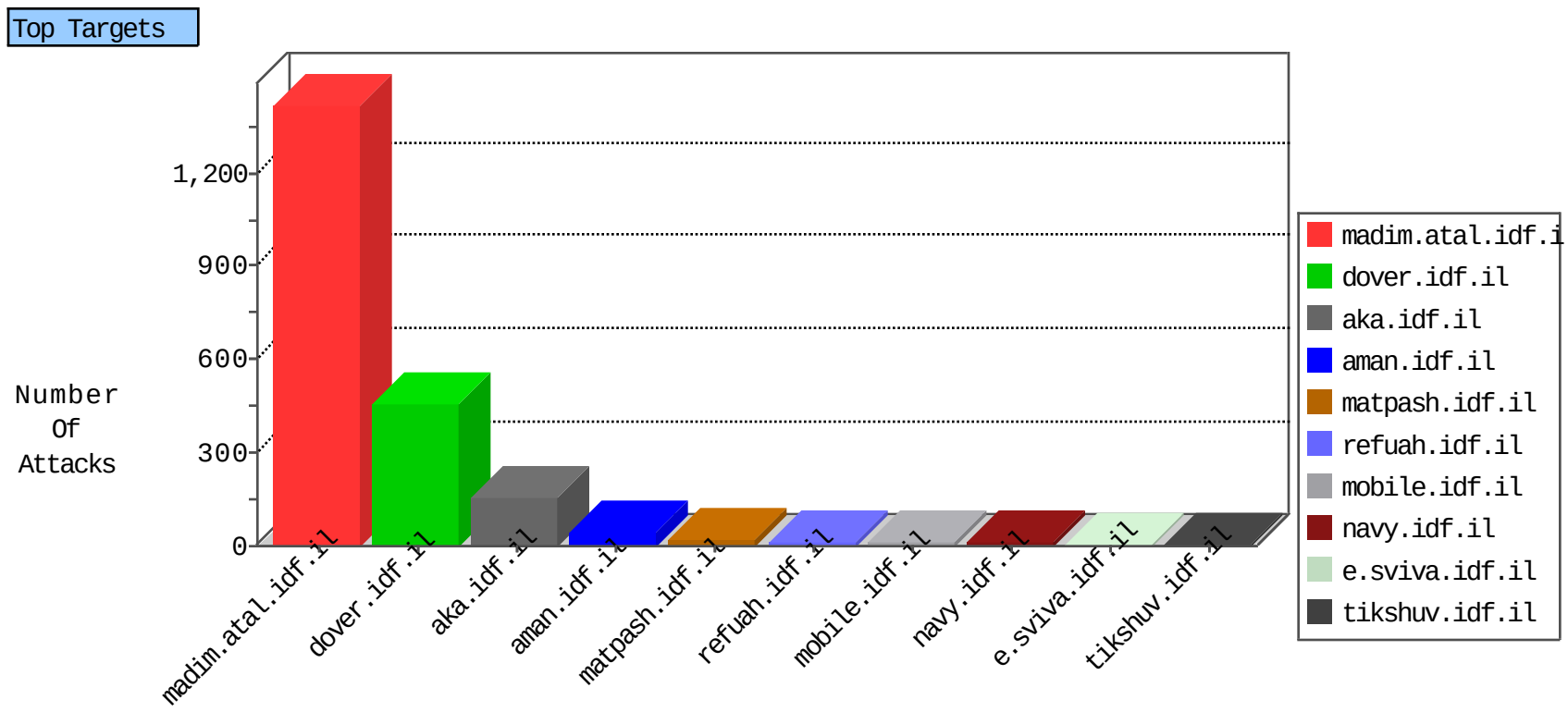
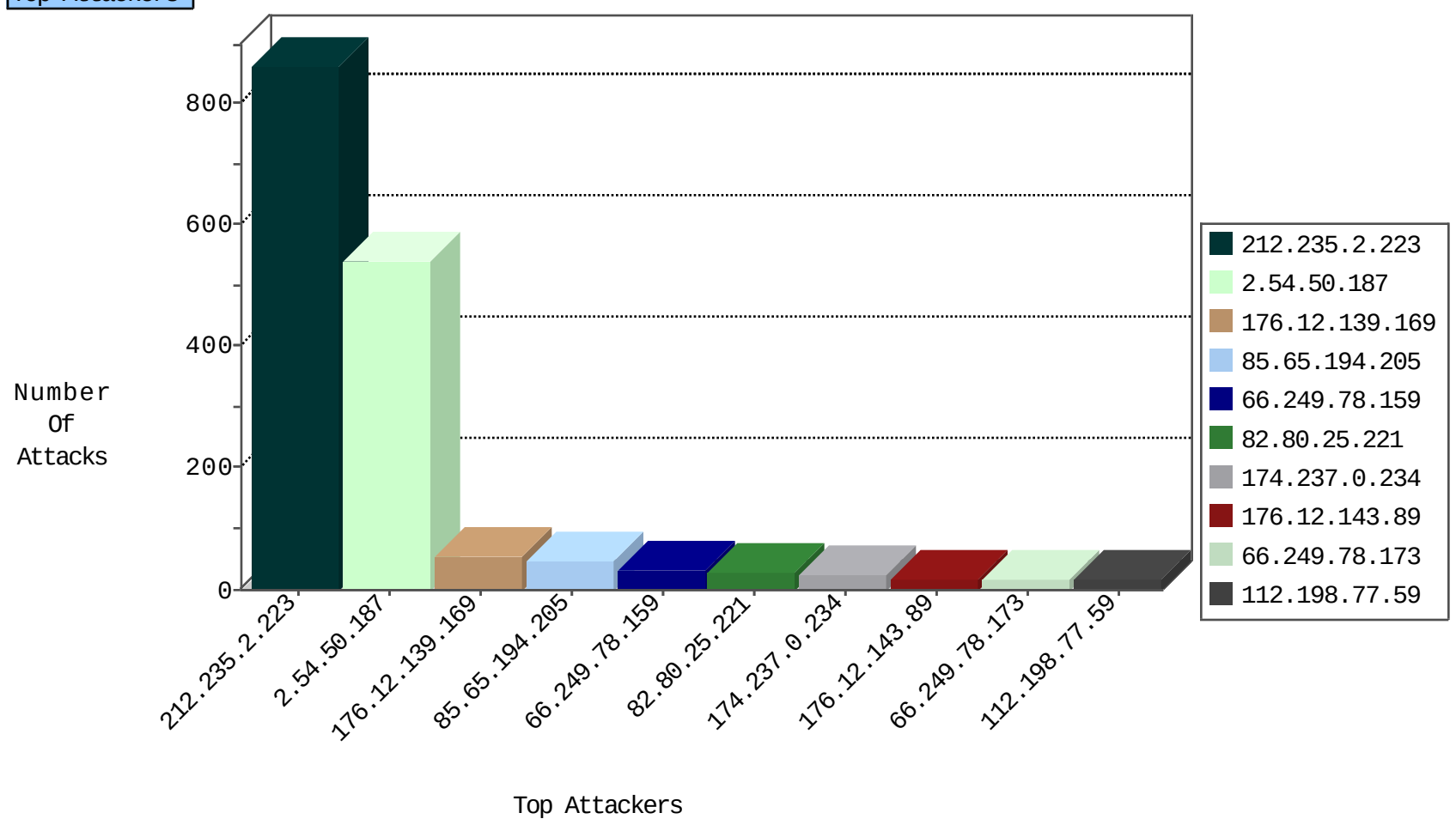
03-29-2015-19:03:01 to 03-29-2015-20:03:01

IDF Under Attack
03-29-2015-19:03:01

Top Targets



Top Attackers



03-29-2015-19:03:01 to 03-29-2015-20:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
85.65.194.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	405
112.198.77.59	Philippines	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	17
105.232.141.125	Namibia	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	11
82.102.207.197	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	9
24.6.102.42	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	7
106.76.225.47	India	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	7
82.205.4.27	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	7
149.254.250.165	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
207.161.238.192	Canada	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
216.126.116.149	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
66.249.78.159	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
157.55.39.6	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
87.66.105.142	Belgium	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
77.21.110.153	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
178.8.133.190	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
86.108.13.137	Jordan	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
58.148.34.10	Korea, Republic of	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	3
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
188.165.15.148	France	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
94.29.125.150	Russian Federation	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
31.186.228.66	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
82.38.159.27	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
190.52.113.147	Peru	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
87.50.113.121	Denmark	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
2.110.55.129	Denmark	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
157.55.39.41	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
86.108.13.137	Jordan	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	2
207.46.13.16	United States	147.237.77.74	law.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
125.175.81.14	Japan	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
46.236.24.51	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
17.142.152.15	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
173.252.74.114	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	unblock-sp-traf1	forward	1
54.72.0.55	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
31.186.228.170	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
5.255.253.173	Russian Federation	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
180.76.4.72	China	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
66.249.78.204	United States	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
66.249.64.154	United States	147.237.77.226	www.chamatz.aka.idf.il	unblock-sp-traf1	forward	1

03-29-2015-19:03:01 to 03-29-2015-20:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count

03-29-2015-19:03:01 to 03-29-2015-20:03:01

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
79.178.170.129	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
118.163.21.36	Taiwan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
118.163.21.36	Taiwan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
216.189.148.175	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 4096	1
58.20.54.249	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
118.163.21.36	Taiwan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
216.189.148.175	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
77.21.110.153	Germany	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

03-29-2015-19:03:01 to 03-29-2015-20:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.12.139.169	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.143.89	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
2.54.50.187	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
199.30.25.177	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.147.52	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.148.73	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
174.237.0.234	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
12.71.251.132	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
174.237.0.234	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	9
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
66.249.84.229	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	7
109.253.149.31	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
173.252.102.113	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
173.252.102.118	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
46.116.65.102	Israel	147.237.0.19	madim.atal.idf.il	First packet isn't SYN	drop	drop	6
173.252.102.119	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
173.252.102.115	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
46.116.65.102	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.65	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
84.94.32.100	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
174.237.0.234	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
173.252.102.116	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
173.252.102.117	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	4
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
188.120.148.245	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
159.224.160.225	Ukraine	147.237.77.216	dover.idf.il	SAM rule	drop	drop	4
46.116.65.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.177.164.152	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
46.19.86.222	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
79.177.164.152	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
31.186.228.91	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
173.252.102.112	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.168	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
157.55.39.41	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
196.217.193.121	Morocco	147.237.77.176	matpash.idf.il		drop	drop	2
212.179.146.134	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
159.224.160.225	Ukraine	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	2
31.186.228.63	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
201.230.23.193	Peru	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
176.12.145.201	Israel	147.237.0.15	kosher-kravi.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.86.211	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.1	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
149.88.85.31	United States	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.50.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	526
212.235.2.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	476
212.235.2.223	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 212.235.2.223	Block	381
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	6
79.179.57.94	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.179.57.94	Block	6
17.142.151.198	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.198	Block	5
109.160.200.66	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	5
17.142.152.15	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
66.249.78.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	4
213.57.97.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
17.142.151.197	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.197	Block	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	4
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
212.235.2.223	Israel	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 212.235.2.223	Block	3
17.142.152.15	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.15	Block	2
79.180.58.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
149.78.87.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
164.138.118.106	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	2
2.54.18.236	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/shared/ajax/updatemakatqauntity.aspx	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
84.228.53.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.138.192.225	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
79.179.57.94	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	2
17.142.151.197	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/048.stm	Block	1
157.55.39.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-map.stm	Block	1
82.98.149.41	Spain	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
2.54.155.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.186.184.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
46.120.19.104	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
212.235.2.223	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
93.93.64.93	Spain	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
176.12.142.168	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.111.209.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
5.172.44.25	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
108.59.9.143	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.69.24	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
216.17.46.2	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
85.250.217.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	1
17.142.151.198	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
82.98.149.41	Spain	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
5.29.7.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.138.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0305-5.stm	Block	1
62.210.113.189	France	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /cgi-bin/php	Block	1
93.93.64.93	Spain	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
84.111.209.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1