	chinuch.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
94.102.52.27	Netherlands	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
79.182.142.94	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.50	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
46.159.132.211	Russian Federation	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4

06-06-2015-00:00:04 to 06-07-2015-00:00:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	277
192.115.180.20	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	16
66.249.64.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.64.151	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
46.121.75.145	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
109.253.145.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
192.254.200.162	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
61.49.45.46	China	147.237.77.235	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
61.49.45.46	China	147.237.76.38	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
43.255.188.134	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.135	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.134	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.135	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	3
37.26.150.172	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.135	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
5.22.130.140	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.151.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
46.120.2.93	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.15.100	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
199.203.59.121	Israel	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
79.178.181.49	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.135	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	Germany	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.135	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
199.203.59.121	Israel	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
109.64.109.153	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
207.46.13.18	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
188.138.9.51	Germany	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.171	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.131	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.86.217	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.110.81.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.130	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.40	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
46.121.81.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.123.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2

06-06-2015-00:00:04 to 06-07-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
141.0.12.162	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4956
46.32.215.98	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1788
192.115.180.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	865
89.139.168.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	811
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	661
84.228.3.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	444
5.29.123.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	431
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	402
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	366
46.19.86.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	348
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	329
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	297
91.156.185.200	Finland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	240
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	181
72.15.59.172	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	176
72.15.59.177	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	172
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	162
84.108.153.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	148
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	148
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	139
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	138
79.181.16.101	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	137
109.66.39.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	135
91.184.107.21	Georgia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	133
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	120
77.125.99.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	114
46.19.86.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
180.189.167.26		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
192.115.180.20	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	92
185.93.35.202		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	90
5.46.44.54	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	90
207.46.13.81	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	89
5.46.110.128	Turkey	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	86
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	86
82.145.216.205	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	75
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	74
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	74
149.88.146.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	73
157.55.39.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
84.111.138.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	71
137.135.176.145	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
109.42.106.69	Germany	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	68
46.19.86.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
95.220.125.219	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
80.178.136.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
86.32.24.21	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
46.19.86.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
37.142.229.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
217.250.212.94	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.210.121.29	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.210.121.29	Block	147
192.115.180.20	Israel	147.237.77.216	dover.idf.il	Too Many of the Same Response Code (404) in IP from 192.115.180.20	Block	134
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	90
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	89
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	84
80.246.136.186	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.186	Block	81
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
192.115.180.20	Israel	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
207.46.13.81	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.81	Block	27
157.55.39.240	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.240	Block	26
176.12.148.72	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.148.72	Block	22
142.4.96.178	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 142.4.96.178	Block	21
157.55.39.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.142	Block	20
84.228.173.48	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.173.48	Block	11
176.12.146.64	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.146.64	None	11
23.234.25.99	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 23.234.25.99	Block	10
157.55.39.23	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.23	Block	9
81.144.138.34	United Kingdom	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 81.144.138.34	Block	9
84.109.87.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
41.33.231.88	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	8
46.229.164.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.114	Block	8
46.229.164.111	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.111	Block	8
213.251.182.103	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	8
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	7
84.228.251.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
84.228.110.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
89.139.31.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
31.168.214.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
46.210.129.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
178.137.84.254	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	6
94.153.10.249	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	6
2.54.28.86	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
109.253.142.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	6
46.229.164.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.102	Block	6
77.125.144.99	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	6
5.9.151.67	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.9.151.67	Block	6
197.242.159.201	South Africa	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 197.242.159.201	Block	5
157.55.39.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.26	Block	5
89.139.190.85	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	5
109.160.151.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
192.115.180.20	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 192.115.180.20	Block	4
89.139.31.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	4
149.78.234.184	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
174.36.228.154	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 174.36.228.154	Block	4
109.66.143.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.78.85	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/938-he/cogat.aspx	Block	4
2.54.34.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
207.46.13.25	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.25	Block	4

06-06-2015-00:00:04 to 06-07-2015-00:00:04