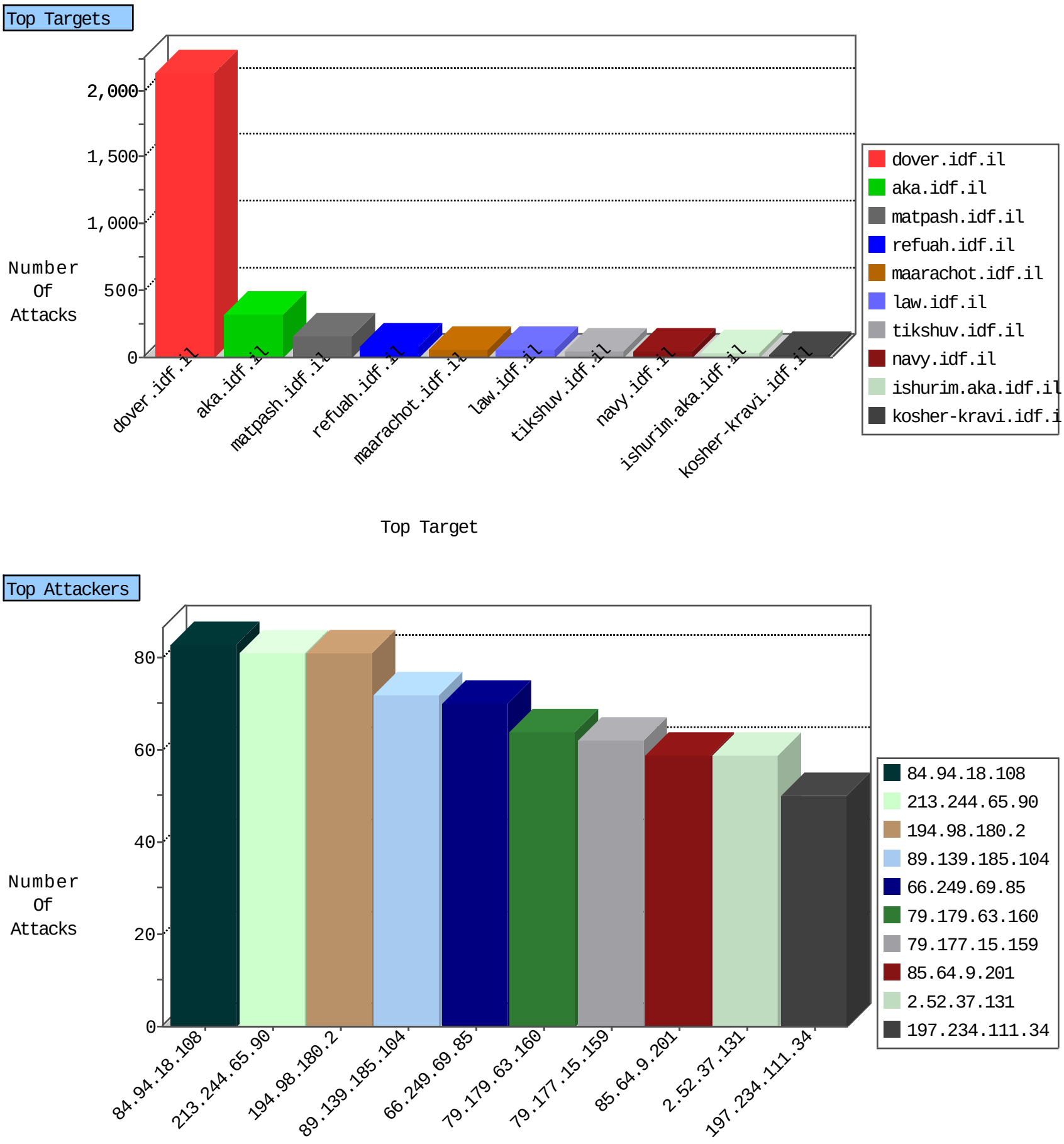
04-11-2015-13:03:08 to 04-11-2015-14:03:08

IDF Under Attack
04-11-2015-13:03:08



04-11-2015-13:03:08 to 04-11-2015-14:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.147	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	360
37.142.216.177	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
85.250.151.221	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	110
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	70
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	46
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	39
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	32
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	26
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	25
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	21
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	16
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.69.87	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	12
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
87.69.153.226	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.93.174	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	10
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
66.249.93.254	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.69.105	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.78.11	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.93.204	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.93.142	United States	147.237.77.243	mobile.idf.il	Block_Ip_Web_In	drop	5
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.67.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.146	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.93.212	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5
66.249.69.120	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	5
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	4
66.249.93.162	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	4
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.78.18	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4

04-11-2015-13:03:08 to 04-11-2015-14:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
91.207.4.22	Ukraine	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	5
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.29.33.196	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.121.26.21	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
93.120.27.62	Romania	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
79.179.63.160	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
149.78.229.75	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.111.114.29	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-11-2015-13:03:08 to 04-11-2015-14:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
61.160.224.130	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.210.234.87	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
180.210.234.87	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
104.131.210.84		147.237.0.16	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.128.144.130		147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.231	Netherlands	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
206.117.7.4	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.210.234.87	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
180.210.234.87	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
119.97.231.102	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.130		147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.56.231	Netherlands	147.237.77.19	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.236.44.115	Korea, Republic of	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1

04-11-2015-13:03:08 to 04-11-2015-14:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.94.18.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83
194.98.180.2	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
213.244.65.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	68
79.177.15.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
79.179.63.160	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	62
85.64.9.201	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
2.52.37.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
197.234.111.34	Namibia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
194.90.83.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
46.19.86.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
37.236.200.45	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
79.181.116.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
149.78.172.226	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
84.108.34.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
46.120.32.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
84.109.203.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
118.241.234.224	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
87.69.190.119	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
174.24.228.118	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
77.125.213.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
37.236.200.54	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
84.229.31.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
37.237.119.54	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
109.160.249.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
85.250.151.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
37.237.102.169	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
46.19.85.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
85.64.61.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
84.95.59.184	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
157.55.39.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
109.88.163.84	Belgium	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
49.98.156.220	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
78.95.101.80	United Kingdom	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	14
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
83.244.5.108	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
89.211.101.144	Qatar	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
46.19.85.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
94.159.155.119	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
109.253.145.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
78.95.101.80	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.221.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
85.64.94.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.186.146.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	3
5.102.254.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	3
79.182.111.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
109.65.117.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
162.243.110.109	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 162.243.110.109	Block	2
65.94.23.120	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
79.178.18.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.170.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.146.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.108.65.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
79.178.168.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
162.243.251.175	United States	147.237.76.86	navy.idf.il	Unauthorized Method HEAD for /	Block	1
46.117.214.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
149.78.229.75	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
87.69.210.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
2.54.16.221	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected , Observed ********** ********** ********** **********	None	1
79.182.170.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/giyus/haredim/haredim.aspx	None	1
37.142.175.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
84.228.166.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.63.160	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.179.63.160	Block	1
176.12.147.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.120.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.114	Block	1
93.172.187.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
79.183.24.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
157.55.39.206	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
77.125.1.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
46.19.85.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
109.253.128.115	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
79.182.111.81	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.111.81	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/grapheat.stm	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/november/6.stm	Block	1
61.135.190.72	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
104.131.210.84		147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
5.144.49.178	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.195.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
77.237.138.51	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on //	Block	1
46.19.86.32	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.133.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.79.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.82	Block	1
157.55.39.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.131.210.84		147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar	Block	1
84.94.88.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1