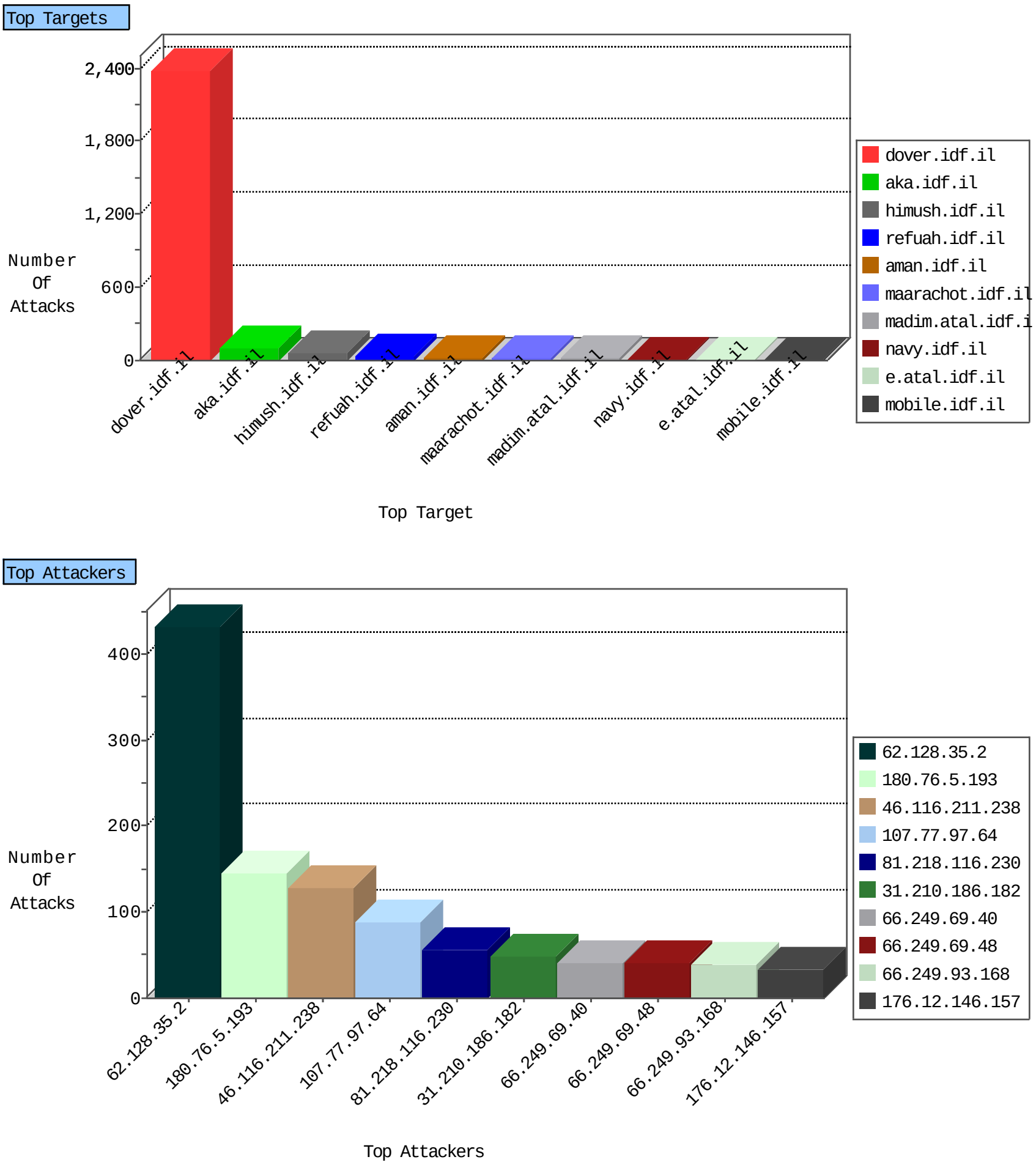
04-27-2015-08:03:07 to 04-27-2015-09:03:07

IDF Under Attack
04-27-2015-08:03:07



04-27-2015-08:03:07 to 04-27-2015-09:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2908
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	635
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
176.12.139.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	105
2.54.141.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
91.135.111.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
91.135.111.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.64.109.35	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.86.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
88.198.68.148	Germany	147.237.8.24	e.lifestyle.idf.il	Invalid L4 Header Length	drop	1
109.253.129.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.168.14.177		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
24.99.57.122	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
74.207.243.81	United States	147.237.77.121	e.navy.idf.il	Invalid L4 Header Length	drop	1
192.168.14.177		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-27-2015-08:03:07 to 04-27-2015-09:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	146
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	16
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	7610: IP Reputation	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.233	atal.idf.il	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
31.210.186.182	Israel	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	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
130.185.155.130	Sweden	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.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
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.86	navy.idf.il	7610: IP Reputation	Block	1
91.135.111.75	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.135.131	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	7610: IP Reputation	Block	1

04-27-2015-08:03:07 to 04-27-2015-09:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
176.12.146.157	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
176.12.137.104	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
43.255.191.161	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
58.20.54.249	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
58.20.54.249	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
109.253.156.225	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
101.69.199.71	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
81.218.118.124	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
58.20.54.249	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
176.12.148.227	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
109.226.17.195	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
100.7.37.183	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
73.11.61.110	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1

04-27-2015-08:03:07 to 04-27-2015-09:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
62.128.35.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	433
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	128
107.77.97.64	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	89
81.218.116.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
31.210.186.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
213.151.49.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
2.54.24.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
217.194.199.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
79.178.2.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
212.179.132.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
130.25.71.130	Italy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
87.68.155.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
176.106.227.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.69.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
195.160.240.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
62.90.76.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
46.19.86.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
66.249.69.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
37.26.146.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
37.26.148.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
5.255.253.124	Russian Federation	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	16
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	16
94.159.143.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
87.69.97.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
176.12.146.157	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	alert	15
66.249.69.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
24.148.91.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.12.146.157	Israel	147.237.76.30	himush.idf.il	Invalid ACK number	Bad TCP sequence	monitor	13
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.12.143.156	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
149.78.233.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.69.32	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
149.88.90.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.140.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.86.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
85.250.118.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
212.179.61.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
37.26.147.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
62.0.231.129	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.141.157	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.141.157	Block	13
5.255.253.93	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	4
5.102.254.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
185.32.178.86	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.133.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.93.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
192.157.245.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/pricing	Block	1
109.65.21.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71831-he/maarachot.aspx	Block	1
212.179.46.21	Israel	147.237.77.74	law.idf.il	SQL injection on parameter SearchText in www.law.idf.il/657-en/patzar.aspx	Block	1
180.76.4.93	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.19.86.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl88.x in www.aka.idf.il/main/sachar/payslips.aspx	None	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
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.40	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.52	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/chinuch/faq/default.asp	None	1
109.65.99.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
212.179.46.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71518-he/maarachot.aspx	Block	1
180.76.4.217	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
46.119.113.155	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.48	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aka	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.100.81	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
109.65.115.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
52.6.132.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//newsite/english/main.stm	Block	1
2.54.141.157	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
147.236.138.212	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
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0113-1.stm	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/pirsumim.asp	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=5&catid=22707&docid=72354	Block	1
109.253.140.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.114.148.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
64.187.228.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.18.206.13	Poland	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/golani/golani.stm	Block	1
212.117.143.250	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Unknown SSL Session	None	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/yoman/	Block	1
37.142.90.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1