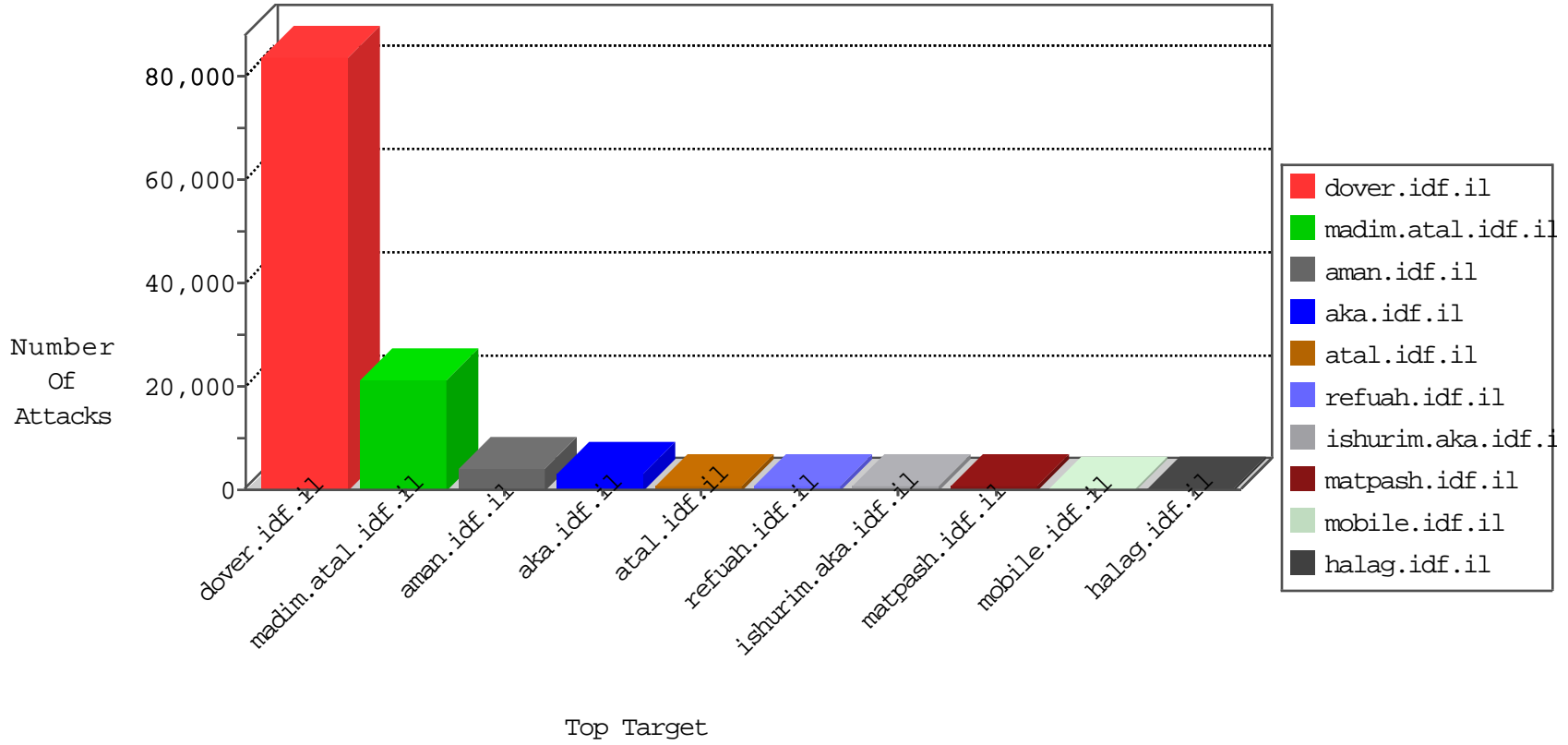


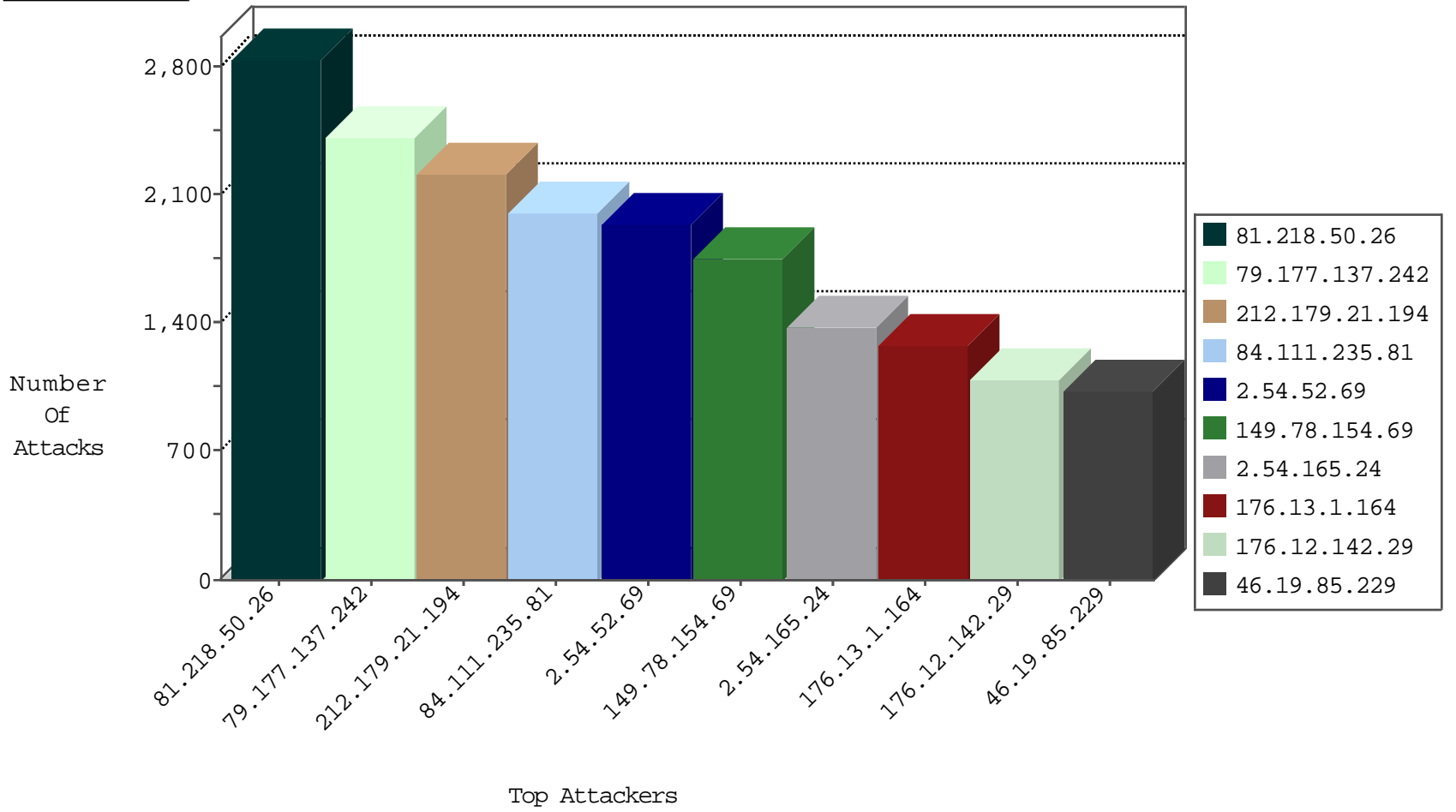
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
46.19.85.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	2698
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2511
80.178.164.222	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	975
66.249.69.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	589
31.154.92.151	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	381
85.250.92.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	362
79.176.165.78	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	358
46.117.233.12	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	349
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	305
194.90.167.81	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	300
81.218.181.240	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	295
77.127.26.79	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	259
77.126.14.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	239
109.64.34.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	223
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
95.86.114.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	207
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
109.64.12.236	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
213.57.209.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
84.229.187.69	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
46.120.102.218	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	174
46.120.21.70	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	169
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
46.120.34.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
149.88.3.168	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	158
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	156
79.181.33.233	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	135
164.138.127.3	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	129
85.250.230.142	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
79.182.153.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
5.29.28.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
81.218.46.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
2.54.147.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	92
89.138.231.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
79.178.215.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
84.229.116.168	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
37.26.146.237	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
80.246.136.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
37.142.210.42	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
79.181.61.94	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
109.65.215.110	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
46.19.85.71	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	59
192.116.54.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	46
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	42
46.19.85.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	36
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	36
174.109.38.159	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	34

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.250.92.188	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	22
194.90.167.81	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	19
77.126.14.48	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	16
77.127.162.62	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	14
138.134.102.16	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	14
138.134.102.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
109.67.201.223	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
37.142.64.69	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
85.250.65.52	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.158	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.109.224.205	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.200	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.64.26.92	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.177	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
213.57.45.243	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
132.74.210.232	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
189.203.218.251	Mexico	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.134	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.143.120.84	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.152	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.116.207.229	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.177.25.117	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
31.168.25.209	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.51	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
81.218.26.138	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
181.46.154.27	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.117.128.149	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.111.83.139	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.183.32.155	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
115.195.47.206	China	147.237.77.216	dover.idf.il	16527: TCP: Evaluated Base64 PHP Code	Permit	3
185.32.179.247	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
2.54.145.128	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
2.54.179.39	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
105.235.128.183	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
62.82.15.26	Spain	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.172	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
176.221.120.210	Poland	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.172.150.87	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.22.129.203	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
91.205.174.145	Germany	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
79.182.194.80	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.160.213.83	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.121.134.167	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.250.65.52	Israel	147.237.0.15	kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.64.60.69	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.29.223.233	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.102.141.250	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.168	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

Top Attackers In ID

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	96
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	6
66.249.75.134	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
45.114.11.47		147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	4
45.114.11.47		147.237.72.156	aman.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
45.114.11.47		147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	3
221.203.3.117	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.47		147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
45.114.11.49		147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
177.37.169.67	Brazil	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
131.161.20.84		147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
210.61.150.154	Taiwan	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	2
45.114.11.47		147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
59.46.193.114	China	147.237.0.16	my-kosher-kravi.idf.il	GPL SCAN nmap TCP	2
45.114.11.46		147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
89.248.169.50	Netherlands	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
37.60.42.117	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
45.114.11.46		147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.152	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.121.40.6	Israel	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
45.114.11.47		147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.28	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.47		147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.59	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.46		147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.46		147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
210.61.150.154	Taiwan	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	2
45.114.11.46		147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
89.248.169.50	Netherlands	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
45.114.11.46		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
213.204.103.36	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.47		147.237.77.227	e.hamaz.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
62.219.24.52	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
221.203.3.117	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.50.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2830
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1885
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1749
2.54.165.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1367
109.160.142.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	982
201.55.56.115	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	897
148.177.1.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	859
91.201.208.18	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	831
37.142.142.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	796
82.145.223.29	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	771
59.177.172.191	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	746
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	731
77.125.164.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	717
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	622
79.182.123.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	600
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	572
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	540
77.126.2.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	540
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	525
84.94.72.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	514
188.165.15.152	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	507
168.235.197.119		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	495
46.116.88.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	476
132.68.179.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	474
109.186.76.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	453
62.0.15.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	393
83.130.107.129	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	391
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	366
170.61.18.228	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	365
66.249.69.34	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	330
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	328
66.249.69.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	324
66.249.69.26	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	324
46.23.113.228	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	317
94.44.254.55	Hungary	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	315
46.19.85.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	310
46.19.86.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	289
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	287
46.19.86.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	280
54.244.22.103	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	277
212.199.205.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	275
84.228.247.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	273
2.52.9.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	257
2.54.45.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	257
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	253
31.168.126.158	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	243
37.26.149.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	239
54.244.22.103	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	238
207.46.13.149	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	232

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.177.137.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2405
84.111.235.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1996
2.54.52.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1935
176.13.1.164	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.1.164	Block	1248
176.12.142.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1086
176.12.146.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	916
176.13.13.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	836
46.19.85.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	834
2.54.15.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	712
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	697
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	664
2.54.44.144	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.44.144	Block	654
109.64.212.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	530
2.54.168.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	482
176.12.137.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	456
80.246.136.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	456
176.13.23.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	416
46.19.86.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	400
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.223	Block	374
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.229	Block	328
2.54.130.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	308
176.12.141.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	308
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.112	Block	282
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	280
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	222
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	218
82.166.22.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	212
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	210
176.13.2.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	206
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	202
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	194
2.54.7.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	174
2.54.27.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	168
80.246.136.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	148
79.179.199.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	142
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	126
2.54.4.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	118
176.13.5.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	112
46.210.216.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	102
37.26.149.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	92
2.54.49.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	88
185.32.179.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	82
173.208.235.162	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 173.208.235.162	Block	62
2.54.7.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
176.13.0.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	52
185.32.179.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	44
185.32.179.196	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	40
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	38