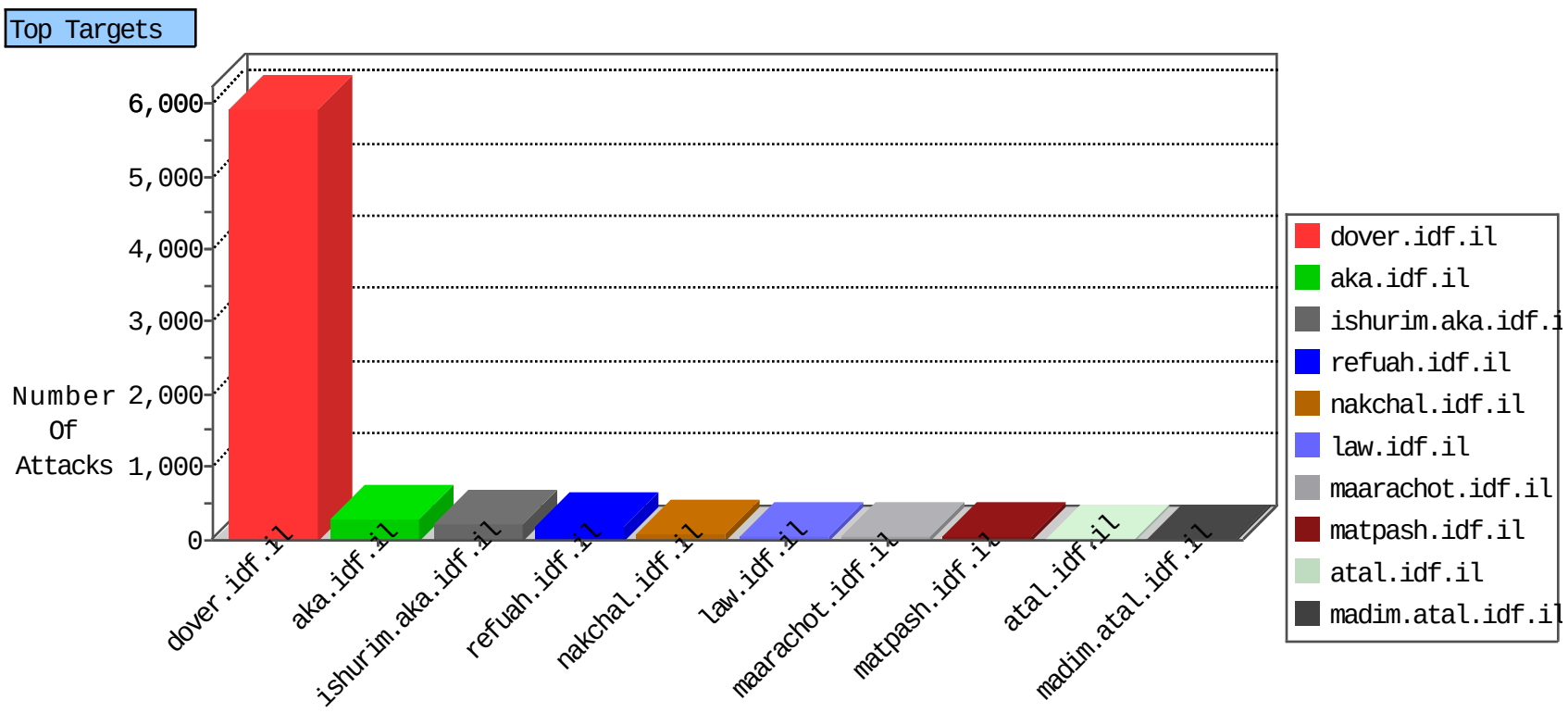
05-04-2015-10:03:04 to 05-04-2015-11:03:04

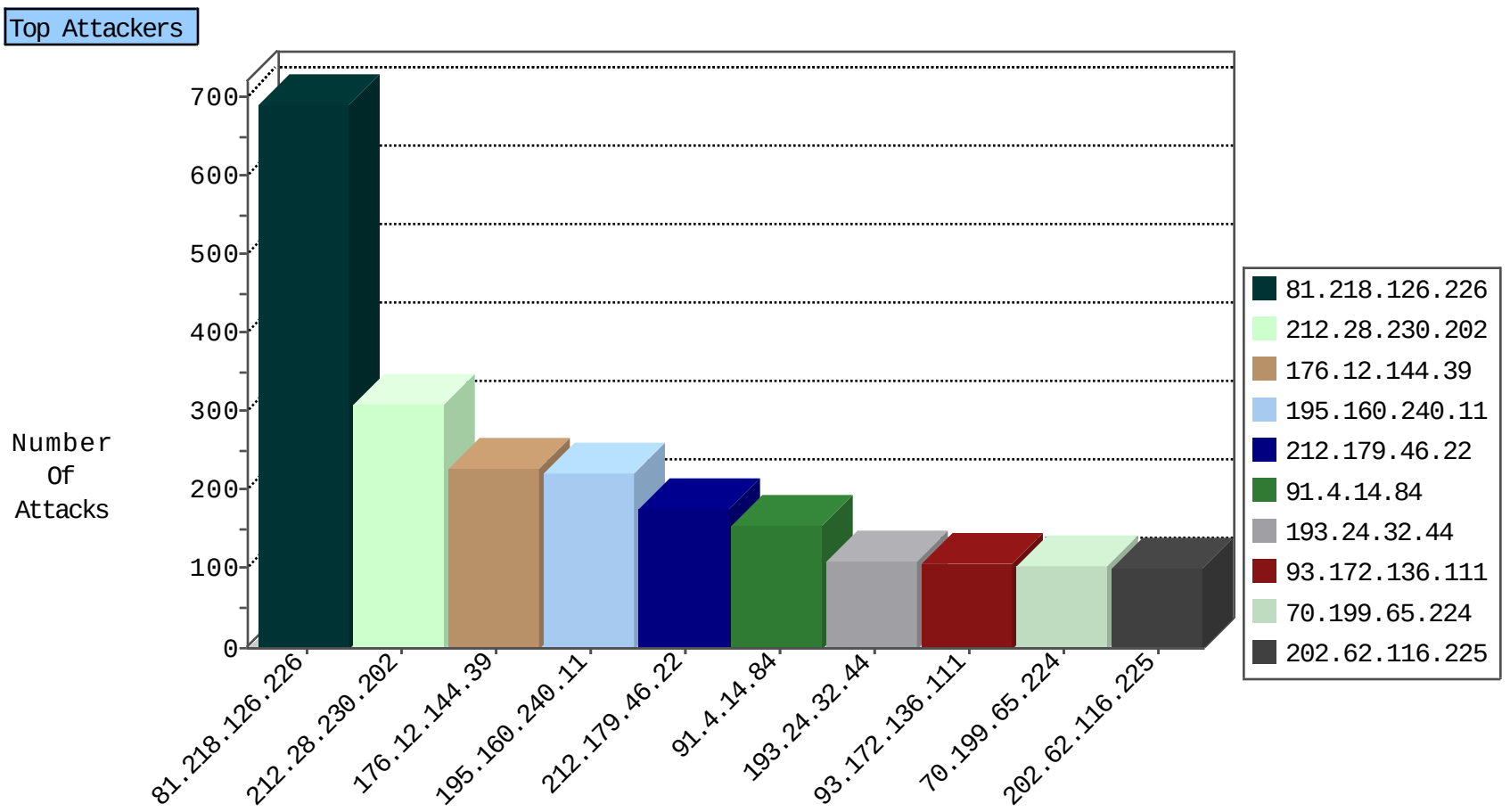
IDF Under Attack
05-04-2015-10:03:04

Top Targets



Top Target

Top Attackers



Top Attackers

05-04-2015-10:03:04 to 05-04-2015-11:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.86.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	83
37.142.129.150	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
80.246.140.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
85.64.135.225	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
182.224.114.72	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	4
116.93.59.209	Philippines	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
10.0.0.4		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
213.151.59.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.0.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
91.4.14.84	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
213.151.32.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.221.105.7	Iceland	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
95.172.79.236	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

05-04-2015-10:03:04 to 05-04-2015-11:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	84
37.60.46.2	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	23
213.151.44.148	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
5.28.137.52	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.151.36.20	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
164.138.122.68	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
82.166.202.245	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
2.54.165.111	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.178	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	2
213.151.39.216	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	2
95.86.122.172	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
109.64.151.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.26.146.221	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
37.26.147.216	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.160.248.50	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
2.54.166.184	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
62.219.46.122	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
95.86.112.12	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
31.7.57.198	Switzerland	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
2.52.0.0	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
37.26.147.241	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	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.233	atal.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
95.86.121.76	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
31.7.57.198	Switzerland	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
2.52.187.146	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	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
212.179.46.22	Israel	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	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
164.138.122.203	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	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1

05-04-2015-10:03:04 to 05-04-2015-11:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.66	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.163	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.56.55	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.61.127	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.105.99	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
87.98.244.215	Germany	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.19.86.80	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.130	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
203.194.234.109	Hong Kong	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
91.224.132.118	Russian Federation	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.100.213	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

05-04-2015-10:03:04 to 05-04-2015-11:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.126.226	Israel	147.237.77.216	dover.idf.il		SQL Injection	monitor	557
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	310
176.12.144.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	228
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	175
91.4.14.84	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	155
193.24.32.44	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	110
70.199.65.224	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	105
202.62.116.225	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
88.49.249.246	Italy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	96
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	75
114.75.10.18	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
37.26.147.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
81.218.126.226	Israel	147.237.77.216	dover.idf.il	command injection detected in URL: 'convert'	Command Injection	monitor	65
93.172.136.111	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	60
80.74.110.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
93.172.136.111	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	47
84.228.144.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
77.125.26.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
46.19.86.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
199.203.215.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
147.236.38.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
109.64.26.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
81.218.126.226	Israel	147.237.77.216	dover.idf.il		Command Injection	monitor	37
212.179.159.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
66.249.82.210	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
41.160.210.200	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.253.128.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
81.218.126.226	Israel	147.237.77.216	dover.idf.il	command injection detected in request: 'convert'	Command Injection	monitor	29
79.179.153.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.19.86.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
212.179.71.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
154.99.183.226	Sudan	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	27
212.235.77.210	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
109.253.158.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
195.160.240.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.19.86.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
195.212.93.2	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
46.19.85.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
46.19.85.45	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	25
91.144.30.96	Syrian Arab Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
5.28.137.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
134.191.232.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
212.199.121.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.19.86.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22

05-04-2015-10:03:04 to 05-04-2015-11:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in IP from 195.160.240.11	Block	195
142.54.174.178	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 142.54.174.178	Block	28
118.123.8.135	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 118.123.8.135	Block	18
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
46.229.164.114	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	5
46.229.164.102	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.102	Block	4
46.229.164.113	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.113	Block	4
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
142.54.174.178	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	4
46.19.85.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
178.137.19.143	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
46.19.86.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
77.126.83.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.158.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
208.50.101.151	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/ac/	Block	1
93.173.178.239	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
79.177.148.25	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.75.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/modules/forums/forum.aspx	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
118.123.8.135	China	147.237.77.170	maarachot.idf.il	Admin Blocking	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/contact	Block	1
46.229.164.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/forms	Block	1
207.46.13.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.91	Block	1
84.94.32.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.147.243	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
184.105.139.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/news_gaza/pages/toniblair.aspx	Block	1
66.249.64.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
142.54.174.178	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/includes/advertiser/uploadtester.asp	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/general	Block	1
109.64.52.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.205.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many 404: Response Code per IP	Block	1
5.28.137.52	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19075-he/dover.aspx	Block	1
62.0.67.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.229.164.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
85.64.20.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.60.46.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.179.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.173	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
66.249.64.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.235	Block	1
147.236.113.1	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1

05-04-2015-10:03:04 to 05-04-2015-11:03:04