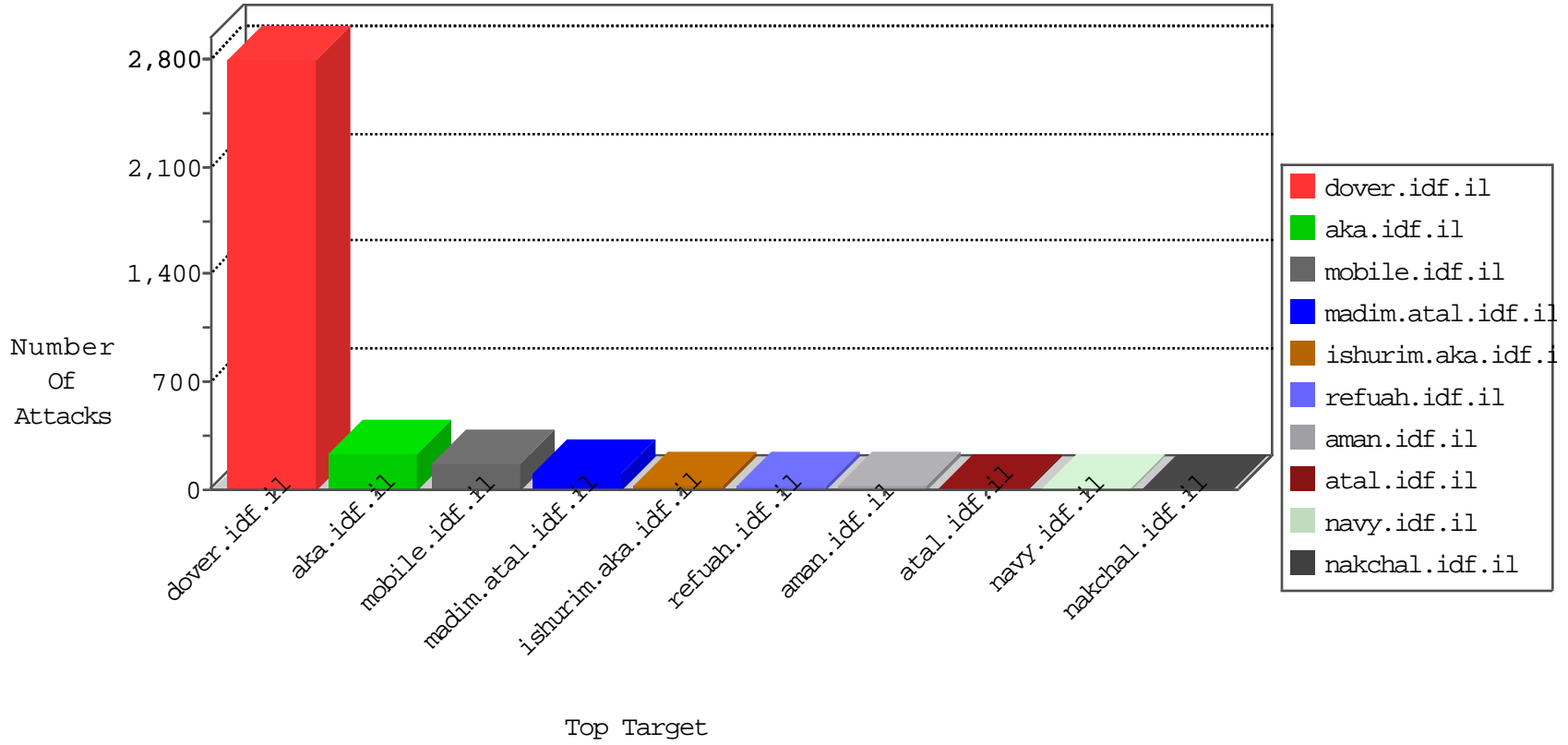
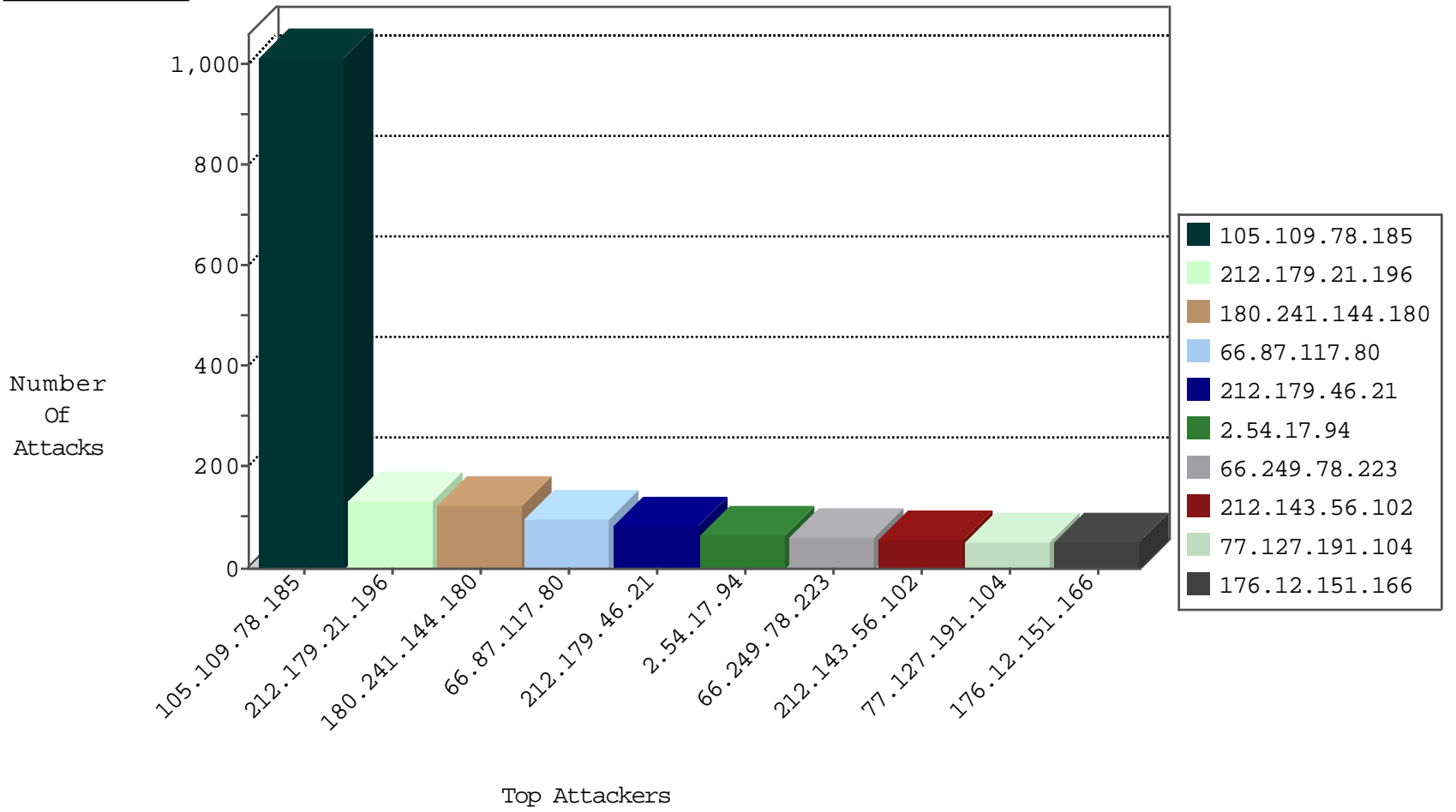


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
105.109.78.185	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	640
213.57.106.188	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	196
105.109.78.185	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	168
208.87.234.180	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
208.87.234.180	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.228.16.182	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
5.29.238.104	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
5.29.238.104	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.54.180.66	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
182.250.170.41	Japan	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.12.147.74	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
132.70.66.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
5.28.162.18	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
2.54.180.66	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.179.46.21	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.58.125	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
2.54.212.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.47.238.77	France	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
140.242.64.131	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
37.26.147.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.145.36	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.32.179.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.47.238.77	France	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
147.236.238.250	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
147.236.238.75	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
37.26.147.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
129.194.8.73	Switzerland	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.78	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
129.194.252.43	Switzerland	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
46.19.85.76	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	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.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
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
2.52.29.231	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.132	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
37.26.148.254	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.147	chinuch.aka.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
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
82.166.102.6	Israel	147.237.76.42	refuah.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	3
66.249.67.121	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	3
54.72.73.168	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.74.59	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.62.66	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.57.10	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.171.167	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.81.184	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.56.102	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
199.83.91.149	United States	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.151	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
187.11.121.110	Brazil	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
2.54.132.215	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.132.118	Russian Federation	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.110.55.39	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.77.119	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
199.83.91.149	United States	147.237.76.34	yochalan.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
105.109.78.185	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	630
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	131
180.241.144.180	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
66.87.117.80	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	97
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	83
2.54.17.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
212.143.56.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
77.127.191.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
109.253.157.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
185.32.178.207	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
80.179.197.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
80.246.130.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
37.26.148.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
207.232.58.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
109.67.65.117	Israel	147.237.72.156	aman.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.64.148.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
192.114.23.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
83.101.10.63	Belgium	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
84.94.193.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
82.166.20.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
212.143.134.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
24.136.26.46	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
80.178.239.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
77.125.114.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
85.130.243.70	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
2.54.60.89	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
77.125.241.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
213.151.32.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
92.98.185.240	United Arab Emirates	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.181.148.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
66.249.64.253	United States	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
147.236.238.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
217.139.39.193	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.166.33.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
93.173.144.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
146.185.30.93	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
89.138.61.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
87.69.230.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.223	Block	58
176.12.151.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
109.253.143.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	50
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.216	Block	44
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.230	Block	36
31.44.139.134	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	15
66.249.64.248	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.64.248	Block	10
66.249.64.133	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.64.133	Block	7
66.249.64.253	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.64.253	Block	5
80.178.239.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	4
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
79.181.8.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
88.208.252.213	United Kingdom	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 88.208.252.213	Block	3
46.117.88.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.66.127.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
185.32.178.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.146.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.94.22.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.176.43.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
178.137.19.143	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
79.178.66.112	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.178.66.112	Block	1
37.46.39.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
132.66.40.116	Israel	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/2004/february/0218-1.stm	Block	1
66.249.64.248	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unknown Parameter doc.. in aka.idf.il/giyus/forum/	None	1
46.19.86.242	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
180.76.5.167	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cdl/english/main_index.stm	Block	1
31.168.70.88	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.65.117	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.73.217	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
85.64.69.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
66.249.64.133	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listfaq/1853	Block	1
188.165.129.51	Spain	147.237.76.42	refuah.idf.il	Multiple signatures from 188.165.129.51	Block	1
37.142.2.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;catId in www.aka.idf.il/giyus/general/default.asp	None	1
79.178.66.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/6_s3_	Block	1
2.52.167.180	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
212.29.231.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
96.39.77.62	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
180.76.6.46	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/press_conference_16may00.stm	Block	1
80.246.133.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1