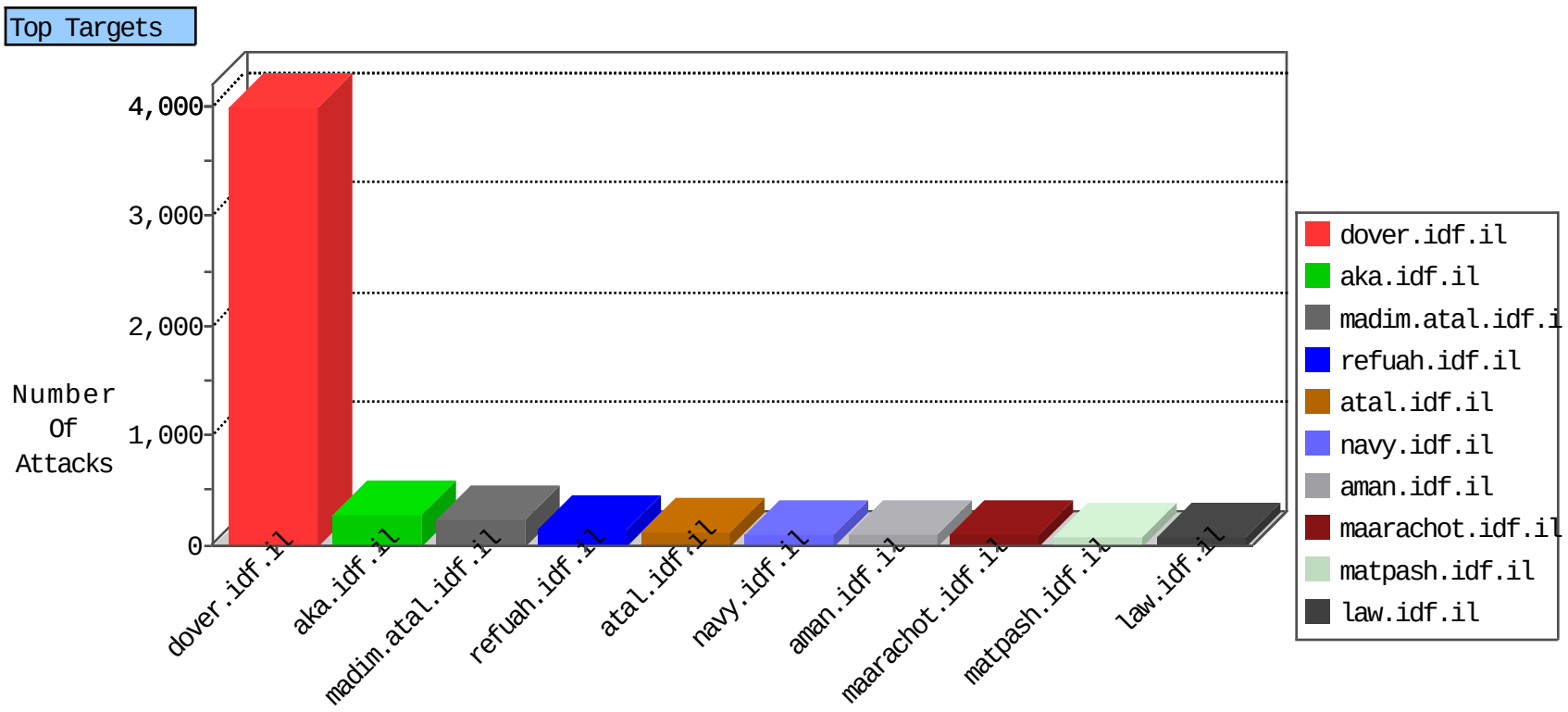
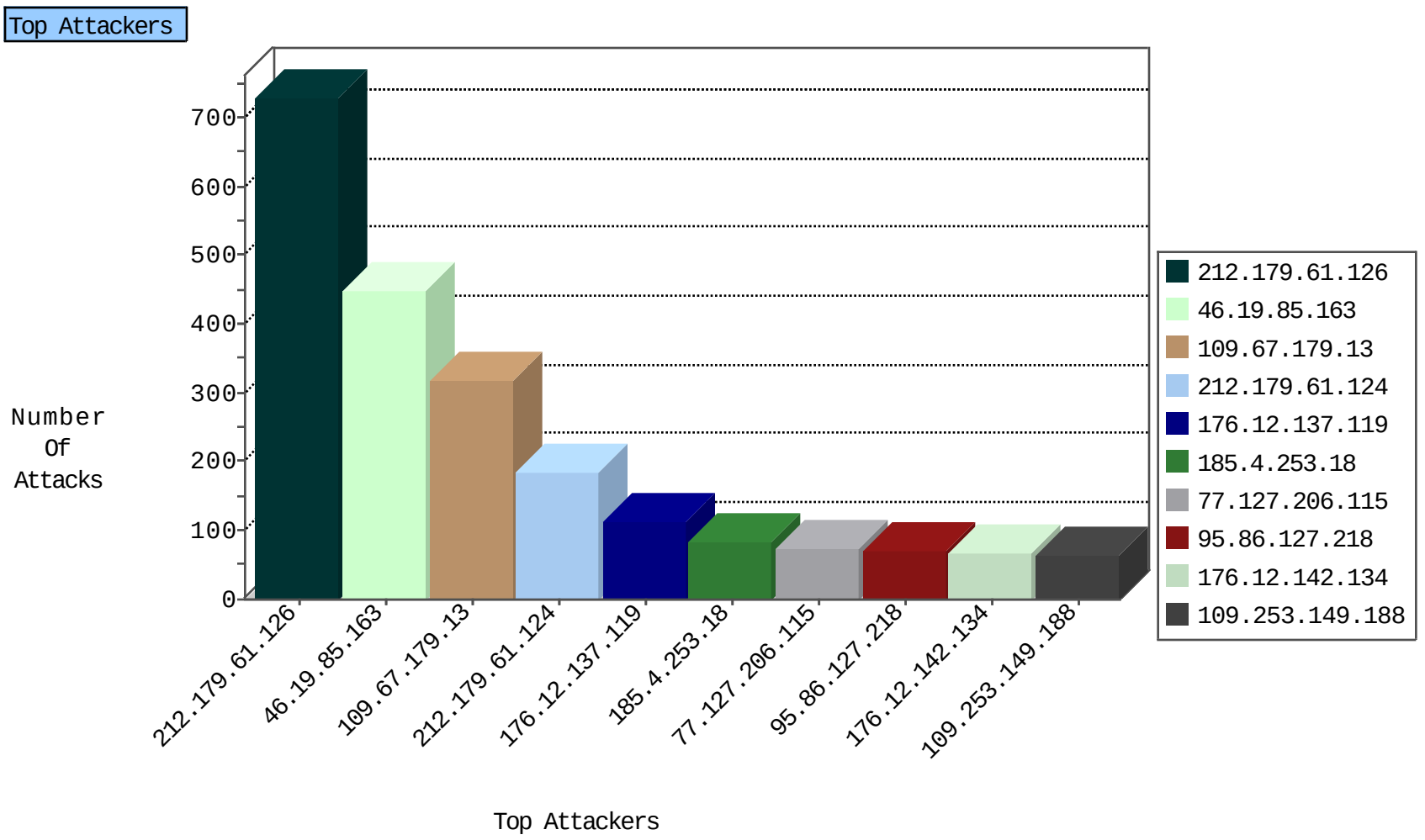
04-08-2015-11:03:06 to 04-08-2015-12:03:06

IDF Under Attack
04-08-2015-11:03:06

Top Targets



Top Attackers



04-08-2015-11:03:06 to 04-08-2015-12:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.85.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1207
207.46.13.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1082
24.0.95.198	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1010
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	894
109.253.132.248	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	886
46.19.85.248	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	660
216.185.39.231	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	631
199.30.24.66	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	599
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	557
46.121.194.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	511
85.250.255.33	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	399
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	259
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
2.54.148.96	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	221
46.19.85.163	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	211
212.199.182.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	198
5.29.171.56	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
46.19.86.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
79.177.176.124	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	47
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	43
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	40
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	38
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	33
66.249.75.44	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	33
66.249.75.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	32
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	32
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	29
66.249.75.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	27
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	27
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	26
66.249.67.13	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	26
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	25
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	23
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	22
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	22
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	19
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	19
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.69.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.81.218	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.69.58	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	14
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.69.66	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.81.215	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12

04-08-2015-11:03:06 to 04-08-2015-12:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.178.5	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.138	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
195.242.152.50	Netherlands	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.206.115	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
212.25.105.125	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
79.181.197.52	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.64.172.32	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-08-2015-11:03:06 to 04-08-2015-12:03:06

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	25
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
5.22.129.239	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
93.172.189.121	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.52.165.13	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
185.60.229.32		147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 2048	1
221.235.188.213	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.56	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.213	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.32		147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -f -sS	1
221.235.188.213	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.60	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.188.213	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.32		147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1

04-08-2015-11:03:06 to 04-08-2015-12:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	730
46.19.85.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	442
109.67.179.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	319
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	183
77.127.206.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
109.253.149.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
192.118.61.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
212.143.57.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
95.86.127.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
79.177.176.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
109.45.3.74	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
109.253.149.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
109.253.147.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
46.19.86.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
80.246.130.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	34
46.19.86.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
81.218.63.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.19.86.89	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
72.184.166.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.19.86.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.19.86.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
77.127.164.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
109.67.125.177	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	21
212.143.76.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
109.253.132.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
91.135.102.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
83.244.5.103	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
5.22.129.239	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	16
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
176.12.140.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.85.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.116.241.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.67.143.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.66.20.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
80.246.133.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.176.163.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
185.4.253.18	Lebanon	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	13
46.19.85.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
79.176.153.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
192.115.29.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.137.119	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.119	Block	111
176.12.142.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
176.12.150.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
95.86.127.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	15
77.126.163.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
80.246.130.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	7
84.111.112.224	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.65.128.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.234.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
109.160.218.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
176.12.136.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	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
109.64.101.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
94.230.86.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
72.184.166.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english address	Block	1
199.203.240.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/iturim/iturim.aspx	None	1
213.57.178.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
188.143.232.72	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.72	Block	1
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
2.54.4.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/atuda	Block	1
199.203.240.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter count in www.aka.idf.il/homas/site/resources/services/wsmaterials.asmx/getmaterialpossiblenamesbynamestart	None	1
109.66.115.172	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
216.218.206.67	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
188.143.232.72	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/searchresults/searchresults.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
61.135.190.201	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
2.54.156.86	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.127.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
80.191.200.75	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
212.101.252.7	Lebanon	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.143.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.108.167	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
216.244.83.168	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
84.228.56.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/terms.aspx	None	1
188.165.15.239	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
64.233.172.161	United States	147.237.72.166	aka.idf.il	Unknown Parameter moduleT.oGoTo in www.aka.idf.il/main/giyus/login.aspx	None	1
109.64.62.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.8.41.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
46.119.120.118	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/+	Block	1
126.203.209.78	Japan	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
93.172.61.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0202-5.stm	Block	1
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
176.12.137.119	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
80.246.130.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1