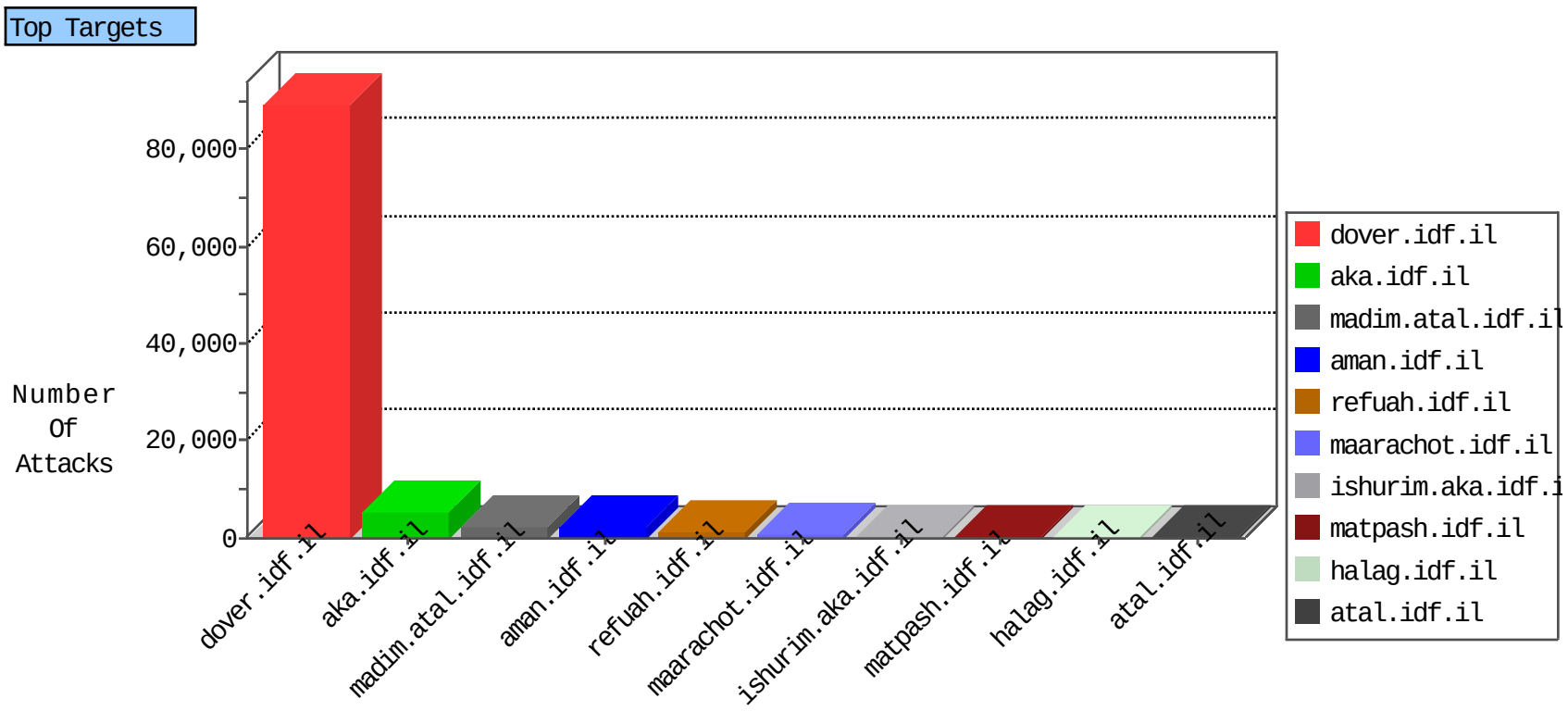
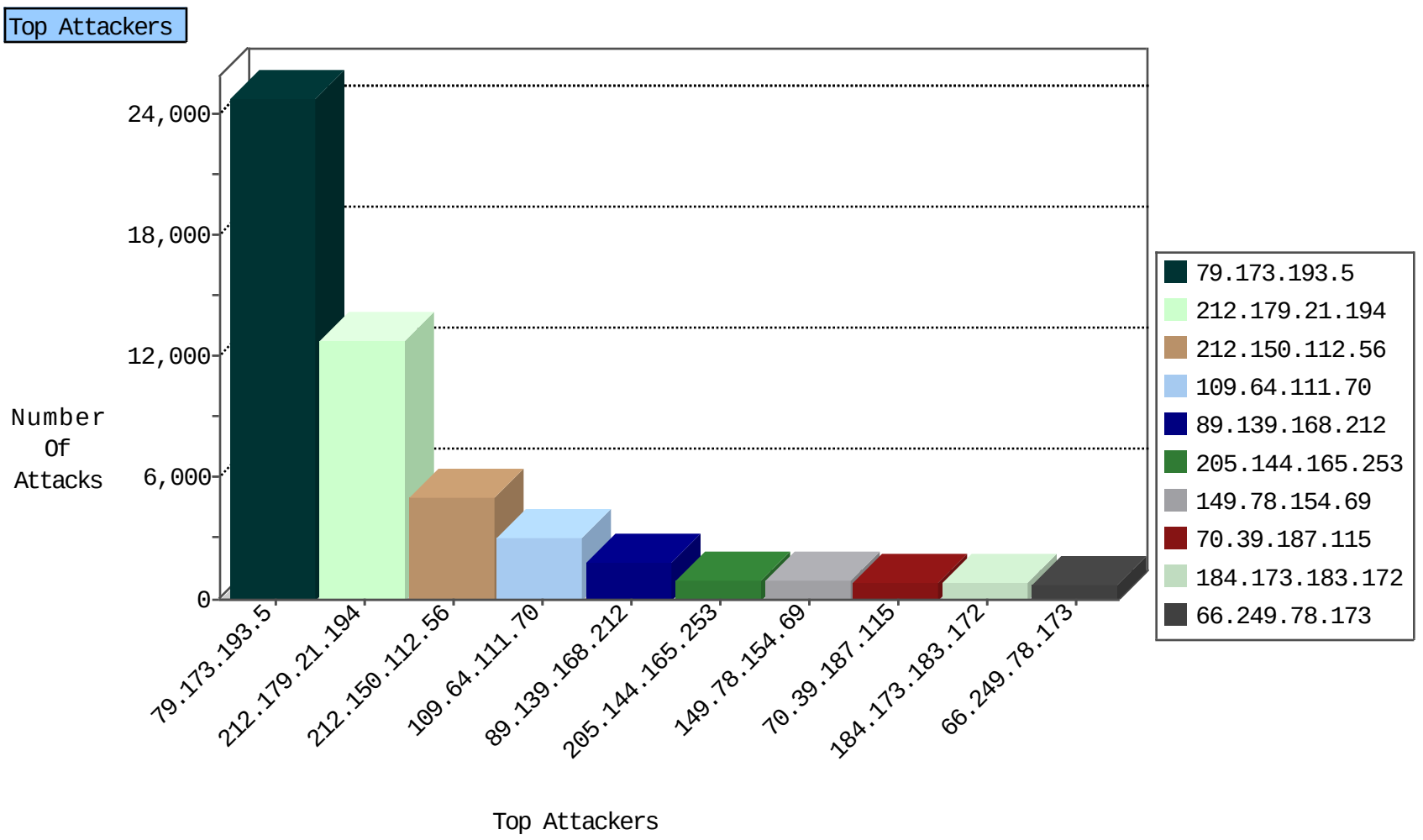
06-10-2015-00:00:04 to 06-11-2015-00:00:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



06-10-2015-00:00:04 to 06-11-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	13517
66.249.79.79	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9518
66.249.64.151	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	6687
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2793
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1354
5.29.157.92	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1223
66.249.79.243	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1170
66.249.79.53	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1136
81.218.37.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	692
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	598
46.19.86.13	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	427
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	393
109.64.12.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	390
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	377
5.28.181.20	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	354
212.199.154.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	341
46.120.158.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	312
54.244.22.103	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	311
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	277
81.218.126.226	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	267
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	238
188.120.148.146	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	222
46.121.248.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	222
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
84.228.195.100	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
220.181.108.145	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	178
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
109.67.184.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	169
52.28.101.18	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	157
5.29.75.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	146
82.80.156.16	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	140
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	136
176.12.136.3	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
5.29.7.28	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
77.126.117.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
79.173.193.5	Jordan	147.237.77.216	dover.idf.il	DOS-WEB-HOIC-HTTP-80-snc	dest-reset	114
82.166.20.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
217.14.208.54	Croatia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	112
79.177.113.94	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
109.186.181.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
2.54.30.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
220.181.108.76	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	106
37.26.147.192	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
79.173.193.5	Jordan	147.237.77.216	dover.idf.il	DOS-HOIC-TCP-80-gbo	forward	96
84.95.199.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
220.181.108.178	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	94
132.76.10.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89

06-10-2015-00:00:04 to 06-11-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.111.70	Israel	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	1566
109.64.111.70	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1441
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	411
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	236
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	190
184.173.183.172	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_P-N_40-59	Permit	133
64.79.144.10	United States	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	50
197.35.6.247	Egypt	147.237.77.216	dover.idf.il	C1000203: HTTP: Thorshammer - Post to root dir	Block	29
89.139.168.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	25
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
138.134.102.16	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
212.199.112.144	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
2.52.172.255	Israel	147.237.72.166	aka.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	11
121.146.93.228	Korea, Republic of	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	8
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	7
2.54.14.108	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
192.118.78.57	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	7
77.127.203.182	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
46.19.85.197	Israel	147.237.77.216	dover.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	7
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	6
31.154.2.82	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.177.54.219	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.183.239.58	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
77.234.44.184	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
109.67.54.95	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.89	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
82.80.219.164	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
37.142.235.37	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	5
93.172.31.6	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.57.62.193	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	5
46.19.85.169	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	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

06-10-2015-00:00:04 to 06-11-2015-00:00:04

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	142
37.238.116.28	Iraq	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	87
2.52.32.234	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	18
176.12.145.61	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	16
91.106.207.102	Russian Federation	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
89.139.168.212	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	4
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	3
95.110.228.68	Italy	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
207.46.13.30	United States	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
176.12.143.130	Israel	147.237.72.166	aka.idf.il	INDICATOR-SCAN myscan	2
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.21	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
199.203.59.121	Israel	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
199.203.59.121	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
2.52.42.187	Israel	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
176.12.143.130	Israel	147.237.72.166	aka.idf.il	GPL SCAN myscan	2
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
61.183.128.6	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
81.218.77.162	Israel	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	2
221.235.189.244	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
85.250.198.145	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.179.89.90	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	Cote D'Ivoire	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.137.95.121	Ireland	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
124.158.5.131	Vietnam	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
2.54.165.90	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.20		147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
77.127.152.159	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.155	Taiwan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.146.42	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.188.132	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
116.231.218.102	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.135	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.238.82.119	Ukraine	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.235.189.244	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
62.0.34.177	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.59.121	Israel	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

06-10-2015-00:00:04 to 06-11-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.173.193.5	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24611
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12626
212.150.112.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5018
89.139.168.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1707
205.144.165.253	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	997
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	933
70.39.187.115	Satellite Provide	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	836
85.65.52.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	734
77.126.253.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	725
95.211.225.201	Netherlands	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	686
167.114.156.198	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	659
70.39.185.41	Satellite Provide	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	619
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	542
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	517
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	515
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	474
82.132.244.222	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	469
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	456
199.116.175.105	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	450
132.76.61.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	440
54.244.22.103	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	418
200.53.156.250	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	355
79.179.121.34	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	345
132.76.61.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	293
37.238.116.28	Iraq	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	279
212.199.57.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	278
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	275
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	274
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	272
46.19.86.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	270
46.19.86.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	269
41.234.41.61	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	253
2.52.153.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	225
46.246.5.35	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	224
195.3.144.108	Latvia	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	204
93.173.39.140	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	193
136.243.36.97	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	190
80.243.189.232	United Kingdom	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	185
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	183
184.101.181.54	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	177
47.19.130.146	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	167
93.173.152.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	165
207.158.41.99	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	164
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	162
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	161
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	154
207.232.55.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	149
12.139.185.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	145
203.116.187.1	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	143

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.23	Block	317
109.253.139.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	227
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	213
109.253.147.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	200
2.54.131.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	179
109.253.158.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.158.99	Block	173
176.12.147.252	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.147.252	Block	150
46.19.86.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	144
2.54.45.254	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.45.254	Block	128
176.12.148.113	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.148.113	Block	78
37.26.147.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
109.253.158.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
176.12.146.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
80.246.137.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
109.253.133.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
2.54.178.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	37
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	32
80.246.136.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
80.246.136.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
80.246.136.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
80.246.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
80.246.136.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	19
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	19
2.52.143.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
79.181.141.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
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	15
80.246.137.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
80.246.137.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
46.19.85.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	13
2.52.56.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	13
95.86.67.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/webresource.axd	Block	12
46.19.85.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
109.64.98.164	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	10
37.26.147.200	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.200	Block	9
46.19.86.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
84.108.172.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
37.142.71.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
79.180.163.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
79.178.205.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
200.53.156.250	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
109.64.22.76	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
46.19.86.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
2.54.17.246	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.17.246	Block	6
176.12.138.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
93.173.228.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
109.253.131.228	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6

06-10-2015-00:00:04 to 06-11-2015-00:00:04