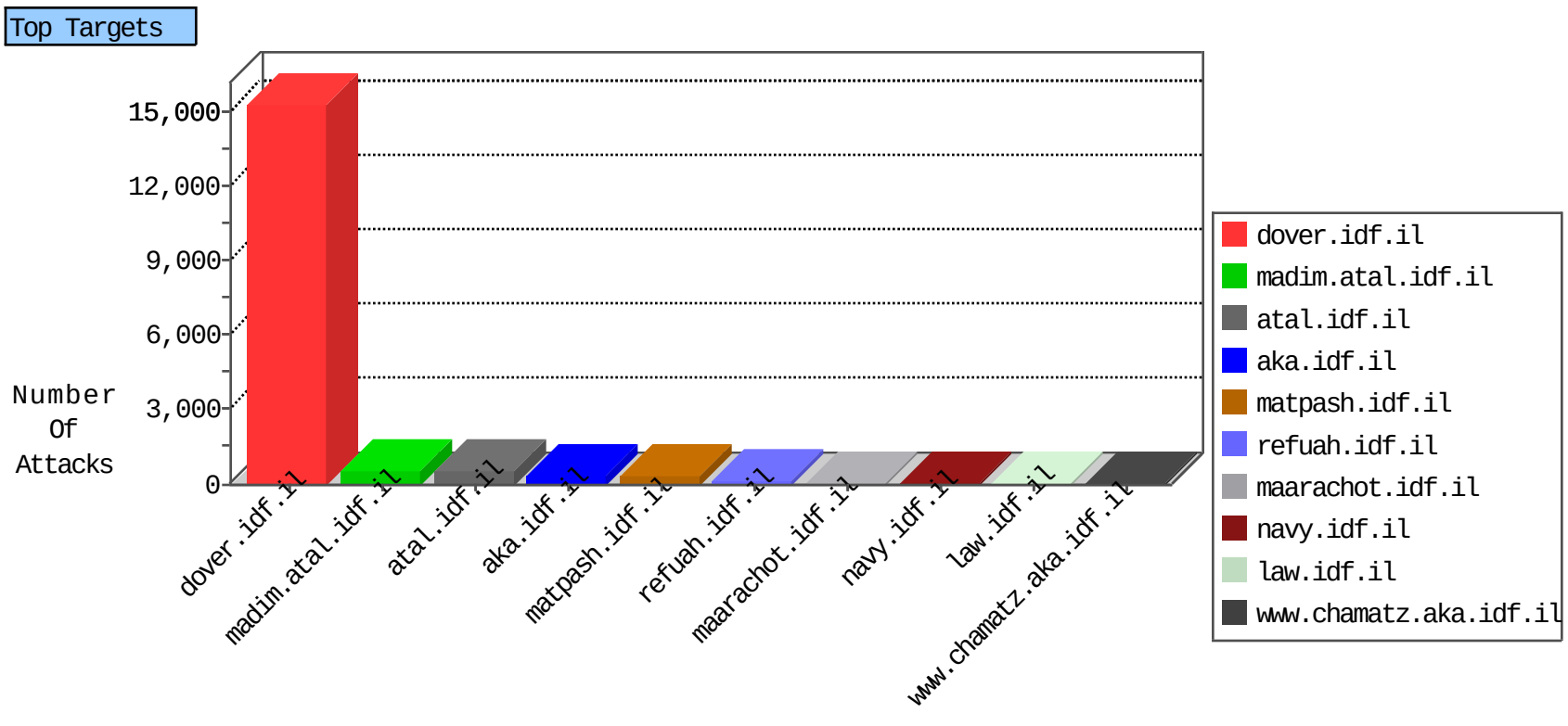
04-08-2015-14:03:01 to 04-08-2015-15:03:01

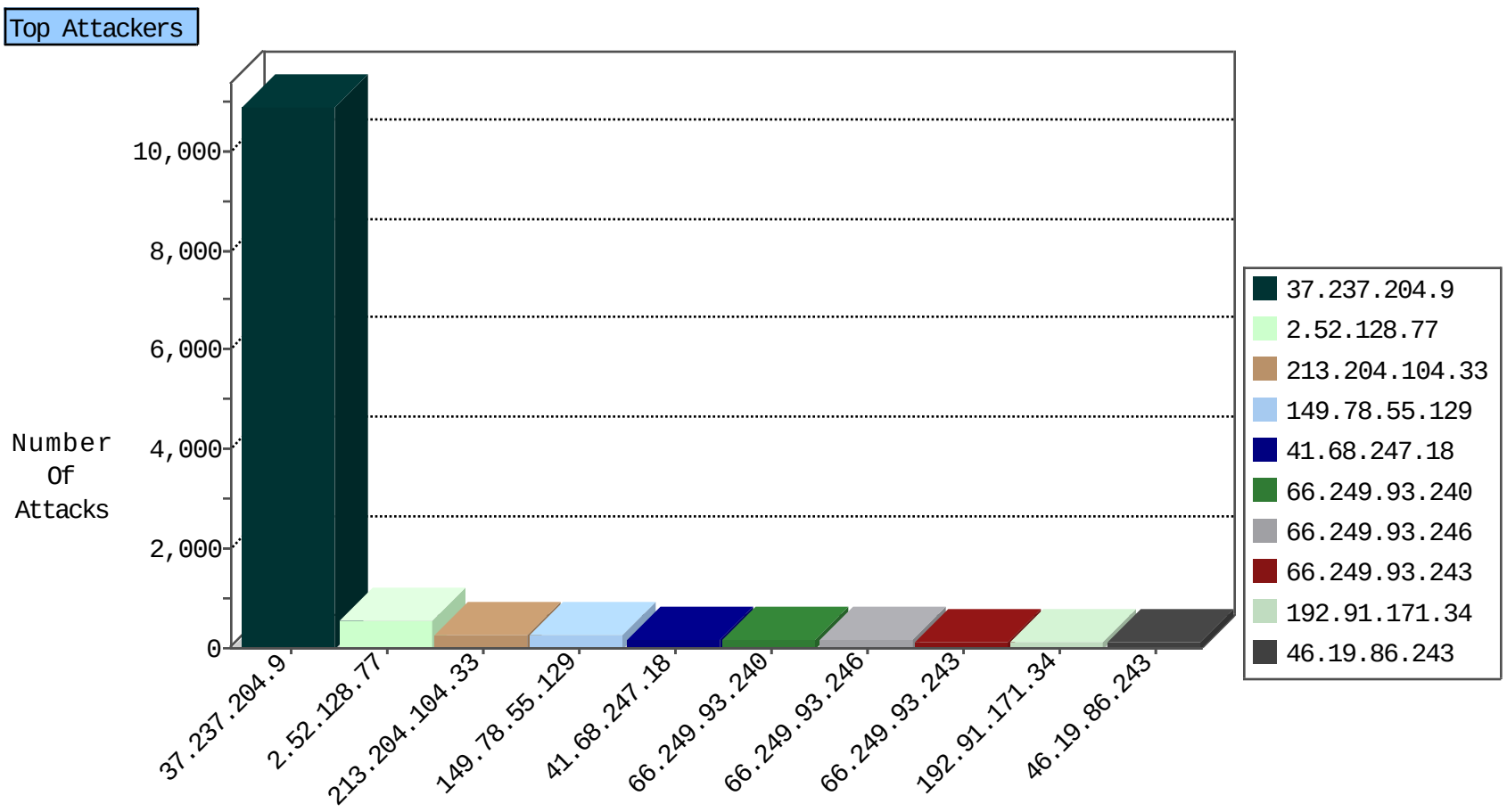
IDF Under Attack
04-08-2015-14:03:01

Top Targets



Top Target

Top Attackers



Top Attackers

04-08-2015-14:03:01 to 04-08-2015-15:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
136.243.5.219	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2849
62.210.90.118	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1058
85.64.249.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	886
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	820
213.204.104.33	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	650
82.80.25.221	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	451
10.0.0.3		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	355
46.19.86.243	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	340
80.246.133.72	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	335
82.145.219.185	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	283
66.249.93.240	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	174
66.249.93.246	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	163
149.78.127.118	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	155
37.237.204.9	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	151
66.249.93.243	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	139
66.249.93.171	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	105
66.249.93.175	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	83
84.108.168.122	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	80
66.249.93.179	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	75
157.55.39.41	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	60
66.249.64.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	27
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	27
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	26
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	24
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	23
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	22
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.93.154	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	20
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	19
66.249.67.21	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	19
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	19
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.64.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	18
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.67.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	15
66.249.64.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	15
66.249.93.249	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.67.159	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10

04-08-2015-14:03:01 to 04-08-2015-15:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.120.27.62	Romania	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.228	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
192.114.23.18	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
62.201.200.5	Iraq	147.237.77.216	dover.idf.il	10714: HTTP: Netsparker Security Scanner	Block	1
80.82.70.198	Netherlands	147.237.8.28	e.mobile-ks.idf.il	DVRep_P-N_40-59	Permit	1
80.82.70.198	Netherlands	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	1
46.19.85.205	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-08-2015-14:03:01 to 04-08-2015-15:03:01

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	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
62.201.200.5	Iraq	147.237.77.216	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	5
62.201.200.5	Iraq	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	5
109.67.0.135	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.201.200.5	Iraq	147.237.77.216	dover.idf.il	ET SCAN Netsparker Default User-Agent	2
87.69.162.253	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
175.143.109.18	Malaysia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.201.200.5	Iraq	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
122.228.207.76	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
61.240.159.254	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
50.252.197.194	United States	147.237.0.33	idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.76	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
50.252.197.194	United States	147.237.0.33	idf.il	ET SCAN NMAP -f -sS	1
128.61.240.66	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.159.254	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
50.252.197.194	United States	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.27	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-08-2015-14:03:01 to 04-08-2015-15:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.237.204.9	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10573
213.204.104.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	264
149.78.55.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	254
41.68.247.18	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	190
192.91.171.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	116
46.19.86.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	108
84.228.90.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	104
46.19.85.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
120.16.30.10	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	88
37.237.204.9	Iraq	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	86
46.19.85.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	80
31.25.137.84	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	80
89.108.159.50	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
84.108.168.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	64
5.22.129.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	62
94.159.175.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
41.134.235.1	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
82.145.219.185	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
185.26.182.38	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
84.109.115.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
46.19.86.36	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
41.248.173.14	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
176.12.143.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
79.180.15.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
212.76.98.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.141.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
79.182.216.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
71.190.218.119	United States	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.128.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
72.209.25.84	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
87.69.40.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.19.86.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
109.253.157.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
96.11.127.162	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
46.19.86.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.86.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
85.64.80.56	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	20
95.86.122.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
72.15.30.50	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
204.237.22.235	Canada	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
101.160.52.46	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
192.115.29.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.52.128.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.128.77	Block	540
37.237.204.9	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.237.204.9	Block	60
37.237.204.9	Iraq	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	57
149.78.181.22	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
79.182.179.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
77.127.32.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.8.87.156	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	3
89.189.85.74	Yemen	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	2
84.228.208.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.136.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.237.204.9	Iraq	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	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
94.230.86.187	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.79.54	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/miluim/login.aspx	None	1
79.178.172.64	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
212.235.18.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.96.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	1
80.246.141.100	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	1
5.29.39.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.179.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
213.204.104.33	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en/	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.128.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
93.172.151.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
84.94.140.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.229.27	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
188.138.17.205	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
31.25.137.84	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//en/	Block	1
109.67.56.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
85.64.80.56	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
79.180.136.172	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/login/	None	1
93.173.242.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.108.10.216	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/medical/medical.stm	Block	1
149.78.89.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
85.65.177.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
79.182.62.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.143.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.57.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.228.39.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
207.46.13.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1360-he/atal.aspx	Block	1
85.250.95.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
176.12.144.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fatah/english/main_index.stm	Block	1
2.54.189.41	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1