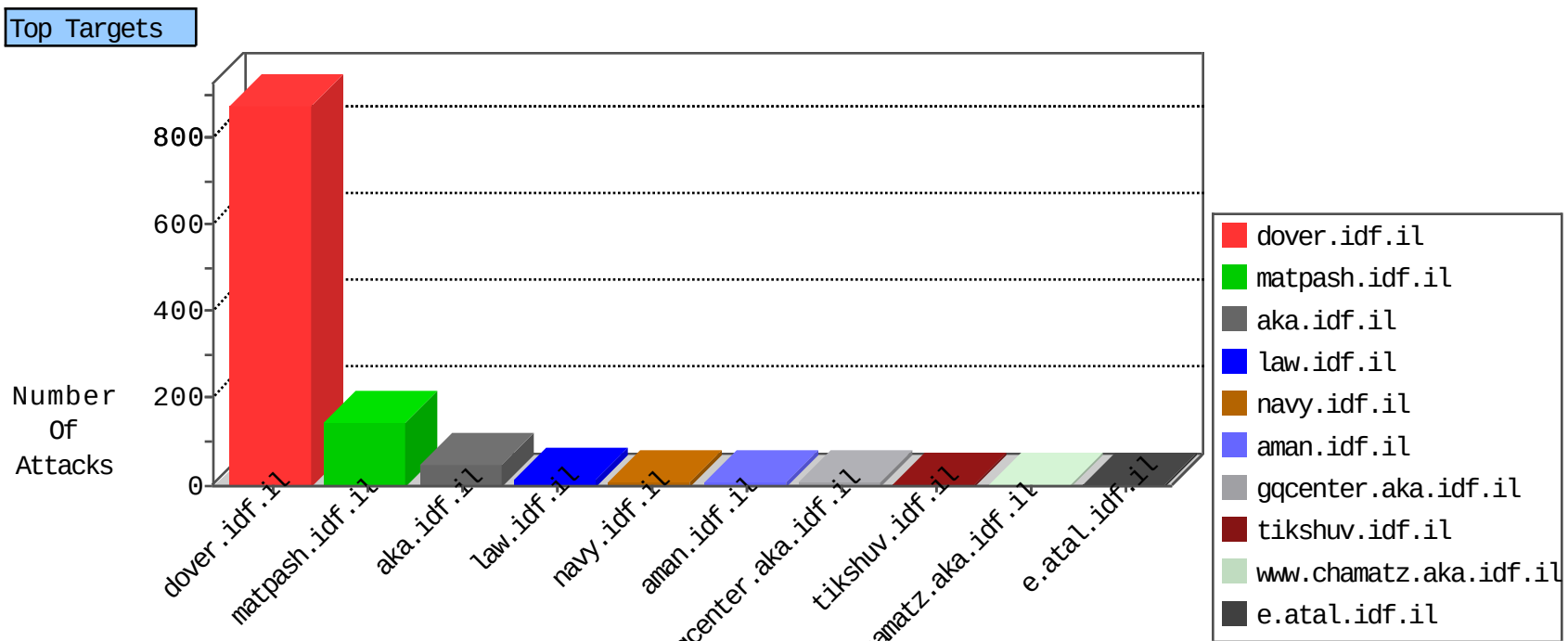
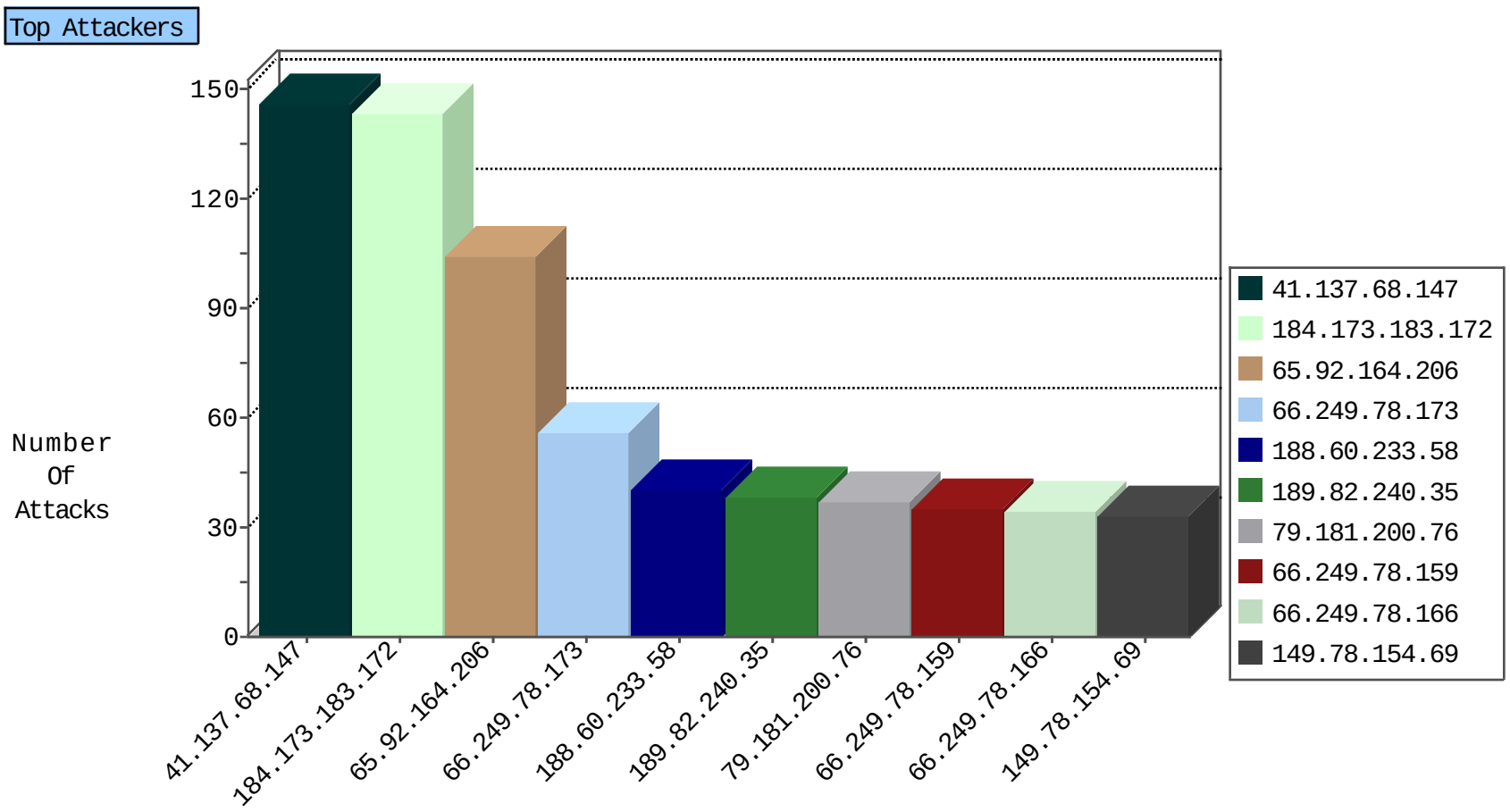
05-04-2015-03:03:09 to 05-04-2015-04:03:09

IDF Under Attack
05-04-2015-03:03:09





05-04-2015-03:03:09 to 05-04-2015-04:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4174
66.249.93.245	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	201
220.181.108.87	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	144
220.181.108.92	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	37
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
103.31.203.52	China	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

05-04-2015-03:03:09 to 05-04-2015-04:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	143
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	11
66.240.236.119	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.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
93.120.27.62	Romania	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
96.44.189.101	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.214.11.209	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1

05-04-2015-03:03:09 to 05-04-2015-04:03:09

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	6
82.166.241.209	Israel	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.64.61	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
82.166.241.209	Israel	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
43.255.191.162	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
82.166.241.209	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.162	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
104.155.50.94		147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.162	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.0.200	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.77.79.43	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.241.209	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.162	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.39.116.219	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.162	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
112.101.64.5	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.76.201	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
104.167.118.60		147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.162	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
104.167.118.60		147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
82.166.241.209	Israel	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.196.147.122	Germany	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.155.50.94		147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.166.241.209	Israel	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.162	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.136.216.4	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
82.166.241.209	Israel	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

05-04-2015-03:03:09 to 05-04-2015-04:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.137.68.147	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	146
65.92.164.206	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	104
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
188.60.233.58	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
189.82.240.35	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
79.181.200.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
203.116.187.3	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
172.56.12.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
70.27.254.122	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.64.76	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
121.72.232.102	New Zealand	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
107.167.107.227	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
68.180.228.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
65.118.187.143	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
172.248.197.98	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.64.72	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
157.55.39.192	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
206.196.186.156	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.64.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
173.252.88.184	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
81.218.80.226	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
207.46.13.101	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
2.54.177.38	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
92.239.170.17	United Kingdom	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
173.252.88.185	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
128.242.249.12	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
173.252.88.186	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
178.255.215.87	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
84.229.193.95	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
79.183.168.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
92.239.170.17	United Kingdom	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	2
173.252.81.112	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
37.139.52.36	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
173.252.81.118	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	5
46.229.164.114	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.114	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
66.249.67.63	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//mobile/	Block	2
157.55.39.61	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
207.46.13.101	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.229.164.99	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/general	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dov	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
66.249.64.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
64.124.203.78	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bc/	Block	1
74.217.148.76	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bg/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13097-he/dover.asp	Block	1
188.138.1.218	Germany	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//edim/yoman/enlarge.asp	Block	1
46.229.164.113	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/441-he/patzar.aspx	Block	1
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip.storage/files/4/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/gyus/general.aspx	Block	1
74.217.148.77	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bg/	Block	1
64.124.203.78	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bg/	Block	1
188.165.15.110	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/eitan	Block	1
66.249.67.71	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/asp	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18774-en/dover.aspxfor	Block	1
74.217.148.72	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bg/	Block	1
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/forms/do...72&catid=30701	Block	1
66.249.64.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/×©×§×•×¤×™××ª 9	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
85.250.104.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.10	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/798-3157-he/patzar.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mazi.idf.il	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
207.46.13.20	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19926-he/dover.aspx	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14160-he/dover.aspx×″×?×•×'×“×″	Block	1
54.87.88.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
74.217.148.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/ac/	Block	1
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//main/giyus/general.aspx	Block	1
208.50.101.158	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bc/	Block	1
66.249.64.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/chinuch/miktzoa/default.asp	None	1
157.55.39.199	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
119.127.91.147	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1