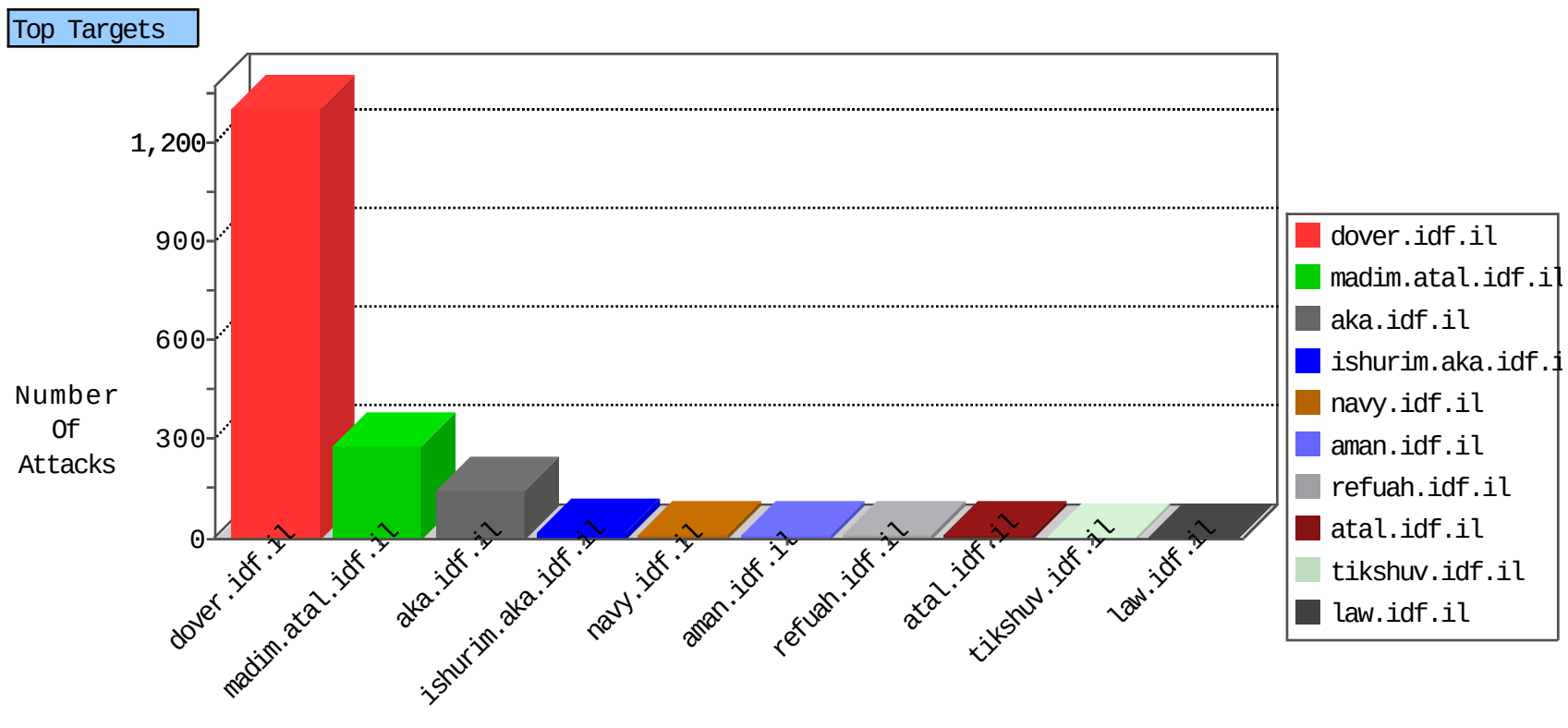
04-24-2015-09:03:08 to 04-24-2015-10:03:08

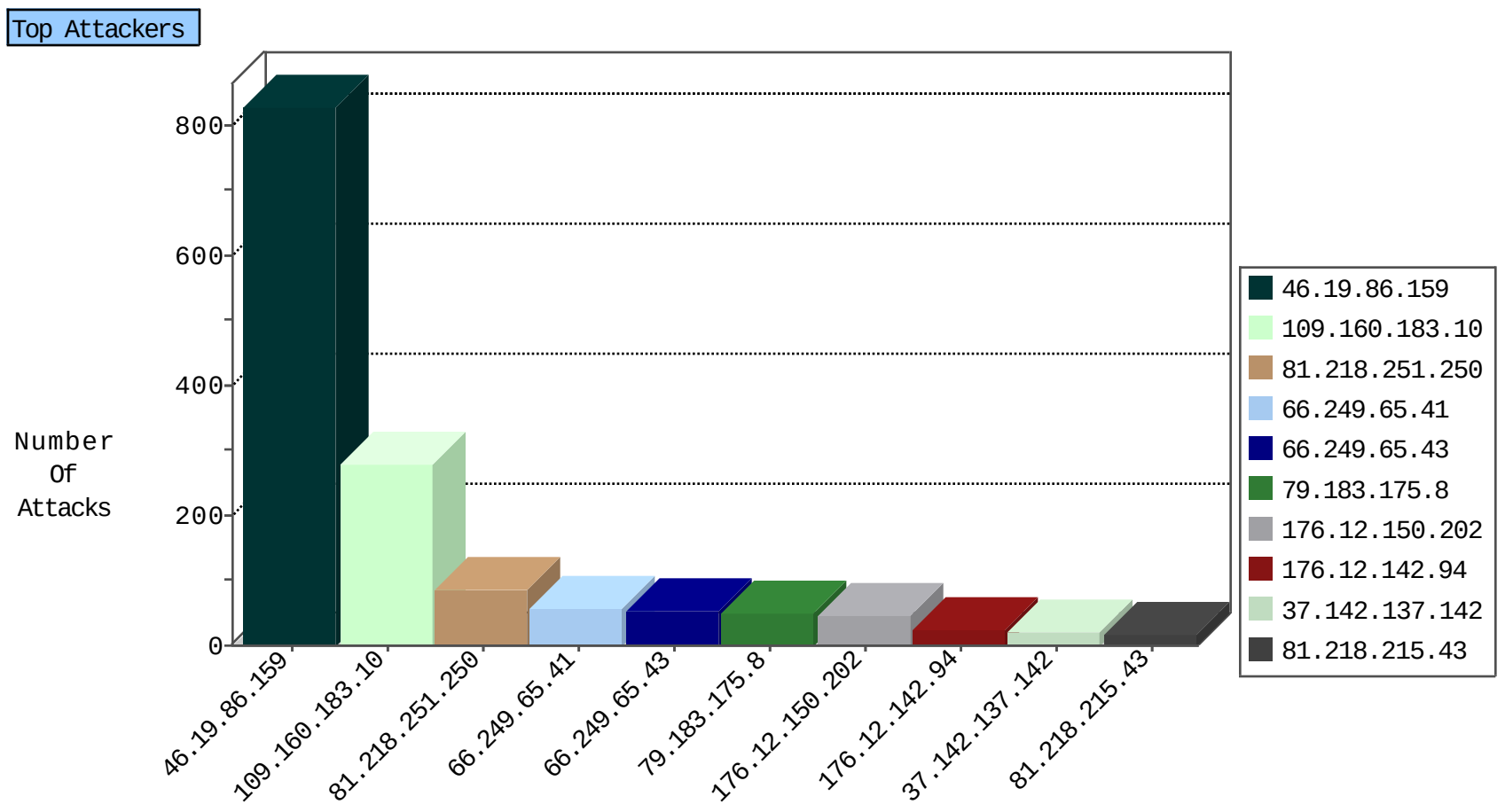
IDF Under Attack
04-24-2015-09:03:08

Top Targets



Top Target

Top Attackers



Top Attackers

04-24-2015-09:03:08 to 04-24-2015-10:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.104	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	516
37.142.137.142	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
46.19.86.236	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
31.154.242.175	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.95.202.55	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.95.202.55	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
50.135.7.134	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
87.68.19.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

04-24-2015-09:03:08 to 04-24-2015-10:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.201.154.140	Netherlands	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	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	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
76.91.203.162	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
148.251.183.105	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
37.46.174.171	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.113	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
31.7.57.198	Switzerland	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.189	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-24-2015-09:03:08 to 04-24-2015-10:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.37	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
84.228.66.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.37.190	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.162	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
5.29.252.2	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
201.239.118.143	Chile	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 2048	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.162	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
123.138.215.145	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.162	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
31.154.242.175	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
61.183.128.6	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
201.239.118.143	Chile	147.237.72.217	e.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.162	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
123.138.215.145	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1

04-24-2015-09:03:08 to 04-24-2015-10:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	830
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	84
66.249.65.43	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
79.183.175.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
66.249.65.41	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
176.12.150.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
176.12.142.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
81.218.215.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
46.19.86.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
37.231.170.178	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
41.134.251.18	South Africa	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
95.179.41.76	Russian Federation	147.237.72.166	aka.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	10
68.100.193.64	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
2.54.17.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
109.67.180.147	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
109.253.136.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
176.12.137.167	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
2.54.58.141	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
105.210.152.246	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
197.89.27.68		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
79.181.117.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
81.218.181.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
87.69.63.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
2.54.154.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.14	Israel	147.237.77.233	atal.idf.il	SAM rule	drop	drop	4
213.151.56.53	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.98	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
118.165.226.106	Taiwan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
213.57.34.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
176.12.151.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
176.12.148.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
2.54.23.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
114.32.178.177	Taiwan	147.237.76.86	navy.idf.il	SAM rule	drop	drop	2
84.228.92.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.19.85.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
176.12.149.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
2.54.48.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
84.229.191.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.19.85.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
80.246.130.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
176.12.141.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
2.52.134.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
89.139.31.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.160.183.10	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.183.10	Block	278
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	7
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	6
87.68.154.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	6
79.180.30.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	5
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
109.253.146.0	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.65.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.127.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	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
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
194.90.129.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.73.240	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
66.249.65.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
95.179.41.76	Russian Federation	147.237.76.42	refuah.idf.il	Multiple Admin Blocking from 95.179.41.76	Block	1
141.212.122.82	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.167//	Block	1
66.249.65.60	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
95.173.171.224	Turkey	147.237.76.31	nakchal.idf.il	Illegal HTTP Version	Block	1
66.249.79.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10624-he/dover.aspx	Block	1
66.249.79.1	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/general.aspx	Block	1
207.112.70.10	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.65.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.65.41.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1
80.246.130.179	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
142.4.208.208	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.65.70	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
46.28.105.84	Czech Republic	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
95.179.41.76	Russian Federation	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
68.180.228.167	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/eitan	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.41	Block	1
109.160.183.10	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
81.218.181.239	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/2004/february/0218-1.stm	Block	1
157.55.39.4	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
66.249.65.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.116.70.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
95.179.41.76	Russian Federation	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 95.179.41.76	Block	1
216.167.192.135	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.65.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
158.222.13.84		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
66.249.65.11	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
95.179.41.76	Russian Federation	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1
79.176.110.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1

04-24-2015-09:03:08 to 04-24-2015-10:03:08