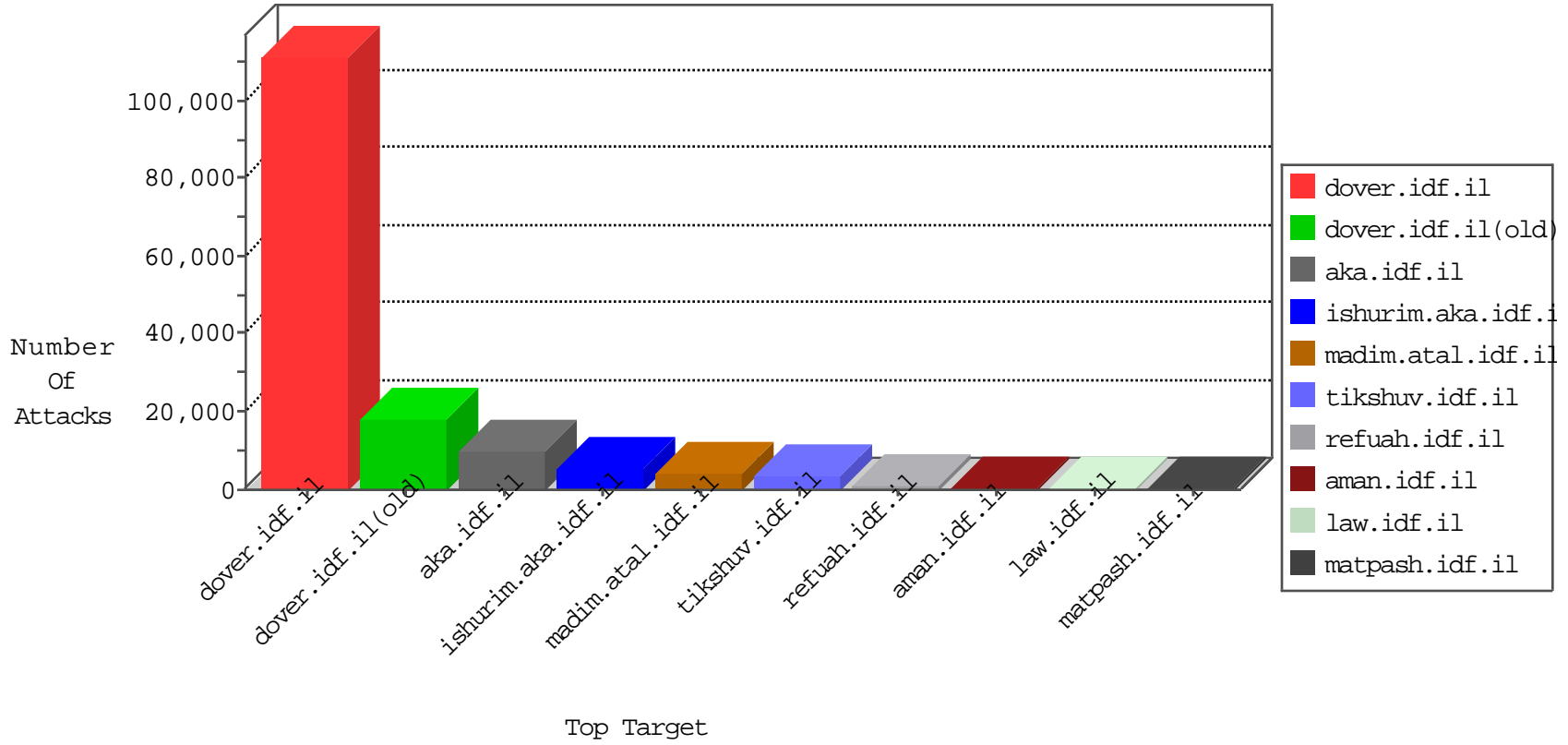


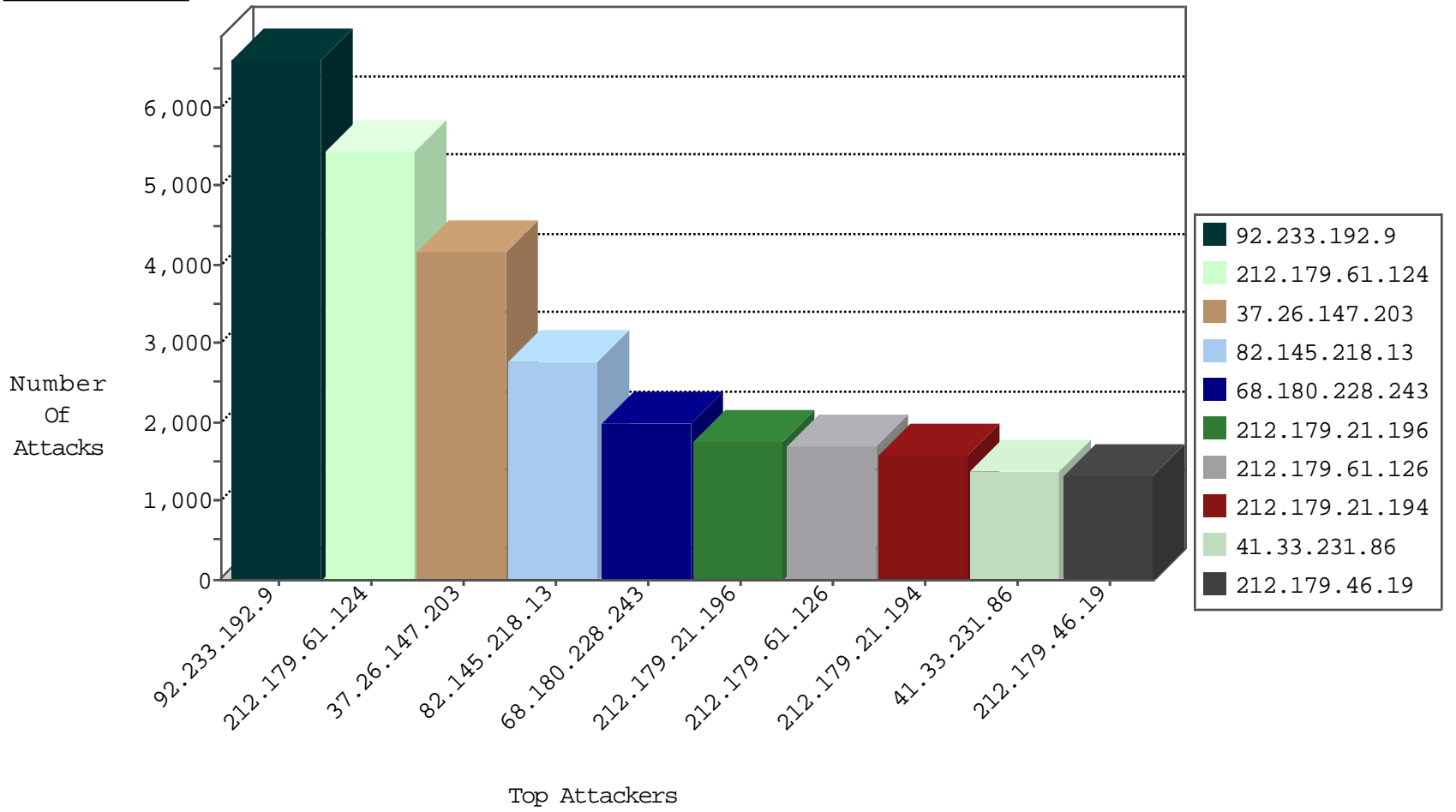
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	13198
66.249.64.45	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12833
66.249.78.165	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12377
66.249.78.172	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10012
82.145.219.28	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8612
66.249.64.37	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6736
66.249.78.158	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4678
68.180.228.243	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	4422
66.249.78.59	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4187
66.87.116.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3777
109.144.137.190	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3543
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3532
109.84.3.152	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3374
66.249.64.124	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3311
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	3129
91.246.218.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2994
31.52.59.150	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2732
5.29.56.176	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2639
66.249.78.203	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2586
66.249.78.21	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2398
66.249.78.133	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1999
66.249.67.41	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1742
66.249.67.49	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1728
27.153.233.66	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1358
148.177.129.210	Europe	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	1316
193.68.41.17	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1175
66.249.78.126	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1143
66.249.64.149	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1089
68.180.228.121	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1082
135.0.63.132	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1024
66.249.78.101	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	999
66.249.64.41	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	978
171.33.196.88	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	793
24.246.72.73	Canada	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	777
188.27.82.15	Romania	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	749
94.249.93.173	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	737
24.13.203.8	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	729
66.249.81.196	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	727
50.18.102.132	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	664
66.249.78.95	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	651
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	645
66.249.78.88	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	643
223.176.186.136	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	642
148.177.129.213	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	622
104.131.146.121		147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	619
66.249.67.62	United States	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	588
205.144.215.226	United States	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	586
220.181.125.15	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	560

11-18-2014-00:00:03 to 11-19-2014-00:00:03

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.120	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	558
222.99.244.216	Korea, Republic of	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	558

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il	Tehila_Rep_Block	Block	3973
27.153.233.66	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	119
85.9.20.154	Romania	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	53
162.255.180.197		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	34
198.57.228.2	United States	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	24
198.57.228.2	United States	147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	24
195.211.155.160	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	20
84.42.144.53	Czech Republic	147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
84.42.144.53	Czech Republic	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	11
104.194.12.145		147.237.72.14	dover.idf.il(old)	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
193.201.224.168	Ukraine	147.237.72.14	dover.idf.il(old)	C1000108: HTTP: Trying to locate existing FCKeditor	Block	7
87.69.88.251	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
103.242.217.250	Bangladesh	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
192.114.23.208	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
162.255.180.206		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
79.183.1.224	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
184.77.85.126	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
82.102.141.193	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
93.173.255.124	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
220.237.121.6	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
37.26.147.227	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
74.73.181.128	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
190.200.145.195	Venezuela	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.247	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
207.232.27.5	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.186.77.185	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
99.231.128.151	Canada	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
82.102.141.192	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
81.155.177.98	United Kingdom	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
93.172.20.81	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.229.127.104	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.179.191.98	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.181.194.186	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
128.240.225.121	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.253.34.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.84.81.209	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.120.121.72	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
93.173.154.82	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.13.61.52	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.102.141.205	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
68.83.208.212	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.93.189.161	France	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
188.165.243.209	France	147.237.77.74	law.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	2
104.194.12.145		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
63.156.59.66	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.75.66.70	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
106.138.62.39	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.12.63.97	France	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
185.14.20.122	Turkey	147.237.77.74	law.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	2
82.102.141.207	Israel	147.237.76.31	nakchal.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
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	147
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	91
79.177.159.199	Israel	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	56
82.102.141.203	Israel	147.237.76.42	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	35
212.199.143.202	Israel	147.237.0.19	madim.atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
37.130.227.133	United Kingdom	147.237.77.176	matpash.idf.il	SERVER-WEBAPP backup access	6
109.64.149.156	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
79.177.159.199	Israel	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	6
79.177.159.199	Israel	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	5
84.111.156.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
186.202.127.228	Brazil	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	4
84.109.211.20	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
213.57.245.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
46.116.254.144	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
37.9.84.253	Russian Federation	147.237.77.233	atal.idf.il	Tehila - Perl LWP with fake user agent	3
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	2
109.64.129.206	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.199.178.198	Singapore	147.237.77.74	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
212.179.243.144	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	2
91.236.75.11	Poland	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
2.54.10.106	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.168.88.140	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.87.186	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.117.43.92	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
17.78.122.225	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.111.231	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.98.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.179.196.109	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.2.204	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.27.75	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.8.33.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.93.189.161	France	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
5.102.216.34	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.67.63.90	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.94.75.117	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.155.196	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
194.114.146.227	Israel	147.237.72.156	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
218.77.79.43	China	147.237.76.176	test.noore.idf.il	ET SCAN Potential SSH Scan	2
46.116.102.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.195.195	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
68.190.126.16	United States	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
128.199.181.156	Singapore	147.237.77.74	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
85.64.217.75	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 1024	2
2.54.37.46	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
212.179.228.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.199.146.226	Singapore	147.237.77.74	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
79.176.124.110	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.145.227	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.121.202.69	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.124	Israel	147.237.77.216	dover.idf.il		drop	drop	5436
37.26.147.203	Israel	147.237.77.216	dover.idf.il		drop	drop	4141
82.145.218.13	Europe	147.237.0.34	tikshuv.idf.il		drop	drop	2763
92.233.192.9	United Kingdom	147.237.77.216	dover.idf.il		drop	drop	2402
212.179.21.196	Israel	147.237.77.216	dover.idf.il		drop	drop	1709
212.179.61.126	Israel	147.237.77.216	dover.idf.il		drop	drop	1696
68.180.228.243	United States	147.237.72.14	dover.idf.il(old)		drop	drop	1592
212.179.21.194	Israel	147.237.77.216	dover.idf.il		drop	drop	1569
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1376
212.179.46.19	Israel	147.237.77.216	dover.idf.il		drop	drop	1301
212.179.61.120	Israel	147.237.77.216	dover.idf.il		drop	drop	1243
176.88.50.94	Turkey	147.237.77.216	dover.idf.il		drop	drop	1166
109.64.185.46	Israel	147.237.77.216	dover.idf.il		drop	drop	1003
95.86.116.155	Israel	147.237.77.216	dover.idf.il		drop	drop	985
212.25.102.63	Israel	147.237.77.216	dover.idf.il		drop	drop	964
82.102.141.250	Israel	147.237.77.216	dover.idf.il		drop	drop	953
82.145.219.28	Europe	147.237.77.216	dover.idf.il		drop	drop	937
54.72.0.55	United States	147.237.77.216	dover.idf.il		drop	drop	915
193.68.41.17	Hungary	147.237.77.216	dover.idf.il		drop	drop	846
54.72.73.168	United States	147.237.77.216	dover.idf.il		drop	drop	782
208.115.113.89	United States	147.237.77.216	dover.idf.il		drop	drop	749
197.77.220.63	South Africa	147.237.77.216	dover.idf.il		drop	drop	708
77.127.43.165	Israel	147.237.77.216	dover.idf.il		drop	drop	684
171.33.196.88	United Kingdom	147.237.77.216	dover.idf.il		drop	drop	599
95.86.117.107	Israel	147.237.77.216	dover.idf.il		drop	drop	532
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	523
142.54.175.15	United States	147.237.77.216	dover.idf.il		drop	drop	519
212.179.61.127	Israel	147.237.77.216	dover.idf.il		drop	drop	514
50.87.144.145	United States	147.237.77.216	dover.idf.il		drop	drop	450
68.180.228.121	United States	147.237.77.216	dover.idf.il		drop	drop	449
89.138.195.114	Israel	147.237.77.216	dover.idf.il		drop	drop	449
77.126.27.11	Israel	147.237.77.216	dover.idf.il		drop	drop	427
91.64.172.51	Germany	147.237.77.216	dover.idf.il		drop	drop	416
162.213.197.163	United States	147.237.77.216	dover.idf.il		drop	drop	412
62.153.206.202	Germany	147.237.77.216	dover.idf.il		drop	drop	394
212.179.132.202	Israel	147.237.77.216	dover.idf.il		drop	drop	382
213.151.55.10	Israel	147.237.77.216	dover.idf.il		drop	drop	377
190.17.238.173	Argentina	147.237.77.216	dover.idf.il		drop	drop	368
190.24.146.71	Colombia	147.237.77.216	dover.idf.il		drop	drop	361
46.117.186.61	Israel	147.237.77.216	dover.idf.il		drop	drop	356
77.126.68.40	Israel	147.237.77.216	dover.idf.il		drop	drop	332
95.86.120.222	Israel	147.237.77.216	dover.idf.il		drop	drop	327
104.129.192.61		147.237.77.216	dover.idf.il		drop	drop	317
212.179.61.125	Israel	147.237.77.216	dover.idf.il		drop	drop	316
37.26.146.161	Israel	147.237.77.216	dover.idf.il		drop	drop	315
62.219.77.120	Israel	147.237.77.216	dover.idf.il		drop	drop	312
66.249.78.165	United States	147.237.77.216	dover.idf.il		drop	drop	307
2.54.40.237	Israel	147.237.77.216	dover.idf.il		drop	drop	305
195.34.150.18	Austria	147.237.77.216	dover.idf.il		drop	drop	302
65.49.68.170	United States	147.237.77.216	dover.idf.il		drop	drop	292

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.122.110	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.182.122.110	Block	489
46.19.85.76	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.76	Block	369
109.253.135.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	349
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	335
46.19.85.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	244
109.253.130.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	224
10.110.110.38		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	217
109.253.130.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	204
2.54.147.20	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.147.20	Block	189
31.168.181.79	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	188
37.130.227.133	United Kingdom	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 37.130.227.133	Block	188
185.32.179.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	172
176.12.144.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.144.45	Block	149
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	143
82.102.141.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	136
46.210.229.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	131
2.54.152.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	122
176.12.141.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	120
109.253.158.171	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.158.171	Block	116
109.253.129.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	103
80.246.138.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	91
176.12.156.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	91
176.12.138.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	90
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	72
157.55.39.135	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	69
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	67
85.64.39.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	65
66.249.78.158	United States	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.158	Block	59
79.178.172.189	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	55
157.55.39.123	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	53
80.246.138.100	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.246.138.100	Block	48
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	48
185.32.178.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
95.86.111.106	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	42
66.249.78.165	United States	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.165	Block	40
164.138.122.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	40
66.249.78.172	United States	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.172	Block	39
46.19.85.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	35
37.60.41.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	34
79.177.159.199	Israel	147.237.77.216	doover.idf.il	Multiple Admin Blocking from 79.177.159.199	Block	33
66.249.64.124	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.124	Block	33
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.94	Block	30
31.210.187.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	29
66.249.64.120	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.120	Block	27
79.182.6.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	26
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	26
80.246.138.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	25
81.218.176.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	22
66.249.78.94	United States	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.94	Block	21
93.173.154.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	21