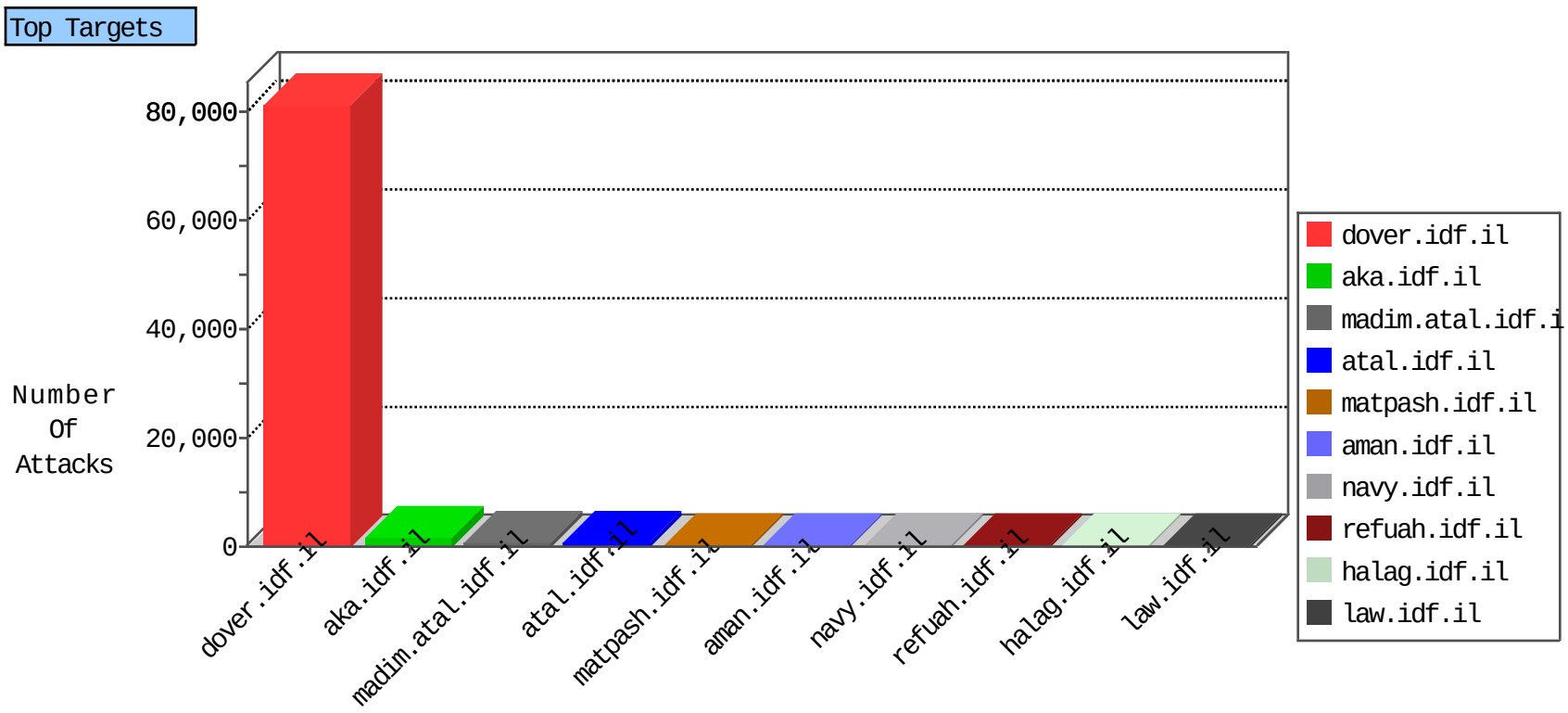
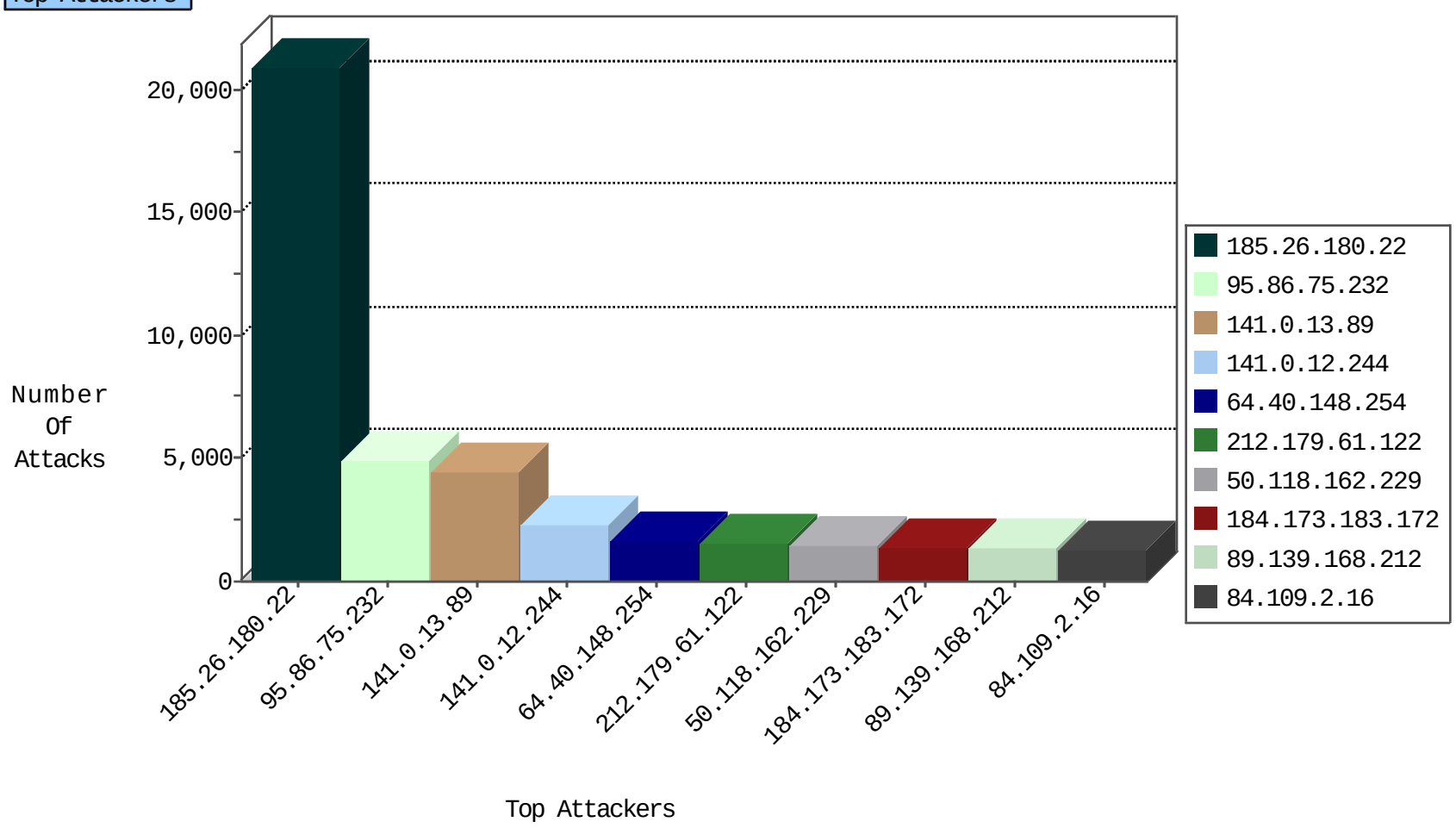
06-05-2015-00:00:08 to 06-06-2015-00:00:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



06-05-2015-00:00:08 to 06-06-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	91289
65.18.198.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	42464
217.79.247.233	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41845
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	20441
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	15815
66.249.64.55	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11063
66.249.78.18	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	10378
66.249.64.60	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10214
141.0.13.89	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10183
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	9991
66.249.64.225	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9988
185.26.180.22	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6522
66.249.64.34	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5954
210.186.54.184	Malaysia	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4344
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3524
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3080
89.139.168.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2770
220.181.108.88	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	883
66.249.64.230	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	511
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	351
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	351
41.152.117.183	Egypt	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	346
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	320
87.69.158.69	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	258
84.229.167.137	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	252
84.108.93.19	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
220.181.108.163	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	193
109.186.181.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
46.19.86.72	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
88.226.3.197	Turkey	147.237.76.86	navy.idf.il	DOS-WEB-HOIC-HTTP-80-snc	dest-reset	159
192.117.138.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
82.166.20.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
89.138.44.134	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
82.166.20.34	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
5.102.254.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
84.111.240.122	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
46.116.249.42	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
77.127.224.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
46.120.158.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
84.228.125.83	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
46.120.73.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	95
176.12.151.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
84.109.87.82	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
220.181.108.139	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	86
77.125.2.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
79.176.151.226	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
176.12.143.181	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
77.125.83.68	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79

06-05-2015-00:00:08 to 06-06-2015-00:00:08

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	535
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	443
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	248
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	170
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	94
89.139.168.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	48
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	29
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
210.186.54.184	Malaysia	147.237.77.216	dover.idf.il	C1000205: HTTP: Opisrael 2015 - key words and groups	Block	13
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
105.156.255.197	Morocco	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
79.180.100.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	8
79.180.178.26	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
79.183.52.149	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
110.85.57.3	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	6
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	6
84.110.48.49	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
79.180.119.85	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
2.54.41.192	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
5.29.167.28	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
84.94.180.35	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	4
89.105.194.76	Netherlands	147.237.77.216	dover.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
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	4
96.47.226.21	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4

06-05-2015-00:00:08 to 06-06-2015-00:00:08

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	274
88.226.3.197	Turkey	147.237.76.86	navy.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	43
91.121.89.16	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	7
91.121.89.16	France	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
61.49.45.42	China	147.237.76.86	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
61.49.45.42	China	147.237.76.30	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
66.249.93.154	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
176.12.137.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
91.121.89.16	France	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	3
95.110.228.68	Italy	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
61.49.45.47	China	147.237.77.179	e.mazi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
88.226.3.197	Turkey	147.237.76.86	navy.idf.il	ET CURRENT_EVENTS High Orbit Ion Cannon (HOIC) Attack Inbound Generic Detection Double Spaced UA	3
221.235.189.245	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
46.31.101.25	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
104.207.136.109		147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
221.235.189.245	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
46.121.113.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.249.6	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.147.54	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.183.220.8	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.133	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.245	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
79.180.37.121	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
176.12.149.84	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.135	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
37.142.93.144	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.183.128.6	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
79.179.30.24	Israel	147.237.77.74	law.idf.il	SERVER-APACHE Apache Byte-Range Filter denial of service attempt	2
5.29.91.50	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.34	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
176.12.147.120	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.148.141	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.188.135	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
79.176.222.3	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
2.54.16.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.198	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
176.12.143.181	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

06-05-2015-00:00:08 to 06-06-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.180.22	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20952
95.86.75.232	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4955
141.0.13.89	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4416
141.0.12.244	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2301
64.40.148.254	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1637
212.179.61.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1571
50.118.162.229	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1431
84.109.2.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1231
89.139.168.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1228
50.118.162.4	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	983
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	949
46.185.220.96	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	765
1.9.96.15	Malaysia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	733
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	701
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	670
84.59.179.147	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	666
66.249.75.66	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	527
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	527
66.249.75.58	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	512
37.60.47.191	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	496
95.86.122.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	465
81.218.182.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	455
66.249.75.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	424
212.25.102.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	412
50.118.162.32	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	394
95.86.65.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	374
5.102.241.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	348
199.203.240.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	346
213.57.37.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	280
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	270
177.214.32.22	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	254
87.252.254.198	Belarus	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	250
2.54.5.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	224
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	219
2.54.137.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	215
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	210
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	207
85.17.24.66	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	206
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	199
131.137.245.207	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	195
66.87.131.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	189
64.21.103.106	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	188
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	175
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	174
46.19.86.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	168
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	162
199.190.46.194	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	154
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	150
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	150
194.56.4.51	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	149

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.148.180	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.180	Block	403
79.178.138.16	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.138.16	Block	189
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	134
77.126.168.43	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	76
77.125.212.178	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.212.178	Block	61
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	33
157.55.39.240	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.240	Block	31
79.183.27.242	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.183.27.242	Block	24
46.210.140.80	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.210.140.80	Block	23
207.46.13.81	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.81	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
66.249.75.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	20
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.58	Block	20
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	19
157.55.39.24	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.24	Block	16
157.55.39.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.142	Block	14
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	13
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	12
84.228.173.48	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.173.48	Block	12
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.74	Block	11
188.120.148.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	10
37.46.39.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	9
37.26.150.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
37.26.150.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
84.108.51.198	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	7
95.86.103.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
91.121.89.16	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
176.12.144.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
79.180.15.247	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.180.15.247	Block	6
109.67.22.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
109.160.188.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
85.65.20.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
79.180.107.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
77.6.233.32	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.6.233.32	Block	5
79.177.6.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	5
87.68.18.159	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
84.94.20.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
109.65.194.239	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
109.66.121.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
185.86.143.113		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	5
77.127.172.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
91.121.89.16	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	5
79.178.186.115	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
37.26.150.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	4
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	4
164.138.120.201	Israel	147.237.0.16	my-kosher-kravi.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 164.138.120.201	None	4
5.22.129.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4