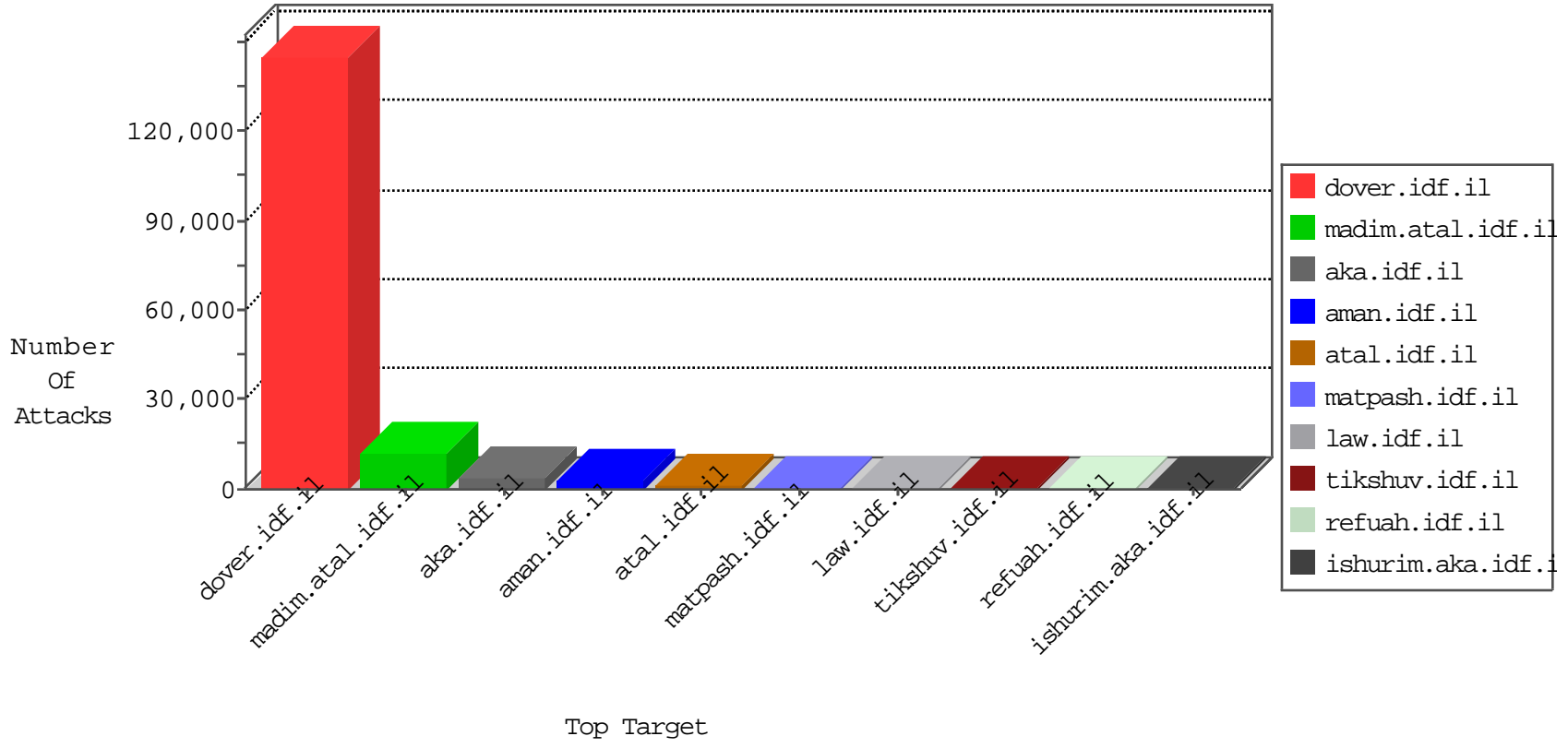


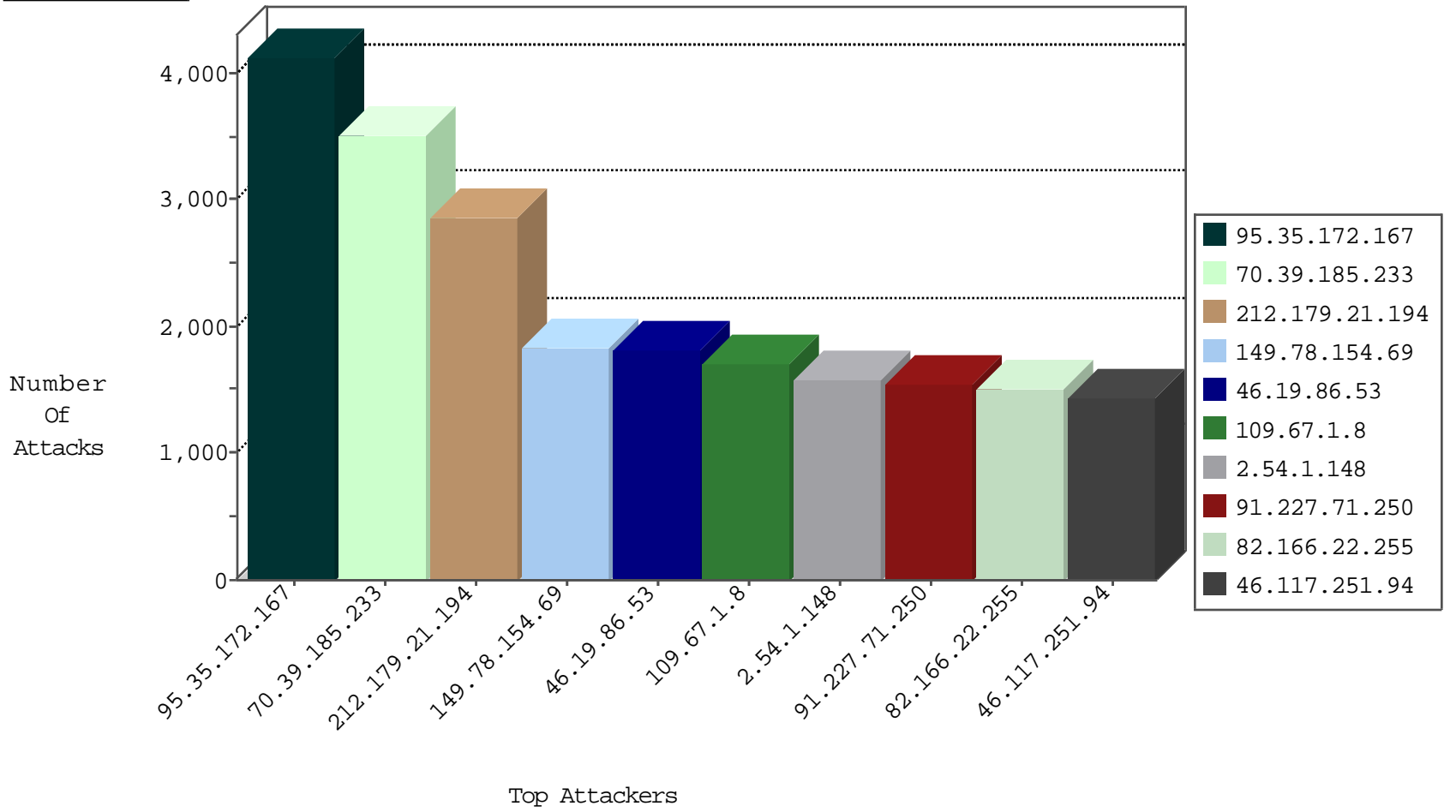
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
62.150.117.251	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8750
66.249.81.218	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5144
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3366
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3219
77.126.20.23	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3023
168.63.139.43	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2912
77.125.151.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1438
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	580
109.65.172.112	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	532
79.181.49.68	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	528
79.178.110.156	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	384
79.182.208.99	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	369
85.250.239.100	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	361
213.57.189.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	323
84.109.179.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	309
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	309
85.64.124.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
84.94.58.4	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	289
80.230.82.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	258
37.142.110.133	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	218
85.250.227.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	208
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	207
62.90.122.234	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	184
31.154.92.134	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
77.127.24.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
109.65.125.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
46.120.21.70	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	158
220.181.108.77	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	145
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
109.64.200.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
79.176.154.60	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
185.13.194.12	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	134
46.19.86.94	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	134
206.167.243.1	Canada	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	133
84.229.116.168	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
62.219.130.240	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
79.177.122.66	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	113
87.68.34.152	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
87.68.83.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
212.25.84.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
46.19.86.71	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	97
109.186.154.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
37.26.146.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	91
109.65.134.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
213.57.175.41	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
46.116.155.53	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
149.88.190.192	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	78
79.177.203.138	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
31.154.92.134	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
105.162.228.216	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
98.126.46.227	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
77.125.85.80	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
80.178.138.115	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
80.178.184.30	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
84.229.155.225	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
213.139.53.32	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
212.143.214.158	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.3	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.150	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.102.254.213	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.67.119.220	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.57.188.188	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.11.45.0	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
192.116.177.166	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.108.67.158	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.178.171.139	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
37.26.148.220	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
62.219.195.42	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
97.90.144.118	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.170	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.154	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.207	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
193.203.233.4	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.177	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.178.106	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.196	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.250.141.242	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
93.172.137.152	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.251	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.250.224.45	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.72	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.26.146.209	Israel	147.237.77.243	mobile.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
147.236.38.106	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
2.54.20.12	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
73.179.86.65	United States	147.237.72.167	ishurim.aka.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.175	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.181.165.128	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.183.142.202	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.172.62.148	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.79	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.178.69	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.6	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.181	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
50.75.220.34	United States	147.237.72.167	ishurim.aka.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

## 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	88
182.50.130.47	Singapore	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	48
182.50.130.47	Singapore	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	43
66.249.67.18	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	24
180.97.106.161	China	147.237.77.176	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	8
180.97.106.36	China	147.237.77.176	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	6
180.97.106.162	China	147.237.77.176	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	5
115.239.212.70	China	147.237.77.176	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	5
180.97.106.37	China	147.237.77.176	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	4
45.114.11.46		147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	4
45.114.11.46		147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.48		147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	3
115.239.212.71	China	147.237.77.176	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	3
45.114.11.46		147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
45.114.11.46		147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	3
115.239.212.66	China	147.237.77.176	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	3
45.114.11.46		147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
74.82.194.10	Canada	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
183.152.151.233	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
176.12.136.56	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
45.114.11.46		147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
183.152.151.233	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.86	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
45.114.11.46		147.237.77.61	e.oogat.idf.il	ET SCAN Potential SSH Scan	2
103.52.137.219		147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
183.152.151.233	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.47		147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
45.114.11.49		147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
199.203.59.121	Israel	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
176.13.4.197	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
45.114.11.47		147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
111.34.177.214	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
115.239.212.68	China	147.237.77.176	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	2
45.114.11.48		147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
111.34.177.214	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	Germany	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
74.82.194.10	Canada	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
183.152.151.233	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
176.12.149.110	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
45.114.11.46		147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
45.114.11.48		147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
183.152.151.233	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
188.54.103.111	Saudi Arabia	147.237.77.216	dover.idf.il	ET SCAN Netsparker Default User-Agent	2
176.12.136.56	Israel	147.237.77.216	dover.idf.il	GPL SCAN myscan	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.35.172.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4127
70.39.185.233	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3500
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2692
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1830
46.19.86.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1814
109.67.1.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1703
2.54.1.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1578
91.227.71.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1537
82.166.22.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1508
46.117.251.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1441
2.54.179.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1313
192.114.23.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1246
87.68.82.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1243
77.125.5.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1179
2.54.28.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1041
46.116.127.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1001
79.183.49.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	911
213.57.189.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	903
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	795
82.145.223.94	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	746
192.116.218.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	734
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	719
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	707
77.126.234.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	660
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	652
79.181.13.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	644
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	629
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	627
188.165.15.152	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	624
46.19.85.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	621
80.246.133.217	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	616
84.228.238.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	603
109.66.33.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	591
37.26.146.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	589
79.182.214.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	572
37.26.147.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	562
87.68.78.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	537
2.54.171.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	525
141.0.11.87	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	525
80.178.206.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	511
141.248.3.252	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	494
46.116.160.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	492
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	467
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	467
79.182.123.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	466
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	459
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	454
68.180.228.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	454
20.132.68.133	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	449
46.210.163.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	424

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.13.14.137	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.14.137	Block	1209
80.246.136.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1031
80.246.136.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	941
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	880
2.54.153.32	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.153.32	Block	646
213.57.39.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	645
77.125.208.239	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 77.125.208.239	Block	630
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	616
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	594
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	582
2.54.39.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	566
46.19.85.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	518
176.13.8.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	484
176.13.21.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	482
176.13.22.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	462
176.12.148.229	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.148.229	Block	457
2.54.167.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	418
46.19.85.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	378
2.54.7.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	348
212.235.8.225	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 212.235.8.225	Block	340
176.13.12.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	330
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	307
176.13.1.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	254
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	235
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	227
46.19.86.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	165
46.19.85.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	162
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	146
182.50.130.47	Singapore	147.237.77.74	law.idf.il	PHP Attempt	Block	144
109.64.31.78	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	144
182.50.130.47	Singapore	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 182.50.130.47	Block	141
182.50.130.47	Singapore	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 182.50.130.47	Block	138
176.13.13.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	136
46.19.86.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	130
182.50.130.47	Singapore	147.237.72.166	aka.idf.il	PHP Attempt	Block	129
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	117
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	115
176.12.145.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	112
37.26.147.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	72
182.50.130.47	Singapore	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 182.50.130.47	Block	69
182.50.130.47	Singapore	147.237.77.74	law.idf.il	Multiple Admin Blocking from 182.50.130.47	Block	69
80.246.133.210	Israel	147.237.77.170	maarachot.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
192.151.159.82	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 192.151.159.82	Block	50
193.201.224.126	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.201.224.126	Block	42
183.206.163.108	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.206.163.108	Block	32
37.26.148.176	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	30
2.54.41.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
192.151.159.82	United States	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 192.151.159.82	Block	28
176.12.150.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
79.176.140.104	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	27