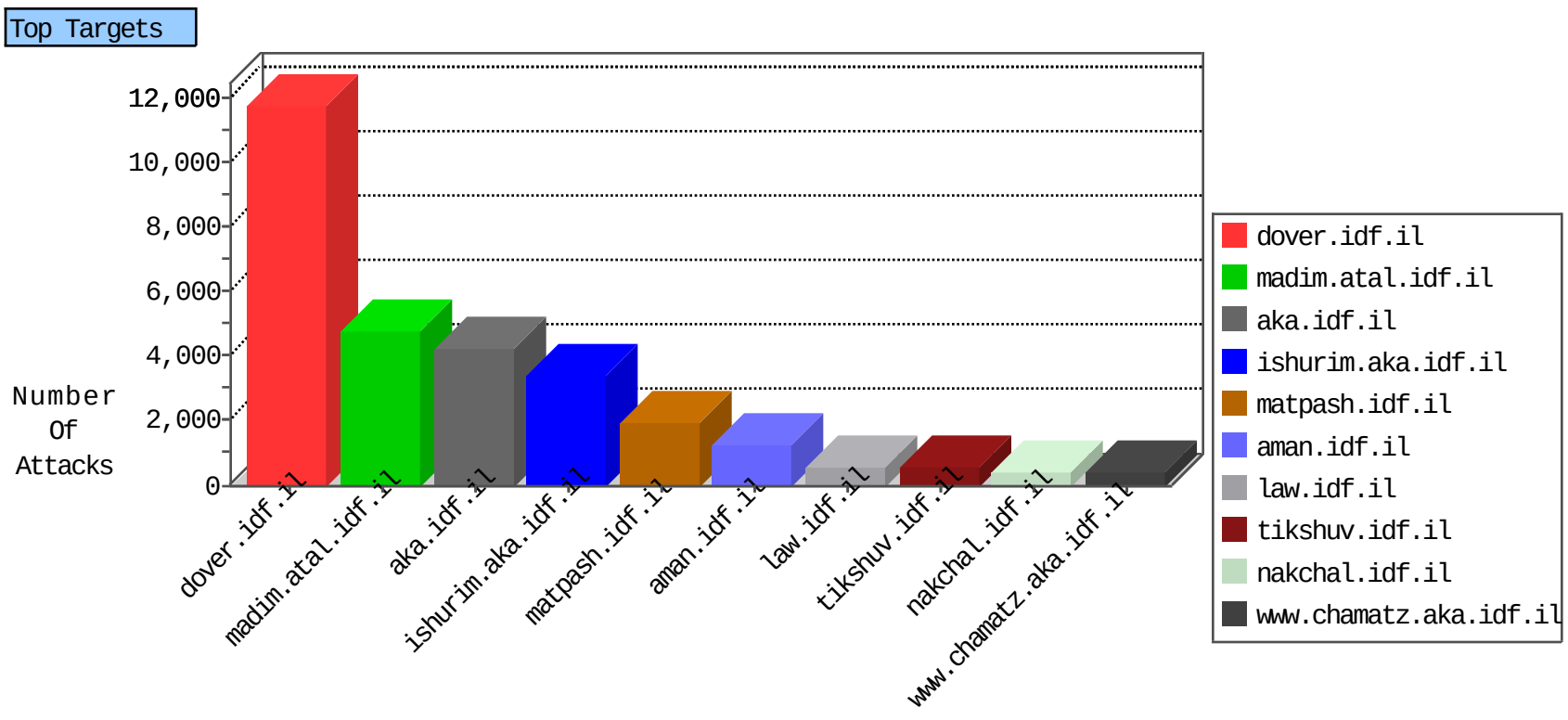
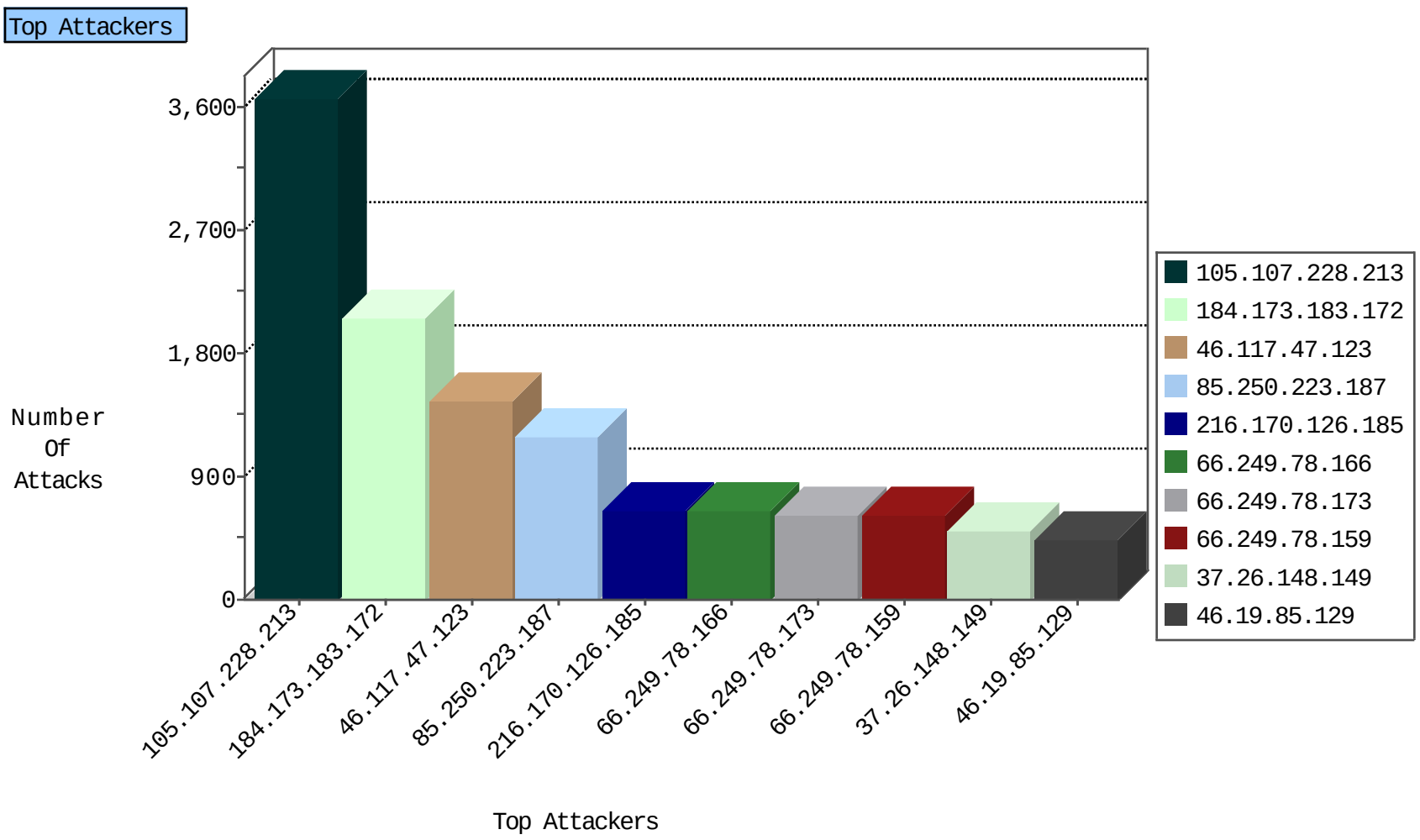
03-02-2015-00:00:07 to 03-03-2015-00:00:07

IDF Under Attack Daily Report





03-02-2015-00:00:07 to 03-03-2015-00:00:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
105.107.228.213	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	19593
66.249.78.25	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2866
109.65.170.243	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1459
79.183.207.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1117
46.120.146.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	591
46.120.38.234	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	588
37.142.76.187	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	564
46.116.171.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	563
185.13.194.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	432
84.110.8.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	386
93.172.168.151	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	367
5.102.193.85	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	364
46.19.85.198	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	330
79.178.20.161	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	303
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	276
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	271
109.160.241.207	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	249
93.172.144.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
5.29.216.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	220
79.177.31.159	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	206
149.78.81.63	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	188
31.210.186.139	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	184
46.19.85.250	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	182
37.60.43.116	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	175
2.54.171.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
89.139.161.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
46.121.142.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
213.8.46.1	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	161
2.54.47.103	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	151
79.178.20.161	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	146
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
31.44.143.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
188.120.148.191	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
164.138.122.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
79.179.33.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
149.78.72.227	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	124
185.32.179.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	117
109.186.185.4	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	116
31.210.186.139	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
46.19.85.216	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	109
109.186.73.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
85.64.195.229	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
46.117.136.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
213.57.46.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
37.26.148.196	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
79.181.125.142	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
85.64.231.196	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	83
93.172.183.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
2.54.39.159	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
93.173.39.104	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75

03-02-2015-00:00:07 to 03-03-2015-00:00:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	854
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	681
216.170.126.185		147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	651
112.198.90.34	Philippines	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	324
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	307
184.173.183.172	United States	147.237.76.31	nakchal.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	139
91.228.248.251	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
81.218.251.251	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
41.239.119.199	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	21
213.229.69.40	United Kingdom	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	11
81.209.103.101	Finland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
84.228.38.82	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
46.117.152.65	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
85.250.188.145	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.19.85.129	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
81.218.251.250	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.251.250	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.135.131	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	5
147.236.238.70	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.181.16.121	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
75.63.16.98	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	4
207.232.27.5	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4
216.183.158.254	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	4
62.128.35.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
175.142.88.137	Malaysia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	3
192.114.91.244	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3
109.66.137.213	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3
77.127.212.221	Israel	147.237.76.30	himush.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	3
106.138.51.199	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	3

03-02-2015-00:00:07 to 03-03-2015-00:00:07

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	355
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	132
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
109.66.29.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.19.85.38	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
66.249.93.131	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
122.228.207.190	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
84.108.166.142	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.160.183.62	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.190	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
46.19.86.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.213.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.190	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
85.65.57.232	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.190	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
122.228.207.190	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
5.29.231.71	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.176.166.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.134.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.127.238.29	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.142.211.164	Spain	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
122.228.207.190	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
109.66.8.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
209.88.157.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.127.180.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.168.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.27	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.183.108.249	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.150.219	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.65.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.183.128.6	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
115.231.218.147	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
85.130.245.123	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.190	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
79.181.48.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.190	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
79.177.35.133	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.190	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
89.138.228.88	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.94.191	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.193.134	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.22.129.130	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
77.127.196.71	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.142.211.164	Spain	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
81.218.156.98	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.91.141	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
79.183.161.195	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.130.176	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

03-02-2015-00:00:07 to 03-03-2015-00:00:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
85.250.223.187	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1182
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	504
37.26.148.149	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	504
46.117.47.123	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	485
46.117.47.123	Israel	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	485
46.117.47.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	485
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	478
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	478
46.22.133.232	Ireland	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	374
91.198.204.122	Denmark	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	254
75.70.21.209	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	215
217.66.234.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	178
207.241.237.166	United States	147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	174
187.57.216.223	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	174
81.209.103.101	Finland	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	102
95.85.156.184		147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	90
68.119.35.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	82
83.249.134.4	Sweden	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	81
212.143.120.175	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	65
37.26.146.229	Israel	147.237.76.42	refuah.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
78.83.74.125	Bulgaria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
79.180.32.203	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
199.203.179.99	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	53
85.250.77.136	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	48
212.199.76.148	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
212.150.94.254	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
62.219.142.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.137.253	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
62.90.35.105	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
212.150.7.49	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	37
109.253.147.148	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
152.91.10.22	Australia	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	34
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
79.180.176.15	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	33
217.132.201.255	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	33
176.12.136.68	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.134.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.147.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.159.192	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.149.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.137.233	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
185.32.177.253	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	29
185.32.177.253	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	29
185.32.177.253	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	29
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	28
46.19.85.167	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	426
80.246.137.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	392
2.54.31.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	377
2.54.48.1	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.48.1	Block	376
2.54.154.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	359
2.54.59.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	305
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	286
80.246.137.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	259
79.176.37.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	255
2.54.22.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	228
5.22.129.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	186
31.210.186.139	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 31.210.186.139	Block	184
37.26.147.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	135
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	130
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	126
109.253.140.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	121
176.12.144.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	115
176.12.148.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
37.26.148.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
176.12.145.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
109.253.140.24	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.140.24	Block	62
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	42
176.12.148.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
176.12.139.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
109.253.140.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
212.199.76.254	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	30
17.142.144.105	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.144.105	Block	20
109.253.145.2	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.145.2	Block	19
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	18
66.249.64.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.142	Block	16
17.142.151.92	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.92	Block	15
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.126	Block	14
17.142.148.12	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.148.12	Block	14
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.134	Block	13
95.86.109.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
17.142.152.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.43	Block	13
17.142.151.174	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.174	Block	13
185.32.178.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
17.142.150.184	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.150.184	Block	12
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.127	Block	12
109.67.175.103	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	12
17.142.152.145	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.145	Block	11
2.52.184.222	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	10
17.142.152.130	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.130	Block	9
17.142.151.140	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.140	Block	9
84.228.58.240	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.228.58.240	Block	9
212.179.21.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
95.86.78.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9