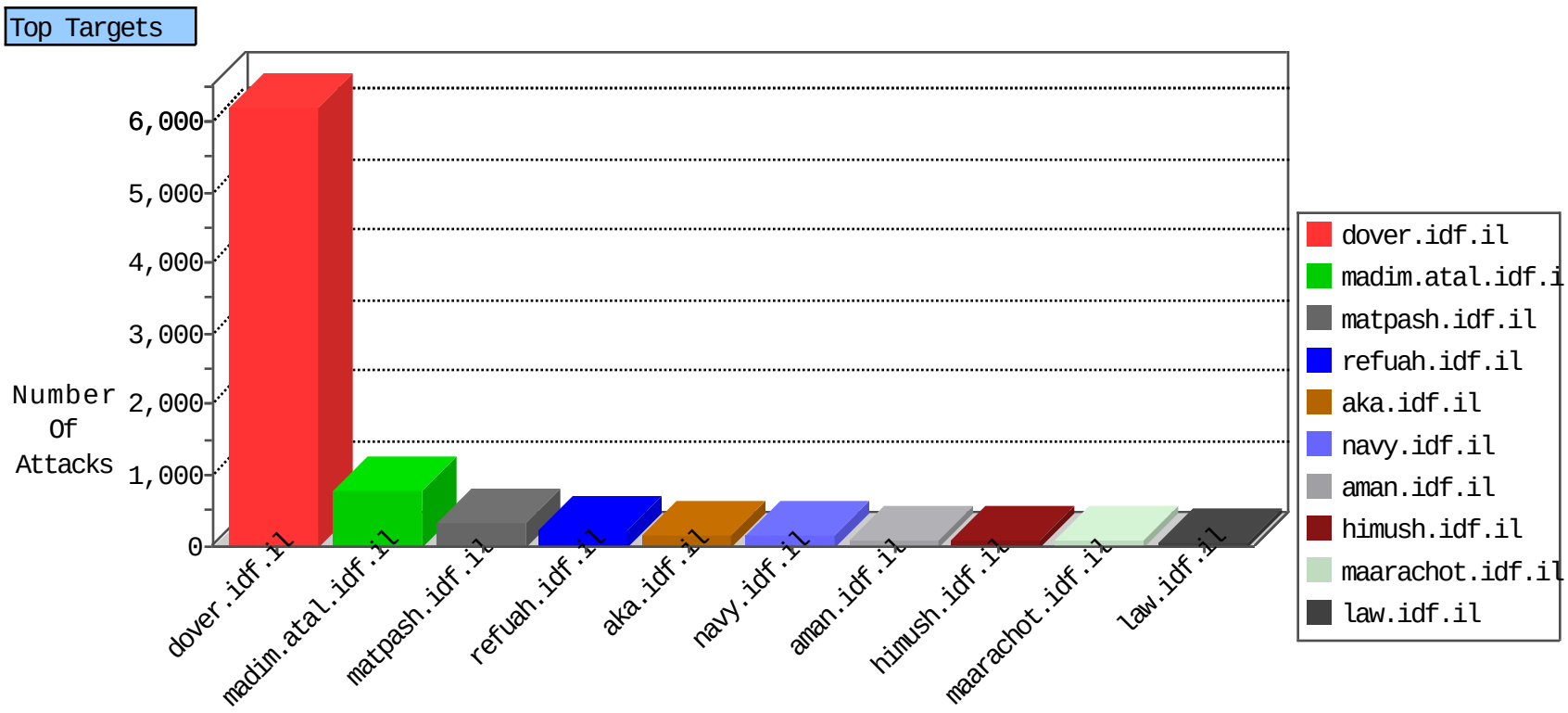
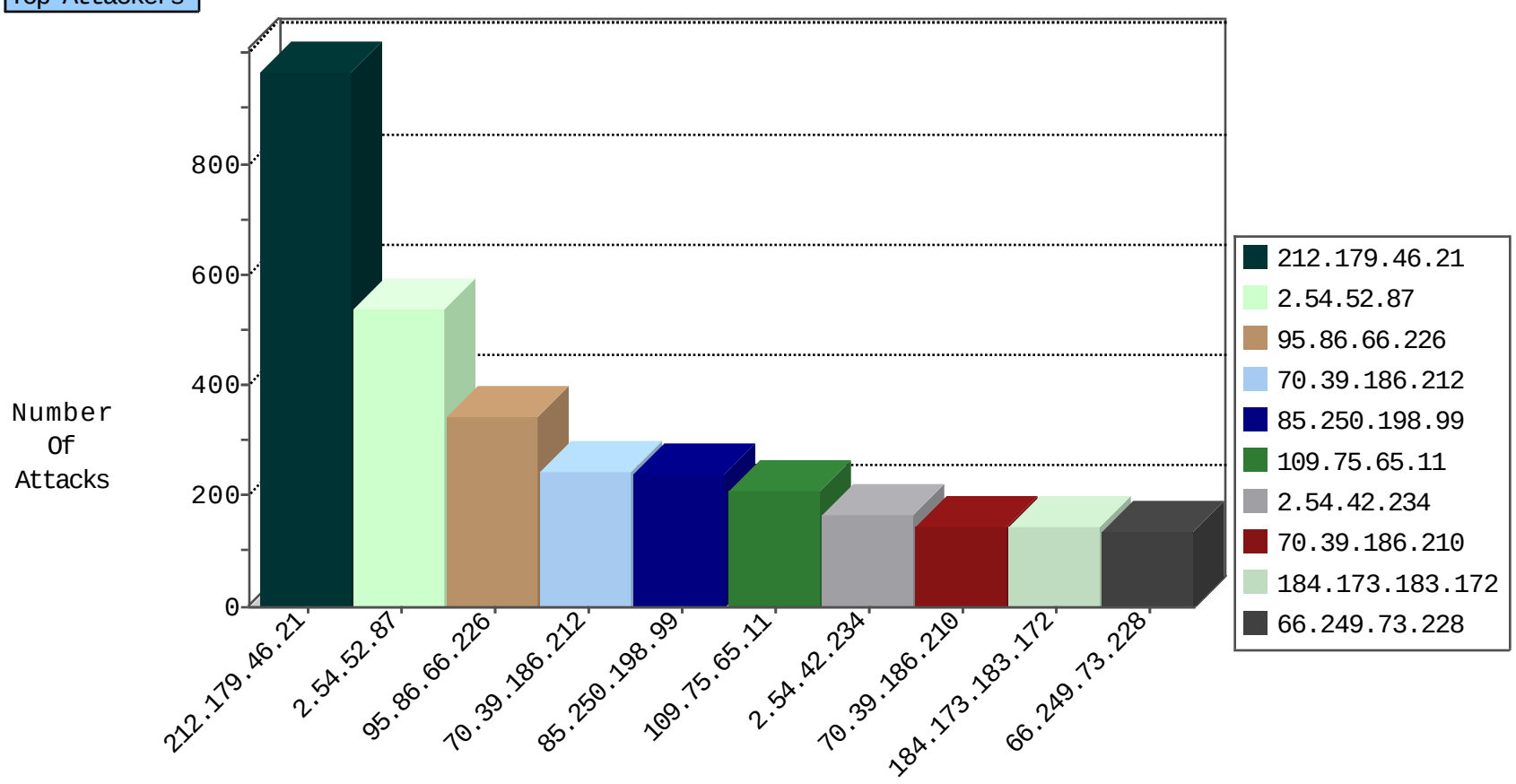
04-08-2015-22:03:04 to 04-08-2015-23:03:04

IDF Under Attack
04-08-2015-22:03:04

Top Targets



Top Attackers



04-08-2015-22:03:04 to 04-08-2015-23:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
70.39.186.212	Satellite Provider	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1235
78.180.205.209	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1144
46.120.65.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	303
70.39.186.210	Satellite Provider	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	281
46.120.169.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	251
87.68.253.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
70.51.146.106	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	156
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	132
81.221.148.28	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	117
5.29.191.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
31.203.107.190	Kuwait	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	99
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	96
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	95
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	82
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	81
108.2.210.43	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	75
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	75
87.68.253.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
46.19.85.121	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	44
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	33
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	30
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	30
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	30
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	28
176.12.138.57	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	23
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	19
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
87.68.229.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	15
66.249.64.55	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	14
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	13
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	13
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.73.239	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	10
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	10
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.73.231	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	9
66.249.75.95	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8

04-08-2015-22:03:04 to 04-08-2015-23:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	143
84.108.121.54	Israel	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	21
46.19.85.204	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
41.176.198.237	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.240.237.185	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
81.221.148.28	Switzerland	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
46.19.85.54	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
79.179.20.214	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
109.65.1.114	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-08-2015-22:03:04 to 04-08-2015-23:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
176.12.144.75	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.223.255	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
185.60.229.64		147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
183.136.216.7	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
99.244.135.30	Canada	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.197.76	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.64		147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.64		147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 3072	1
122.228.207.77	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.64		147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.64		147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
183.136.216.7	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
178.19.107.114	Poland	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
101.226.2.99	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
169.54.233.118	Switzerland	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
99.244.135.30	Canada	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
222.186.197.76	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
192.64.180.14	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.64		147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.60.229.64		147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1

04-08-2015-22:03:04 to 04-08-2015-23:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	968
95.86.66.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	345
70.39.186.212	Satellite Provide	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
109.75.65.11	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	211
2.54.42.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	167
70.39.186.210	Satellite Provide	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	133
185.5.154.48	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	118
5.108.15.208	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	112
46.115.157.85	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
197.132.171.13	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	93
5.108.4.213	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	91
62.90.107.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
185.14.135.102	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	88
5.22.130.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	83
87.68.229.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
37.231.138.144	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
93.172.157.58	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	alert	54
24.114.43.227	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
37.231.60.168	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
149.88.71.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
2.54.8.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
79.182.133.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
84.95.58.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
197.76.140.49	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
99.95.173.96	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
156.110.24.142	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
109.253.131.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
2.54.49.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
197.36.38.45	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
70.51.146.106	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
197.132.127.206	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
109.253.137.53	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
109.160.178.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
93.172.157.58	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	30
109.67.22.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
79.183.35.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
92.241.40.22	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
37.26.147.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
31.203.107.190	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
197.7.42.220	Tunisia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
87.68.155.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
2.52.166.54	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
109.186.114.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
17.142.152.94	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18

04-08-2015-22:03:04 to 04-08-2015-23:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.52.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	537
85.250.198.99	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.250.198.99	Block	238
2.54.34.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
109.67.22.132	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1136-he/navy.aspxhttp:/	Block	3
46.116.186.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.29.45.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kamlar	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
85.250.198.99	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
176.67.111.43	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
2.52.52.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
94.159.238.250	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	1
72.21.217.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.91.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.4.8	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
2.52.166.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.95.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.4.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/giyus/forum/	None	1
85.250.198.99	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/mobile/shared/ajax/updatemakatqauntity.aspx	Block	1
50.87.9.153	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9237-he/refuah.aspx	Block	1
95.86.114.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
80.179.5.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
37.142.117.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.173.13.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
50.87.9.153	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
209.221.90.250	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//894-en/idfgdover.aspx	Block	1
80.246.130.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
46.19.85.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.159.238.250	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.159.238.250	Block	1
216.223.27.29	United States	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../images/shared/home.png	Block	1
2.54.177.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
109.67.197.8	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1

04-08-2015-22:03:04 to 04-08-2015-23:03:04