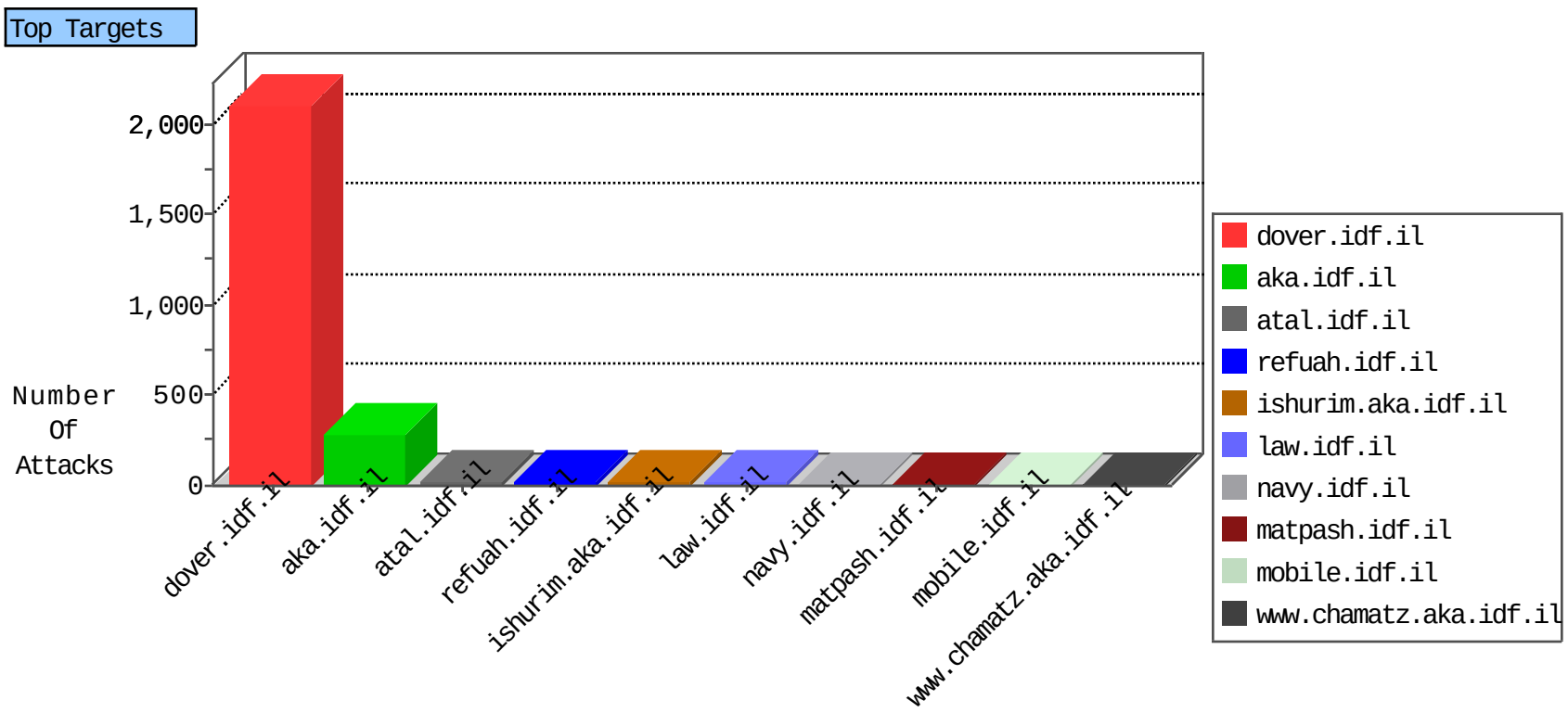
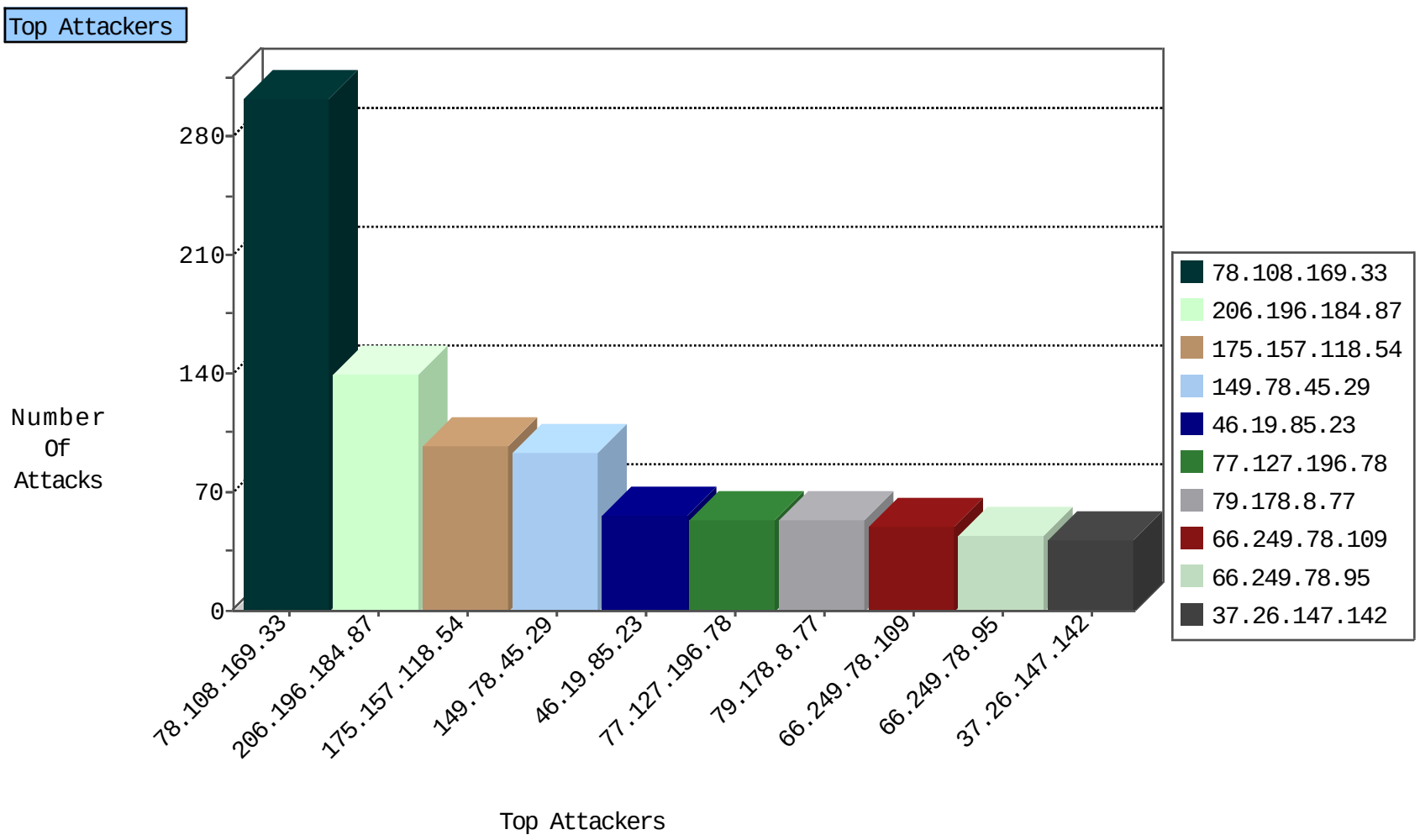
04-29-2015-07:03:03 to 04-29-2015-08:03:03

IDF Under Attack
04-29-2015-07:03:03





04-29-2015-07:03:03 to 04-29-2015-08:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.92	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	315
220.181.108.184	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	313
80.246.141.213	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
220.181.108.102	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	26
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
111.216.3.98	Japan	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
23.250.11.220	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
79.179.219.236	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
23.250.11.220	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
23.250.11.220	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
23.250.11.220	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-29-2015-07:03:03 to 04-29-2015-08:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	2
112.111.191.133	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	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	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
182.50.130.136	Singapore	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
41.185.12.165	South Africa	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
198.20.69.98	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.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
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
185.32.176.212	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
46.116.109.163	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	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.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
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
46.121.81.67	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.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
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1

04-29-2015-07:03:03 to 04-29-2015-08:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
222.69.94.13	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.107.251	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.147.56.190	Switzerland	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 2048	1
61.160.224.128	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
5.102.254.105	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.147.56.190	Switzerland	147.237.72.217	e.idf.il	ET SCAN NMAP -f -sS	1
58.20.54.249	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
201.239.118.143	Chile	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
104.167.96.44		147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.163	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
75.98.175.75	United States	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	1
43.255.191.163	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.197	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.147.56.190	Switzerland	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	India	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
201.239.118.143	Chile	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
147.235.236.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.163	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
107.6.130.113	United States	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
104.167.96.44		147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1

04-29-2015-07:03:03 to 04-29-2015-08:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
78.108.169.33	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	301
206.196.184.87	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	140
175.157.118.54	Sri Lanka	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	98
149.78.45.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	93
46.19.85.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
77.127.196.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
79.178.8.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
37.26.147.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
94.234.170.179	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
2.54.3.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
46.19.86.98	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
192.116.190.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
212.25.84.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
109.160.189.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
206.190.158.78	Netherlands	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	24
46.19.85.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
66.249.78.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
62.0.34.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
192.115.248.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
176.12.141.68	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
66.249.78.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
66.249.78.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
91.221.59.23	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
207.46.13.92	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
157.55.39.10	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
80.246.130.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
89.138.223.74	Israel	147.237.72.166	aka.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.i	First packet isn't SYN	drop	drop	12
79.181.138.6	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.149.113	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.140.61	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
37.142.103.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
91.221.59.27	Germany	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	10
176.12.146.252	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
173.252.81.113	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
176.12.142.45	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
91.221.59.27	Germany	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	10
173.252.81.116	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
176.12.142.150	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.12.149.100	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.109	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	10
87.69.100.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.12.151.233	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.109	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	12
37.26.147.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	7
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
185.32.176.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
89.134.218.126	Hungary	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	3
176.12.149.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.10	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.10	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
31.168.220.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.43	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.43	Block	2
79.181.138.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.44	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 157.55.39.44	Block	2
37.26.147.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
89.138.223.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.149.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//1133-he/dover.aspx	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.178	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/horaot/news/news.asp	Block	1
75.98.175.75	United States	147.237.77.74	law.idf.il	Multiple signatures from 75.98.175.75	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/armored4.stm	Block	1
176.12.142.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0410-3.stm	Block	1
109.253.132.50	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
212.179.61.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
176.12.150.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.177.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
75.98.175.75	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.67.73	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
176.12.146.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.93	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
109.253.136.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.159.253	Block	1
176.12.151.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-16593-ar/	Block	1
176.12.139.83	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
31.193.51.59	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//1133-he/dover.aspx	Block	1
176.12.149.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
125.65.81.124	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
176.12.151.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1