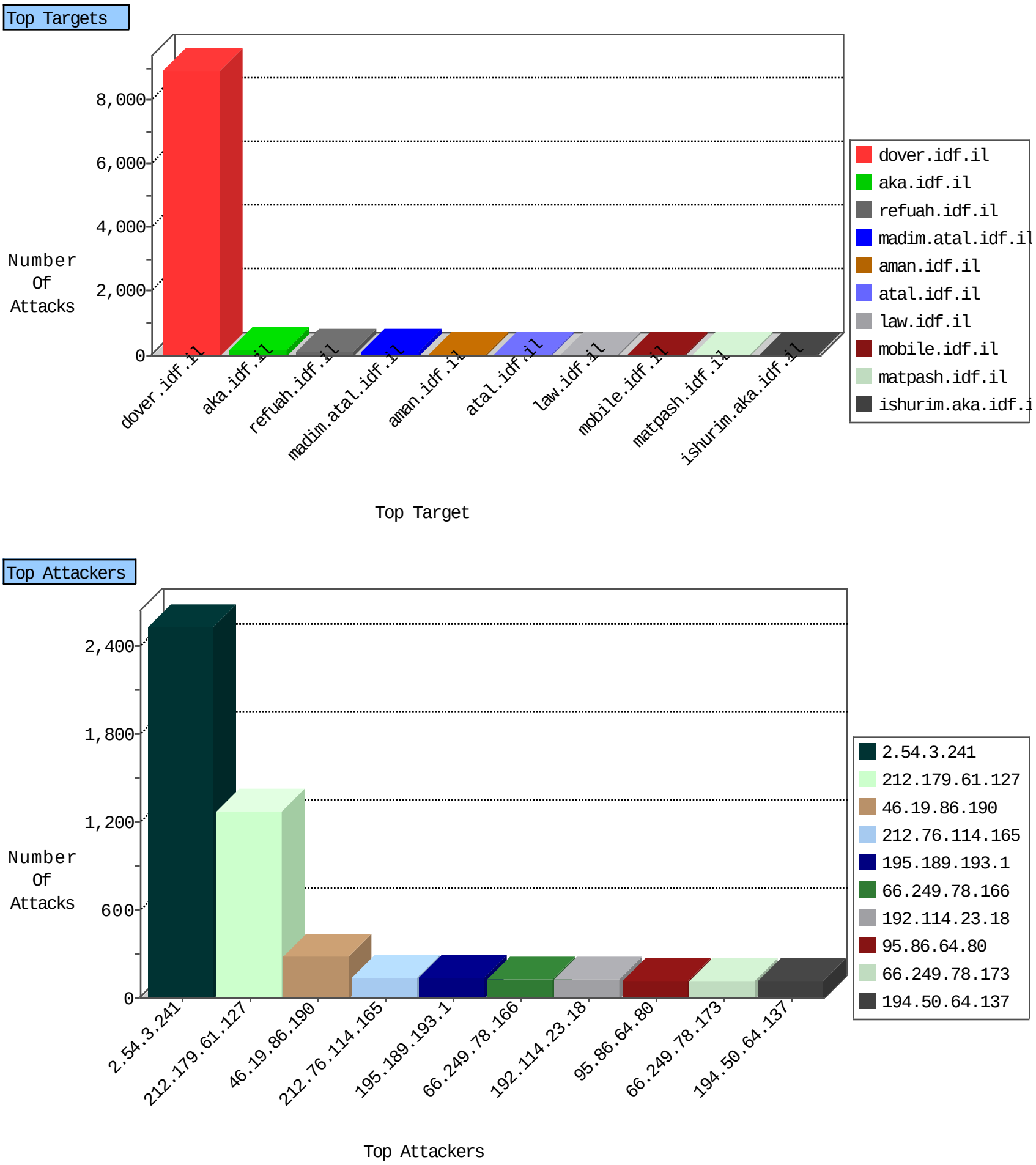
04-16-2015-11:03:05 to 04-16-2015-12:03:05

IDF Under Attack
04-16-2015-11:03:05



04-16-2015-11:03:05 to 04-16-2015-12:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.79.42	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2680
149.88.86.62	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
46.121.58.224	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
31.168.101.163	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	40
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
82.102.141.250	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	10
192.115.139.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
132.66.31.192	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
37.26.147.198	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.176.49.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
211.247.22.8	Korea, Republic of	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	4
91.208.129.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
79.176.105.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
66.249.79.13	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
91.208.129.129	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
81.218.0.158	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.139.252	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.171.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
23.229.51.42	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
188.65.81.178	Italy	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
109.66.114.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.102.141.251	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

04-16-2015-11:03:05 to 04-16-2015-12:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
194.90.134.226	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	7610: IP Reputation	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	7610: IP Reputation	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.216	dover.idf.il	7610: IP Reputation	Block	1
37.26.148.170	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	7610: IP Reputation	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	7610: IP Reputation	Block	1
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.111	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
79.176.164.119	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.200	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	7610: IP Reputation	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
80.246.137.159	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
46.120.244.134	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.66.115.240	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	7610: IP Reputation	Block	1

04-16-2015-11:03:05 to 04-16-2015-12:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
60.208.72.139	China	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
2.52.47.89	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.55	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.92.134	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.188	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	Cote D'Ivoire	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
192.115.97.253	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
43.255.191.163	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
176.12.138.116	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.160.205	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
86.123.141.107	Romania	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.238	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.58	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
43.255.191.163	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.32.177.181	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.163	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
149.78.196.106	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-16-2015-11:03:05 to 04-16-2015-12:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.3.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2522
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1280
46.19.86.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	287
212.76.114.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	142
195.189.193.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	139
192.114.23.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	125
95.86.64.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	122
194.50.64.137	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	117
5.108.3.172	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	102
109.65.2.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
87.68.62.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
212.107.105.226	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
37.26.148.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	64
203.35.82.165	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
213.57.61.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
80.246.133.237	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	59
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
85.250.15.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
192.114.91.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
91.231.92.29	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
46.19.86.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
62.90.35.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
46.19.86.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
2.54.163.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
87.68.218.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
80.246.133.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
46.117.229.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
213.57.165.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
137.191.224.106	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
37.26.148.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
82.80.248.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
212.199.11.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
147.236.138.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
46.19.86.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
80.246.133.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
46.19.86.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
66.249.64.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
64.134.96.240	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.34	Block	103
66.249.79.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//console/core/doc_mgr/general.aspx	Block	5
66.249.79.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//console/core/doc_mgr/general.aspx	Block	4
81.218.251.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
85.250.52.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
37.26.147.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.86.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.67.100.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.183.118.143	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
85.65.106.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.73.211	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.73.211	None	2
66.249.79.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.79.5	Block	2
99.226.210.156	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
37.26.148.170	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
80.246.133.237	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
212.76.111.244	Israel	147.237.72.166	aka.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
68.180.229.36	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.79.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
46.210.216.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
84.228.128.115	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/forms.aspx	None	1
5.135.165.89	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.90.134.226	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.79.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9237-he/refuah.aspx	Block	1
89.139.27.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
80.246.133.252	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
212.107.105.226	Saudi Arabia	147.237.77.74	law.idf.il	Suspicious Response Code	Block	1
69.171.227.113	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0305-4.stm	Block	1
85.64.23.147	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
62.90.99.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
79.183.189.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.13.112.118	Ireland	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.13.112.118	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
91.208.139.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/june/26.stm	Block	1
212.143.172.93	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.79.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1396-he/atal.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.12.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
31.13.112.119	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/common/includes/globaltopbar/resources/images	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.133	Block	1
66.249.79.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
95.173.189.7	Turkey	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version	Block	1
46.19.85.111	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
82.80.86.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.37.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.37.191	Block	1