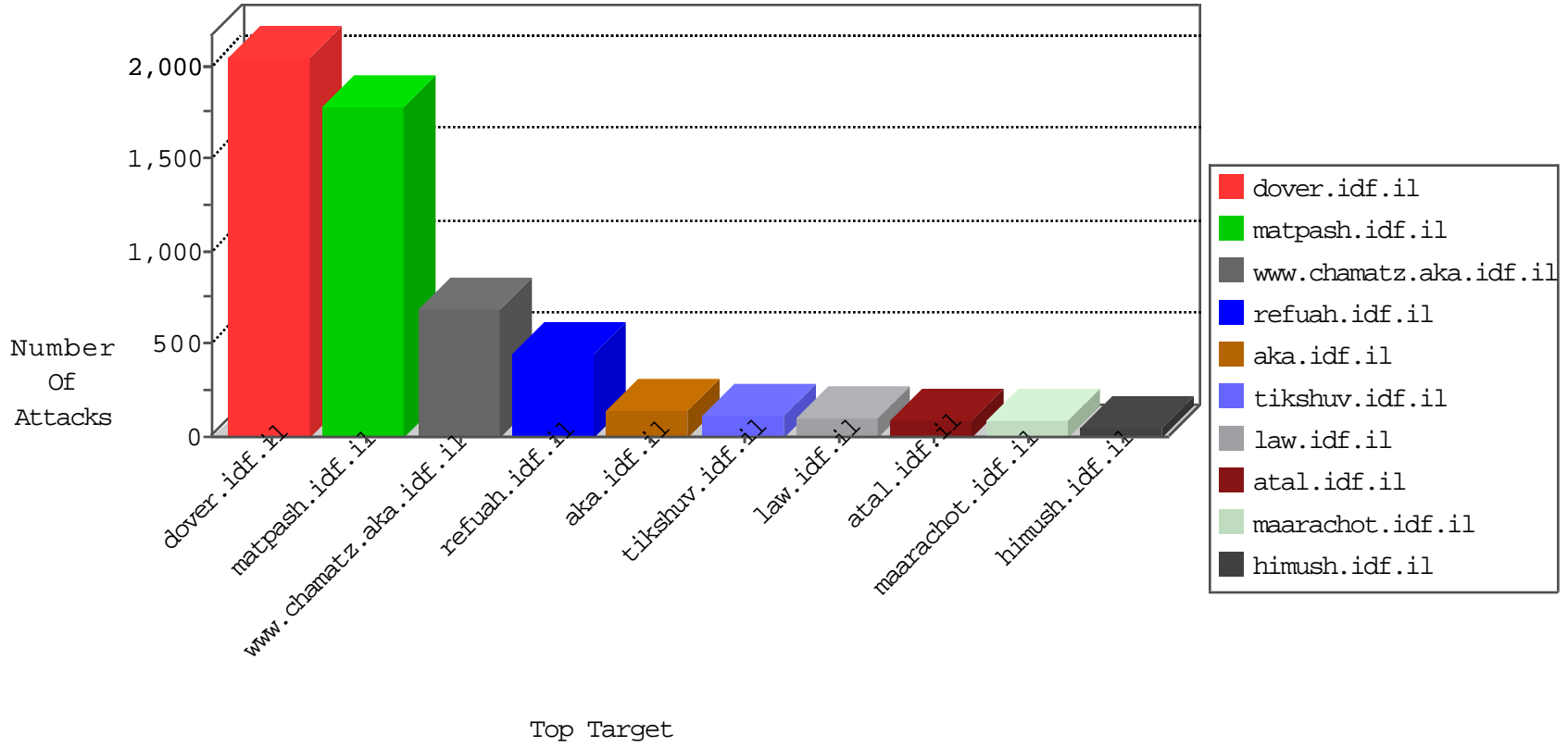
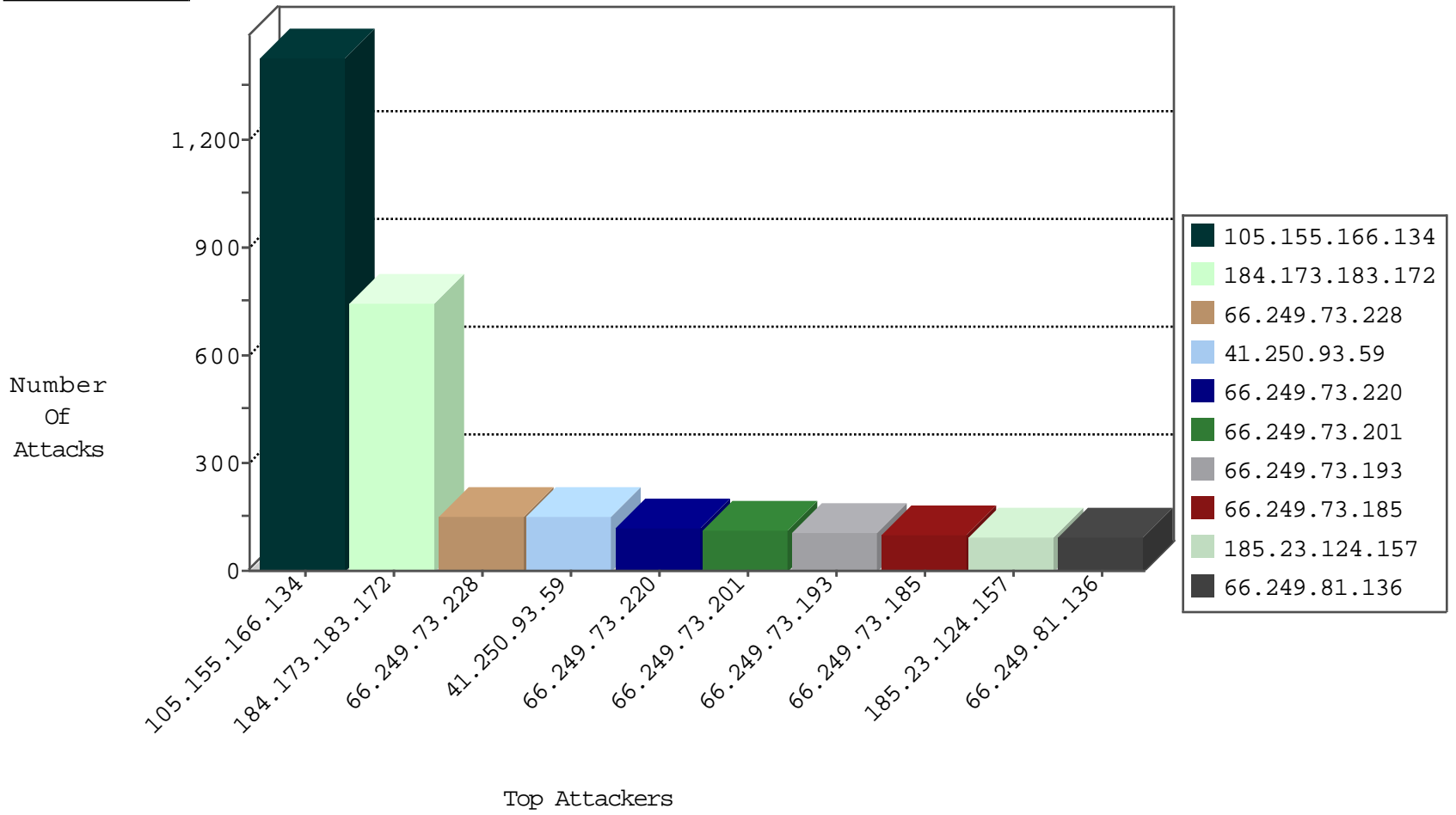




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.110.8.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	152
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	116
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	111
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	105
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	98
220.181.108.77	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	97
66.249.81.136	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	90
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	78
66.249.81.140	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	75
66.249.81.144	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	74
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	63
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	60
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	56
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	34
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	33
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	27
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	25
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	24
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	24
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	20
220.181.108.156	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	20
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	19
66.249.78.45	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	19
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	18
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	17
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	16
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	16
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	14
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.65.185	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	12
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.89.88	United States	147.237.72.166	aka.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	8
66.249.78.67	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.78.208	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	7
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	7
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.65.189	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.78.29	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.75.111	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_P-N_40-59	Permit	645
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	98
105.155.166.134	Morocco	147.237.77.176	matpash.idf.il	C1000205: HTTP: Opisrael 2015 - key words and groups	Block	79
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	7
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
73.48.65.58	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
212.200.69.114		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

## 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	7
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
43.255.191.170	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
178.135.29.91	Lebanon	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.170	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.245.99.48		147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.170	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.245.99.48		147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.170	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.227	e.haraz.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
62.76.184.59	Russian Federation	147.237.72.166	aka.idf.il	SERVER-WEBAPP admin.php access	1
221.235.188.210	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
105.155.166.134	Morocco	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	1343
41.250.93.59	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	149
185.23.124.157	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	94
77.126.238.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
107.167.99.225	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
41.68.135.137	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
97.76.205.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
2.92.142.53	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
85.64.240.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
41.232.36.214	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
176.12.141.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
81.215.215.198	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
79.181.140.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
86.108.56.92	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
5.100.161.150	Yemen	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
85.64.243.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
93.81.90.173	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
188.236.227.53	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
178.135.29.91	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
98.108.211.104	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
185.5.154.148	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
207.46.13.16	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
176.193.129.136	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
46.19.85.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
70.199.66.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
2.92.210.83	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
176.12.151.97	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
45.99.217.57		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
46.19.85.248	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
88.182.94.184	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
120.18.8.19	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.86.114	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	12
70.196.67.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.253.143.20	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
5.29.93.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
207.46.13.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
41.206.138.41	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.153	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
70.199.66.51	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
149.78.239.233	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.76.184.59	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	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
37.142.208.178	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.130.244	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
112.215.66.70	Indonesia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.5.73	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/1048-7536-he/tikshuv.aspx	Block	1
94.159.148.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/gyus/authenticationsservice.aspx/getuserdetails	Block	1
62.76.184.59	Russian Federation	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 62.76.184.59	Block	1
217.69.136.209	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/present.stm	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/327-en/sb_item_levi_s	Block	1
46.19.86.17	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
187.59.52.76	Brazil	147.237.77.176	matpash.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
109.64.108.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
149.88.75.200	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.114	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/history/degania.stm	Block	1
109.169.5.168	United Kingdom	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
62.76.184.59	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/administrator/	Block	1
79.181.201.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/gyus/login.aspx	None	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/html/14.asp	Block	1
109.253.143.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/statistics/security.stm	Block	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
62.76.184.59	Russian Federation	147.237.72.166	aka.idf.il	Admin Blocking	Block	1