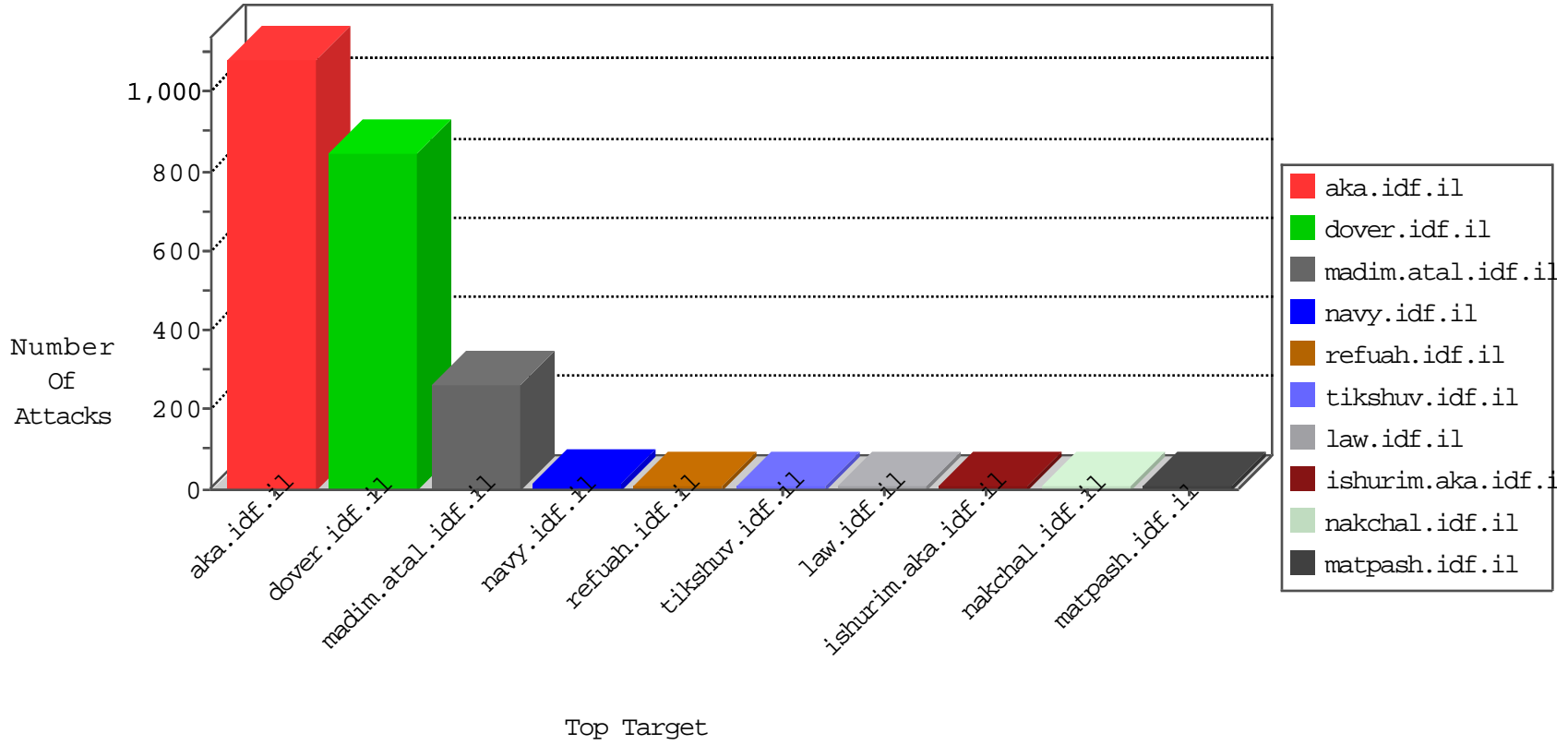
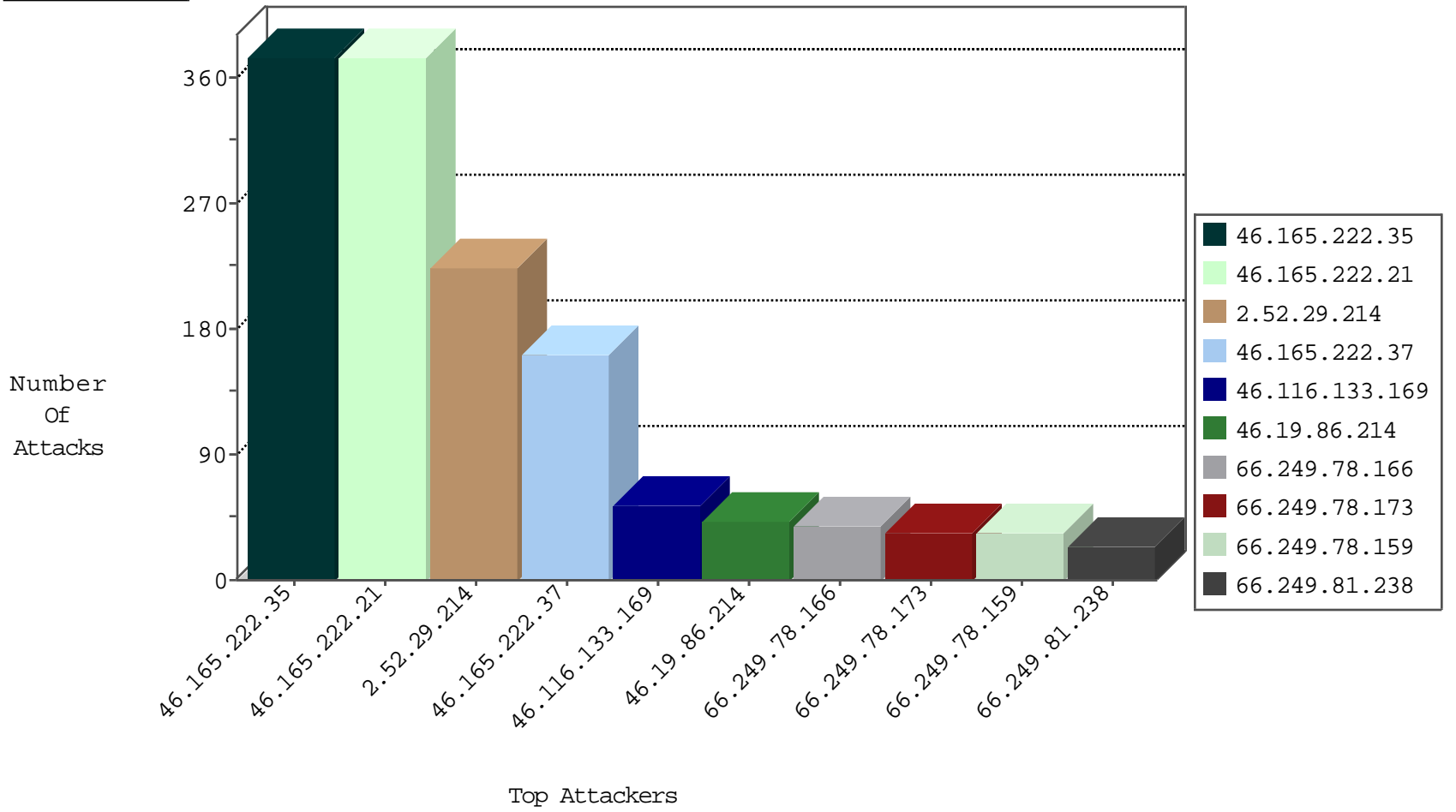


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6823
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3774
46.165.222.21	Germany	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	856
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	655
109.65.102.223	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
77.127.192.116	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	36
213.57.42.76	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
46.19.85.76	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
2.54.149.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
87.68.20.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
212.179.155.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.165.222.37	Germany	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6
89.138.22.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
212.179.155.129	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	6
176.12.150.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
89.138.22.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.12.150.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.182.166.235	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.181.152.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
99.244.191.10	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.182.166.235	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
79.178.29.232	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
195.37.190.86	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
79.178.29.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
31.210.186.131	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
124.232.142.220	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
60.56.48.184	Japan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
31.210.186.131	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.80.140.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.200	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.150.200	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	2
68.115.73.95	United States	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	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
213.57.106.46	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.180.52.223	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chimuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
37.26.146.204	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.187	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
82.102.169.113	Israel	147.237.77.243	mobile.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.121	e.navy.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
46.116.98.203	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
84.229.133.214	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	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
109.66.119.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.178.108.162	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
61.135.189.173	China	147.237.76.31	nakchal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	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	5
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
82.166.148.45	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
5.135.199.12	France	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.139.85	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 2048	1
109.253.130.155	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.231.192.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.67	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.129	China	147.237.76.201	e.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
119.90.139.85	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	1
101.226.2.99	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
91.224.132.118	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.165.222.35	Germany	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	375
46.165.222.21	Germany	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	371
46.165.222.37	Germany	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	156
46.116.133.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
93.173.243.25	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	19
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.86.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.182.166.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
87.68.20.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
68.115.73.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.81.238	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	8
109.64.142.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
85.250.191.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.81.238	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
66.249.81.238	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	8
46.19.86.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.228.221.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
90.215.178.151	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.81.241	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
31.154.17.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
73.36.23.106	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.81.241	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	7
199.30.16.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.136.165	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
79.176.155.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.67.175.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.81.241	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
176.12.136.165	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
46.19.86.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
65.55.210.38	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.158.53	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
82.166.20.5	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.210.186.199	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
79.178.29.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.158.53	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.178.49.126	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
5.102.254.81	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
31.186.228.57	United Kingdom	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.178.54.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.54.134.117	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
66.249.93.245	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
176.12.149.255	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.120.24.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.52.29.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	224
46.19.86.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.214	Block	42
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	16
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
85.130.217.89	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.130.217.89	Block	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	7
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	4
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
79.176.194.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	4
212.179.42.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	4
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
46.120.129.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
93.172.175.25	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	2
5.29.237.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.178.128.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.229.164.102	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	2
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
74.217.148.73	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bc/	Block	2
109.65.128.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.78	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	2
157.55.39.81	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.81	Block	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.126.191.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
46.121.41.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
109.253.138.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
87.68.19.243	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.67.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71800-he/maarachot.aspx	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_text.asp	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/hasata/hasata_eng.stm	Block	1
79.178.109.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	1
157.55.39.107	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/giyus/haredim/haredim.aspx	None	1
66.249.79.128	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.78.51	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
212.199.226.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.193.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
188.165.15.95	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9786-he/refuah.aspx	Block	1
77.127.187.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.aspx/getuserdetails	Block	1
64.124.203.77	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//ag/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter b6e681f8 in www.aka.idf.il/main/home/default.aspx	None	1
46.229.164.99	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	1
149.88.47.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1