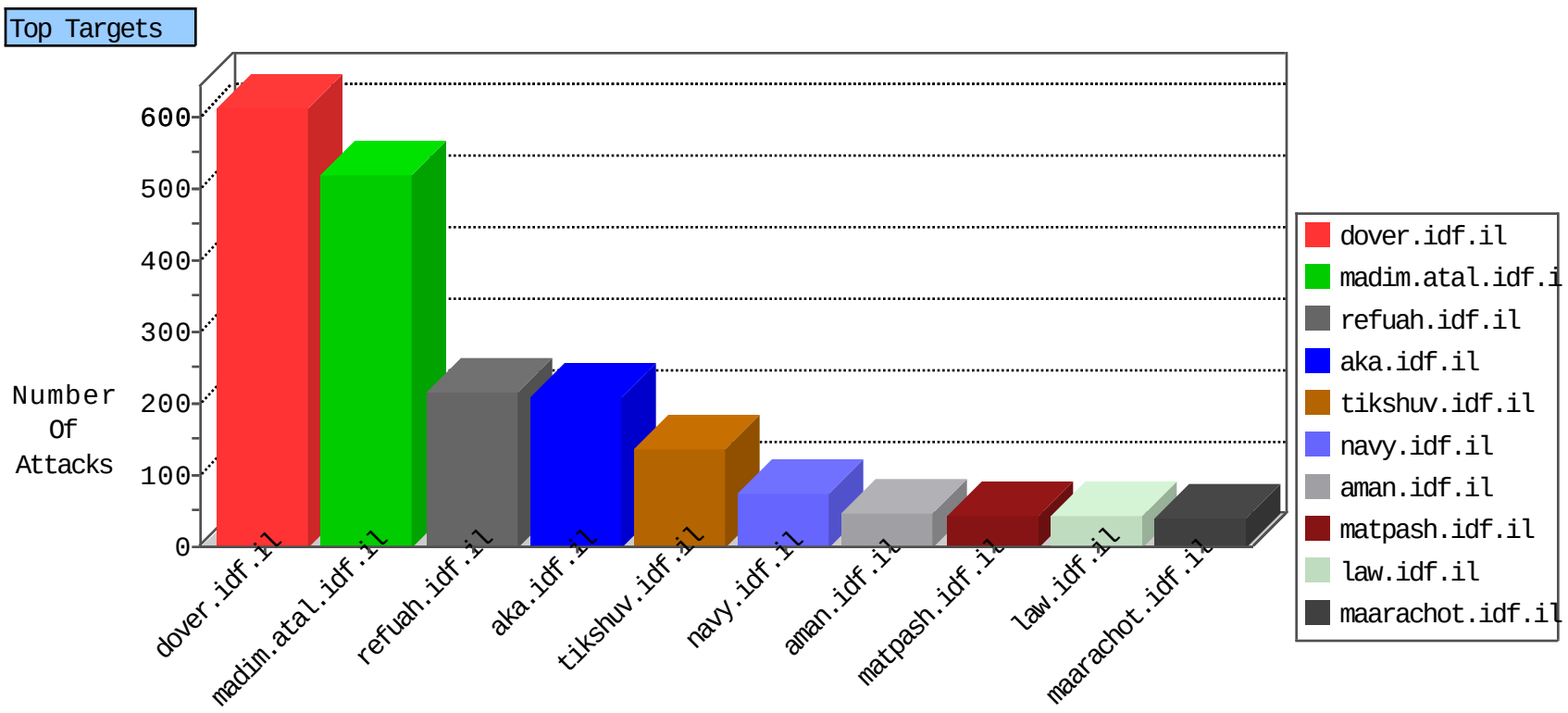
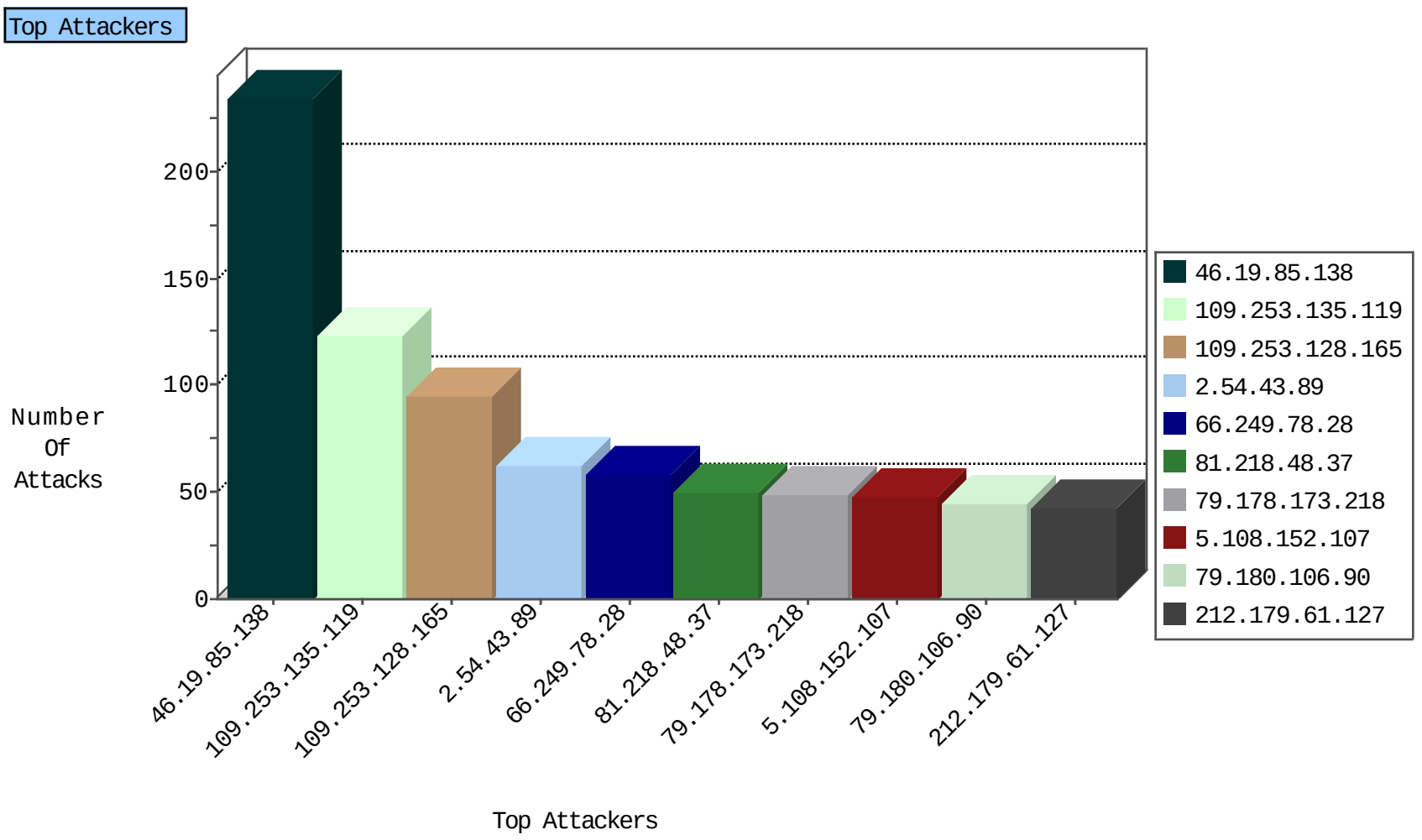
04-12-2015-11:03:04 to 04-12-2015-12:03:04

IDF Under Attack
04-12-2015-11:03:04

Top Targets



Top Attackers



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
81.218.186.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	220
80.246.139.231	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	58
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	40
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	40
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	33
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	32
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	29
66.249.93.168	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	20
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	20
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	20
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	20
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	20
87.69.144.172	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	17
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
85.250.83.16	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	9
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.65.200	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	8
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.65.177	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ip_Web_In	drop	7
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.64.59	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
79.183.52.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.64.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.5.245	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.178.173.218	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
213.57.73.176	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.108.116.208	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.64.82.184	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

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

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
31.168.230.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.6.186	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243		147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
213.244.123.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.4.207	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.7.41	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.87.4	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
63.251.104.172	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
176.12.139.140	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
46.162.115.130	Sweden	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.245.97	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.88.239	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.209.108	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.160.39	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.204.117	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.34.114	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.187.15	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.160.113	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
63.251.104.172	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
176.12.143.148	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
124.234.13.254	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
113.21.226.56	New Zealand	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.89.79	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
93.173.38.115	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.43.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	62
81.218.48.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
5.108.152.107	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
79.178.173.218	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	43
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
212.150.189.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.116.88.239	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
62.219.229.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
212.199.244.112	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.121.253.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
212.117.143.250	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
82.80.179.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
212.117.143.250	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	8
94.159.238.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
132.69.202.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.179.162.234	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
212.117.143.250	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
132.64.30.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
148.177.129.212	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
62.0.103.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.29.147.167	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
212.76.96.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.179.46.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.102.254.107	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
79.183.101.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
109.160.203.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.153.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.125.6.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.65.239.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
199.203.61.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.131.247.74	Italy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.64.195.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.143.120.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.145.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
86.85.5.55	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.51.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.109.105.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
62.219.62.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
132.72.10.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.102.254.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
90.215.71.5	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.235.26.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.144.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
140.242.217.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.173.147.203	Israel	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
109.253.135.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	123
109.253.128.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	95
79.180.106.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
31.168.71.189	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	34
85.7.204.38	Switzerland	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.7.204.38	Block	21
109.253.143.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
5.102.254.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
77.127.232.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
81.218.164.125	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
212.150.112.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
149.78.232.153	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
80.246.138.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	Block	2
212.16.233.141	Germany	147.237.0.34	tikshuv.idf.il	PHP Attempt	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
62.90.131.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
147.235.185.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
46.117.137.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.69.58.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.108.227.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.186.128.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.147.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
213.8.62.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
195.248.193.136	Falkland Islands (Malvinas)	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
62.219.126.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.157.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.19.86.12	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
89.138.81.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
2.54.27.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.186.147.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
54.153.14.125	United States	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
38.126.15.49	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
217.69.136.203	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/hamez.stm	Block	1
85.7.204.38	Switzerland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/[object object]	Block	1
195.248.193.136	Falkland Islands (Malvinas)	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
79.180.179.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.219.209.173	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
132.66.50.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.25.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
93.172.164.66	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.27.79.18	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
2.54.144.224	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
212.150.112.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.112.56	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx	None	1
38.126.15.49	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
85.250.238.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.179.135	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gyius	Block	1