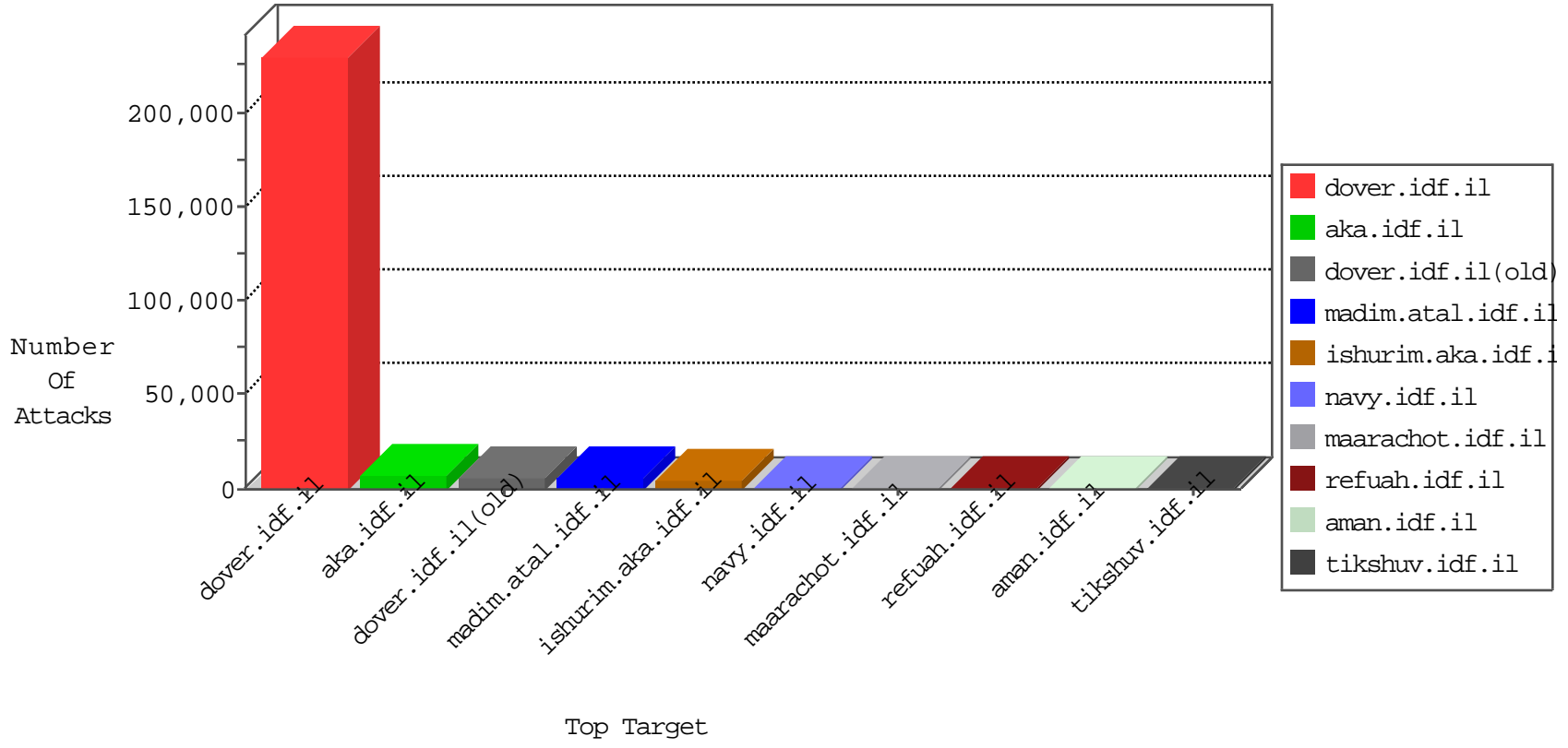


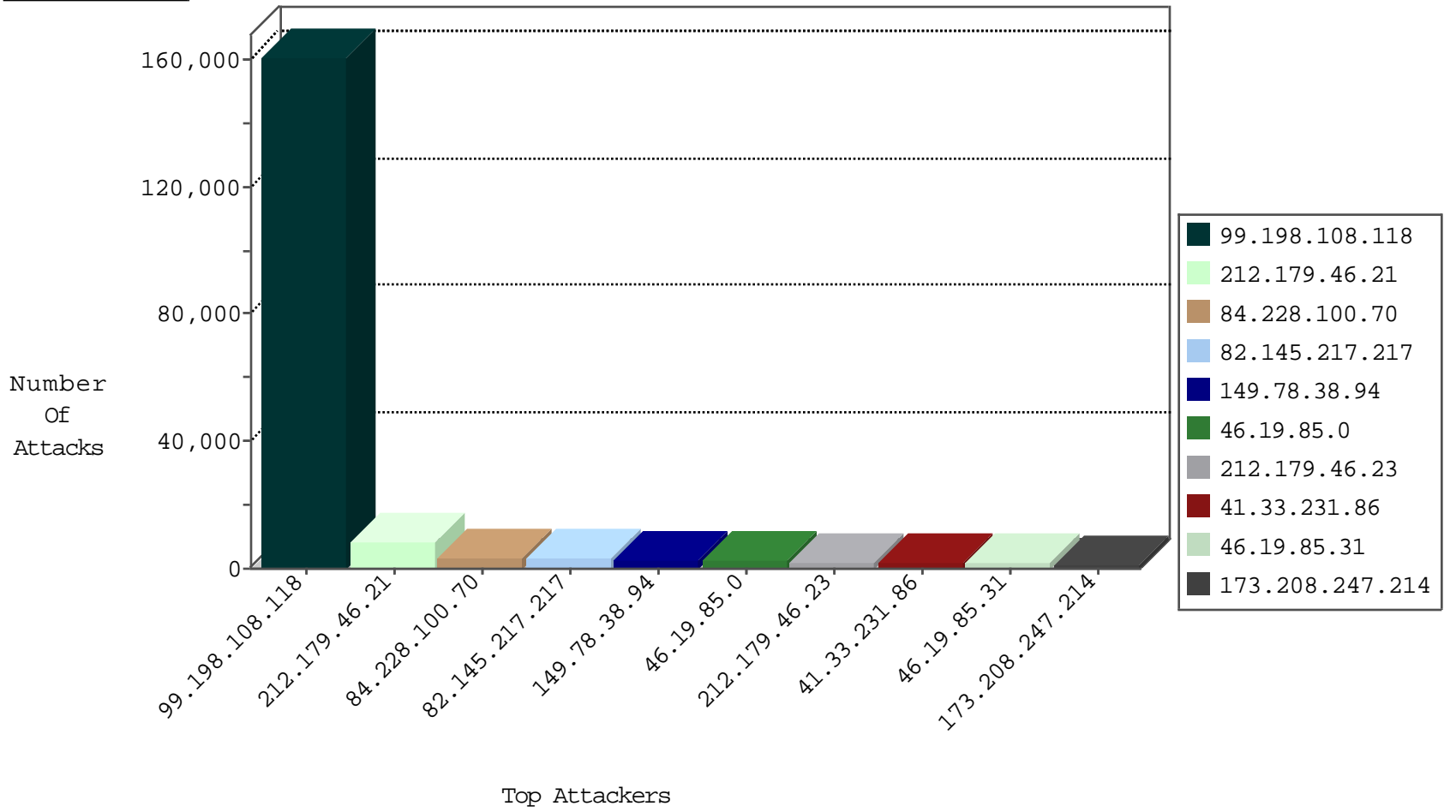
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.172	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	112108
66.249.78.115	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	77214
66.249.78.158	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	68882
66.249.78.101	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	51719
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	42199
66.249.78.108	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	29515
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	26750
66.249.78.165	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25610
66.249.64.45	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	18311
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16961
66.249.64.124	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	13656
66.249.64.37	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	9258
66.249.78.196	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	7660
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7442
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7291
66.249.64.41	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	7066
66.249.93.217	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6108
75.25.142.48	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6058
66.249.78.81	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5956
66.249.64.116	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5803
5.108.52.236	Saudi Arabia	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	5759
31.186.228.57	United Kingdom	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	5737
208.115.113.86	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	5514
66.249.64.170	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	4940
66.249.64.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4830
66.249.64.174	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	4537
66.249.78.203	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	4341
66.249.64.70	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	4063
80.99.212.128	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3778
85.25.43.84	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3714
66.249.64.120	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3678
66.249.67.23	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3562
68.180.228.121	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3528
66.249.78.95	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3486
66.249.67.39	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3482
66.249.78.21	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3338
66.249.78.37	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	3281
31.186.228.31	United Kingdom	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3254
144.76.95.232	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3143
184.58.212.189	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3046
66.249.89.36	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	3042
66.249.67.49	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2928
66.249.64.80	United States	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	2786
173.252.113.114	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	2723
66.249.64.74	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	2723
66.249.64.13	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2699
208.115.111.70	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	2677
84.94.192.40	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2597

11-15-2014-00:00:08 to 11-16-2014-00:00:08

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
31.186.228.23	United Kingdom	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	2590
66.249.78.44	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2583

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	22
27.153.248.175	China	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
27.153.248.175	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
27.153.248.175	China	147.237.77.234	halag.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
27.153.248.175	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
27.153.248.175	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
27.153.248.175	China	147.237.77.226	www.chamatz.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
61.19.69.198	Thailand	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	6
85.9.20.152	Romania	147.237.77.216	dover.idf.il	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	6
213.8.194.56	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
173.208.247.214	United States	147.237.77.216	dover.idf.il	C037: HTTP: Access to - windows/win.ini	Block	5
73.188.153.5	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
188.161.179.100	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
173.208.247.214	United States	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	4
69.60.121.29	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
185.32.176.137	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.121.206.101	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
136.199.223.61	Germany	147.237.72.14	dover.idf.il(old)	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.117.180.75	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
103.242.217.250	Bangladesh	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
171.25.216.131	Poland	147.237.77.74	law.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	2
88.228.106.24	Turkey	147.237.77.74	law.idf.il	10767: HTTP: Acunetix Security Scanner	Block	2
37.142.136.218	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.94.170.31	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
87.68.221.250	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.176.1.76	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
50.63.202.30	United States	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	2
82.80.216.184	Israel	147.237.72.14	dover.idf.il(old)	C041: HTTP: Access to - index.php?option=com_jce	Block	2
79.181.120.134	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.32	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.139.171.205	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
184.58.212.189	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
173.254.78.29	United States	147.237.77.74	law.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	2
87.106.179.253	Germany	147.237.77.74	law.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	2
213.8.194.56	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.29.100.170	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.94.165.216	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
176.228.21.162	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
89.138.227.144	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.120.31.40	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
87.68.75.26	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.182.130.72	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
130.185.139.213	Denmark	147.237.77.74	law.idf.il	C098: Block - dns poisoning	Block	1
95.15.226.134	Turkey	147.237.76.86	navy.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
46.19.85.69	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.65.62.34	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.10.148	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
91.200.12.75	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
84.228.123.155	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
2.54.32.130	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	239
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	126
176.12.141.215	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	14
79.177.80.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	10
95.86.119.148	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
109.64.149.156	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
61.19.69.198	Thailand	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	6
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	6
66.249.78.172	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
109.67.23.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
212.150.174.186	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.130.186	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.156.151	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.143.112.85	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	2
128.103.64.112	United States	147.237.72.14	dover.idf.il(old)	Tehila - Perl LWP with fake user agent	2
79.182.163.233	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.26.146.199	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.12.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.172.153.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.93.224	United States	147.237.0.17	m.ny-kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	2
173.208.247.214	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP WEB-INF access	2
84.228.185.157	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 4096	2
84.94.71.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	2
77.127.104.129	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
218.76.52.50	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	2
82.102.141.253	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.143.234.229	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.103.64.112	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
87.69.196.91	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.206.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.81.96	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.63.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.253.248.225	Turkey	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
79.176.170.85	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
218.77.79.43	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
46.120.125.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.19.235	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
64.14.51.142	United States	147.237.72.166	aka.idf.il	ET DOS SSL Bomb DoS Attempt	2
5.29.77.90	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
190.232.57.216	Peru	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
84.108.87.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
138.134.102.16	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.126.2.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.138.80.172	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
113.107.233.165	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
99.198.108.118	United States	147.237.77.216	dover.idf.il		drop	drop	160449
212.179.46.21	Israel	147.237.77.216	dover.idf.il		drop	drop	8613
84.228.100.70	Israel	147.237.77.216	dover.idf.il		drop	drop	3322
82.145.217.217	Europe	147.237.77.216	dover.idf.il		drop	drop	3312
149.78.38.94	Israel	147.237.72.14	dover.idf.il(old)		drop	drop	2622
46.19.85.0	Israel	147.237.77.216	dover.idf.il		drop	drop	2601
212.179.46.23	Israel	147.237.77.216	dover.idf.il		drop	drop	2106
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1627
46.19.85.31	Israel	147.237.77.216	dover.idf.il		drop	drop	1570
173.208.247.214	United States	147.237.77.216	dover.idf.il		drop	drop	1337
46.19.85.14	Israel	147.237.77.216	dover.idf.il		drop	drop	1234
149.78.159.22	United States	147.237.77.216	dover.idf.il		drop	drop	1017
208.115.113.89	United States	147.237.77.216	dover.idf.il		drop	drop	732
54.72.73.168	United States	147.237.77.216	dover.idf.il		drop	drop	721
208.115.111.73	United States	147.237.77.216	dover.idf.il		drop	drop	656
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	580
54.72.0.55	United States	147.237.77.216	dover.idf.il		drop	drop	579
212.179.21.194	Israel	147.237.77.216	dover.idf.il		drop	drop	469
109.65.10.21	Israel	147.237.77.216	dover.idf.il		drop	drop	375
93.172.167.188	Israel	147.237.77.216	dover.idf.il		drop	drop	372
66.249.78.158	United States	147.237.77.216	dover.idf.il		drop	drop	371
23.99.21.1	United States	147.237.77.216	dover.idf.il		drop	drop	360
66.249.78.172	United States	147.237.77.216	dover.idf.il		drop	drop	321
46.19.85.105	Israel	147.237.77.216	dover.idf.il		drop	drop	320
99.198.108.118	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	305
68.180.228.121	United States	147.237.77.216	dover.idf.il		drop	drop	292
31.30.47.96	Czech Republic	147.237.77.216	dover.idf.il		drop	drop	289
87.68.150.106	Israel	147.237.77.216	dover.idf.il		drop	drop	286
50.87.144.145	United States	147.237.77.216	dover.idf.il		drop	drop	285
95.86.114.54	Israel	147.237.77.216	dover.idf.il		drop	drop	283
99.198.108.118	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	261
208.115.111.70	United States	147.237.72.14	dover.idf.il(old)		drop	drop	248
195.34.150.18	Austria	147.237.77.216	dover.idf.il		drop	drop	235
213.247.64.26	Netherlands	147.237.77.216	dover.idf.il		drop	drop	229
95.108.158.233	Russian Federation	147.237.77.216	dover.idf.il		drop	drop	199
99.198.108.118	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		195
5.108.52.236	Saudi Arabia	147.237.72.14	dover.idf.il(old)		drop	drop	190
213.204.103.37	Lebanon	147.237.77.216	dover.idf.il		drop	drop	180
208.115.113.86	United States	147.237.72.14	dover.idf.il(old)		drop	drop	179
185.23.124.38	Saudi Arabia	147.237.77.216	dover.idf.il		drop	drop	179
213.8.129.142	Israel	147.237.77.216	dover.idf.il		drop	drop	169
205.189.187.4	Canada	147.237.77.216	dover.idf.il		drop	drop	162
37.142.120.236	Israel	147.237.77.216	dover.idf.il		drop	drop	160
46.19.85.213	Israel	147.237.77.216	dover.idf.il		drop	drop	152
213.205.230.246	United Kingdom	147.237.77.216	dover.idf.il		drop	drop	146
212.199.182.150	Israel	147.237.77.216	dover.idf.il		drop	drop	143
108.59.253.71	United States	147.237.77.216	dover.idf.il		drop	drop	141
75.25.142.48	United States	147.237.77.216	dover.idf.il		drop	drop	136
41.92.35.229	Morocco	147.237.77.216	dover.idf.il		drop	drop	128
212.179.46.20	Israel	147.237.77.216	dover.idf.il		drop	drop	124

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.141.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1340
46.121.70.148	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.70.148	Block	926
109.160.166.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	516
80.246.141.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	484
85.250.74.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	342
2.54.30.116	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.30.116	Block	324
80.246.141.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	308
2.54.191.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	302
10.110.110.38		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	216
46.19.85.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	211
2.54.185.25	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.185.25	Block	186
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	152
79.179.176.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	132
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.52	Block	87
84.228.66.3	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	79
109.66.4.158	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	75
95.86.97.181	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	73
84.110.75.52	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	57
213.151.56.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	54
66.249.64.116	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.116	Block	52
217.69.133.223	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	51
89.138.242.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	50
79.177.102.115	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	48
46.19.86.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
109.65.182.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
209.95.34.86	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	46
66.249.64.124	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.124	Block	44
84.228.44.79	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	44
109.65.6.33	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.65.6.33	Block	41
212.76.115.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	40
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	37
66.249.64.120	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.120	Block	36
213.57.158.251	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	36
94.159.186.0	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	35
109.65.182.83	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	35
66.249.78.101	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.101	Block	34
5.29.173.158	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	33
213.57.234.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	33
95.86.76.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	33
46.116.111.133	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	32
79.183.169.74	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	32
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	32
89.139.168.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	30
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
66.249.78.172	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.172	Block	29
66.249.78.94	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.94	Block	28
46.121.243.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	28
79.181.101.136	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	28
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	27
84.229.154.238	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Suspicious Response Code	Block	24