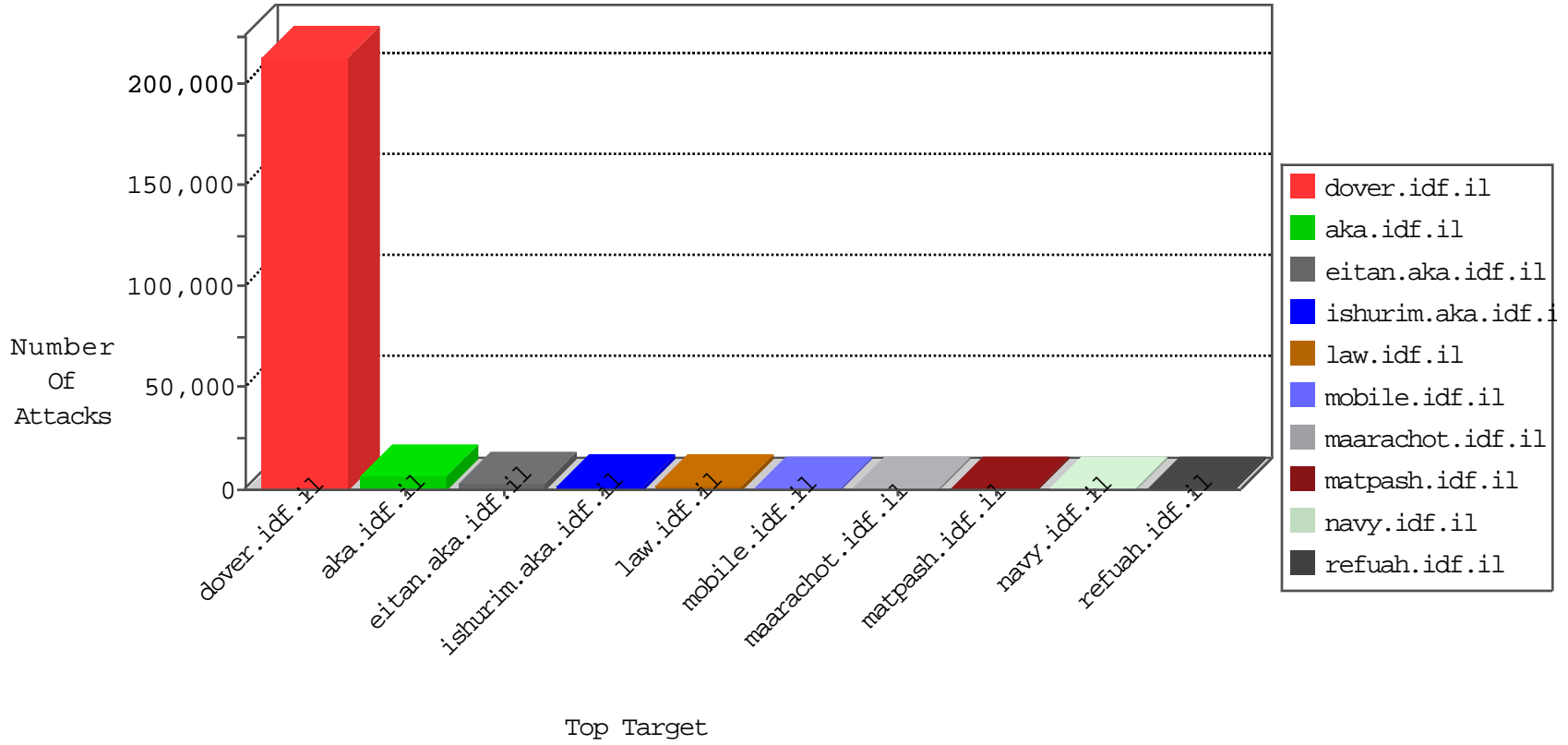


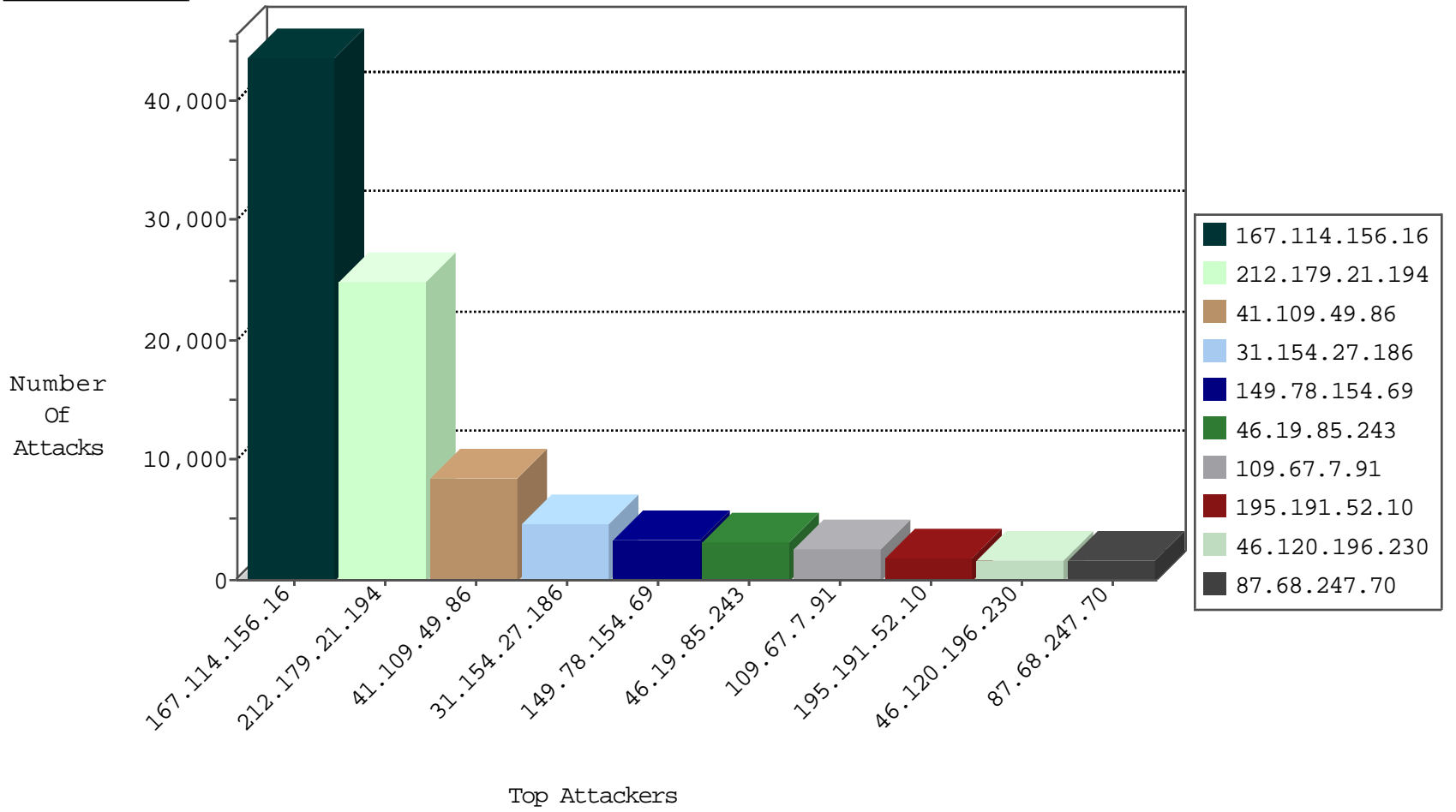
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	70011
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	68533
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	41391
66.249.69.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34756
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	33111
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	30728
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27806
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	26887
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	17060
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	16002
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14616
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8737
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	7777
142.4.214.124	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6243
66.249.64.191	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4214
24.237.235.129	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3690
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3688
66.102.9.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3632
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3490
109.65.177.8	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3318
125.239.162.207	New Zealand	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3168
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2919
98.169.20.31	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2913
66.171.228.83	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2747
79.44.140.55	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2652
66.249.67.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2640
46.118.155.220	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2559
46.19.86.125	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2537
87.69.158.155	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2534
176.13.1.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2506
80.82.69.128	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2453
37.26.148.212	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2376
207.46.13.114	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2312
72.197.87.188	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2216
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2094
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2060
216.218.147.199	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2021
66.249.64.186	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1909
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1700
186.159.143.221	Costa Rica	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1601
88.103.90.45	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1573
37.26.146.211	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1549
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1542
151.80.31.112	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1506
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1297
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1246
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1184
167.220.196.128	United Kingdom	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1142
197.35.18.32	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1114
132.3.57.81	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1099

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.155.224.27	United States	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
104.155.224.27	United States	147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
212.117.151.42	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
62.219.154.115	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
95.86.107.10	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
202.134.8.135	Bangladesh	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
212.25.106.78	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
82.80.51.175	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
109.160.225.187	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.251.252	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
10.0.0.24		147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.183.198.161	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
148.177.1.218	United States	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
77.127.239.68	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
93.172.116.167	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.25.102.57	Israel	147.237.76.30	himush.idf.il	20170: HTTP: Suspicious Range Header Field	Block	3
109.67.103.122	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.142.97.248	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
82.81.17.28	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
204.45.15.186	United States	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
80.82.69.128	Netherlands	147.237.77.216	dover.idf.il	C067: HTTP: attempt to access .config page	Block	2
212.25.79.205	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
94.126.81.100	Sweden	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
213.208.214.206	United Kingdom	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
217.12.204.163	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
95.30.146.146	Russian Federation	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
187.122.224.78	Brazil	147.237.77.176	matpash.idf.il	16643: HTTP: Protected File Access ( /proc/self/environ)	Block	1
101.181.130.74	Australia	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
95.30.146.146	Russian Federation	147.237.0.34	tikshuv.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
217.12.204.163	Ukraine	147.237.0.34	tikshuv.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
204.15.96.67	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
95.30.146.146	Russian Federation	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
193.169.71.243	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
95.30.146.146	Russian Federation	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
217.12.204.163	Ukraine	147.237.76.30	himush.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
140.232.211.8	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
2.54.54.177	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
95.30.146.146	Russian Federation	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
85.250.194.72	Israel	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
198.20.69.74	United States	147.237.8.24	e.lifestyle.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
217.12.204.163	Ukraine	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
95.30.146.146	Russian Federation	147.237.76.30	himush.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
80.179.205.25	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
5.29.147.113	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
95.30.146.146	Russian Federation	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
213.67.16.58	Sweden	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
69.30.215.122	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
198.27.82.147	Canada	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	109
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	55
198.143.138.122	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	20
198.143.138.122	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP login.htm access	20
198.143.138.122	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP admin.php access	17
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	15
198.143.138.122	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP adminlogin access	10
89.234.68.69	147.237.72.166	Ireland	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	10
66.249.83.254	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	5
198.143.138.122	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP backup access	4
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
188.138.9.51	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.232	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.67.224	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
185.58.201.28	147.237.77.170	Lebanon	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
176.13.12.184	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
80.82.69.128	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP .htaccess access	2
66.249.67.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.84.69	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.6	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.45	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
104.155.224.27	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	2
80.82.69.128	147.237.77.216	Netherlands	dover.idf.il	GPL WEB_SERVER .htaccess access	2
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.60	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.79	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
198.143.138.122	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
176.13.12.184	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
80.82.69.128	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP .htpasswd access	2
66.249.67.27	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
185.58.201.28	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	2
80.82.69.128	147.237.77.216	Netherlands	dover.idf.il	GPL WEB_SERVER .htpasswd access	2
66.249.65.17	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
200.114.65.142	147.237.72.156	Chile	aman.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
46.116.232.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.169.20.145	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
2.226.65.19	147.237.0.34	Italy	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.67.61.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.174.28.18	147.237.0.16	Italy	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.219.127.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.198.151.45	147.237.72.166	Europe	aka.idf.il	portscan: TCP Distributed Portscan	1
36.79.190.38	147.237.8.46	Indonesia	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
132.162.117.239	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
91.135.170.240	147.237.76.39	Austria	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
77.125.3.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.7.209.9	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24533
41.109.49.86	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8527
31.154.27.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4617
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3399
46.19.85.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3228
109.67.7.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2667
195.191.52.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1758
46.120.196.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1652
87.68.247.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1581
95.86.122.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1563
146.185.58.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1301
46.19.86.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1248
2.54.177.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1130
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1043
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1031
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	997
46.19.86.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	955
37.26.146.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	878
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	862
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	820
212.179.159.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	819
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	809
84.228.37.70	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	798
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	725
79.183.124.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	722
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	675
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	617
2.54.43.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	612
95.35.178.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	611
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	605
37.142.64.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	580
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	579
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	569
95.86.107.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	566
2.52.180.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	539
87.68.149.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	530
46.19.86.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	517
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	512
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	509
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	495
2.54.182.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	465
95.86.124.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	444
5.28.189.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	430
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	403
2.54.48.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	382
46.19.85.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	370
79.180.32.110	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	369
37.26.146.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	366
2.54.173.31	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	348
5.29.224.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	333

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.37.70	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.37.70	Block	156
176.13.12.137	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	115
132.74.211.94	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 132.74.211.94	Block	40
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	38
193.202.110.184	Netherlands	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 193.202.110.184	Block	29
109.64.221.199	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqantity.aspx	Block	28
149.88.143.163	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.143.163	Block	26
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	24
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.7	Block	23
72.9.148.10	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
95.86.115.228	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 95.86.115.228	Block	19
79.180.32.110	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.32.110	Block	18
66.249.83.218	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
5.28.140.117	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.28.140.117	Block	17
87.69.87.158	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.87.158	Block	16
92.105.25.0	Switzerland	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.141	Block	15
84.228.220.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.220.148	Block	15
212.25.102.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.25.102.57	Block	13
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
82.80.56.21	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.80.56.21	Block	12
81.218.241.25	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	12
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	12
46.116.80.231	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 46.116.80.231	Block	12
95.86.115.228	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
201.228.207.160	Colombia	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationsservice.aspx/getauthuser	Block	12
66.249.83.210	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
149.88.90.179	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 149.88.90.179	Block	11
176.12.137.34	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.34	Block	10
84.110.36.99	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtPersonalId in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	10
66.249.83.214	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/gyus/forum/asp/showforum.asp	Block	10
2.54.173.31	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.173.31	Block	10
138.134.102.16	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 138.134.102.16	Block	10
66.249.78.128	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
79.178.178.149	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/gyus/miyun/miyunprocessquestionnaire.aspx parameter	None	9
185.32.179.112	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	9
46.116.80.231	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	9
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	9
82.81.25.167	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	9
82.81.25.167	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	Block	9
213.57.157.76	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
213.57.157.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	8
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx	Block	8
84.228.220.148	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	8
46.116.80.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	8
46.116.80.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	8
46.120.69.107	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.120.69.107	Block	7
5.29.196.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	7