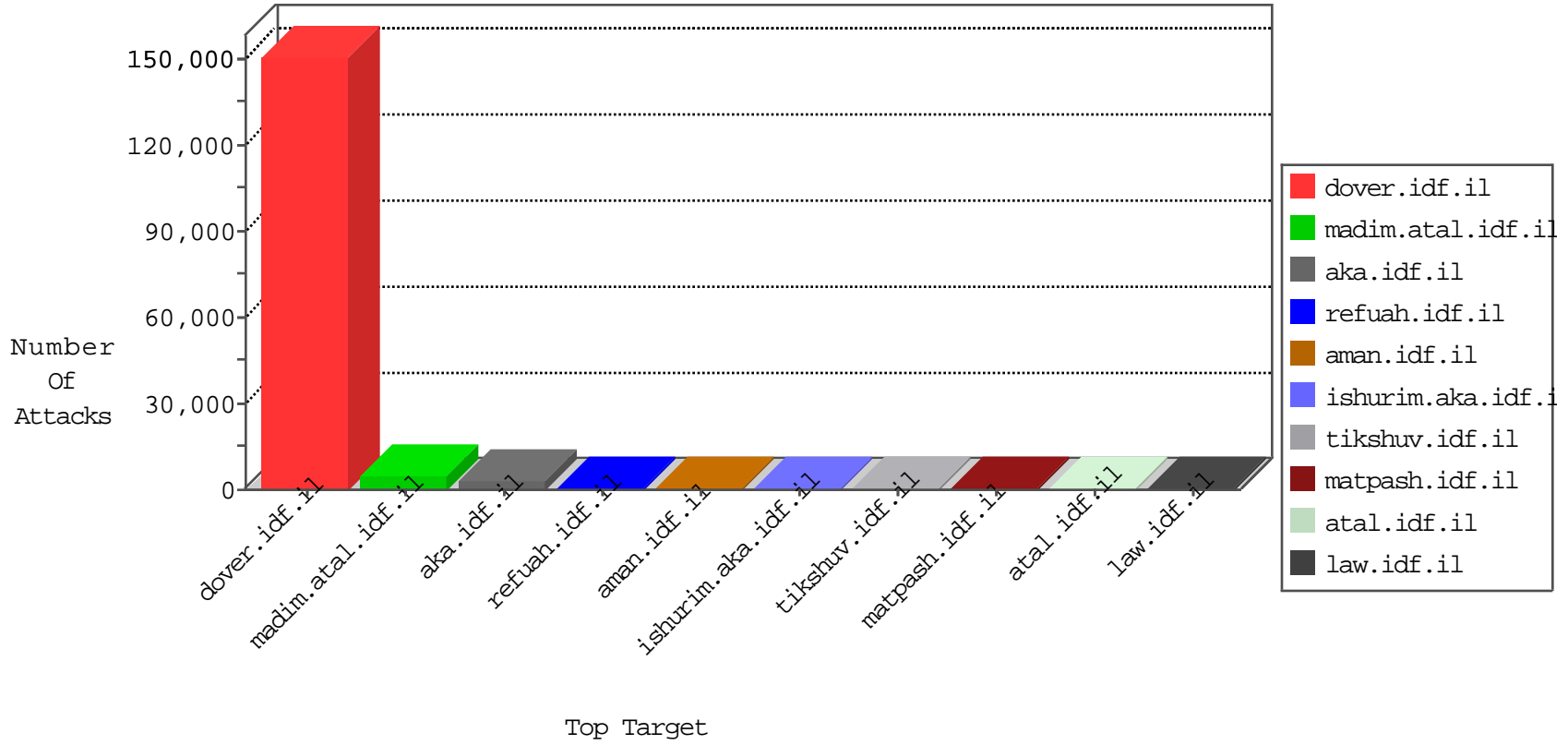


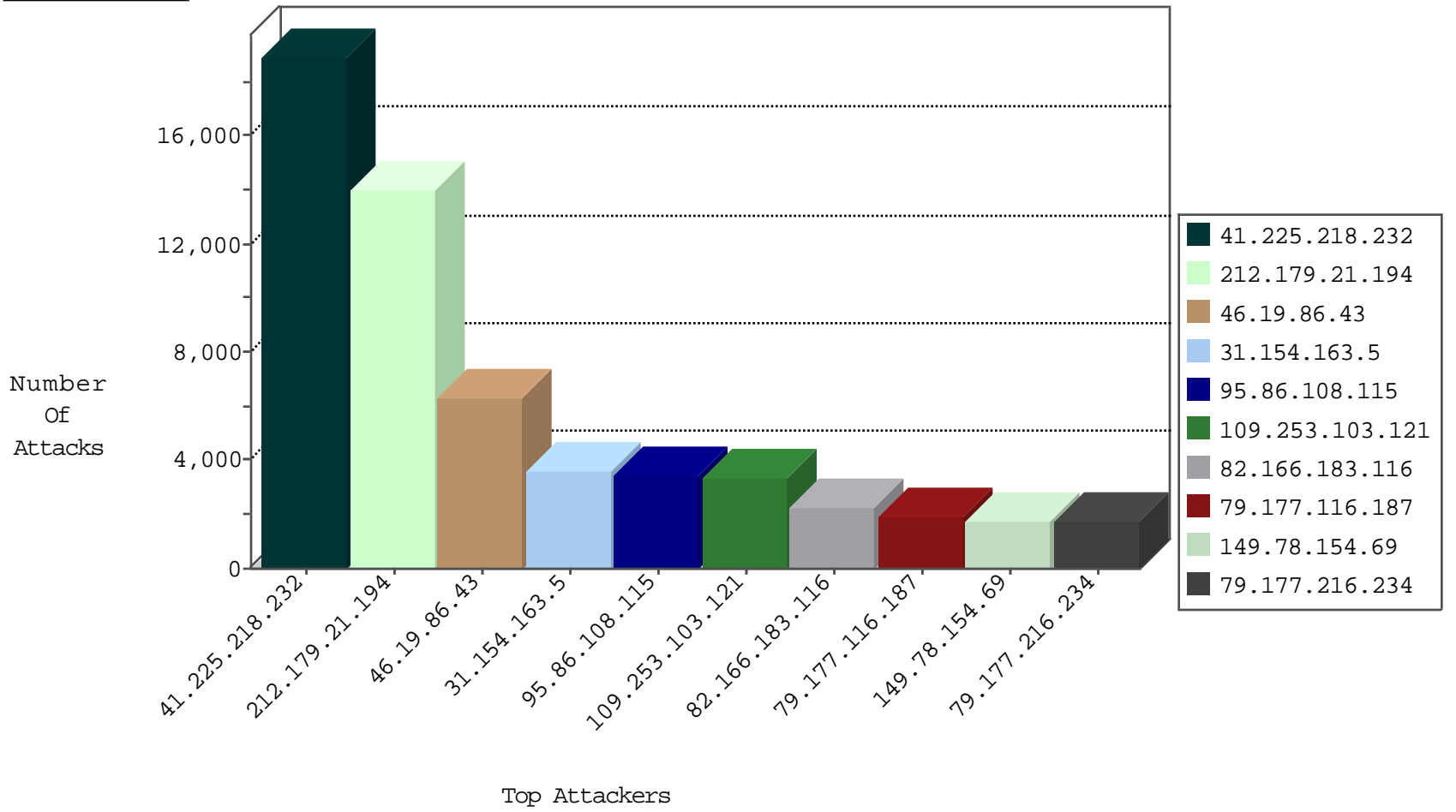
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
46.19.86.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2925
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2711
31.186.228.94	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2541
81.218.126.226	Israel	147.237.0.34	tikshuv.idf.il	TCP Scan (vertical)	drop	2174
46.117.253.250	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	718
109.186.42.171	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	596
79.177.216.234	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	557
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	533
46.120.28.168	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	485
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	460
82.166.103.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	448
213.57.186.253	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	433
66.249.67.79	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	368
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	364
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	350
79.179.62.66	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	333
5.29.18.244	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	329
84.109.201.16	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	326
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	320
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	319
46.121.78.245	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	287
85.65.86.3	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	274
79.181.174.57	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	251
149.78.167.143	United States	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	201
82.166.75.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	200
31.168.172.250	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
77.125.82.84	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	182
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	171
46.120.17.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
46.120.111.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
46.120.241.14	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
149.78.195.56	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	151
212.199.149.78	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
85.64.214.156	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
79.181.142.47	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
79.183.68.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	122
89.139.63.92	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	114
84.108.94.107	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
87.68.43.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
46.19.86.110	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
212.199.218.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
149.78.47.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
85.64.134.3	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	91
109.67.55.201	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
149.88.118.60	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
85.65.17.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
46.19.86.248	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
192.114.67.140	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
176.97.116.159	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	22
91.228.248.251	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
176.97.116.159	Ukraine	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	9
79.176.133.246	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
79.182.185.81	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
178.234.155.240	Russian Federation	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
147.236.238.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
109.64.13.54	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
194.176.105.146	United Kingdom	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
85.250.214.251	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
149.78.241.248	United States	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
31.210.189.210	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
93.172.61.95	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
126.99.203.74	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.239	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.183.244.230	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
87.68.23.148	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
213.8.44.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.177.8.143	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
149.88.58.52	United States	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
5.102.254.211	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.143.54.217	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.85.119	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.179.62.66	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
154.121.251.128		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.64.240.67	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.252.167.176	Turkey	147.237.76.86	navy.idf.il	12373: HTTP: WordPress admin Login	Block	4
37.26.146.254	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
84.108.82.54	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
74.65.142.210	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.226.35.5	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
192.117.105.110	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.232	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.234	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.252.167.176	Turkey	147.237.77.74	law.idf.il	12373: HTTP: WordPress admin Login	Block	2
41.35.167.239	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.34.11.3	Jordan	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	2
189.0.125.92	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.84	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.252.167.176	Turkey	147.237.77.216	dover.idf.il	12373: HTTP: WordPress admin Login	Block	2
132.3.49.81	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.26.147.170	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
185.32.178.14	Israel	147.237.72.156	anan.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.229.205.91	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
87.211.152.194	Netherlands	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.250.58.117	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
213.8.44.227	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
77.127.181.150	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	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	32
208.80.155.225	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
54.209.60.63	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
82.166.22.63	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	3
43.255.188.133	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.209	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
31.210.186.133	Israel	147.237.77.216	dover.idf.il	GPL SCAN myscan	2
43.255.188.135	Japan	147.237.76.177	noore.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.247	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
46.116.164.13	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.133	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
31.210.186.133	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
43.255.188.131	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
107.179.95.29	United States	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
24.132.212.111	Netherlands	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
81.200.91.2	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
60.18.162.244	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
178.173.145.6	Iran, Islamic Republic of	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
115.68.23.201	Korea, Republic of	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.130	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
86.131.220.230	United Kingdom	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
69.108.99.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
203.147.5.124	Thailand	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.188.135	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
123.30.211.183	Vietnam	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.147	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
145.52.173.242	Netherlands	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.188.132	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
109.253.147.124	Israel	147.237.77.243	mobile.idf.il	INDICATOR-SCAN myscan	1
31.184.194.114	Russian Federation	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.111.175.7	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.188.134	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
118.163.130.147	Taiwan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.131	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.164	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.225.218.232	Tunisia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18925
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13966
46.19.86.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6291
31.154.163.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3556
95.86.108.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3421
109.253.103.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3313
82.166.183.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2235
79.177.116.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1901
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1742
79.177.216.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1724
37.236.136.12	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1082
89.187.221.1	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1079
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1023
2.54.55.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1019
84.110.48.237	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	883
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	851
82.166.22.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	825
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	726
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	721
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	698
46.121.65.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	696
204.93.58.243	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	684
37.142.10.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	680
109.186.0.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	663
37.142.11.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	659
37.26.147.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	634
46.210.106.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	629
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	570
2.54.41.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	537
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	523
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	520
79.177.191.249	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	509
79.178.49.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	499
2.54.140.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	498
2.54.145.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	490
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	483
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	463
121.220.125.46	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	455
118.189.27.144	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	451
45.216.202.3		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	450
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	447
45.98.150.103		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	440
68.180.229.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	431
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	409
82.145.219.40	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	405
2.54.45.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	396
149.255.208.11	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	359
188.165.15.233	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	336
79.177.151.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	325
2.54.41.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	317

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.163.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	701
176.12.148.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	480
2.54.12.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	433
176.12.146.46	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.146.46	Block	318
109.253.131.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	292
149.78.167.143	United States	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	243
109.253.145.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	201
85.250.224.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
149.78.77.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	194
176.13.5.177	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.5.177	Block	186
176.12.149.139	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.149.139	Block	139
176.12.148.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	131
2.54.0.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
109.253.136.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	124
109.253.140.54	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.140.54	Block	117
176.13.3.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	112
176.12.137.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
176.228.38.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	96
176.13.12.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.12.199	Block	79
176.13.18.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	75
176.12.139.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
46.19.85.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	51
176.13.22.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
185.32.178.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
66.249.78.159	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	40
66.249.78.166	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	37
66.249.78.173	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	37
93.173.250.243	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	34
176.12.140.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
109.253.139.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
82.102.141.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
2.52.159.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
109.64.51.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
185.32.178.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
46.117.9.164	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	22
79.181.148.203	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	21
94.159.198.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	21
77.125.1.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	18
46.120.90.12	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 46.120.90.12	Block	18
37.142.249.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
5.28.140.98	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master\$ContentPlaceHolder1\$password in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	14
79.179.10.22	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	14
185.32.178.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
109.253.139.152	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
109.186.37.67	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	13
5.144.57.228	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
46.120.71.224	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
2.52.5.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12