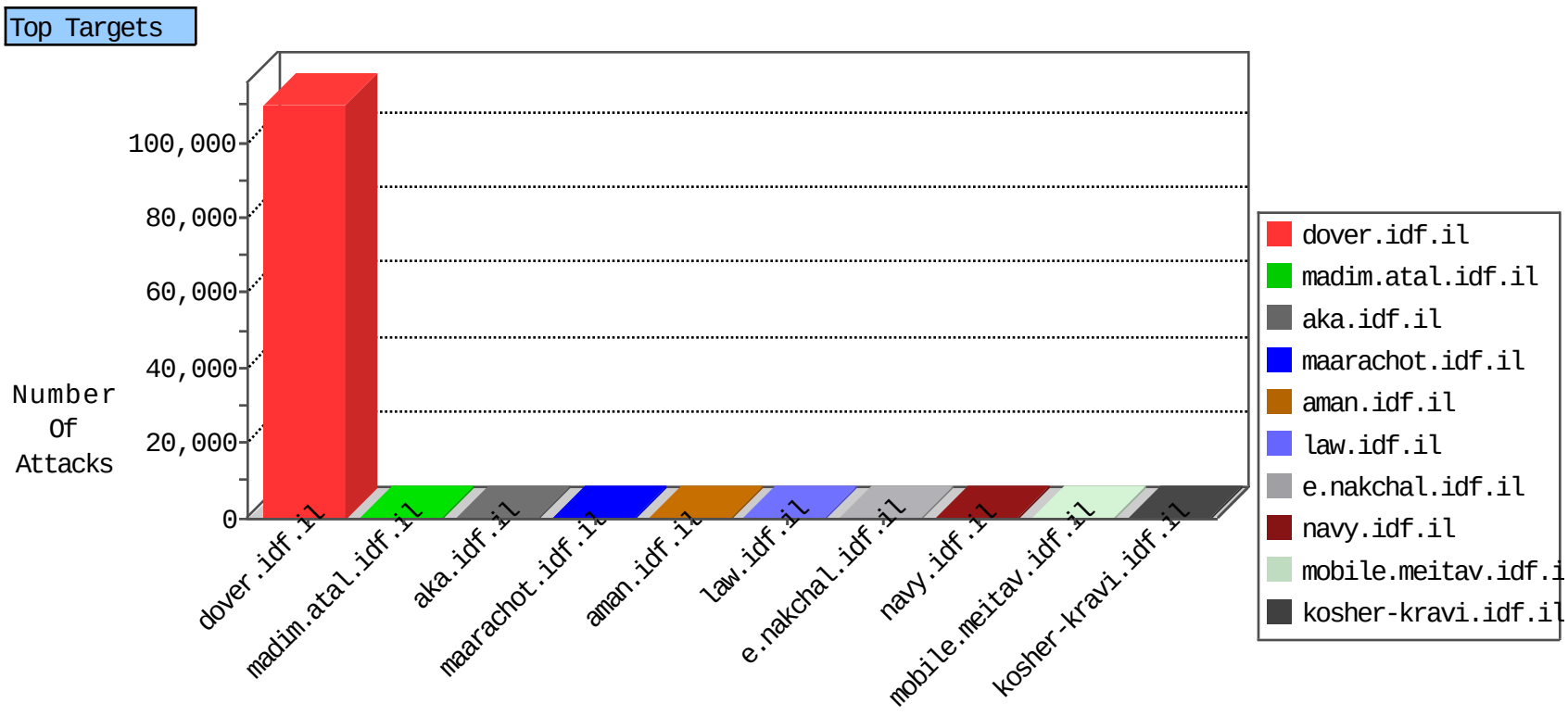
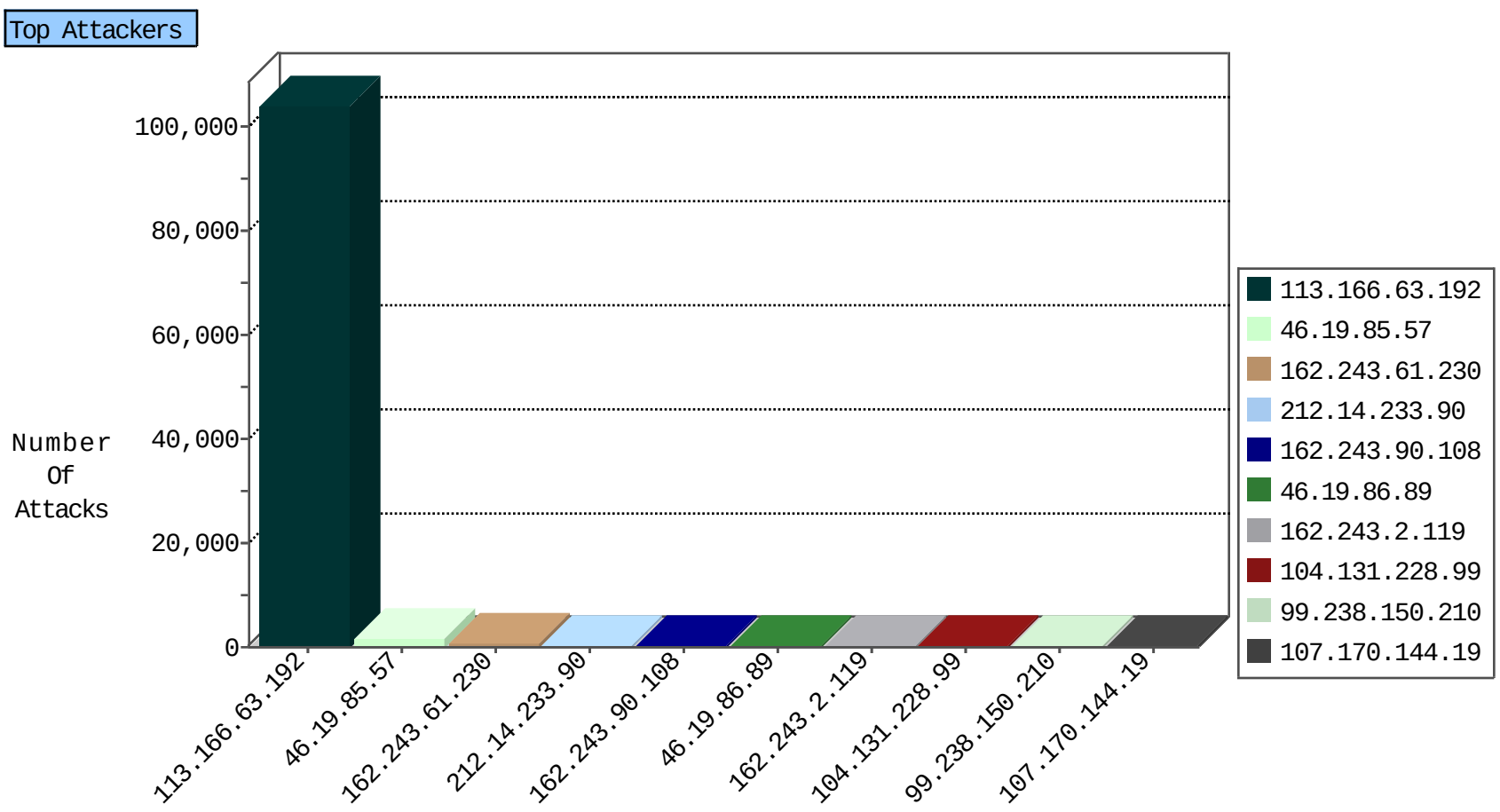
04-21-2015-06:03:08 to 04-21-2015-07:03:08

IDF Under Attack
04-21-2015-06:03:08

Top Targets



Top Attackers



04-21-2015-06:03:08 to 04-21-2015-07:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.32	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	579
220.181.108.169	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3
190.36.98.48	Venezuela	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2

04-21-2015-06:03:08 to 04-21-2015-07:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.88	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.177	ncore.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
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.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	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.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	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.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	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.17	m.my-kosher-kravi.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
85.25.103.50	Germany	147.237.76.176	test.ncore.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
46.19.85.124	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1

04-21-2015-06:03:08 to 04-21-2015-07:03:08

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
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.79.74	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.160.224.128	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
92.50.82.18	Germany	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.195	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.195	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
162.253.66.6	United States	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
162.253.66.6	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.183.11.253	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
162.253.66.6	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
92.53.45.135	Macedonia, the Former Yugoslav Republic of	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.195	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
184.154.52.26	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
162.253.66.6	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.183.11.253	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
162.253.66.6	United States	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
92.53.45.135	Macedonia, the Former Yugoslav Republic of	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1

04-21-2015-06:03:08 to 04-21-2015-07:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
113.166.63.192	Vietnam	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	104148
46.19.85.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1781
162.243.61.230	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	557
212.14.233.90	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	340
162.243.90.108	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	248
162.243.2.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	146
104.131.228.99		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	138
99.238.150.210	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
107.170.144.19	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	122
209.52.88.56	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	80
189.253.3.211	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	76
46.19.86.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	65
166.137.118.23	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
46.19.86.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
172.56.32.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
140.139.231.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
85.72.40.4	Greece	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
79.183.13.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
79.179.17.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
210.55.186.168	New Zealand	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	34
109.253.146.181	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
85.130.206.112	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
14.152.68.55	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
14.152.68.80	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
58.215.136.70	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
14.152.68.115	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
14.152.68.113	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
2.52.9.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
14.152.68.114	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
14.152.68.47	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
109.66.147.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
73.222.82.108	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
58.215.136.69	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
14.152.68.52	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
82.102.169.113	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
176.12.148.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
31.116.149.50	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
89.138.68.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
212.179.159.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
212.179.23.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
199.203.8.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19

04-21-2015-06:03:08 to 04-21-2015-07:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.89	Block	212
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
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	2
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	2
66.249.79.112	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
180.76.5.169	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	1
66.249.64.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
202.46.57.137	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
149.78.242.127	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
67.82.45.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.67.55	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
184.105.247.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
77.125.83.185	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.64	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
202.46.63.131	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/62312	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
66.249.67.63	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//m/	Block	1
188.165.15.27	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/january/26.stm	Block	1
79.183.13.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org.il	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0227-1e.stm	Block	1
66.249.67.71	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	1
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/shared/ajax/updatemakatqauntity.aspx	Block	1
202.46.49.25	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13606-he/dover.aspx×³Ã—×³Â?"×³Ö³Æ'Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½	Block	1
66.249.64.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in aka.idf.il/chinuch/miktzoa/default.asp	None	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/kamlar/klali/default.asp	None	1
69.30.240.46	United States	147.237.0.15	kosher-kravi.idf.i	Illegal HTTP Version	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
46.117.137.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.46.57.136	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
119.75.9.242	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//894-en/idfgdover.aspx	Block	1

04-21-2015-06:03:08 to 04-21-2015-07:03:08