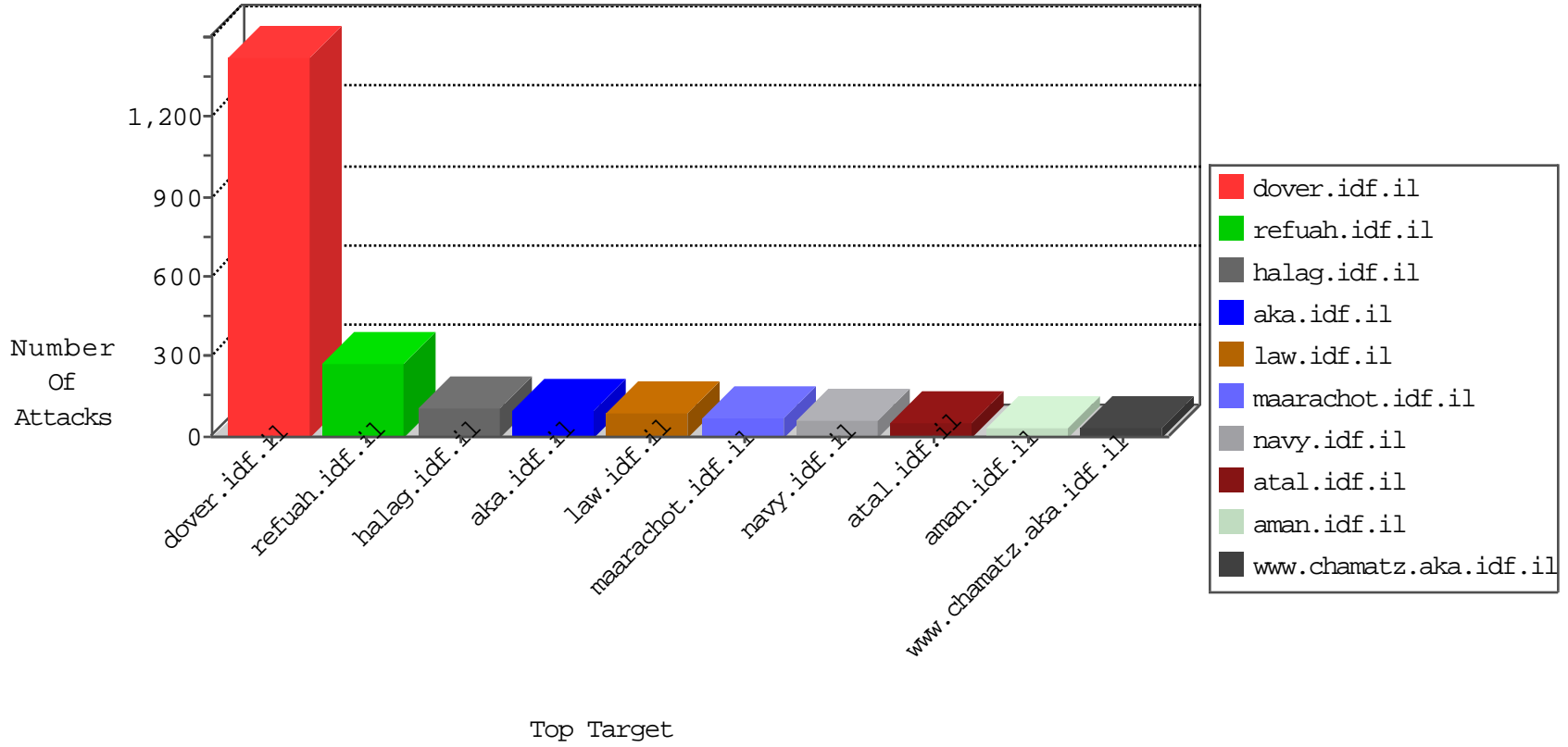
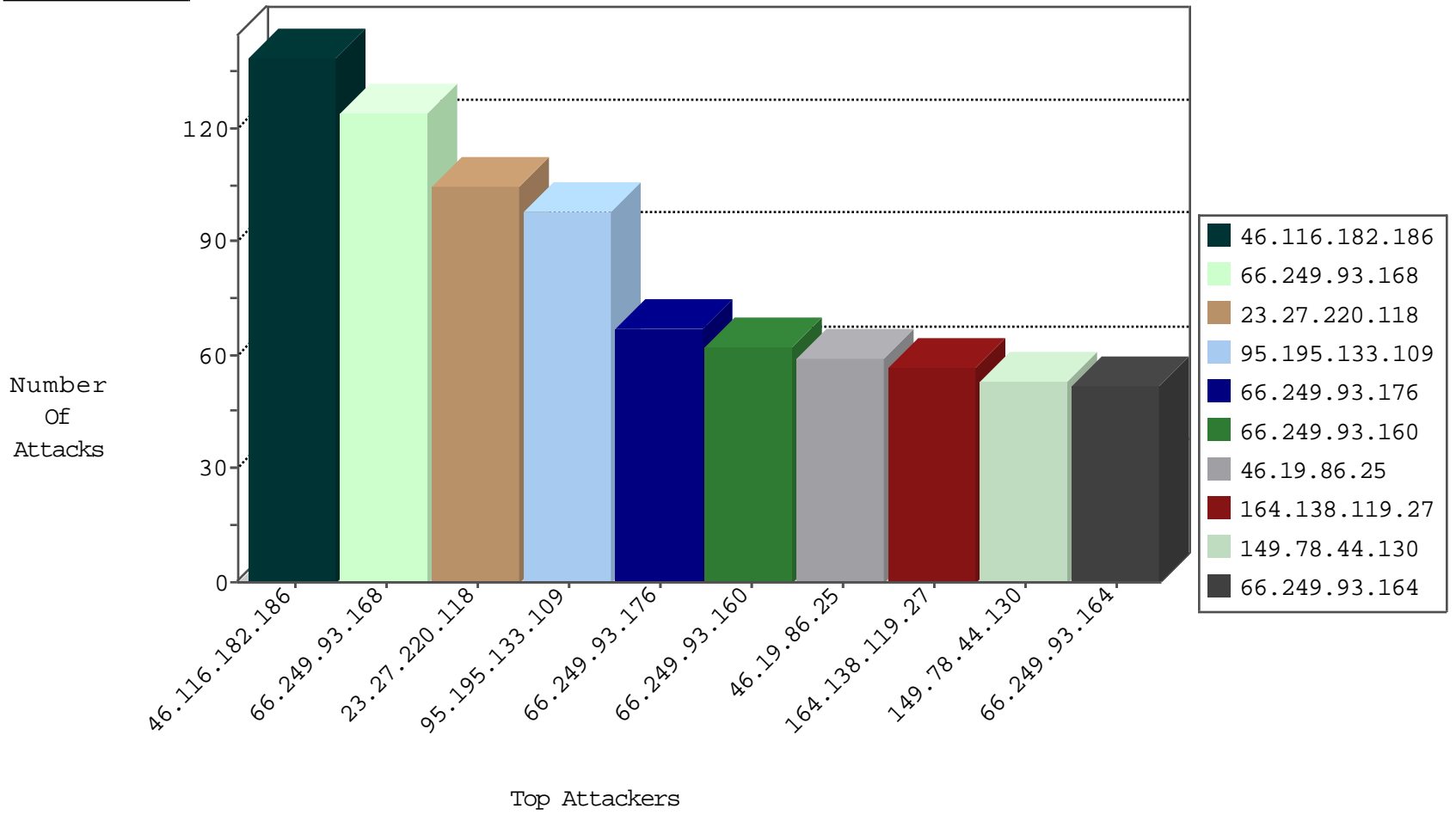




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.187	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	347
37.142.36.142	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	67
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	67
46.19.85.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	62
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	57
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	52
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	42
220.181.108.149	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	38
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	37
220.181.108.156	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	36
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	34
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	31
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	22
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.65.44	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.65.46	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	17
66.249.73.219	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	17
66.249.65.50	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.65.26	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	15
66.249.73.201	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.73.217	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.73.211	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.73.203	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	13
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	13
66.249.65.28	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.65.30	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.65.41	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.65.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	10
66.249.65.48	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	10
66.249.65.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.65.12	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.73.238	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	9
66.249.65.191	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.73.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.65.1	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	8
66.249.65.39	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.73.222	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.65.32	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.79.13	United States	147.237.76.177	noore.idf.il	Block_Ip_Web_In	drop	5
66.249.93.158	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	5

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	2
93.120.27.62	Romania	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	2
93.120.27.62	Romania	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.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
66.166.189.133	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.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
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.130.204.67	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	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.197	e.hinush.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
71.204.139.189	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.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	6
61.240.144.64	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	Russian Federation	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
159.8.35.146	Switzerland	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
77.127.127.122	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.76	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
159.8.35.146	Switzerland	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.76	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
159.8.35.146	Switzerland	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.19	Ukraine	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.76	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.116.182.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	139
23.27.220.118	United States	147.237.77.234	halag.idf.i	First packet isn't SYN	drop	drop	103
95.195.133.109	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	98
46.19.86.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
164.138.119.27	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
149.78.44.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
31.210.187.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
46.19.86.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
84.109.102.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
85.250.135.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
176.12.139.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
46.19.86.68	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
37.26.146.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
164.82.32.13	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
85.64.163.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
212.116.177.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
207.46.13.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
71.204.139.189	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
157.55.39.6	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
212.179.159.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
149.88.123.107	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
71.239.237.8	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
46.116.125.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
2.54.26.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
46.19.85.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
109.160.250.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
66.99.28.98	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.253.149.227	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
171.96.248.10	Thailand	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
46.116.137.38	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
176.12.136.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
37.236.200.86	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
37.26.148.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
188.236.252.138	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
85.65.106.92	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	6
85.65.106.92	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
85.65.106.92	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	6
50.67.132.26	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.46.13.82	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
85.72.40.4	Greece	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
80.178.11.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.86.111.61	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
87.69.160.116	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/chinuch/general/default.asp	None	3
95.86.111.61	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 95.86.111.61	Block	2
37.236.200.86	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
213.57.198.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.143.232.15	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	1
82.137.12.241	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/homefront3.stm	Block	1
5.22.129.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
46.19.86.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/fagselecion.aspx	None	1
216.130.192.12	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
188.143.232.15	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/general.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
84.228.97.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.82	Block	1
136.243.36.88	Germany	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	1
87.69.152.39	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/april/08.stm	Block	1
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/123103-3.stm	Block	1
178.162.205.80	Germany	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info06.stm	Block	1
188.143.232.15	Russian Federation	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	1
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.241.237.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
180.76.4.210	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.181.146.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
188.165.15.78	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0104.stm	Block	1