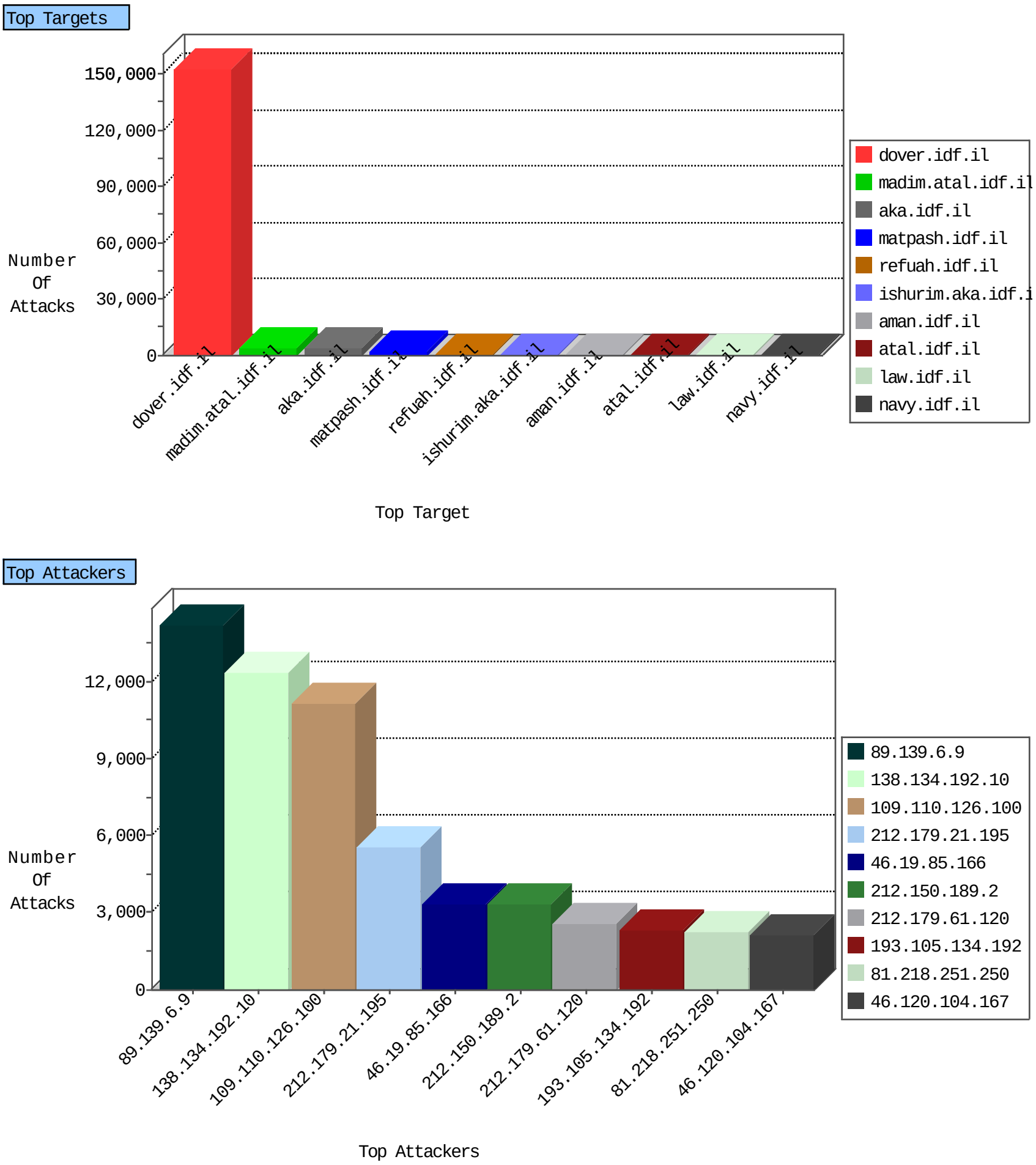
04-17-2015-00:00:03 to 04-18-2015-00:00:03

IDF Under Attack Daily Report



04-17-2015-00:00:03 to 04-18-2015-00:00:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	7864
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5423
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4843
109.110.126.100	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4422
66.249.67.23	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4281
66.249.67.24	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3961
166.137.8.45	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3447
220.181.108.118	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3321
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3282
93.173.14.174	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3183
66.249.67.34	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2885
108.211.78.223	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2518
66.249.67.157	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1073
66.249.67.33	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	933
83.130.113.24	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	923
213.57.105.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	845
220.181.108.151	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	809
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	664
138.134.192.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	517
220.181.108.179	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	474
220.181.108.87	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	413
220.181.108.146	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	402
220.181.108.89	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	390
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	350
84.110.60.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	331
84.108.65.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	330
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	293
50.17.173.39	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	238
79.177.31.71	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	235
84.109.210.29	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	195
204.93.154.199	United States	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	172
84.110.86.59	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
66.249.67.31	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	148
132.72.229.37	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	117
213.57.57.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
46.19.85.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	115
85.65.39.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
149.78.140.224	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
46.116.206.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
79.182.138.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
149.78.74.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
2.54.136.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
2.54.11.68	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
109.253.149.243	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	78
80.246.137.53	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	77
85.250.198.251	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
168.235.194.180		147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
85.64.79.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
93.173.227.96	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	73

04-17-2015-00:00:03 to 04-18-2015-00:00:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
193.105.134.192	Sweden	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2300
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	382
221.10.102.199	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	327
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	223
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	150
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	113
146.148.125.210		147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	32
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
221.10.102.199	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	18
119.30.35.180	Bangladesh	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	7
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	7
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	7
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	7
212.34.12.145	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.66.102.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.111.240.252	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.151	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	6
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	6
81.218.251.252	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
149.78.135.192	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
190.17.51.210	Argentina	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.236.119	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	6
212.34.12.129	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	5
46.116.246.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	5
180.76.5.193	China	147.237.0.19	madim.atal.idf.il	DVRep_P-N_40-59	Permit	5
188.138.9.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
85.64.162.45	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4

04-17-2015-00:00:03 to 04-18-2015-00:00:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	1066
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	201
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	133
66.249.67.89	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	70
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	18
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	18
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	18
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	16
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	10
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
46.43.106.159	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	5
93.190.92.127	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
77.126.137.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
221.235.188.212	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	4
66.249.67.49	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.5	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	4
52.4.243.253	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
66.249.78.137	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.12	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	4
221.235.188.212	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	4
66.249.79.73	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
52.6.13.145	United States	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
221.235.188.212	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.212	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.212	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.212	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.212	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	3
221.235.188.212	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	3
122.228.207.77	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.212	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	3
221.235.188.210	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	3
221.235.188.212	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
221.235.188.212	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.141	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.243	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.121.99.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.158.222	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.202	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
221.235.188.210	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
37.26.147.173	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
46.120.24.6	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.157	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.89	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2

04-17-2015-00:00:03 to 04-18-2015-00:00:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
89.139.6.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14237
138.134.192.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12361
109.110.126.100	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10963
212.179.21.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5535
46.19.85.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3371
212.150.189.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3321
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2584
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2267
46.120.104.167	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2130
37.142.184.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1999
195.28.82.69	Slovakia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1943
46.19.86.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1735
82.145.221.137	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1625
92.103.133.164	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1264
94.159.154.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1253
195.28.82.137	Slovakia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1204
5.28.165.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1177
95.86.70.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1059
79.178.188.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	978
77.127.84.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	915
95.86.118.96	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	875
62.90.107.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	801
84.108.246.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	689
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	640
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	632
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	628
164.138.127.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	615
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	598
95.86.121.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	585
46.19.86.174	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	574
2.54.56.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	562
46.116.246.201	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	549
134.173.78.2	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	548
212.179.61.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	516
87.68.22.101	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	514
5.29.26.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	507
212.45.46.32	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	456
149.78.186.96	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	437
213.57.188.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	435
212.76.105.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	428
212.179.46.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	412
212.76.105.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	410
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	370
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	354
38.99.190.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	346
37.26.147.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	345
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	336
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	329
37.26.147.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	323
31.168.214.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	321

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.139.53.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	971
87.68.78.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	560
109.66.0.65	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.0.65	Block	448
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	439
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	339
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	307
2.54.167.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	303
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	301
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	300
109.253.136.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	240
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.22	Block	218
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.219	Block	204
46.116.212.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	159
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	108
185.32.177.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	100
80.246.138.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	96
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.126	Block	90
46.19.85.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	61
149.78.238.249	United States	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 149.78.238.249	Block	60
80.246.141.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
185.32.178.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	39
79.176.13.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
87.69.41.39	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 87.69.41.39	Block	37
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	34
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	32
77.127.95.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	29
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	26
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.45	Block	26
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	22
125.65.112.121	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.112.121	Block	21
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	18
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	18
172.56.29.114	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	15
105.158.173.189	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.158.173.189	Block	12
109.64.186.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
66.249.67.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
88.97.23.136	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
207.46.13.133	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
149.78.82.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
93.172.136.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.93.245	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	8
2.54.173.156	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
185.13.195.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
5.102.199.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7