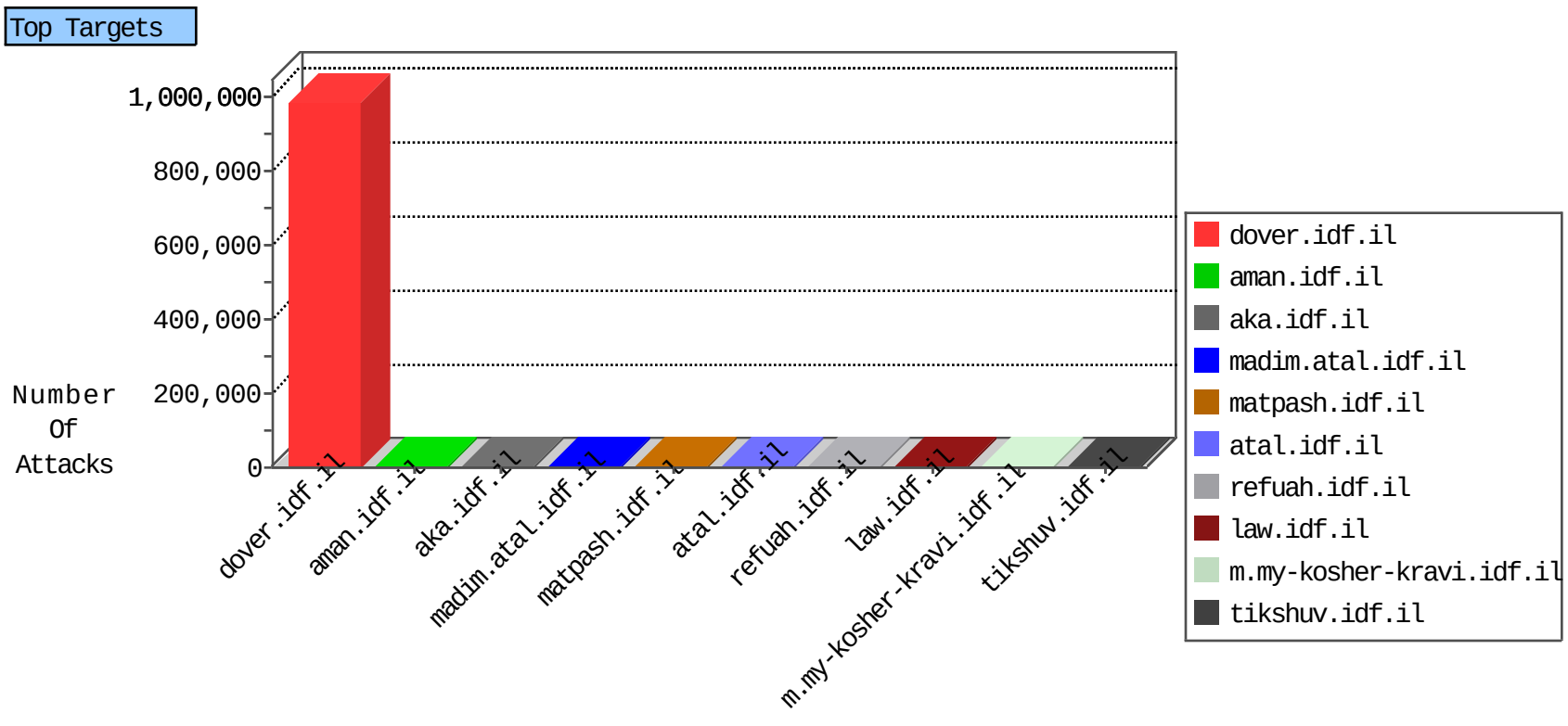
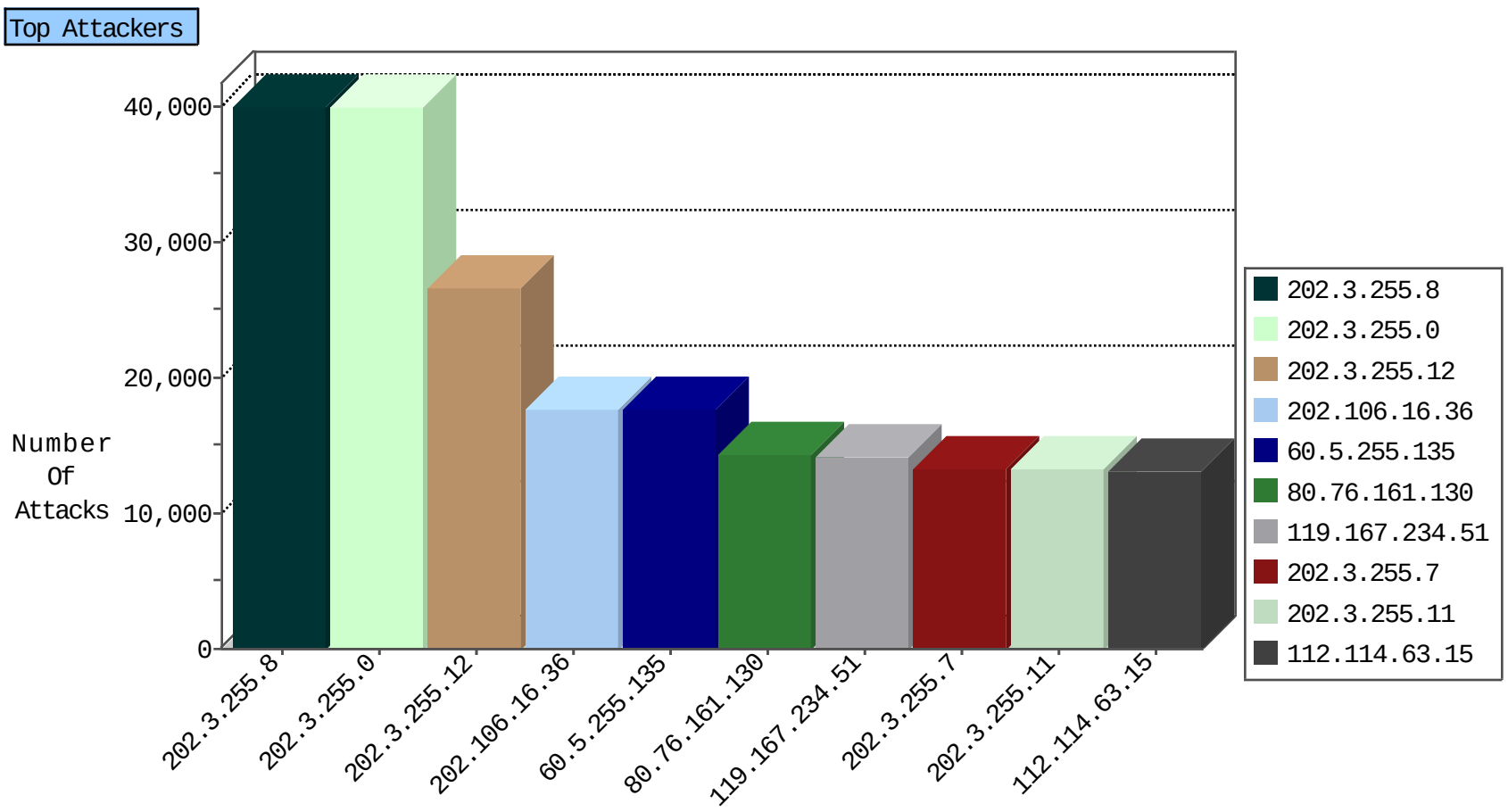
08-01-2015-00:00:07 to 08-02-2015-00:00:07

IDF Under Attack Daily Report



Top Target



Top Attackers

08-01-2015-00:00:07 to 08-02-2015-00:00:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	483530
66.249.78.62	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	364061
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	257859
66.249.65.92	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	186567
65.19.138.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	160425
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	83162
66.249.67.34	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	56459
98.110.222.170	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	44055
66.249.67.79	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	39443
199.115.115.209	United States	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	32689
66.249.64.151	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	32196
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	29638
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26601
66.249.65.47	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16522
62.163.165.130	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14701
66.249.65.94	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9003
66.249.65.95	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6320
66.249.64.156	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	4219
2.92.131.88	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4163
111.1.39.226	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	3461
199.115.115.209	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	3187
54.244.22.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3136
66.249.65.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3042
66.249.65.14	Israel	147.237.77.243	mobile.idf.il	TCP handshake violation, first packet not syn	drop	2868
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2773
89.138.227.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2645
84.228.32.88	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2508
184.72.191.180	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2473
199.115.115.209	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2202
81.137.247.232	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1864
46.120.131.152	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1446
220.165.10.41	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	1442
131.253.25.230	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1264
112.17.1.16	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	1178
119.167.234.51	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	1175
183.95.132.175	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	1126
112.114.63.15	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	1103
60.5.255.135	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	1102
202.106.16.36	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	991
115.231.40.92	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	917
119.145.151.55	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	876
222.222.193.3	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	816
218.7.121.201	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	750
79.179.57.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	720
117.25.149.19	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	713
219.146.66.45	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	691
220.168.133.35	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	639
199.115.115.209	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	632
218.7.132.15	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	614
111.1.56.19	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	607

08-01-2015-00:00:07 to 08-02-2015-00:00:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.120.148.145	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	31
58.150.60.91	Korea, Republic of	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	21
213.139.52.85	Jordan	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
58.150.60.91	Korea, Republic of	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
93.172.40.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
213.139.52.85	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
92.104.231.234	Switzerland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.250.131.208	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
149.78.57.68	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
89.138.230.76	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.182.125.175	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
108.231.22.57	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.177.111.200	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
92.110.216.85	Netherlands	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
82.192.95.163	Netherlands	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
82.81.240.106	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
93.173.60.139	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
67.67.175.86	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.110.212.59	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.64.177.12	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
62.90.152.189	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.181.61.144	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
197.117.165.80	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.253.87.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
209.213.104.25	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
46.121.91.9	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.175.153	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.70	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.172.61.87	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.229.188.158	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.246	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
87.69.125.177	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.253	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.253.93.113	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.166.70.69	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.25	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
185.12.187.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.246.136.157	Israel	147.237.72.167	ishurim.aka.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
197.7.222.176	Tunisia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.117.196.230	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.64	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.28.160.18	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
87.68.33.183	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
98.214.101.150	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
81.218.174.190	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.142.64.178	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
54.148.33.22	United States	147.237.72.166	aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
176.12.141.105	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1

08-01-2015-00:00:07 to 08-02-2015-00:00:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
202.3.255.8	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	37265
202.3.255.0	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	37233
202.3.255.12	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	24852
202.3.255.7	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	12429
202.3.255.11	French Polynesia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	12361
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	127
61.148.115.22	China	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	34
41.140.8.185	Morocco	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	8
46.19.85.247	Israel	147.237.77.233	atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
176.12.151.234	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
196.206.88.192	Morocco	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
197.207.52.70	Algeria	147.237.77.216	dover.idf.il	XSS - IMG (POST)	4
66.249.65.95	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
41.140.8.185	Morocco	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
45.114.11.47		147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	3
221.203.3.117	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.47		147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.44		147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.47		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	3
196.206.88.192	Morocco	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	3
45.114.11.44		147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.47		147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.44		147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	3
221.203.3.117	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.44		147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	3
221.203.3.117	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.44		147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.47		147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
197.207.52.70	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP encoded cross site scripting HTML Image tag attempt	2
113.175.193.73	Vietnam	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	2
66.249.83.141	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
221.203.3.117	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
2.54.151.227	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
45.114.11.46		147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
41.140.8.185	Morocco	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
45.114.11.47		147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.199	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.47		147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.44		147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
177.93.68.60		147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2

08-01-2015-00:00:07 to 08-02-2015-00:00:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
202.106.16.36	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17515
60.5.255.135	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17486
119.167.234.51	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14068
80.76.161.130	Qatar	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13733
112.114.63.15	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13042
220.165.10.41	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12715
218.7.121.201	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11848
119.145.151.55	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10077
117.25.149.19	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9752
117.25.148.140	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9676
60.5.255.143	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9513
119.167.197.118	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9409
220.168.133.55	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9275
218.61.39.37	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9038
115.231.40.92	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9012
119.167.197.110	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8693
120.192.84.226	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8639
183.95.132.175	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8328
120.192.88.86	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7611
218.7.132.15	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7413
183.232.82.133	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7287
219.146.66.45	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7073
111.1.56.19	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6914
222.222.193.3	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6870
118.123.203.164	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6318
218.7.121.203	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6266
60.211.211.47	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6230
119.145.151.31	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6204
220.170.79.46	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6130
220.168.133.35	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6103
120.192.84.235	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6032
120.192.84.239	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5903
117.25.148.152	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5891
223.99.253.144	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5688
117.25.149.25	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5442
163.177.21.73	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5320
112.17.1.16	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5150
218.205.79.117	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4958
119.167.234.57	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4862
200.54.109.220	Chile	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4814
120.192.88.89	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4808
182.247.242.87	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4603
199.115.115.209	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4473
218.205.79.199	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4360
183.129.177.243	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4341
182.247.240.35	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4296
183.95.132.174	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4151
119.167.197.108	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4110
190.203.82.88	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4104
113.107.99.49	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4042

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.121.62.155	Netherlands	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	670
85.64.80.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.80.99	Block	612
66.249.65.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.95	Block	442
66.249.65.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.89	Block	406
213.57.104.198	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.104.198	Block	392
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.92	Block	376
24.153.241.93	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	290
218.46.25.115	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	290
117.239.50.210	India	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	214
109.65.168.149	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.65.168.149	Block	212
2.54.36.84	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.36.84	Block	190
80.76.161.130	Qatar	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 80.76.161.130	Block	102
80.76.161.130	Qatar	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 80.76.161.130	Block	102
80.76.161.130	Qatar	147.237.77.216	dover.idf.il	Multiple Malformed URL from 80.76.161.130	Block	102
80.76.161.130	Qatar	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 80.76.161.130	Block	102
220.255.3.186	Singapore	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	100
212.43.104.56	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	68
109.65.191.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	58
54.68.70.105	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	50
186.88.53.209	Venezuela	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	42
37.142.196.243	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	38
207.91.10.234	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	34
93.173.11.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.173.11.233	Block	32
84.95.49.154	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.49.154	Block	32
109.186.1.93	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.186.1.93	Block	30
109.66.133.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/resources/images/	Block	24
186.89.134.128	Venezuela	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
190.74.70.112	Venezuela	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
62.201.200.13	Iraq	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
221.204.223.248	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
46.121.114.155	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	20
54.68.191.66	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
37.142.196.243	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	20
120.192.88.84	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
120.192.88.86	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
117.187.10.140	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
66.249.65.92	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	18
59.90.132.207	India	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
190.207.183.119	Venezuela	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
218.205.79.207	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
176.13.0.228	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	16
120.192.88.85	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
111.1.56.11	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
221.204.223.245	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
37.142.226.233	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	14
109.64.142.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
62.219.155.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
72.14.199.124	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
218.205.79.205	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12