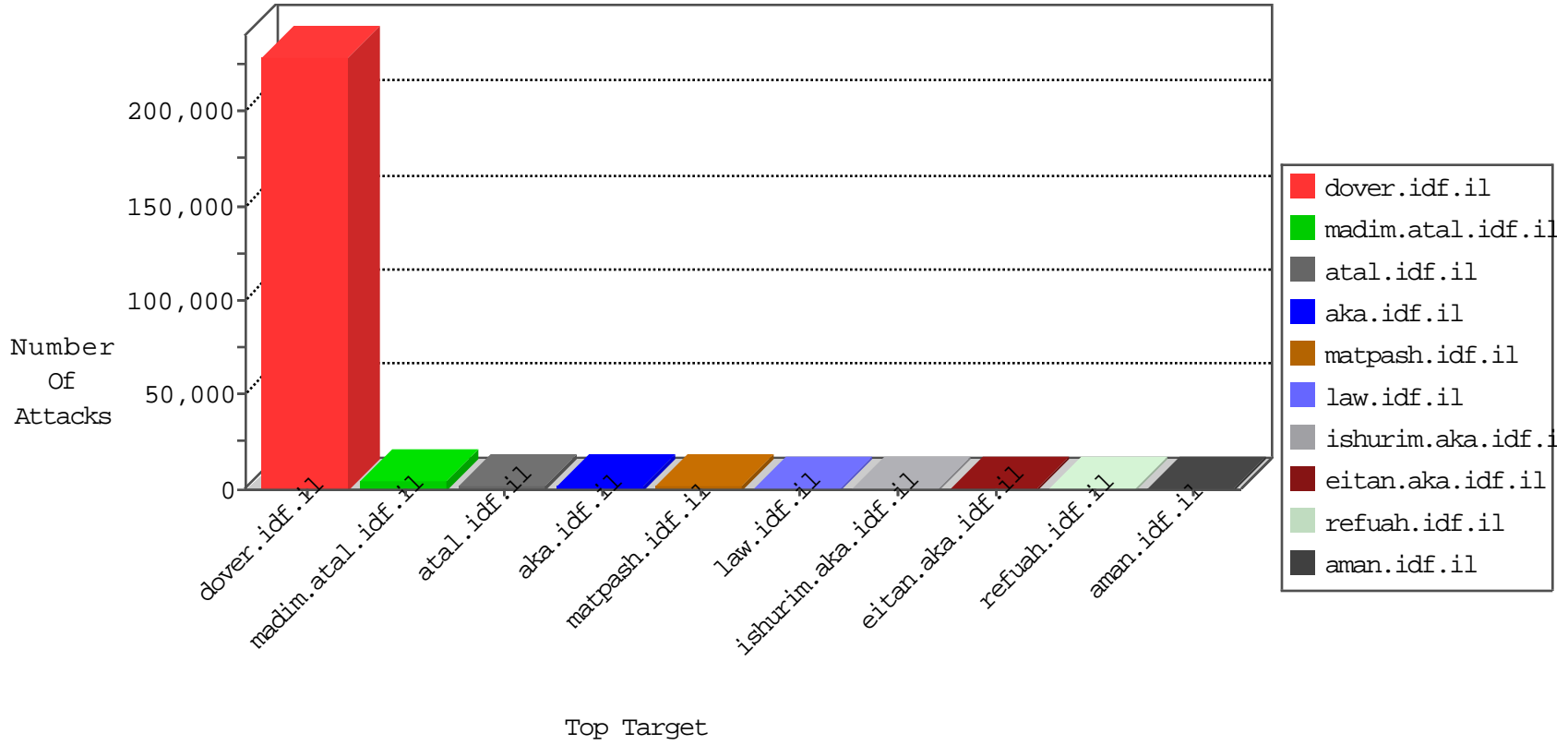


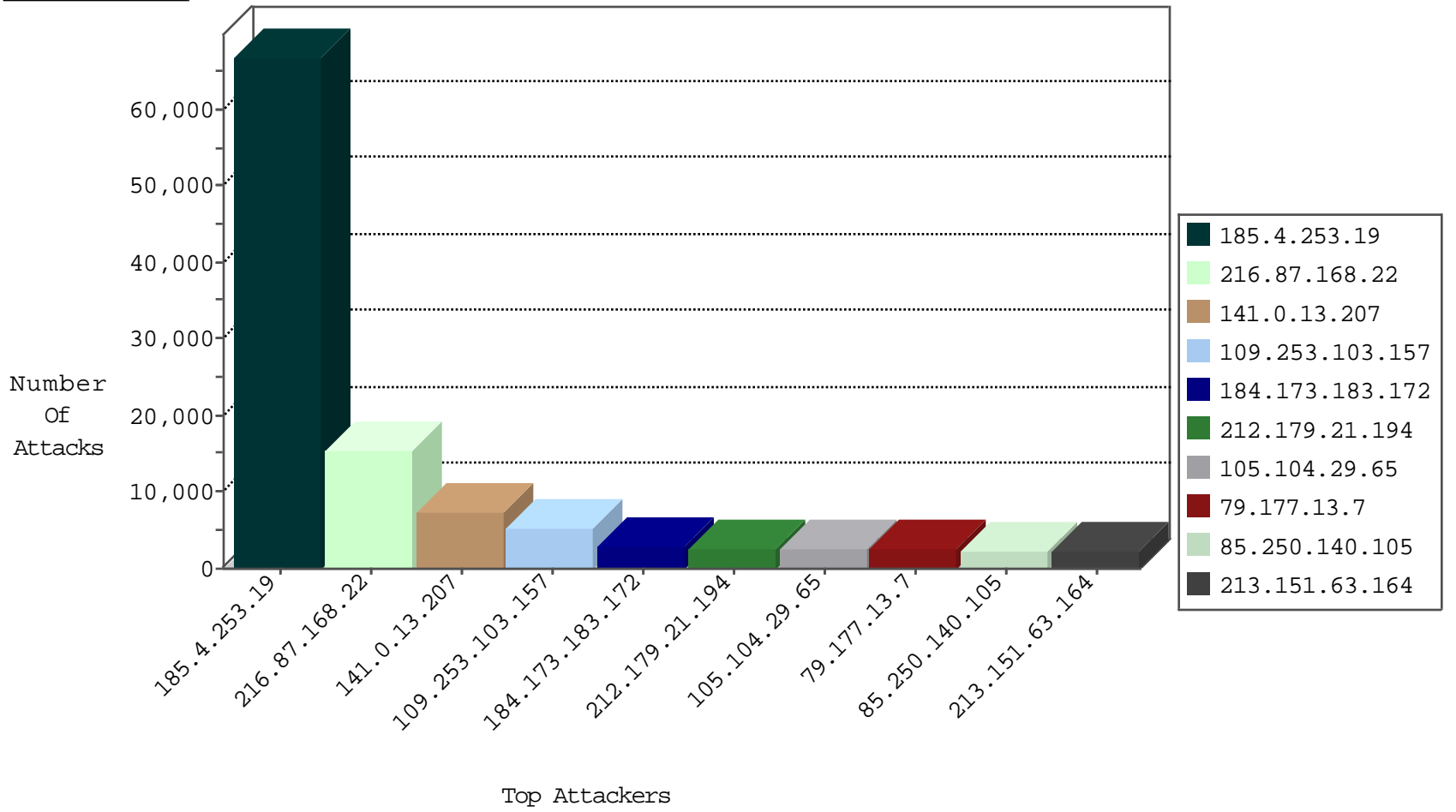
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	112451
216.87.168.22	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	106126
216.87.168.22	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	36964
216.87.168.22	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14855
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6302
212.178.108.82	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3247
109.253.103.157	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3170
85.68.168.139	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3140
74.6.254.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2979
84.228.142.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2967
192.116.239.196	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2597
212.179.61.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2584
200.53.156.138	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1404
212.150.244.226	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1301
141.105.160.160	Satellite Provider	147.237.77.176	matpash.idf.il	HTTP-POST-Segmented-DoS	dest-reset	838
37.142.215.100	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	607
141.0.13.207	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	550
46.19.85.6	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	519
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	425
89.139.6.176	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	404
79.179.135.57	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	370
82.80.178.57	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	357
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	350
31.168.189.32	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	345
87.69.165.71	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	345
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	340
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	320
79.176.160.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	315
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	311
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	280
109.67.30.139	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	260
84.110.86.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	240
79.180.133.6	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	221
37.142.3.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	213
93.172.129.42	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	210
178.214.65.115	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	205
79.178.143.141	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
95.86.112.193	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	189
85.65.45.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
82.166.22.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
109.253.159.182	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	157
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
89.139.40.63	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
95.86.85.104	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	140
84.94.17.73	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	137
109.66.181.49	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
199.203.172.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
46.19.86.73	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	1756
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	426
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	351
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	278
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	169
50.116.62.182	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	157
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	147
184.173.183.172	United States	147.237.76.200	eitan.aka.idf.il	DVRep_P-N_40-59	Permit	111
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
138.134.192.10	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
62.0.42.2	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
178.234.210.25	Russian Federation	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
79.182.145.131	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
218.77.79.43	China	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	9
88.77.192.10	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	8
218.77.79.43	China	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	7
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	7
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	7
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	6
218.77.79.43	China	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
46.121.203.117	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.67.161.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	6
87.69.218.68	Israel	147.237.77.226	ww.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
218.77.79.43	China	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	6
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	5
93.172.175.20	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5

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	95
94.23.254.103	France	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	36
216.87.168.22	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	12
173.201.196.214	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	7
184.168.27.101	United States	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	6
43.255.188.132	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	3
197.202.132.21	Algeria	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	3
197.202.132.21	Algeria	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	3
95.86.94.109	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
43.255.188.131	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
31.131.251.132	Russian Federation	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
91.236.74.6	Poland	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
197.202.132.21	Algeria	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.132	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
81.218.77.162	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
43.255.188.131	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.175	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
43.255.188.132	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
91.236.74.6	Poland	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.132	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
91.236.74.6	Poland	147.237.76.148	gocenter.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
91.236.74.6	Poland	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
77.89.246.62	Moldova, Republic of	147.237.72.166	aka.idf.il	SERVER-WEBAPP admin.php access	1
203.194.234.109	Hong Kong	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5800-5820	1
188.122.91.100	Netherlands	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
113.160.150.62	Vietnam	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
43.255.188.132	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
84.111.25.98	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
222.69.94.13	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
43.255.188.130	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
197.202.132.21	Algeria	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63119
141.0.13.207	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7340
109.253.103.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5278
105.104.29.65	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2472
79.177.13.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2424
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2415
213.151.63.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2289
85.250.140.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2275
46.19.85.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2017
213.8.54.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2012
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1797
95.86.122.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1534
82.80.89.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1533
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1443
205.203.135.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1335
79.182.145.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1294
200.53.156.138	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1273
199.190.46.130	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1258
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1174
95.86.108.216	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1149
213.204.103.36	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1131
212.179.61.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1126
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1112
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1085
2.54.11.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1053
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1011
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	986
46.19.85.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	982
54.224.21.23	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	895
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	814
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	752
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	722
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	661
192.114.23.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	652
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	646
46.210.192.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	578
84.94.21.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	574
84.229.135.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	565
207.46.13.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	552
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	543
157.55.39.60	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	527
80.230.92.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	524
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	523
212.76.116.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	521
95.86.113.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	489
109.67.115.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	480
36.77.235.226	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	480
95.86.70.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	466
46.19.86.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	459
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	457

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/undefined	Block	1931
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	1744
185.6.57.137	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/undefined	Block	920
80.246.136.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	573
2.54.146.252	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.146.252	Block	398
2.54.1.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	320
5.29.12.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	317
109.253.143.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	310
5.28.189.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	274
2.54.149.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	269
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	254
2.54.47.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	211
176.12.142.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
109.253.130.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	184
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	177
68.180.228.175	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 68.180.228.175	Block	168
5.29.139.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	163
176.12.148.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	134
109.253.129.122	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.129.122	Block	84
203.195.140.248	China	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	84
79.180.10.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.10.225	Block	81
212.33.115.21	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/undefined	Block	75
176.12.139.100	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.139.100	Block	73
37.26.146.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
79.182.178.234	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il//shared/ajax/createcaptchaimage.aspx	Block	56
94.23.254.103	France	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	48
46.19.85.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
2.52.147.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
2.54.146.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
193.41.209.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	42
2.54.55.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
46.19.86.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
200.53.156.138	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	40
176.12.138.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
80.246.136.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
109.253.142.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
149.78.126.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
174.64.97.238	United States	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il//shared/ajax/createcaptchaimage.aspx	Block	28
80.246.136.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.34	Block	27
157.55.39.6	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	26
62.219.226.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	24
94.23.254.103	France	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 94.23.254.103	Block	23
46.19.86.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
2.52.47.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
80.246.136.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
80.246.138.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
207.46.13.35	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.35	Block	19
37.26.146.137	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 37.26.146.137	Block	18