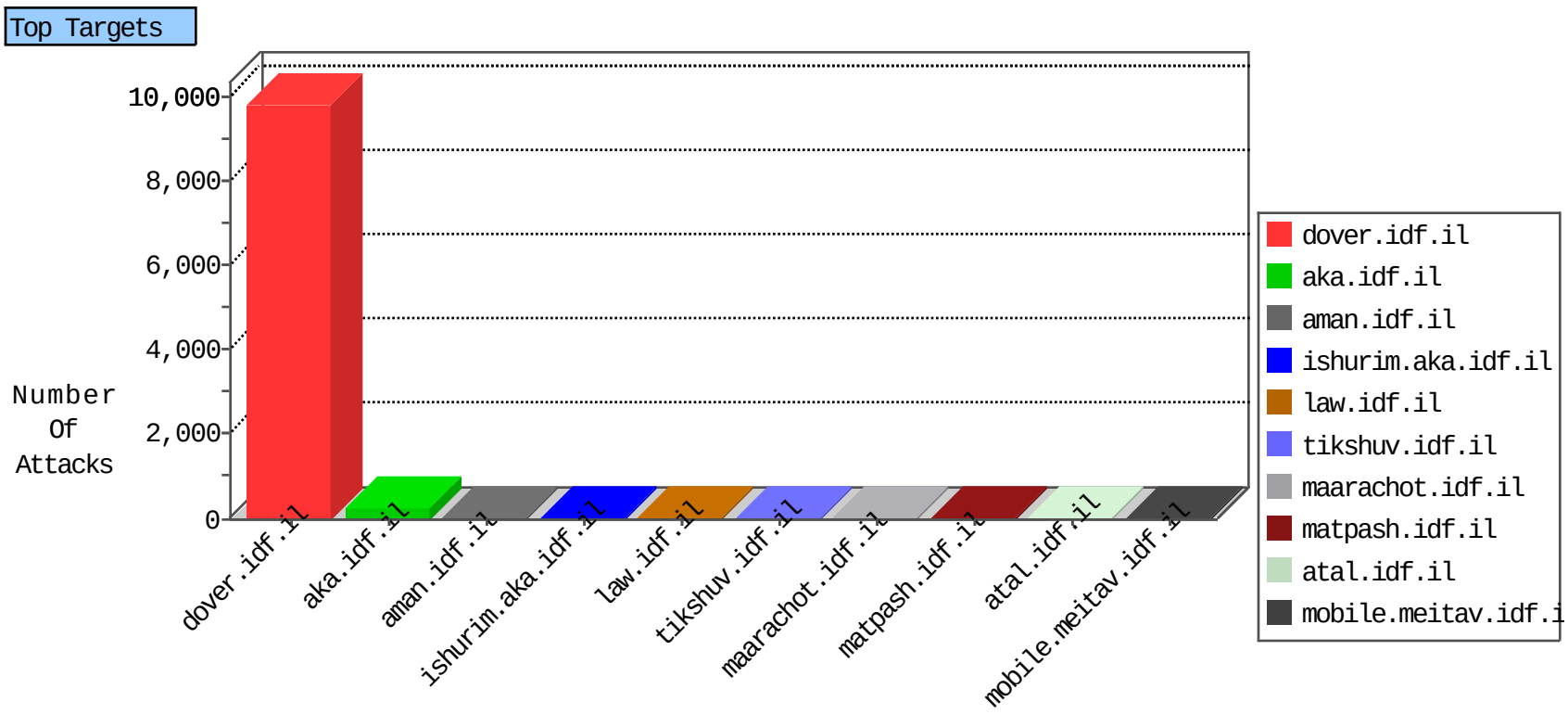
04-19-2015-01:03:04 to 04-19-2015-02:03:04

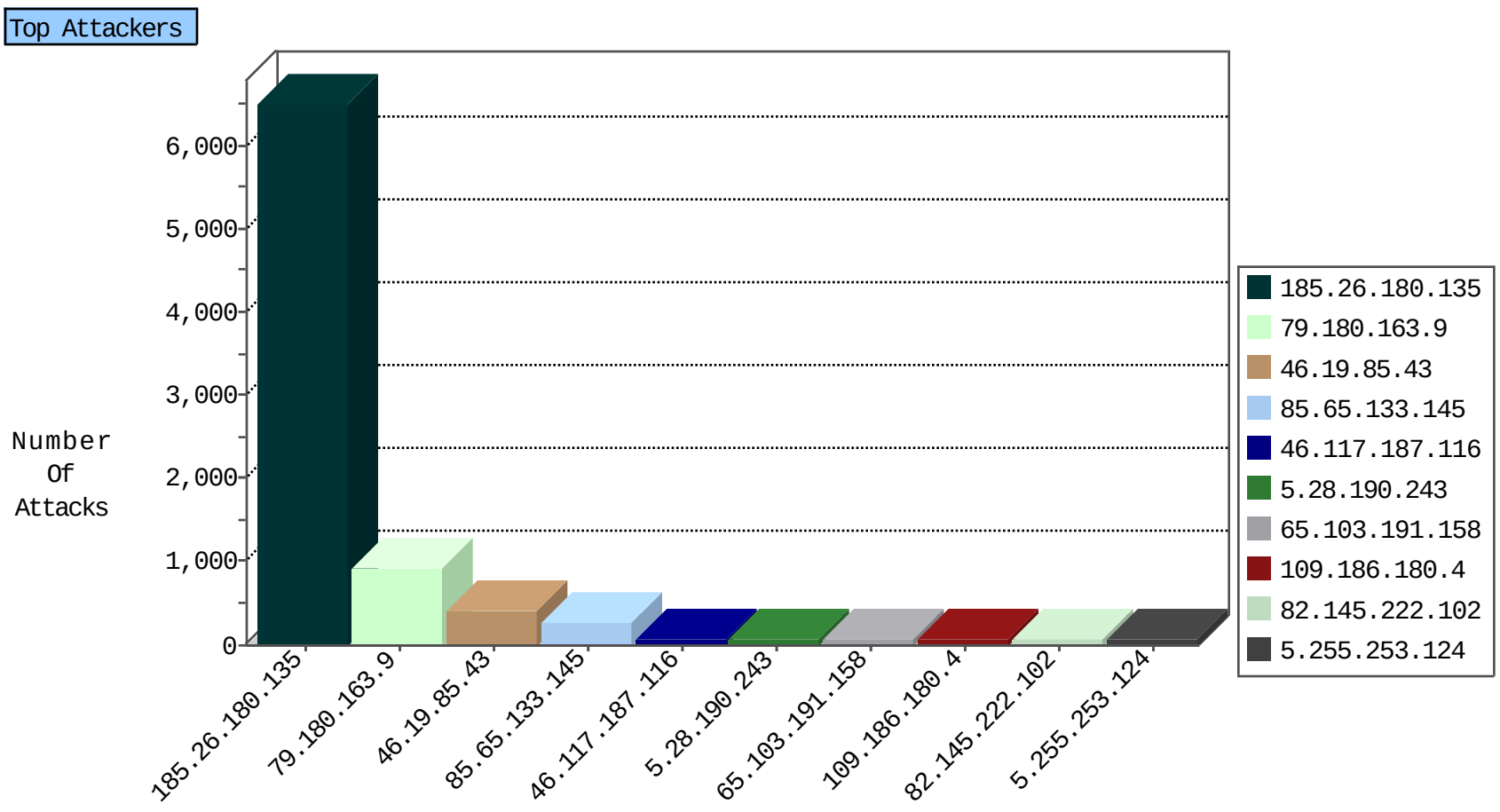
IDF Under Attack
04-19-2015-01:03:04

Top Targets



Top Target

Top Attackers



Top Attackers

04-19-2015-01:03:04 to 04-19-2015-02:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
185.26.180.135	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3775
89.139.179.28	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2532
220.181.108.140	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	252
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	163
46.19.86.7	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
182.20.159.69	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
195.37.190.86	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
124.232.142.220	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

04-19-2015-01:03:04 to 04-19-2015-02:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.65.133.145	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	258
46.19.85.146	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.11	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
132.64.42.98	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.108	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	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
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	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	DVRep_B-N_60_100	Block	1
95.139.206.189	Russian Federation	147.237.72.166	aka.idf.il	3617: HTTP: Paros Proxy HTTP Request	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	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.44	e.refuah.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	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
46.19.85.11	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.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
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1

04-19-2015-01:03:04 to 04-19-2015-02:03:04

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	5
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
79.181.114.172	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.64.12	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
122.228.207.77	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
118.174.68.206	Thailand	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
58.20.54.249	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
118.174.68.206	Thailand	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
212.47.248.0	France	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
94.25.149.220	Russian Federation	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
118.174.68.206	Thailand	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
212.47.248.0	France	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
95.185.5.111	Romania	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
94.25.149.220	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1

04-19-2015-01:03:04 to 04-19-2015-02:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.180.135	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6490
79.180.163.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	925
46.19.85.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	405
46.117.187.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
5.28.190.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	75
65.103.191.158	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
82.145.222.102	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	64
109.186.180.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	64
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
109.67.177.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
84.108.164.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
166.137.244.50	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
89.139.179.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
109.253.138.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
109.67.127.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
2.24.201.92	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
73.172.99.64	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
79.181.24.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
93.193.44.182	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
85.250.167.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
176.12.138.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
109.253.139.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
46.19.86.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.19.85.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
176.12.147.53	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
79.177.169.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
89.69.183.228	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
213.151.32.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
95.185.5.111	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
109.253.133.226	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
176.12.139.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
75.148.124.46	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
157.55.39.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.149.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
98.231.209.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
99.170.41.94	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.19.86.7	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	10
192.114.91.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.142.142.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.181.24.164	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
85.12.197.62	Russian Federation	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
5.29.252.102	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 5.29.252.102	Block	2
50.87.206.85	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
85.12.197.62	Russian Federation	147.237.77.74	law.idf.il	PHP Attempt	Block	2
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34//scriptresource.axd	Block	1
121.211.236.75	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
85.12.197.62	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20131-he/dover.aspx	Block	1
157.55.39.130	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.131.147.112		147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/skira/default.asp	None	1
61.135.190.72	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
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	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1117-6.stm	Block	1
65.55.210.82	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
123.138.19.142	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//english/news/grapheat.stm	Block	1
37.60.41.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
157.55.39.201	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/undefined	Block	1
66.249.65.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/webresource.axd	Block	1
109.66.38.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
2.52.55.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover.aspx i	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
149.78.226.140	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
94.124.5.10	Poland	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
50.87.206.85	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-12436-he/mmmmmmm=d507e946mmmmmmm_d507e946	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
61.135.190.197	China	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17//	Block	1
109.253.159.184	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.12.197.62	Russian Federation	147.237.77.74	law.idf.il	Admin Blocking	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
213.57.62.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
155.94.176.20		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/grapheat.stm	Block	1
66.249.64.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.193.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.73.203	None	1
61.135.190.199	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/scriptresource.axd	Block	1
120.15.43.54	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/9/279.pdf/trackback/	Block	1
5.29.252.102	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/	Block	1