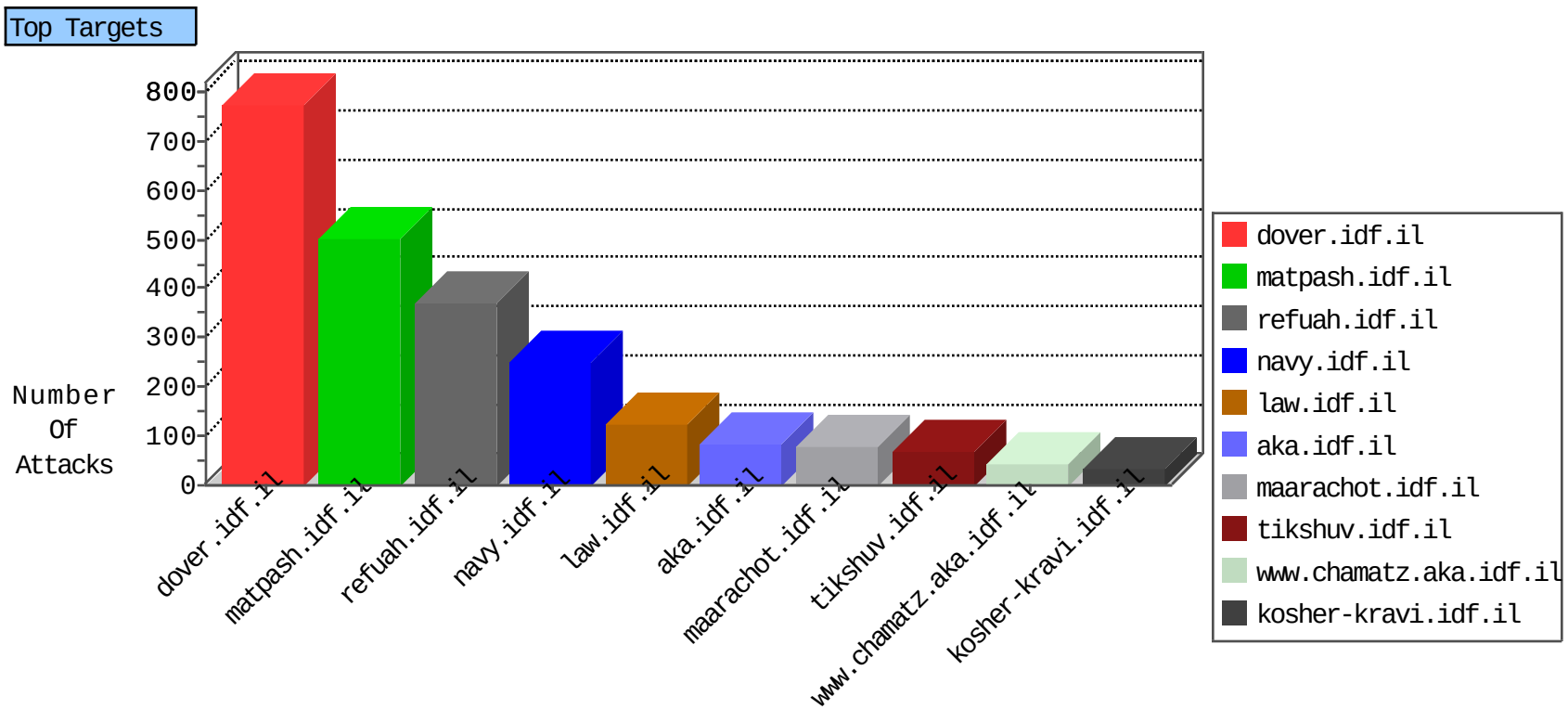
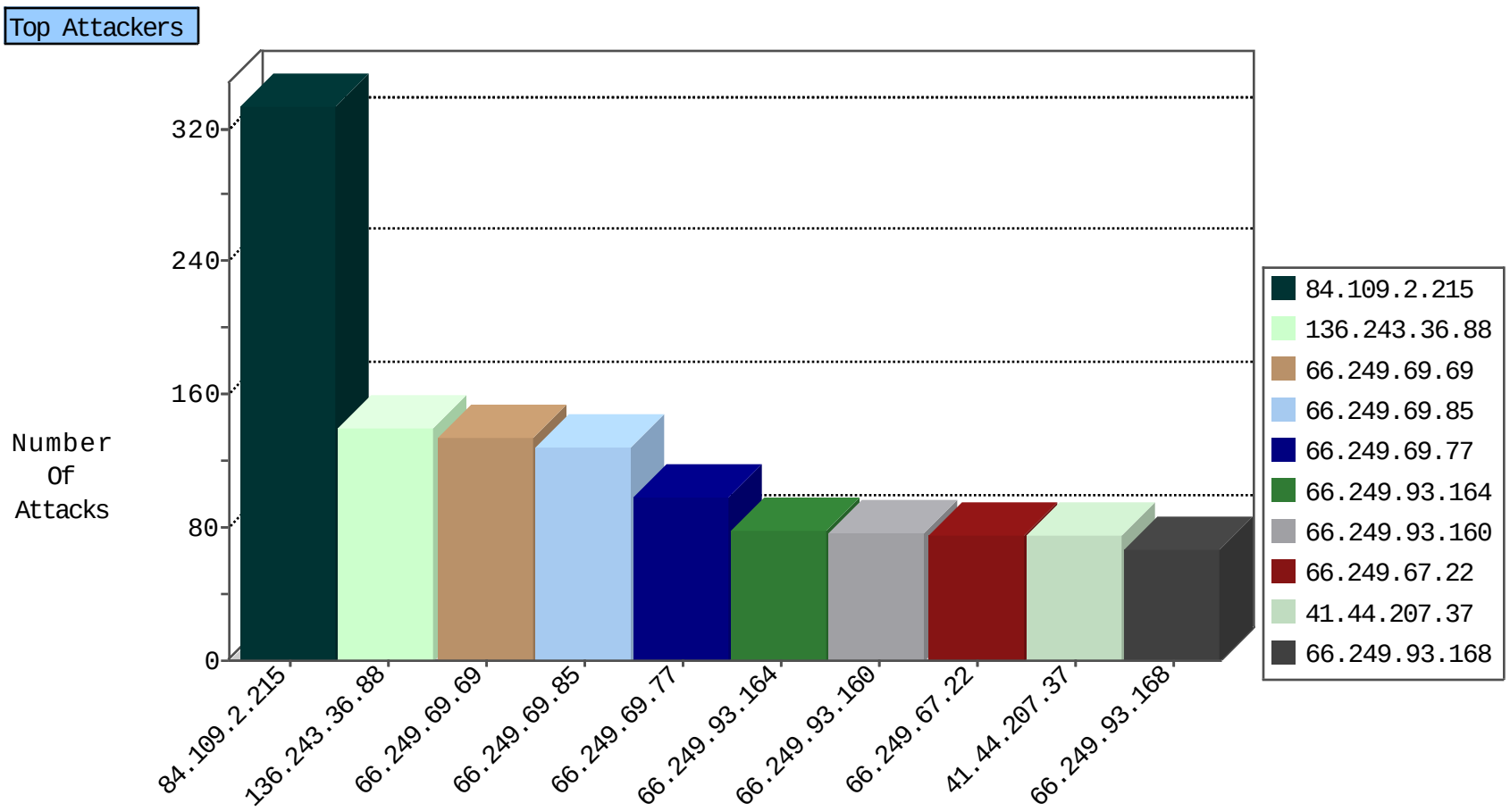
04-11-2015-04:03:04 to 04-11-2015-05:03:04

IDF Under Attack
04-11-2015-04:03:04



Top Target



Top Attackers

04-11-2015-04:03:04 to 04-11-2015-05:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	134
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	127
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	98
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	78
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	77
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	75
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	67
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	52
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	49
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	49
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	30
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	30
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	28
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	26
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	23
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	21
66.249.69.87	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	21
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	20
62.219.155.238	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	17
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.67.34	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.67.50	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	15
66.249.69.112	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	14
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.67.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.69.117	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ip_Web_In	drop	7
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.69.120	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	7
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.67.66	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.69.105	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.69.125	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ip_Web_In	drop	5
66.249.69.54	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	5
66.249.64.142	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.69.97	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	4
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
66.249.69.89	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	4

04-11-2015-04:03:04 to 04-11-2015-05:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.33.59.160	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
96.255.43.151	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-11-2015-04:03:04 to 04-11-2015-05:03:04

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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
193.107.17.72	Russian Federation	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.76.147	chinuch.aka.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
221.235.188.210	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
119.97.231.102	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
85.125.127.77	Austria	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
76.164.222.5	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
221.235.188.210	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
212.7.209.11	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
43.255.191.165	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1

04-11-2015-04:03:04 to 04-11-2015-05:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.109.2.215	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	168
84.109.2.215	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	166
136.243.36.88	Germany	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	139
41.44.207.37	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	75
174.124.169.24	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
46.19.86.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
84.109.6.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
93.80.79.93	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
46.121.51.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
98.210.231.138	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
70.39.187.112	Satellite Provider	147.237.76.86	navy.idf.il	Response out of state	Block HTTP Non Compliant	monitor	8
207.46.13.82	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
74.104.130.252	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
190.181.201.93	Honduras	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
62.219.155.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
85.250.30.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.177.168.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
176.228.23.8	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.89.42.35	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
17.142.151.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
68.197.45.0	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
87.69.79.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
8.37.227.81	Anonymous Proxy	147.237.76.86	navy.idf.il	Response out of state	Block HTTP Non Compliant	monitor	3
27.66.38.96	Vietnam	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.129.197	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
17.142.149.126	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
184.33.59.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
173.252.110.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
197.37.145.103	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
69.171.227.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
173.252.110.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
17.142.151.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

04-11-2015-04:03:04 to 04-11-2015-05:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	2
17.142.151.181	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.181	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
155.94.222.12		147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
17.142.151.116	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
17.142.151.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/24.stm	Block	1
190.181.201.93	Honduras	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 190.181.201.93	Block	1
69.171.227.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.114	Block	1
192.171.235.97	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/august/14a.stm	Block	1
17.142.151.181	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0817-1.stm	Block	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
125.209.235.178	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//newsite/english/main.asp	Block	1
17.142.151.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/golani/golani.stm	Block	1
157.55.39.143	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1

04-11-2015-04:03:04 to 04-11-2015-05:03:04