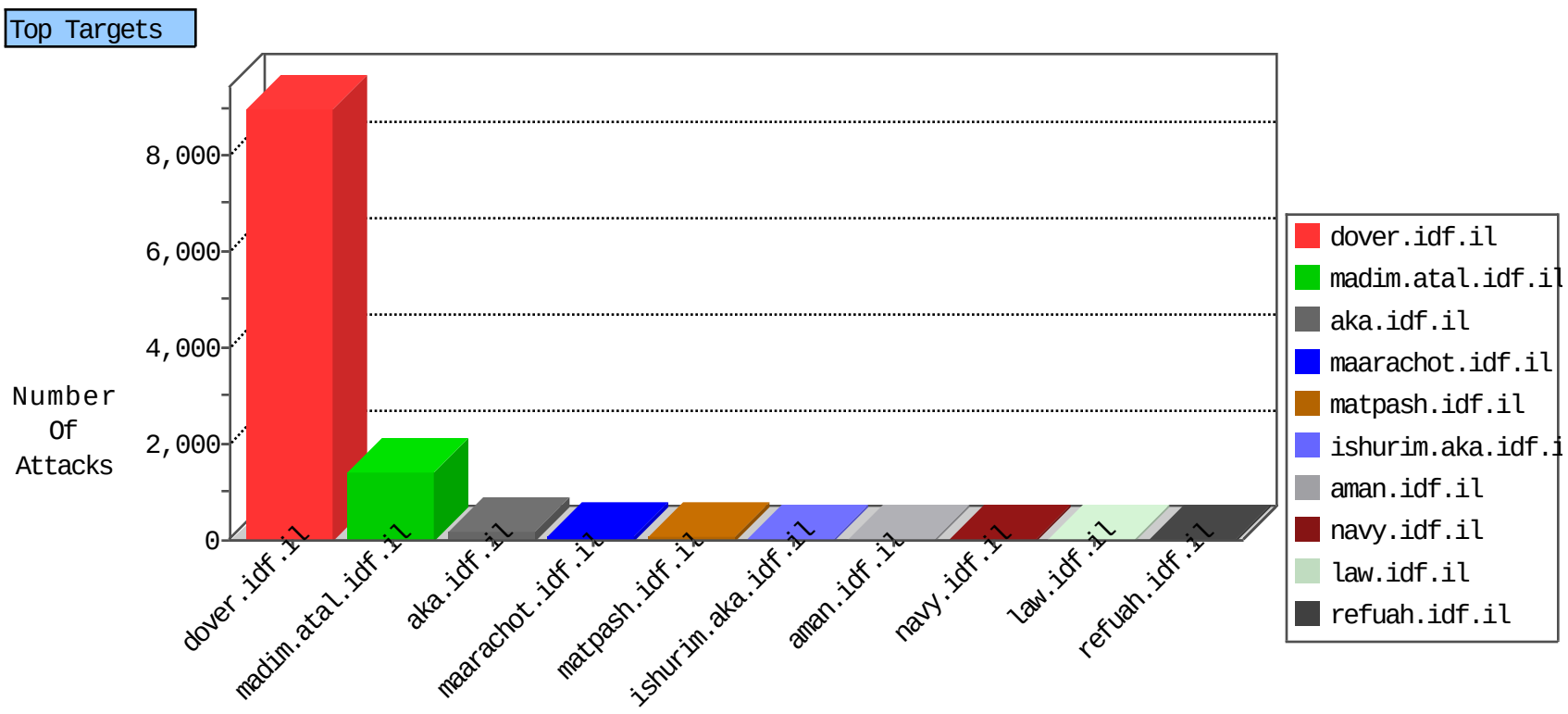
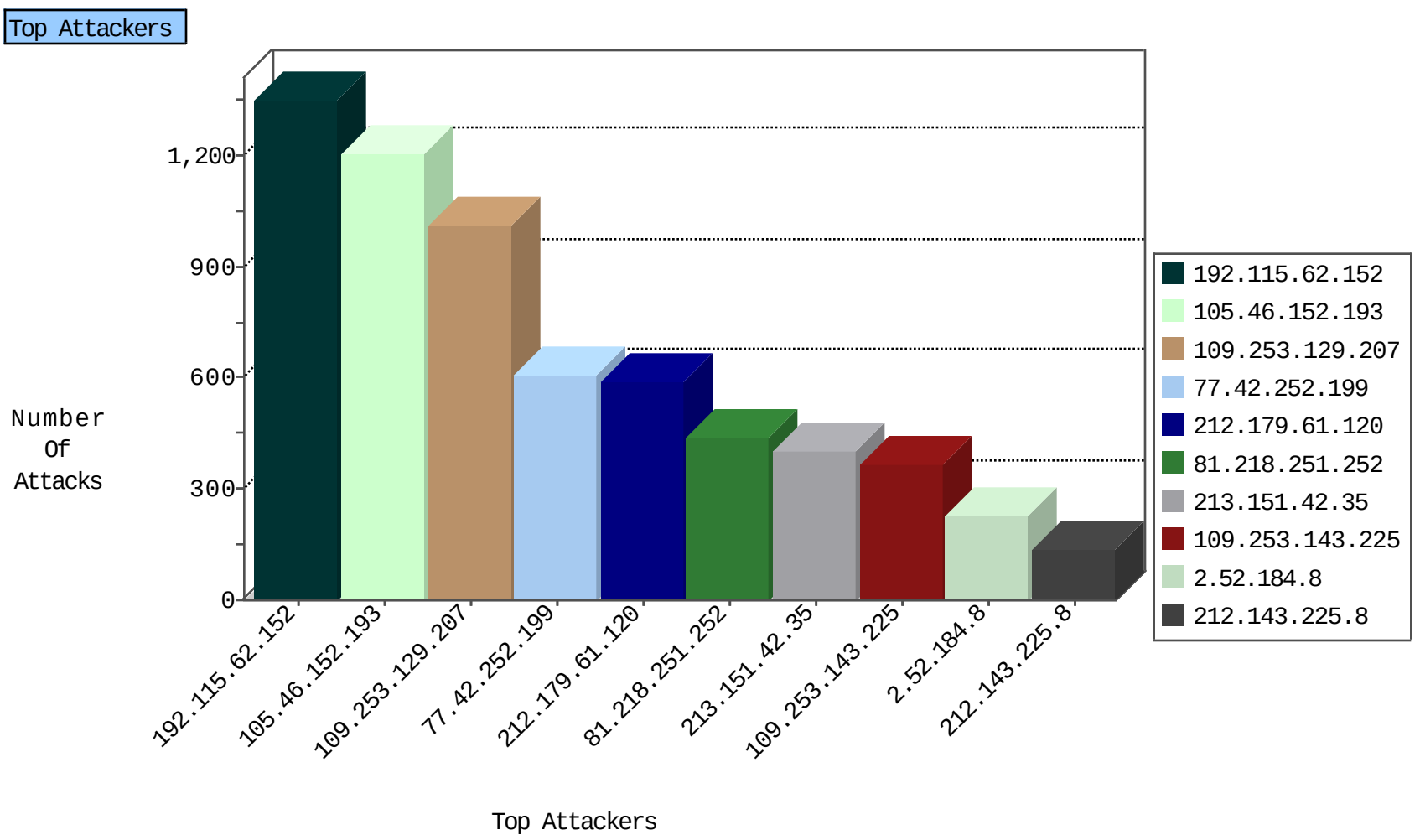
05-04-2015-12:03:02 to 05-04-2015-13:03:02

IDF Under Attack
05-04-2015-12:03:02

Top Targets



Top Attackers



05-04-2015-12:03:02 to 05-04-2015-13:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
213.57.118.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2980
77.42.252.199	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2642
37.142.129.150	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
89.139.9.163	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
213.151.42.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.102.141.254	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	3
31.154.24.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.224.96	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
105.46.152.193		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
116.49.0.221	Hong Kong	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2
84.94.32.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
184.105.247.196	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
80.246.141.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
213.8.80.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-04-2015-12:03:02 to 05-04-2015-13:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
81.218.116.129	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	75
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	19
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	6
46.19.85.206	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.231	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.74.162	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.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
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
197.205.108.25	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
2.52.158.195	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.67.6.146	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
218.30.103.52	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
79.182.160.108	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
5.29.92.226	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.76.148	gqcenter.aka.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
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1

05-04-2015-12:03:02 to 05-04-2015-13:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
176.181.16.253	France	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.240.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.92.239	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
81.200.91.2	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
212.179.61.120	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
201.239.118.143	Chile	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
199.203.92.42	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.64	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
193.169.70.108	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.120.247	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.95.158.198	Ukraine	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
95.86.94.68	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.192.186	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
81.200.91.2	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1
201.239.118.143	Chile	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
201.239.118.143	Chile	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -f -sS	1
46.120.173.145	Israel	147.237.77.216	dover.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
31.210.189.15	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.95.158.198	Ukraine	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1

05-04-2015-12:03:02 to 05-04-2015-13:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
192.115.62.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1354
105.46.152.193		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1208
77.42.252.199	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	606
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	586
81.218.251.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	440
213.151.42.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	383
2.52.184.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	226
212.143.225.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	134
84.95.131.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	95
154.5.108.18	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
2.52.36.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
212.143.225.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
176.12.141.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
195.202.87.44	Kenya	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
82.209.161.44	Sweden	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	65
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
82.80.157.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
37.26.146.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
17.78.145.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
95.86.94.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
60.241.77.64	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
46.120.185.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.132.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
62.219.233.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
62.90.144.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
95.86.125.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
46.19.85.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
82.166.53.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
37.26.148.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
113.14.107.203	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
37.26.148.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
81.218.40.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
89.139.9.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
41.68.100.77	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
1.2.189.112	Thailand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
192.118.78.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
213.8.7.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
79.178.6.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
5.29.207.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.129.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1014
109.253.143.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	357
62.219.153.212	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	18
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	12
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	11
79.177.182.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
80.246.140.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	7
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	6
80.246.139.19	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
109.253.156.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
46.116.88.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	4
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
207.46.13.101	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.101	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.61	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.61	Block	2
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.32.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	2
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.128.48.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.235.2.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
82.166.20.133	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.12	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5611-he/patzar.aspx	Block	1
198.20.69.74	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
46.116.213.214	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.142.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
31.168.173.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19798-he/idfgdover.aspx	Block	1
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.225	Block	1
109.253.138.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.105.247.195	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
80.246.130.45	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
46.19.86.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
66.249.67.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71883-he/maarachot.aspx	Block	1
213.8.94.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.0.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.253.156.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
84.229.191.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-12321-en	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Malformed URL	Block	1
178.137.19.143	Ukraine	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
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	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/transportation.asp	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/421-2782-he/patzar.aspx	Block	1
66.249.64.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.138.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

05-04-2015-12:03:02 to 05-04-2015-13:03:02