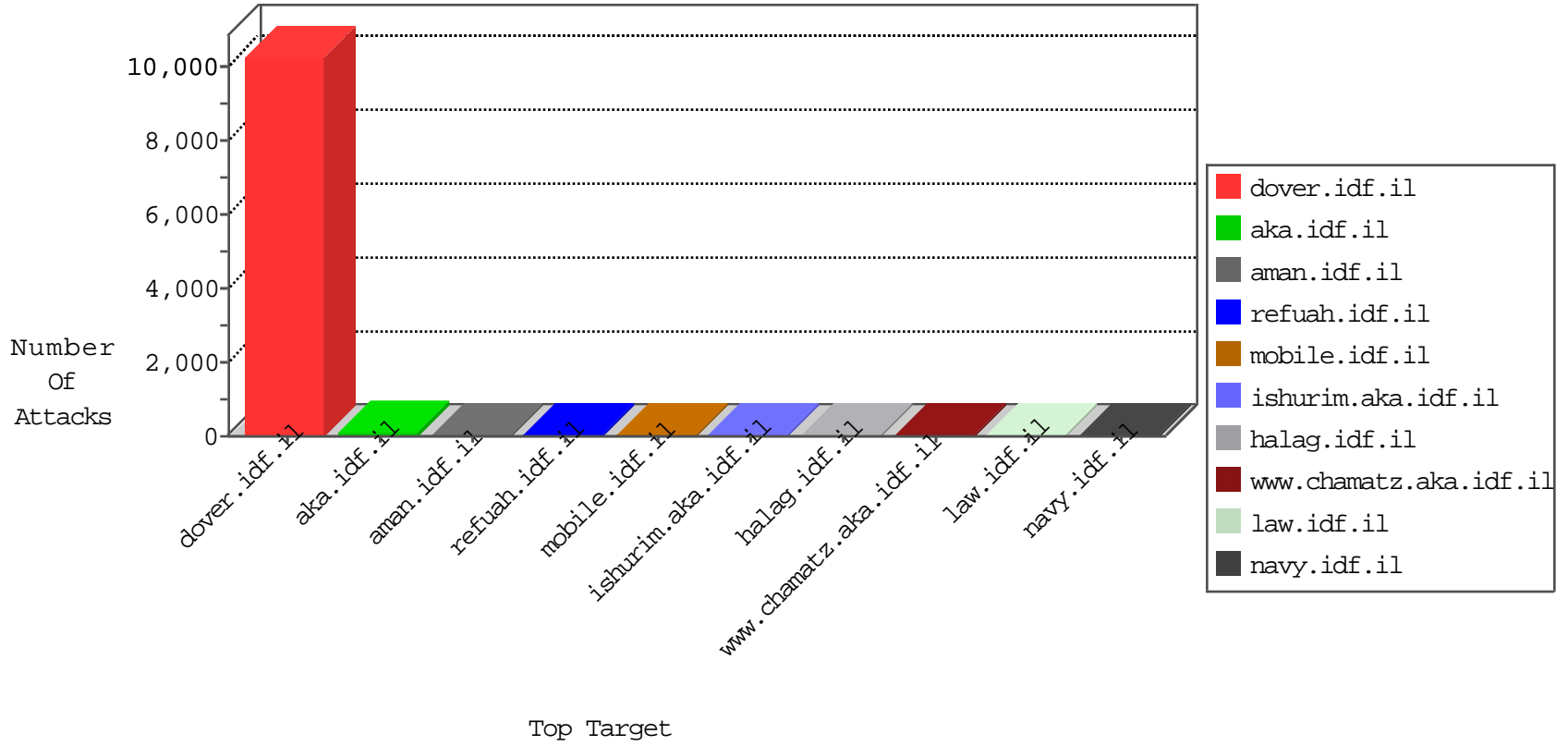
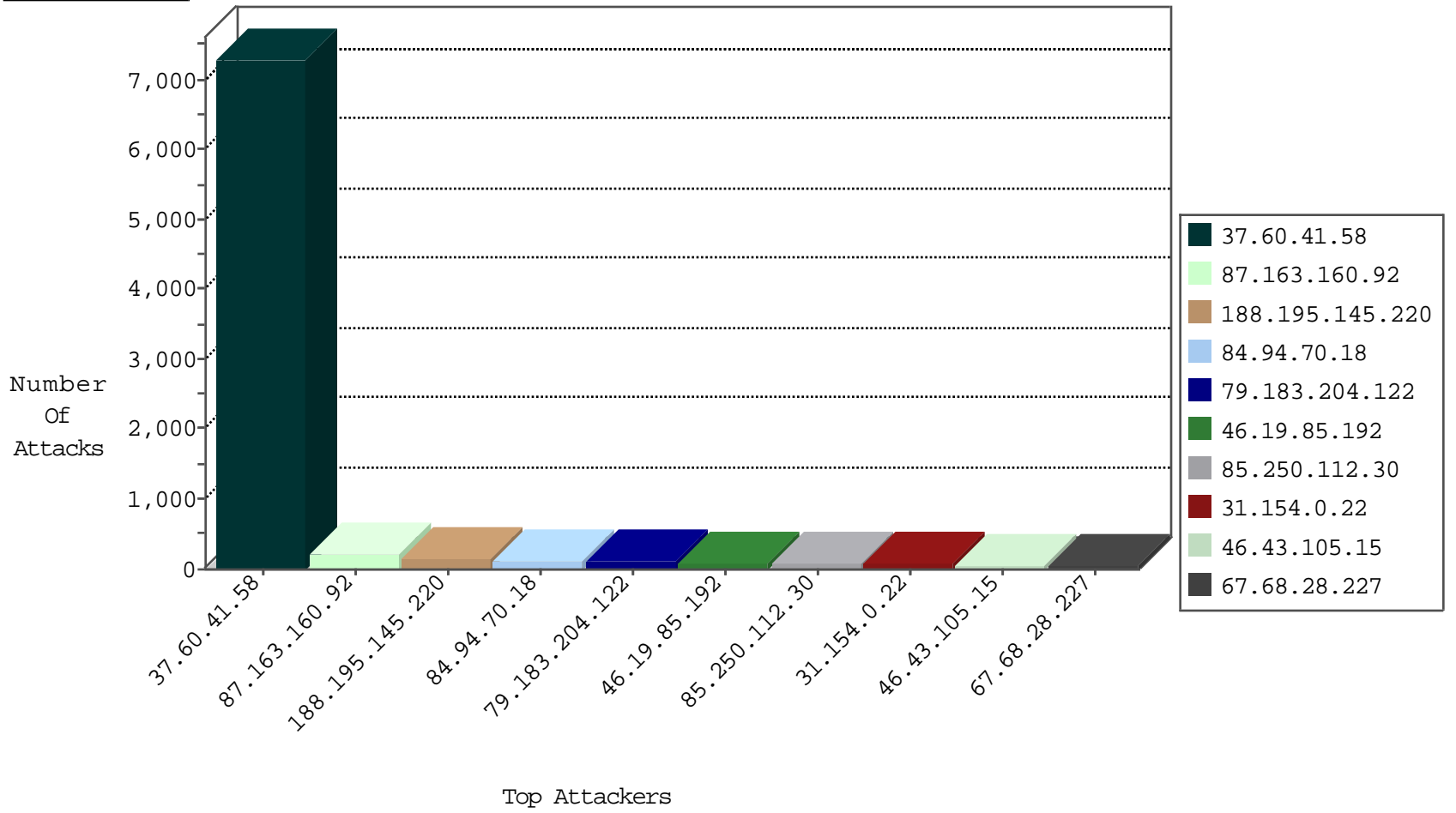




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
89.138.198.8	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	253
220.181.108.91	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	183
212.235.79.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
85.250.228.53	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
85.250.167.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	128
109.65.195.89	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
84.228.253.146	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
122.21.248.8	Japan	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
93.173.48.214	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.52.183.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
116.95.248.44	China	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.163.178	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
79.183.190.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	2
149.78.167.184	United States	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.39	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	147.237.77.212	e.dover.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	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
149.88.4.133	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.176	matpash.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
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.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
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
46.19.86.75	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	36
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
79.178.137.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.188.200	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.90.110.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
211.101.24.200	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.133.63.14	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.133.63.14	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
142.54.181.102	United States	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
50.30.34.56	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
119.90.139.72	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spanhaus DROP Listed Traffic Inbound	1
119.90.139.72	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
218.77.79.43	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.215	Netherlands	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
211.101.24.200	China	147.237.72.217	e.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
211.101.24.200	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.133.63.14	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	ET DROP Dshield Block Listed Source	1
61.133.63.14	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.133.63.14	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
142.54.181.102	United States	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
119.90.139.72	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
218.77.79.43	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
92.47.29.12	Kazakstan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.215	Netherlands	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
211.101.24.200	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.133.63.14	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.60.41.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7296
87.163.160.92	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	217
188.195.145.220	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	141
84.94.70.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	123
79.183.204.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	104
46.19.85.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
85.250.112.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	96
31.154.0.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
67.68.28.227	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
46.43.105.15	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
77.75.77.17	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
46.19.85.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
41.35.71.225	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
109.67.59.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
84.94.193.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
149.88.147.58	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
37.26.147.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
37.142.153.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
79.180.127.108	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
46.116.163.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
162.243.61.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
31.186.228.64	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
88.152.231.40	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.88	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
79.177.197.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
46.19.86.75	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	18
31.186.228.63	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
41.35.95.18	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
46.116.163.178	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	17
31.186.228.25	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
100.11.81.140	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.73.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
84.108.152.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
94.159.221.208	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
31.186.228.86	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
79.178.98.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.27	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
71.57.150.196	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.67.151.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
31.186.228.61	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
2.54.60.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	15
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	9
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	5
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	4
79.180.127.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
192.99.12.99	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/default.aspx	Block	3
46.43.105.15	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	3
85.64.204.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.71.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
149.78.167.184	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
87.68.16.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
103.11.217.26	Cambodia	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 103.11.217.26	Block	2
85.64.184.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
79.180.127.108	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.180.127.108	Block	1
46.116.163.178	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
87.68.163.140	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/_vti_bin/owssvr.dll	Block	1
80.246.133.79	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
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/gyus/general.aspx	Block	1
66.249.64.161	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
109.67.182.14	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.171.165	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
84.94.70.18	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
66.249.65.149	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
85.65.7.22	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.151.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.75.49	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/	Block	1
46.118.119.63	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
95.86.111.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
84.109.152.87	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.81.226	Israel	147.237.76.31	nakchal.idf.il	URL is Above Root Directory nakchal.idf.il/./favicon.ico	Block	1
157.55.39.142	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/gyus/general.aspx	Block	1
79.181.118.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
85.64.168.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
87.68.163.140	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.68.163.140	Block	1
79.182.178.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/gyus/general.aspx	Block	1
52.7.47.37	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.67.8.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1