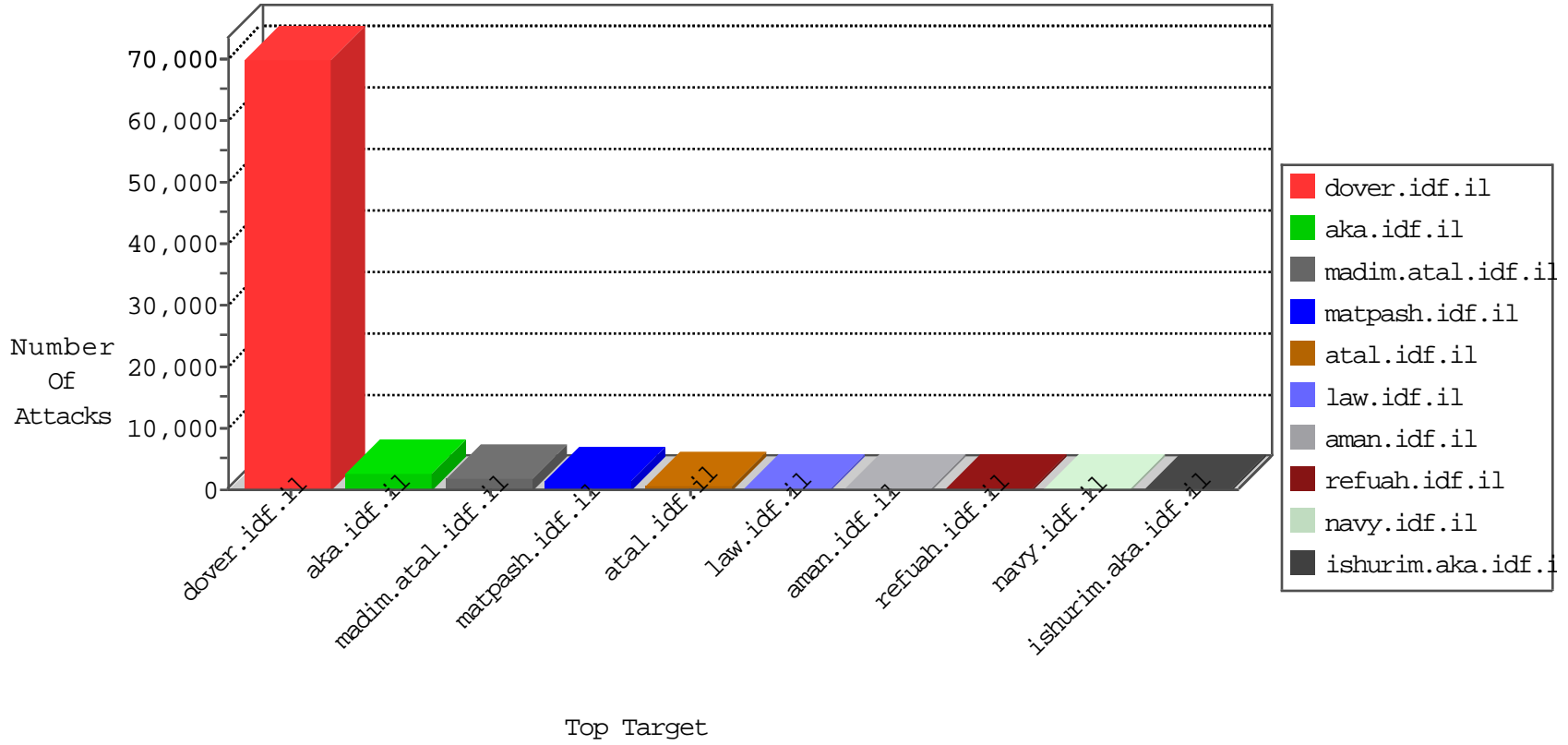


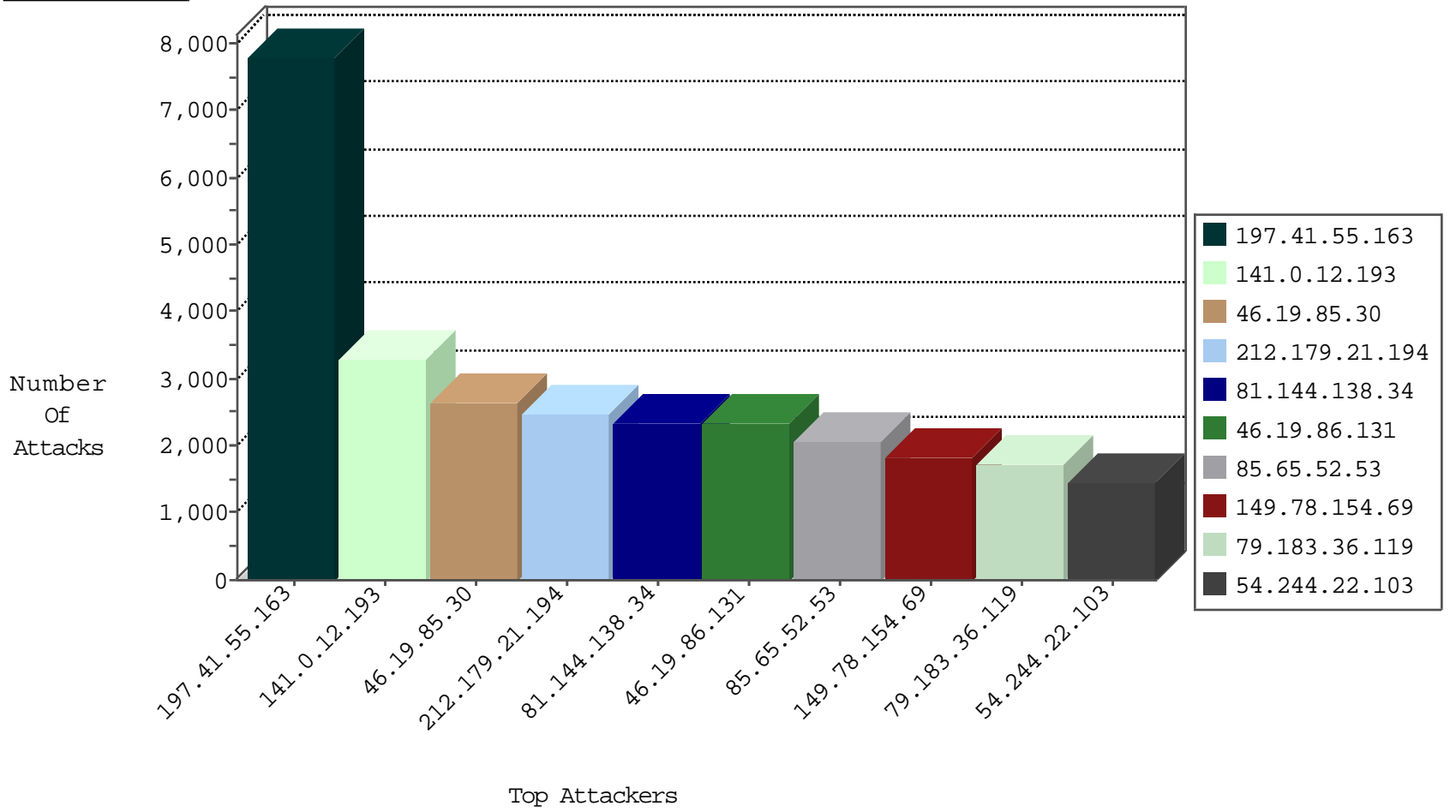
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
82.166.22.63	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6320
66.249.67.65	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2843
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2788
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2649
141.0.12.193	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	449
66.249.69.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	343
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	311
46.120.34.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	301
79.177.18.246	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	248
213.57.164.112	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	219
41.33.141.134	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	205
77.127.204.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
109.64.166.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	184
79.183.97.43	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	183
85.65.171.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
41.200.55.88	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	166
79.182.147.181	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
176.13.16.167	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	164
79.181.142.47	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
79.177.187.96	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
109.186.19.6	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	128
109.65.128.184	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	121
46.31.103.58	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	115
46.19.86.182	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	113
79.180.124.177	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	102
46.117.41.48	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	101
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
5.22.129.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
79.181.213.136	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
77.127.206.17	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
84.94.160.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
80.246.137.190	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
46.120.126.199	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	31
109.67.125.108	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
2.52.13.94	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
46.19.85.188	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
46.121.195.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	12
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	9
109.64.41.49	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
109.64.41.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
10.0.0.2		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
192.168.1.100		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.182.27.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.179.171.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
109.66.80.51	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
93.172.131.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.179.60.30	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
192.115.177.202	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
192.115.177.203	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
77.127.204.103	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
103.228.1.242		147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
62.109.17.206	Russian Federation	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	8
105.62.57.97	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
85.250.23.18	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.181.60.69	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
41.200.55.88	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
82.166.22.63	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.108.236.233	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.183.151.146	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
132.70.66.11	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
37.142.134.40	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.177.187.151	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.52.155.201	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
97.82.131.14	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.229.135.42	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.250.182.120	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
209.213.104.25	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
77.127.32.102	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.121.252.134	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
83.97.83.125	Switzerland	147.237.72.166	aka.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	3
76.163.25.110	United States	147.237.76.42	refuah.idf.il	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	3
84.228.59.219	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.26.147.243	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.181.60.69	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
176.12.146.187	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
85.64.148.87	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
86.169.241.30	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
110.22.212.147	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
111.95.120.171	Indonesia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.181.48.90	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
194.90.15.61	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
93.172.182.21	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.67.33.1	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.126.234.77	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
154.73.15.32		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.208	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.246.136.139	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.183.4.152	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
62.210.251.69	France	147.237.77.74	law.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	2
131.174.81.132	Netherlands	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.94.64.78	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.117.63.134	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
62.210.251.69	France	147.237.77.74	law.idf.il	17031: HTTP: GetSimple CMS File Upload	Block	2
84.94.181.145	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.117.162.127	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
176.228.193.172	Israel	147.237.77.216	dover.idf.il	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
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	81
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	51
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	44
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP cat%20 access	42
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP WEB-INF access	37
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	INDICATOR-SCAN DirBuster brute forcing tool detected	28
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	ET SCAN DirBuster Web App Scan in Progress	28
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	12
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	12
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER CRLF Injection - Newline Characters in URL	11
62.109.17.206	Russian Federation	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	8
182.50.130.105	Singapore	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	8
182.50.130.105	Singapore	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	8
88.241.46.12	Turkey	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	8
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	ET WEB_SERVER Poison Null Byte	6
66.249.67.59	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sa (2)	4
204.93.58.154	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	4
132.74.95.21	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
83.71.247.34	Ireland	147.237.72.156	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
43.255.188.135	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	3
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP /cgi-bin/ access	3
43.255.188.135	Japan	147.237.76.196	e.sviva.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
43.255.188.134	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.134	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.133	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.135	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.73	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sa (2)	2
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
202.106.54.203	China	147.237.77.19	law-forum.idf.il	GPL SCAN nmap TCP	2
43.255.188.133	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.77.234	halag.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
43.255.188.130	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.147	chimuch.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
43.255.188.130	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
72.46.139.154	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP .htaccess access	2
43.255.188.135	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
188.161.183.103	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDos Inbound	2
43.255.188.134	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
197.41.55.163	Egypt	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7742
141.0.12.193	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3292
46.19.85.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2633
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2471
46.19.86.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2327
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2307
85.65.52.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2066
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1820
79.183.36.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1715
82.145.221.31	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1387
82.166.22.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1386
168.235.197.215		147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	1138
82.145.216.66	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1010
107.167.107.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	747
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	704
79.177.26.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	635
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	627
87.68.48.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	608
95.86.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	547
46.210.135.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	514
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	505
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	492
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	474
66.249.67.59	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	458
54.244.22.103	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	449
66.249.67.65	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	437
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	428
66.249.67.53	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	412
105.201.0.227	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	405
77.127.17.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	367
109.42.2.123	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	361
54.244.22.103	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	355
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	348
204.93.58.154	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	330
37.26.148.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	306
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	283
212.179.42.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	254
109.66.155.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	245
46.19.86.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	244
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	236
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	228
87.68.84.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	226
107.77.100.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	222
108.92.158.146	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	217
37.26.146.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	215
50.118.162.16	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	209
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	206
188.165.15.233	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	205
46.120.64.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	198
8.37.225.208	Anonymous Proxy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	196

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	504
46.19.85.17	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.17	Block	368
2.54.170.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.170.214	Block	310
84.111.136.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	305
109.64.81.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	263
2.54.37.45	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.37.45	Block	124
37.26.147.136	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.136	Block	121
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	120
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	106
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	94
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	54
2.52.173.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	31
79.176.21.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.21.72	Block	16
23.239.208.33	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 23.239.208.33	Block	16
2.54.173.252	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.173.252	Block	16
109.66.170.66	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.66.170.66	Block	15
167.114.156.198	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 167.114.156.198	Block	11
176.12.148.245	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	11
204.93.58.154	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 204.93.58.154	Block	11
204.93.58.154	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 204.93.58.154	Block	9
109.67.145.244	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	9
82.80.33.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	7
84.94.165.43	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/	Block	7
2.48.6.45	United Arab Emirates	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	6
5.22.129.226	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 5.22.129.226	Block	6
109.67.145.244	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.67.145.244	Block	6
79.176.171.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	6
116.212.127.209	Hong Kong	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	5
37.139.52.23	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/	Block	5
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	5
213.57.106.28	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	5
80.179.96.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
27.126.184.51	Hong Kong	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
109.64.59.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
176.13.7.19	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.7.19	None	5
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
82.80.33.138	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
62.109.17.206	Russian Federation	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	4
176.12.149.146	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.149.146	None	4
46.229.164.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatiz	Block	4
79.180.212.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
213.57.201.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
182.50.130.105	Singapore	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	4
207.46.13.85	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
188.165.15.233	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.233	Block	4
192.116.220.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/golani/golani.stm	Block	4
87.69.198.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
85.250.121.151	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	4