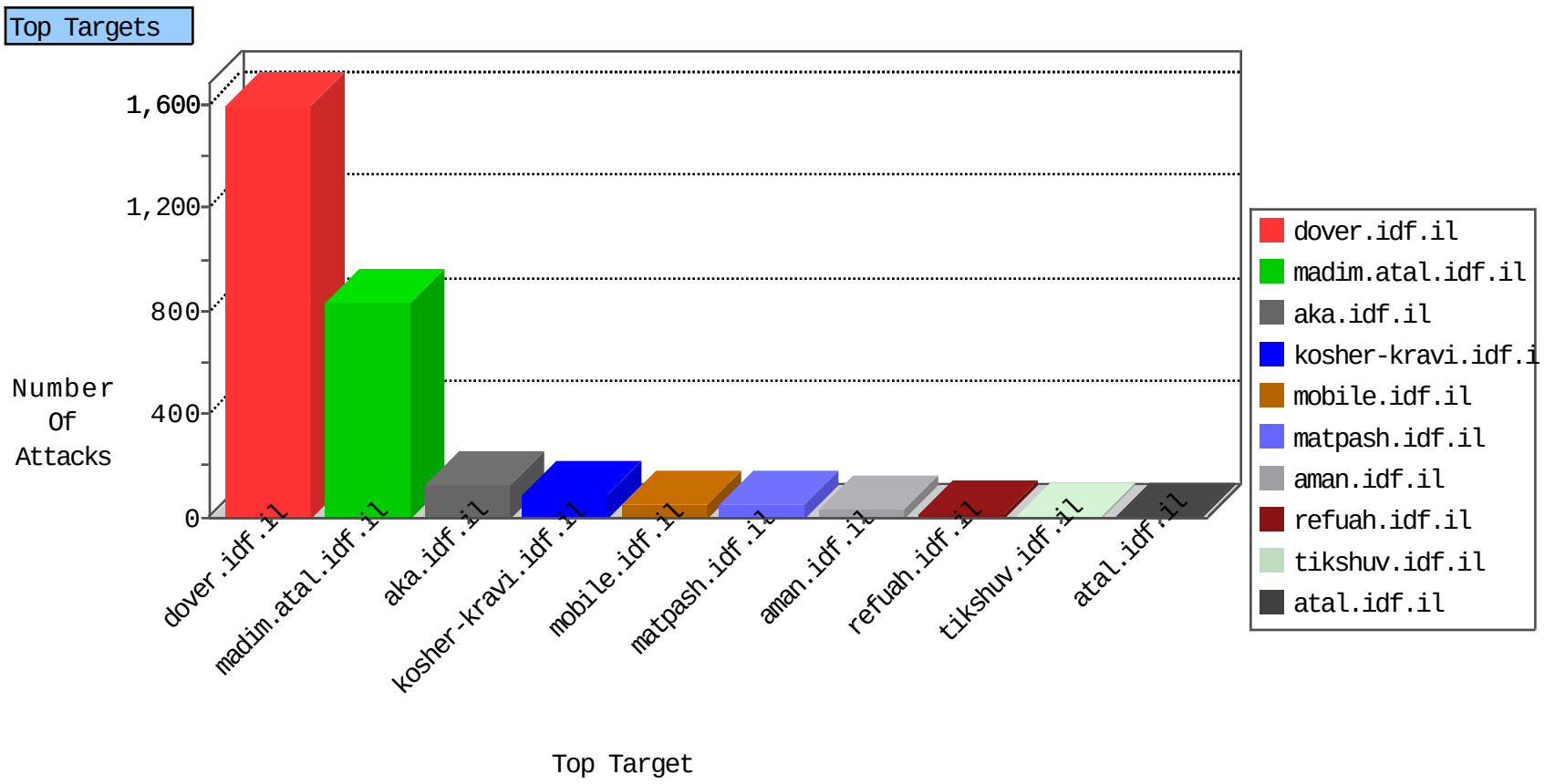
04-30-2015-20:03:06 to 04-30-2015-21:03:06

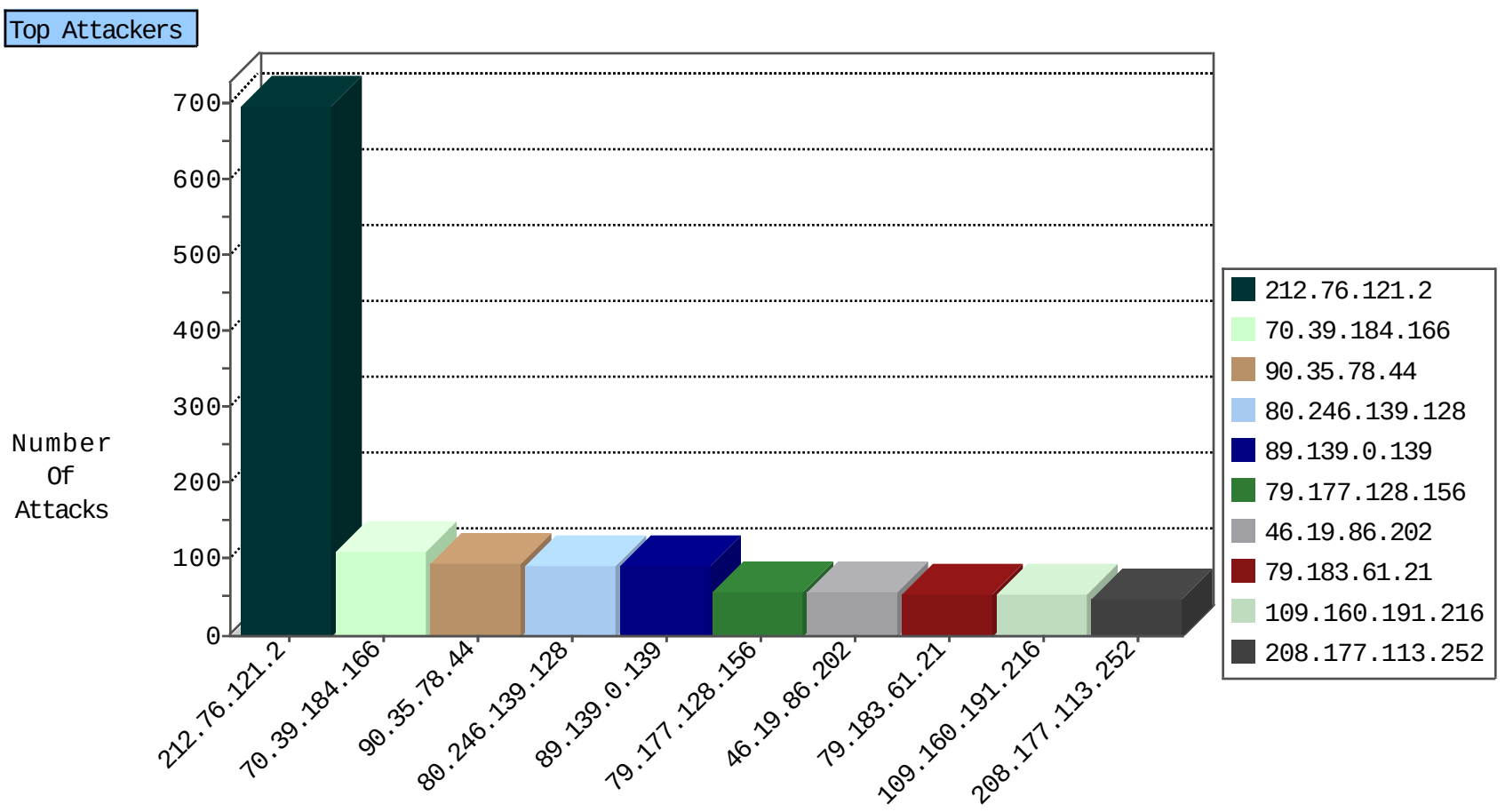
IDF Under Attack
04-30-2015-20:03:06

Top Targets



Top Target

Top Attackers



Top Attackers

04-30-2015-20:03:06 to 04-30-2015-21:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
89.139.0.139	Israel	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	789
46.19.85.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
84.111.28.81	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
79.180.215.220	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
79.180.215.220	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.116.216.71	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
79.178.125.155	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
79.178.125.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
212.235.89.209	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
70.39.184.166	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
116.228.162.125	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
46.19.86.146	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
84.228.53.64	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
116.125.143.84	Korea, Republic of	147.237.77.216	dover.idf.il	BO-Apache-HTTPD-log-Cookie	dest-reset	2
210.5.151.5	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
46.19.85.106	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
37.46.35.57	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
46.19.85.106	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
121.88.5.177	Korea, Republic of	147.237.77.19	law-forum.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
46.19.86.211	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
37.46.35.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
128.234.156.253	Romania	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.211	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
41.13.246.91	South Africa	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
46.19.86.146	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
23.95.5.42	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

04-30-2015-20:03:06 to 04-30-2015-21:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.186.170.59	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
149.88.181.226	United States	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.250.150.191	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.148	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.77.233	atal.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
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.172.16.249	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.65.13.72	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
109.160.174.57	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.117.102.115	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
84.228.234.30	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.250.155.191	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.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
89.138.238.87	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
184.100.86.203	United States	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	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1

04-30-2015-20:03:06 to 04-30-2015-21:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
89.139.0.139	Israel	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.144	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
46.120.5.104	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
176.103.49.29	Ukraine	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.176.103.199	Israel	147.237.76.42	refuah.idf.il	SQL Injection - Paranoid	1
61.240.144.64	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
121.88.5.177	Korea, Republic of	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
114.80.68.151	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.176.103.199	Israel	147.237.76.42	refuah.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	1

04-30-2015-20:03:06 to 04-30-2015-21:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
70.39.184.166	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	108
90.35.78.44	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	78
79.177.128.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
46.19.86.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
79.183.61.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
109.160.191.216	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
208.177.113.252	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
84.39.152.102	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
46.19.86.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
46.244.91.160	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	28
85.250.102.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
176.12.143.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
79.182.26.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
79.176.22.185	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
90.35.78.44	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
79.176.103.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
85.65.100.176	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
77.126.128.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
46.121.78.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
62.219.161.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.182.21.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.132.197	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	12
41.13.246.91	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.132.197	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	12
93.172.46.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
2.52.21.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
188.120.148.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
85.250.155.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
46.19.86.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.221	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.116.216.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.26.148.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.178.133.232	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
204.9.139.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.182.216.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.26.146.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.116.202.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.19.86.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.76	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
152.26.228.64	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.117.55.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
109.64.57.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.157	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.76.121.2	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 212.76.121.2	Block	699
80.246.139.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	89
80.246.140.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	42
213.8.129.152	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	18
93.172.204.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
95.86.65.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
157.55.39.146	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.146	Block	6
84.111.38.250	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.111.38.250	Block	6
79.178.133.232	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	5
157.55.39.33	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.33	Block	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/	Block	3
93.173.40.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.111.153.149	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
37.142.213.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.78.113.19	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	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
79.179.97.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
85.65.100.176	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.64.39.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.103.199	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.176.103.199	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-16670-en/dover.aspx	Block	1
207.46.13.133	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/	Block	1
84.111.38.250	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
157.55.39.33	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/	Block	1
80.179.12.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/minhalnews/pages/edeladcha.aspx	Block	1
98.139.204.33	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 98.139.204.33	Block	1
87.230.26.123	Germany	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
84.108.71.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/june/17.stm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
109.253.145.9	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
79.176.103.199	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/clientscripts/jquery.plugins/sl<!-- start header --> <!--[if lte ie 6]><script type=	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.88.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/merkava3-p	Block	1
98.139.204.33	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
89.138.228.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
84.108.130.224	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.76.203.67	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
180.76.4.162	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
115.25.81.72	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
95.86.65.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//templates/sendtofriend/sendtofriend.aspx	Block	1
46.120.61.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
84.228.147.167	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22152-he/dover.asp<http:/www.idf.il/1133-22152-he/dover.aspx>	Block	1