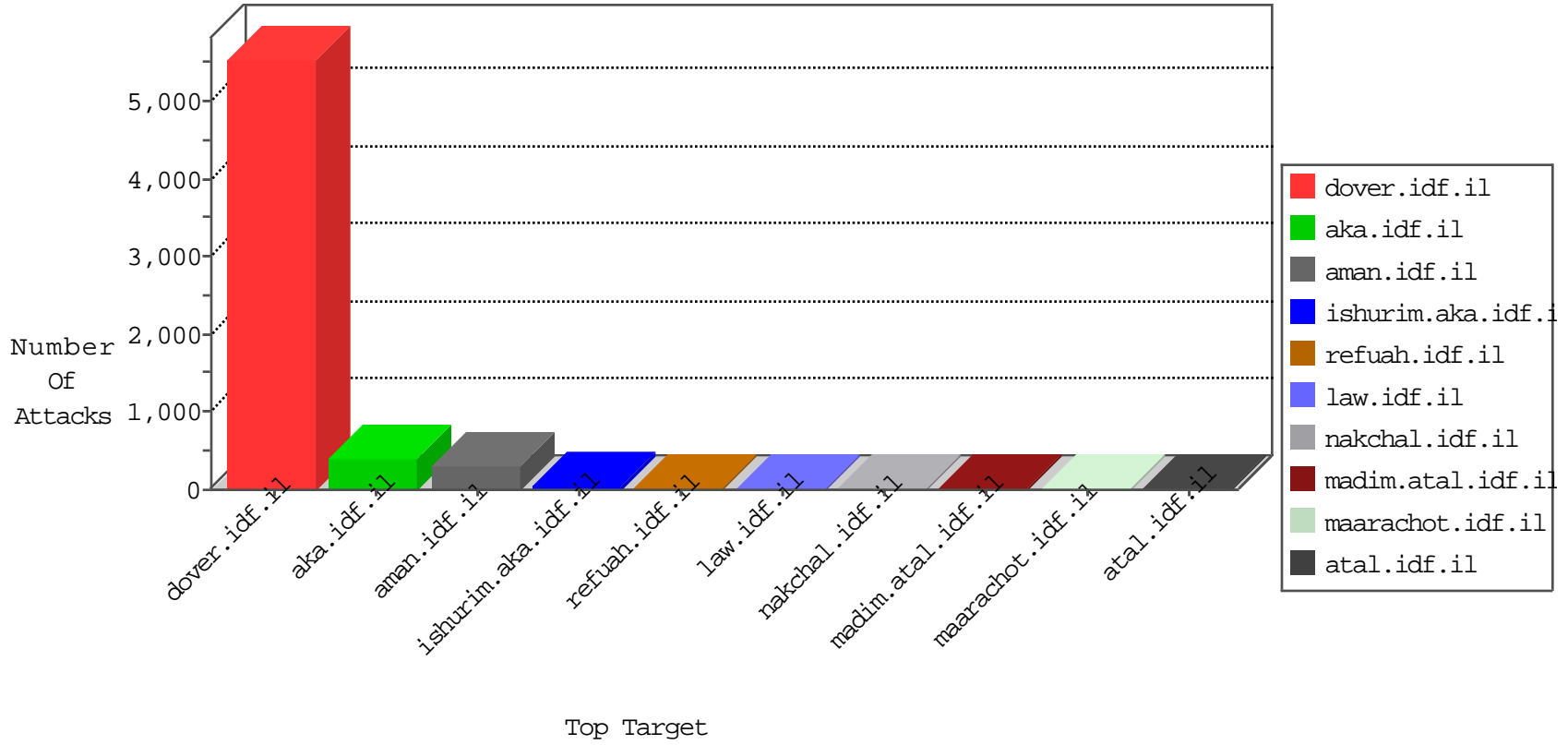
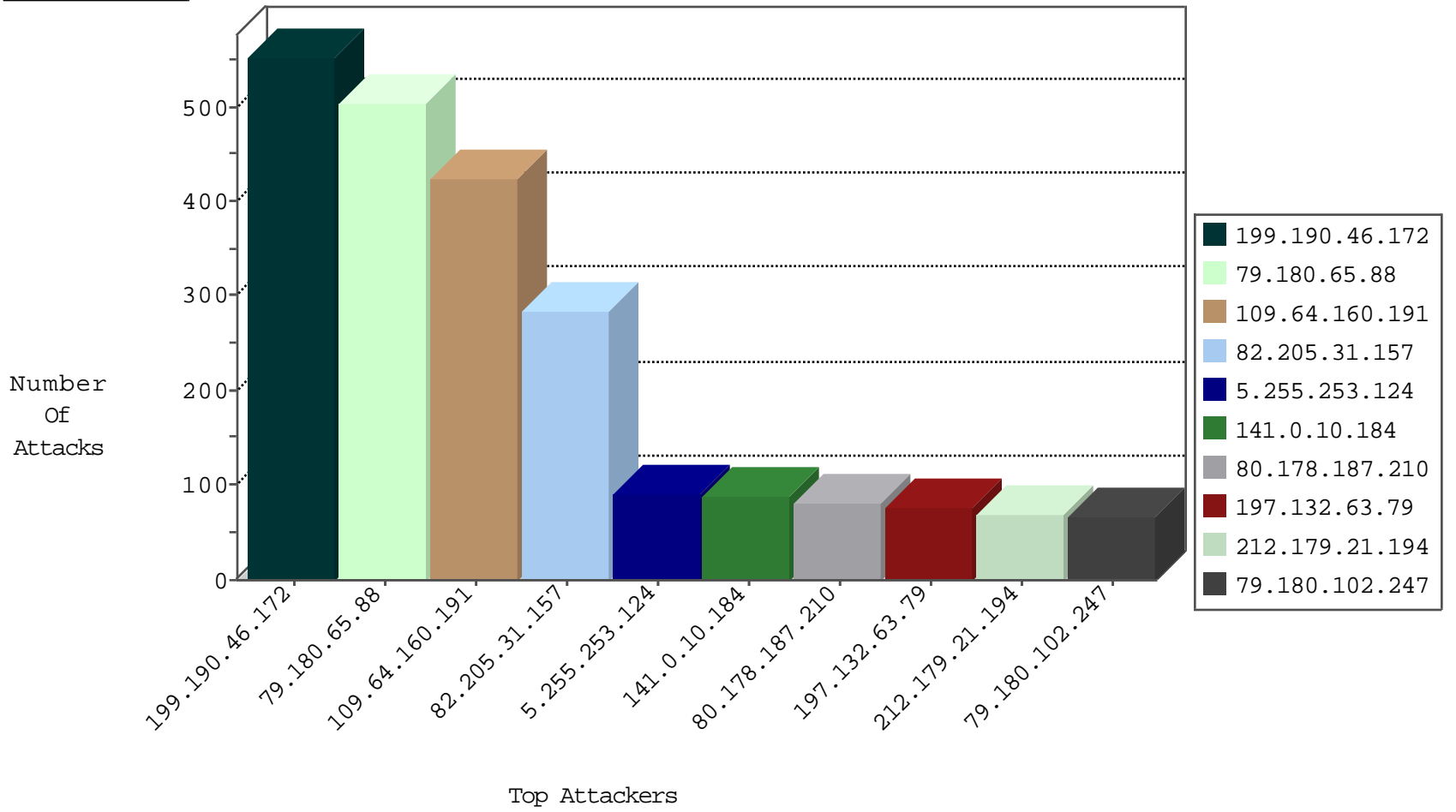




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.81.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5975
85.250.146.233	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	609
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	221
81.218.212.11	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
37.142.224.198	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
109.253.145.30	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
199.190.46.172	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	6
46.120.160.182	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
2.54.7.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
10.0.0.6		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
104.138.218.198		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
212.143.181.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
91.208.129.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
185.5.222.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.108.31.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.179.73.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
46.121.192.92	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
213.151.32.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.142.220	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
46.210.230.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
153.188.229.2	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
62.219.231.231	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
62.219.231.231	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
89.138.40.16	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
80.246.139.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.185	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
213.57.172.90	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.120.160.182	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.139	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	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	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
213.244.82.58	Palestinian Territory, Occupied	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.178	e.matpash.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
87.69.146.190	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	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.178	e.matpash.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
46.19.85.197	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	147.237.8.28	e.mobile-ks.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
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
110.226.57.106	India	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
149.78.145.250	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.134.161	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.90.151	Israel	147.237.77.216	doover.idf.il	portscan: TCP Distributed Portscan	1
212.179.46.16	Israel	147.237.77.216	doover.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	Taiwan	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	Austria	147.237.77.216	doover.idf.il	Tehila - Perl LWP with fake user agent	1
149.88.67.145	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
128.140.230.75	Romania	147.237.8.27	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
87.69.26.126	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.102.102	Israel	147.237.77.216	doover.idf.il	portscan: TCP Distributed Portscan	1
79.177.208.82	Israel	147.237.77.216	doover.idf.il	portscan: TCP Distributed Portscan	1
2.54.14.116	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.128.10	Israel	147.237.77.216	doover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	ET DROP Dshield Block Listed Source	1
183.136.216.3	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
87.69.93.176	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.102.190	Israel	147.237.77.216	doover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
199.190.46.172	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	547
79.180.65.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	503
109.64.160.191	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	424
82.205.31.157	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	285
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	90
141.0.10.184	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	88
80.178.187.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
197.132.63.79	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	76
79.180.102.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
84.94.193.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
91.53.2.167	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
212.179.61.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
79.181.219.225	Israel	147.237.72.156	aman.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	57
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	57
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
147.236.238.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
213.57.32.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
213.204.104.34	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
197.123.96.238	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
95.35.45.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
70.39.187.206	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
213.8.52.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
213.151.46.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
79.145.206.218	Spain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
80.179.125.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
176.12.136.162	Israel	147.237.72.156	aman.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
37.8.31.234	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
82.102.145.122	Israel	147.237.72.156	aman.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
79.181.136.80	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
79.178.133.146	Israel	147.237.72.156	aman.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
109.67.43.144	Israel	147.237.72.156	aman.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
49.150.75.253	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
209.18.49.94	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
79.180.53.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
109.64.96.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
176.12.150.98	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
212.179.46.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
5.22.129.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
212.179.73.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
193.104.119.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
147.236.38.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.76.97.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
149.78.97.192	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
79.181.219.225	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
176.12.150.207	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.150.207	Block	6
109.67.43.144	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
176.12.136.162	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
213.8.242.98	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
192.115.85.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	4
192.115.90.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	4
93.173.28.55	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
79.178.133.146	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
212.179.33.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
95.86.80.64	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
212.179.61.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
5.22.129.213	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.65.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.142.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	3
79.176.200.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
82.102.145.122	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.146.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.150.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.52.56.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.166.20.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.66.133.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.138.81.183	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
2.54.11.239	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.250.150.219	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
109.186.185.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.142.163.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.28.136.53	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.109.188.234	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.173.17.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.205.220	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
79.183.106.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/notified-notifyuser_ebnet	Block	1
109.67.205.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.31.76.161	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.31.76.161	Block	1
180.76.5.170	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ns-welcome.stm	Block	1
2.54.140.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.89.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.97	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/1249-he/navy.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1