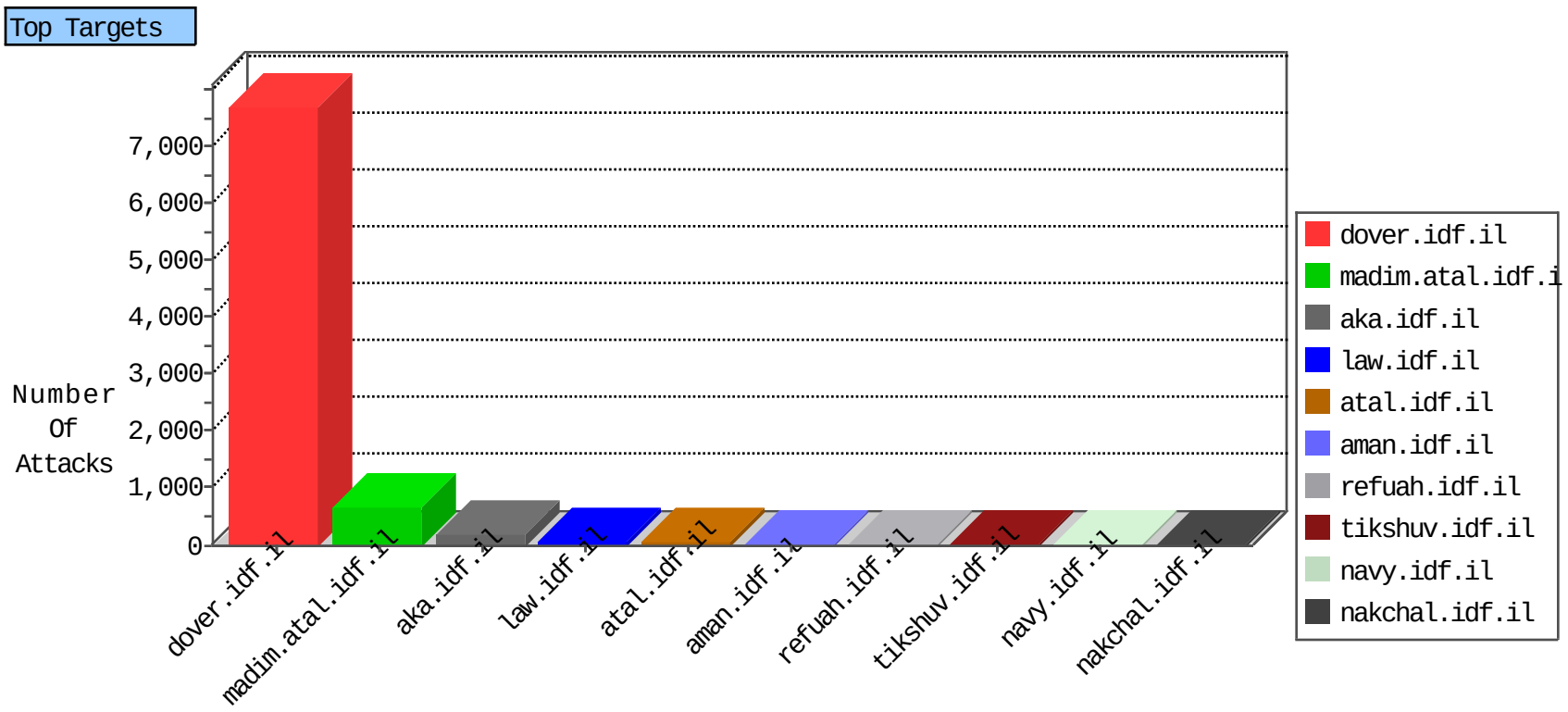
05-04-2015-15:03:06 to 05-04-2015-16:03:06

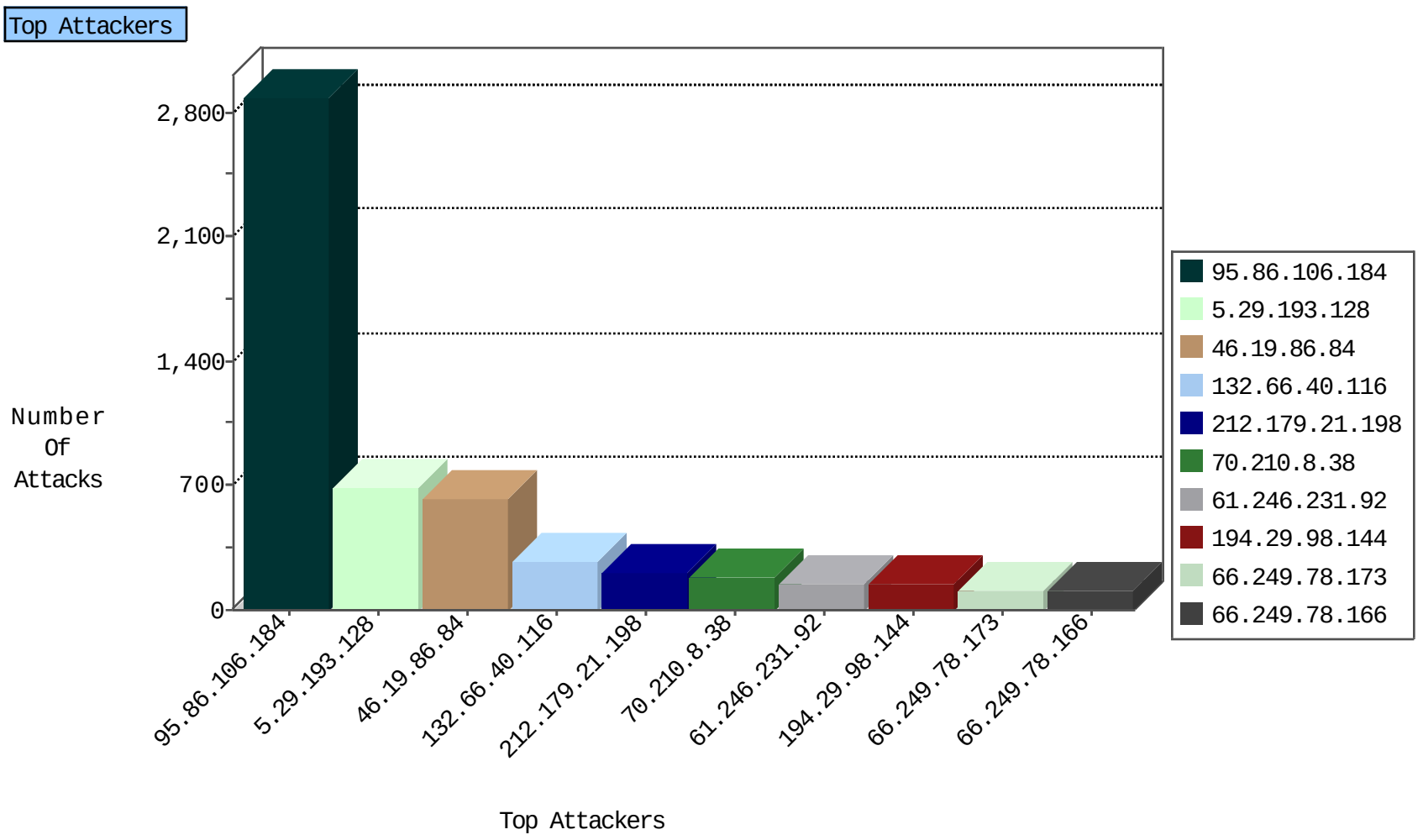
IDF Under Attack
05-04-2015-15:03:06

Top Targets



Top Target

Top Attackers



Top Attackers

05-04-2015-15:03:06 to 05-04-2015-16:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2941
95.86.106.184	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	75
220.181.108.182	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	39
95.86.65.236	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
46.19.85.167	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
85.64.69.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
192.117.113.18	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.40.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.142.240.211	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.102.141.251	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
37.46.45.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.179.229.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.84.138.124	Netherlands	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
80.246.137.67	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.170.84.37	Italy	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.94.97.31	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.253.158.115	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
31.210.186.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-04-2015-15:03:06 to 05-04-2015-16:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.167	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.176.122.245	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.167	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.182.186.167	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
70.114.237.95	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.199	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
194.90.7.35	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.43.94	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
213.57.89.62	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	7610: IP Reputation	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
37.26.147.205	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.175	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
37.59.19.32	France	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
80.82.65.61	Netherlands	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.15	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
80.82.65.61	Netherlands	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
212.179.46.20	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	7610: IP Reputation	Block	1

05-04-2015-15:03:06 to 05-04-2015-16:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.184.3	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
50.157.171.74	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.155.229.165		147.237.77.121	e.navy.idf.il	ET SCAN NMAP -f -sS	1
2.54.168.159	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.132.118	Russian Federation	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.87.92	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.106.146	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
62.219.111.242	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
180.113.238.30	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
104.155.229.165		147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
31.44.132.79	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.60.140	Netherlands	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.35.121	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
82.80.136.92	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
69.119.43.198	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
188.95.158.198	Ukraine	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1

05-04-2015-15:03:06 to 05-04-2015-16:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.106.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2886
46.19.86.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	619
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	272
212.179.21.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	183
70.210.8.38	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	177
61.246.231.92	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	144
194.29.98.144	Belgium	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	142
194.126.7.147	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
46.19.85.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
80.230.47.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
79.183.135.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
109.253.133.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
37.26.148.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
95.86.84.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
194.114.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
79.179.129.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
208.54.37.151	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
212.25.84.200	Israel	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	39
37.58.49.75	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
95.86.108.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
62.219.116.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
190.195.232.2	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
2.54.40.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
213.57.148.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
82.80.59.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
109.64.49.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
192.116.98.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
5.29.24.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
212.29.252.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
212.179.21.198	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	19
212.235.98.139	Israel	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	19
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
85.64.69.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
212.199.233.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
81.218.116.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
212.143.159.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.29.193.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	684
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	30
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	25
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	21
46.121.245.189	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.245.189	Block	16
87.68.253.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	10
84.108.218.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	6
212.143.99.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
192.187.126.162	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.187.126.162	Block	6
192.117.186.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
194.90.7.35	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
212.76.113.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
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	4
109.253.140.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	4
84.94.67.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.160.132.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.52.27.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.142.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//www.tikshuv.idf.il	Block	3
46.121.124.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	3
157.55.39.107	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.107	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	3
63.217.168.125	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
109.67.201.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
81.218.28.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.28.58	Block	2
46.229.164.111	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	2
109.160.183.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
31.168.200.45	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.205.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
94.159.190.96	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
212.29.241.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
192.117.101.245	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
37.142.146.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.224.131	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.224.131	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	1
109.253.141.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.176.182.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.56.220	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
54.205.88.118	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.124.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.9.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.67.22	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
185.32.176.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1