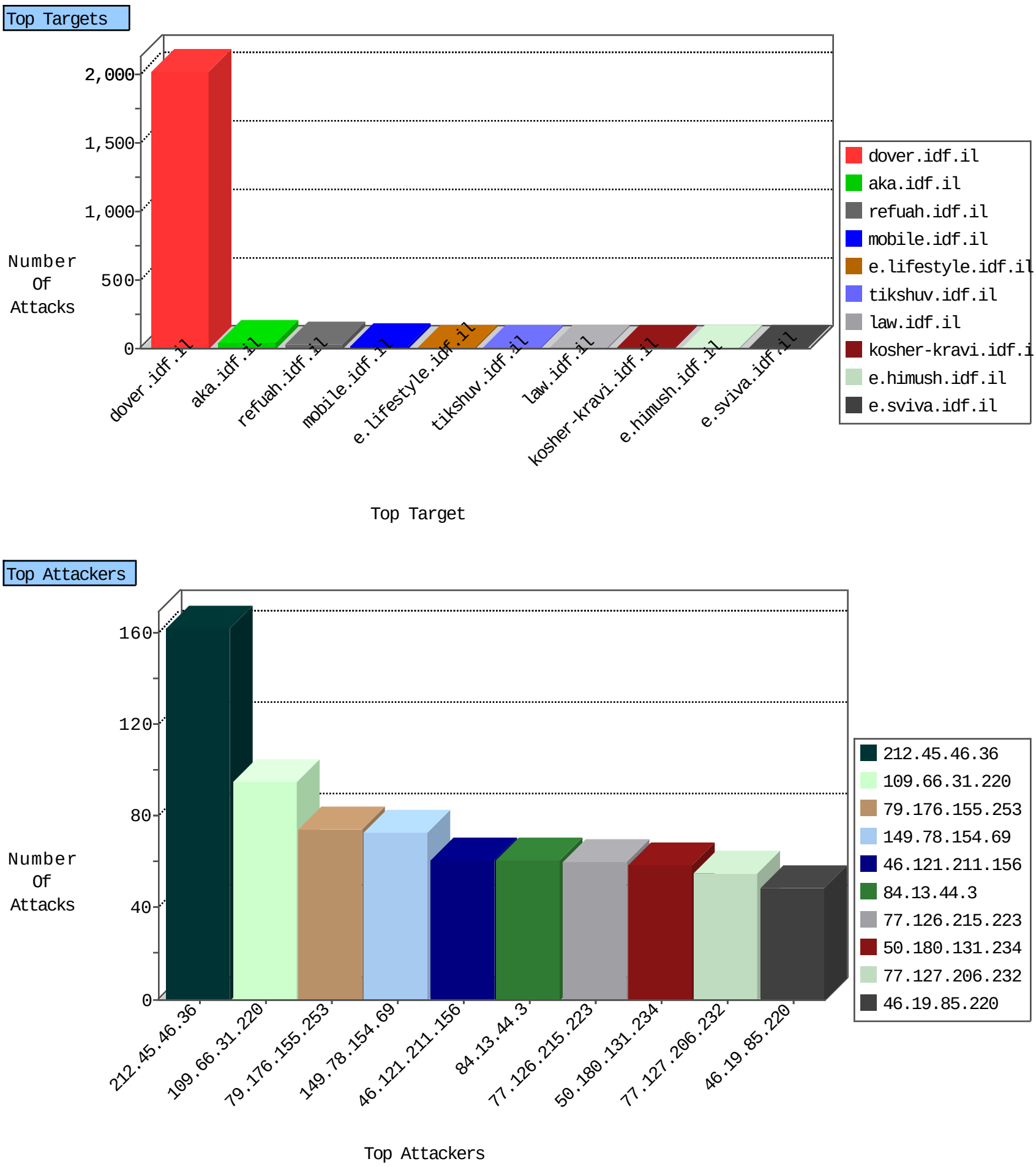
05-06-2015-23:03:05 to 05-07-2015-00:03:05

IDF Under Attack
05-06-2015-23:03:05



05-06-2015-23:03:05 to 05-07-2015-00:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.114	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	471
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	441
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	314
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	161
70.197.4.60	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
5.144.51.38	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
146.185.239.100	Russian Federation	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
200.0.197.26	Argentina	147.237.77.19	law-forum.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
46.183.220.250	Latvia	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

05-06-2015-23:03:05 to 05-07-2015-00:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
66.240.192.138	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.39	mobile.meitav.idf.i	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
77.125.78.164	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	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
195.210.28.78	Slovakia	147.237.76.39	mobile.meitav.idf.i	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.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
85.25.103.50	Germany	147.237.77.178	e.matpash.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
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.i	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
5.29.101.152	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	147.237.8.14	e.orchot.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	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.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
66.240.192.138	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1

05-06-2015-23:03:05 to 05-07-2015-00:03:05

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
79.179.109.167	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
200.0.197.26	Argentina	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
176.12.149.237	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
128.199.254.26	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.180.38.43	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
67.159.16.3	United States	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.89.137.3	China	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
67.159.16.3	United States	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.18.232.63	United Kingdom	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
212.18.232.63	United Kingdom	147.237.76.42	refuah.idf.il	ET SCAN NMAP -f -sS	1
168.235.144.56		147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
67.159.16.3	United States	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
212.18.232.63	United Kingdom	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 2048	1

05-06-2015-23:03:05 to 05-07-2015-00:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.45.46.36	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	162
109.66.31.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	93
79.176.155.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	74
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
84.13.44.3	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
46.121.211.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
77.126.215.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
77.127.206.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
46.19.85.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
176.12.146.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
50.180.131.234	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
87.69.78.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
2.54.135.213	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
93.173.234.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
68.43.212.184	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
109.253.132.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
95.86.113.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
82.145.216.150	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
176.12.151.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
46.19.85.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.138.223.74	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
109.67.160.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
77.127.22.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
50.180.131.234	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
176.12.144.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
200.204.163.148	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.66.107.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
191.189.153.245	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
77.125.78.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
199.168.220.52	Canada	147.237.8.24	e.lifestyle.idf	Geo-location inbound enforcement	Geo-location enforcement	drop	10
84.108.27.228	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
86.155.55.11	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
149.78.182.205	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
2.54.12.238	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
95.86.67.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	7
46.116.54.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/statistics/chiefs.stm	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/421-he/patzar.aspx	Block	1
182.253.224.110	Indonesia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
84.108.27.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	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
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2001/october/31.stm	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
157.55.39.144	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
79.179.17.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
31.168.209.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/913-4401-he/patzar.aspx	Block	1
185.32.177.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
66.249.67.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1424-he/refuah.aspx	Block	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
87.68.147.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	1
162.220.246.180	Italy	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
79.180.199.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
37.16.72.139	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/06z.stm	Block	1
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
62.221.99.118	Moldova, Republic of	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/patzar/home/default.asp	None	1
149.78.107.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.96.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/binladen2.stm	Block	1
79.183.127.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.147.227	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_moreinfo.asp	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
156.56.195.132	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.78.228	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
5.29.135.244	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13089-he/dover.aspx	Block	1
180.76.4.28	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	Block	1
82.205.113.120	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14369-ar/dover.aspx'	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1