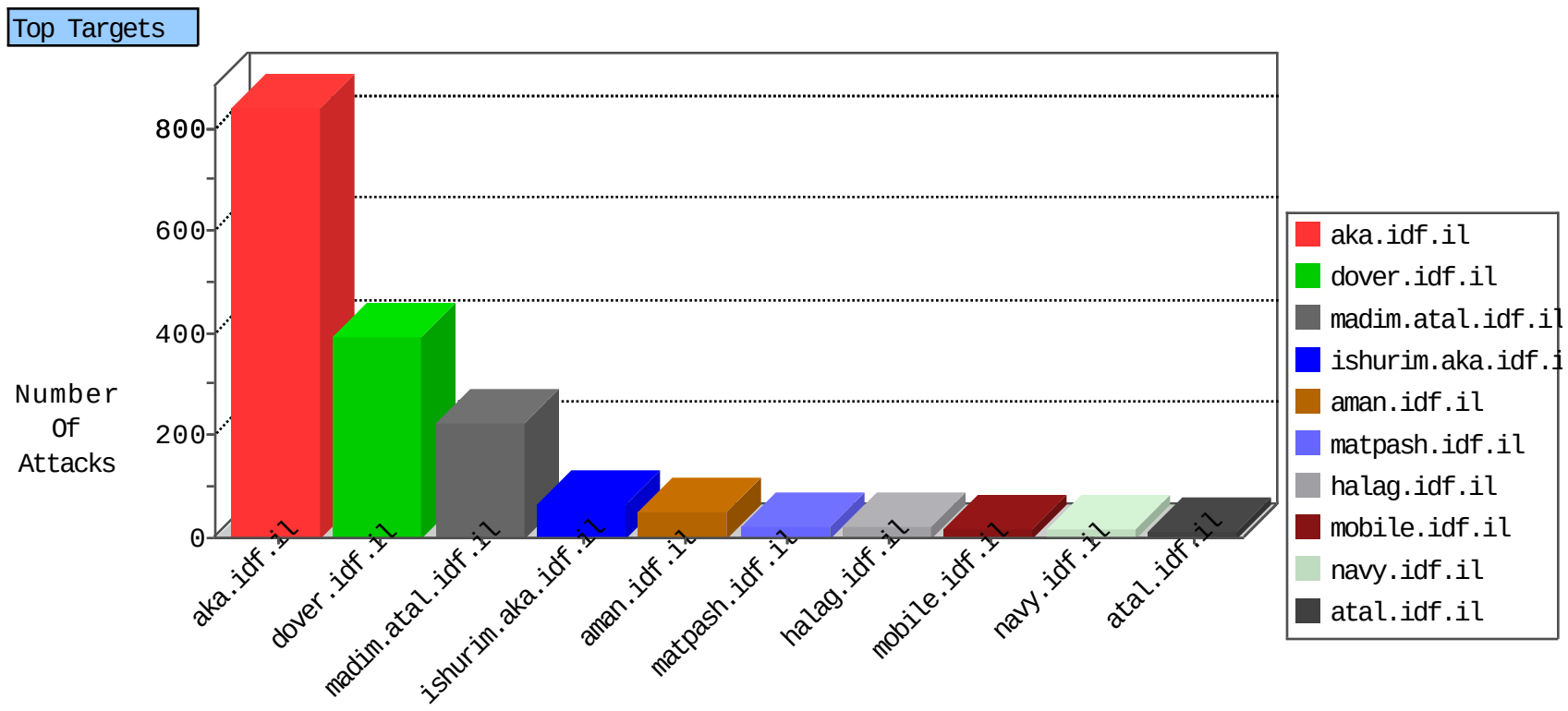
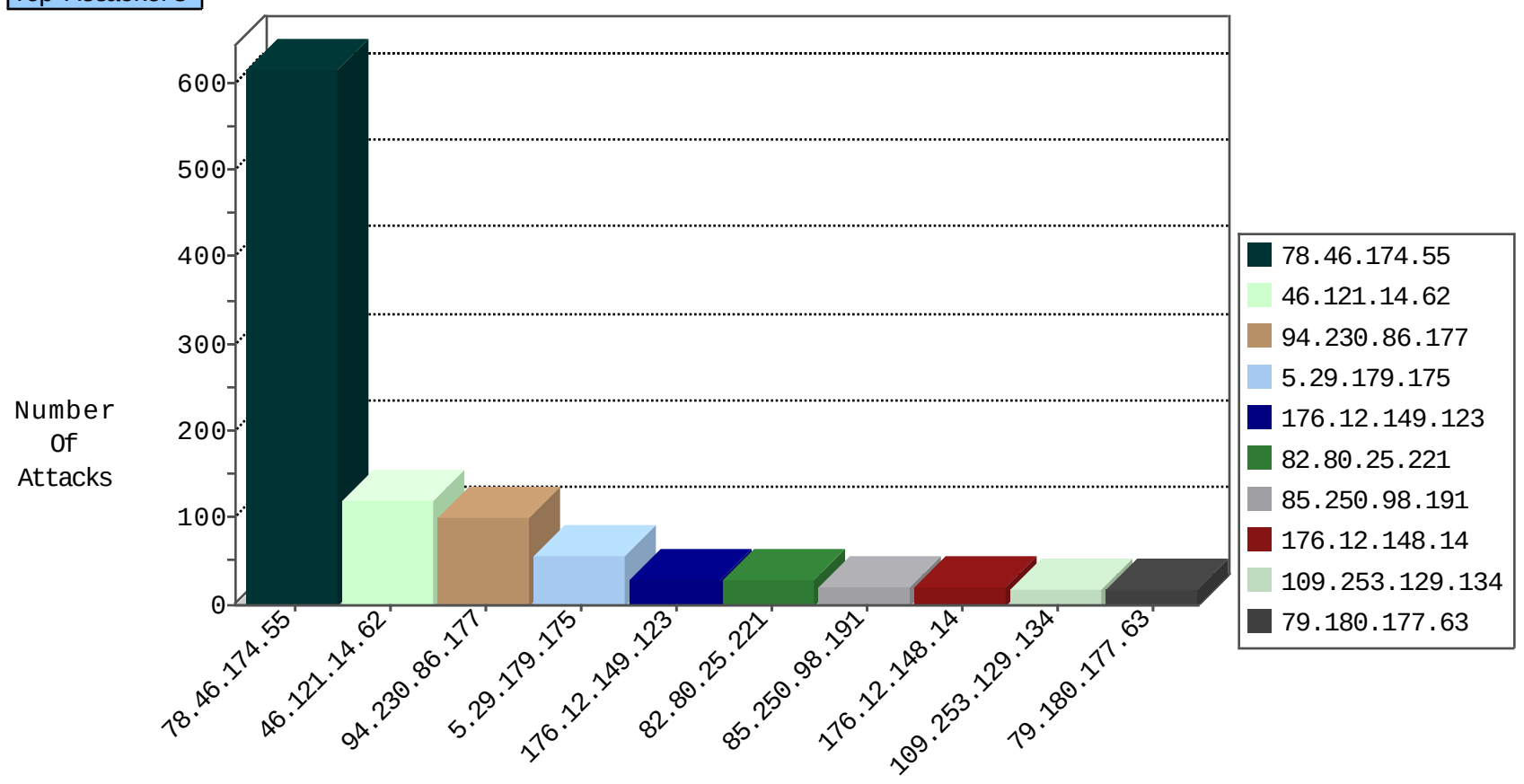
03-29-2015-22:03:09 to 03-29-2015-23:03:09

IDF Under Attack
03-29-2015-22:03:09

Top Targets



Top Attackers



03-29-2015-22:03:09 to 03-29-2015-23:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
5.29.179.175	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	652
79.180.177.63	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
84.228.214.105	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
5.28.147.215	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	68
78.46.174.55	Germany	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	65
77.126.61.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
196.205.128.239	Egypt	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	12
188.161.251.198	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	8
80.6.151.220	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	7
99.248.134.54	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
2.101.82.12	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
66.249.78.166	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
82.9.184.204	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
69.125.116.20	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
82.205.68.134	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
157.55.39.6	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	4
140.180.240.249	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
151.29.235.232	Italy	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
37.8.41.239	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
66.249.78.173	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
176.74.157.137	Czech Republic	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
68.180.228.232	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
212.33.98.164	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
62.201.200.147	Iraq	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
188.161.251.198	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
151.29.235.232	Italy	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
66.41.92.223	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
207.46.13.79	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
95.24.224.254	Russian Federation	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
204.237.22.235	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
95.168.225.233	Bulgaria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
31.13.102.119	Ireland	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
177.220.181.121	Brazil	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
216.223.27.52	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
37.140.141.38	Russian Federation	147.237.77.233	atal.idf.il	unblock-sp-traf1	forward	1
10.0.0.8		147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

03-29-2015-22:03:09 to 03-29-2015-23:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count

03-29-2015-22:03:09 to 03-29-2015-23:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
123.56.45.28	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.5	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
115.231.218.147	China	147.237.76.197	e.himush.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
115.231.218.147	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
62.201.200.147	Iraq	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
216.189.148.175	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
59.188.0.200	Hong Kong	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
216.189.148.175	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -f -sS	1
37.26.147.246	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
27.50.132.60	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
193.107.16.206	Russian Federation	147.237.77.235	sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.54.165.129	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
116.121.137.5	Korea, Republic of	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
115.231.218.147	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
218.57.94.3	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.67	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
216.189.148.175	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.171.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
209.126.72.56	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
27.50.132.60	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
193.107.16.206	Russian Federation	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
27.50.132.60	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1

03-29-2015-22:03:09 to 03-29-2015-23:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
176.12.149.123	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
85.250.98.191	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	22
176.12.148.14	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.253.129.134	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.75.112	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
176.12.140.239	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.136.142	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.144.95	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
93.172.167.84	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
199.30.16.174	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
194.79.196.140	Italy	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	7
109.253.159.225	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
193.43.245.250	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.136	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
173.245.115.76	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
66.249.75.104	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
173.245.115.78	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
66.102.6.131	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
188.161.115.93	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.197	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	4
85.65.99.173	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.54.171.217	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.143.128	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.54.178.6	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
188.120.148.198	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
188.120.148.198	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
173.245.115.77	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
120.138.107.2	India	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
94.230.86.156	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.86.87	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
173.245.115.79	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
94.230.86.212	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.176	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
157.55.39.153	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.117.110.20	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.66.97.183	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	2
46.19.85.176	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.53.178.244	Belarus	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
89.138.87.249	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.66.97.183	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
37.44.66.254	Belarus	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.117.80.176	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
84.110.215.141	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	394
46.121.14.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	120
94.230.86.177	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 94.230.86.177	Block	100
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	50
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	50
93.172.13.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	12
94.159.141.68	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	5
176.12.136.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	3
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	3
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
216.246.23.156	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
80.246.139.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
216.246.23.156	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
149.78.87.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
216.246.23.156	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
46.120.231.171	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage	Block	2
216.246.23.156	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	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
79.180.187.223	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9797-he/refuah.aspx	Block	1
59.90.209.225	India	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
109.253.156.236	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
46.53.178.244	Belarus	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.21.253.49	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//hebrew/history/darom.stm	Block	1
77.127.159.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
176.12.146.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
91.234.34.253	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter 6683f660 in www.aka.idf.il/main/home/default.aspx	None	1
67.222.147.73	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
176.12.139.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.104	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	1
85.250.53.147	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
189.113.2.194	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
180.76.5.71	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-22006-he	Block	1
109.104.94.72	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
74.220.207.163	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
176.12.143.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.159.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
94.230.86.177	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
212.74.177.128	Switzerland	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
91.149.157.154	Belarus	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
193.169.188.90	Ukraine	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
66.249.78.246	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
170.75.146.218		147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
66.249.64.142	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
120.138.107.2	India	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1