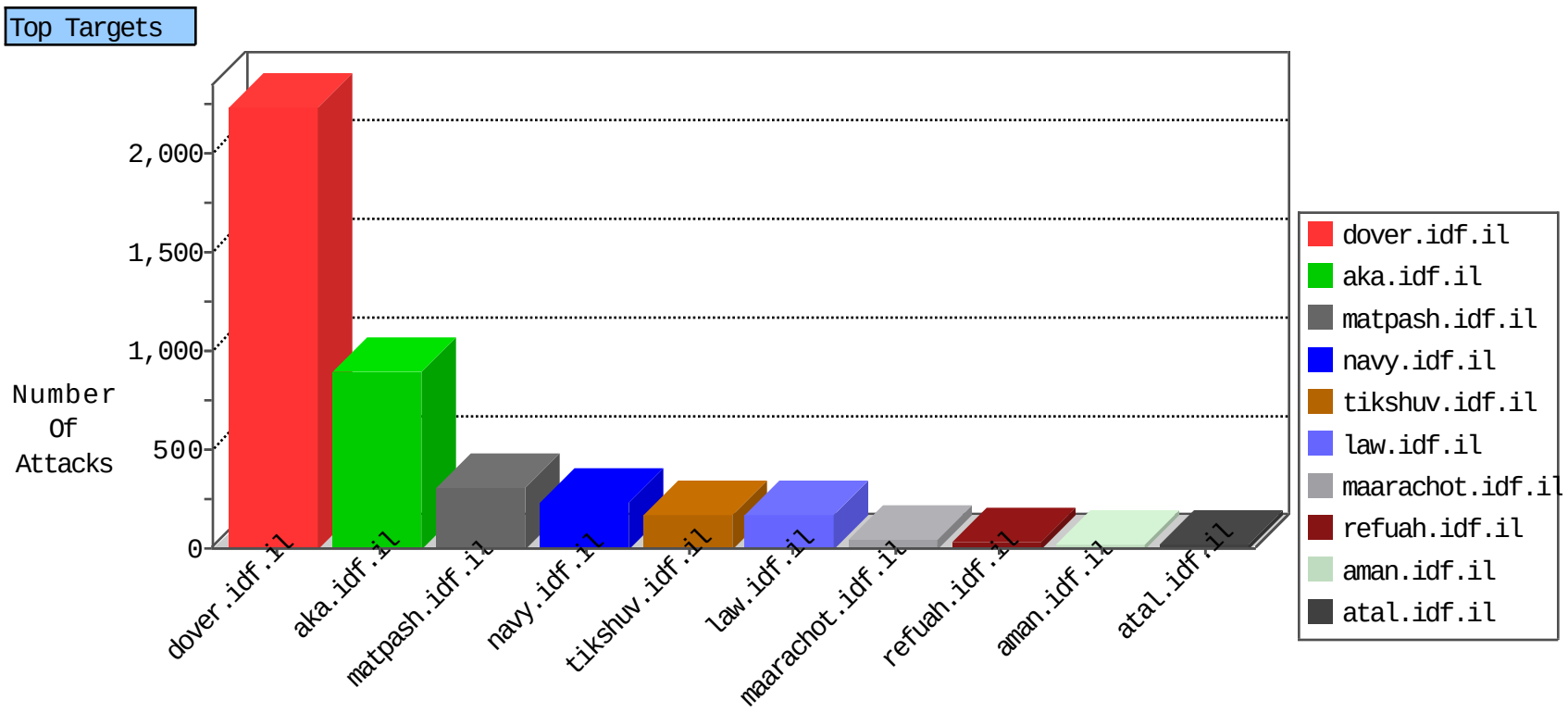
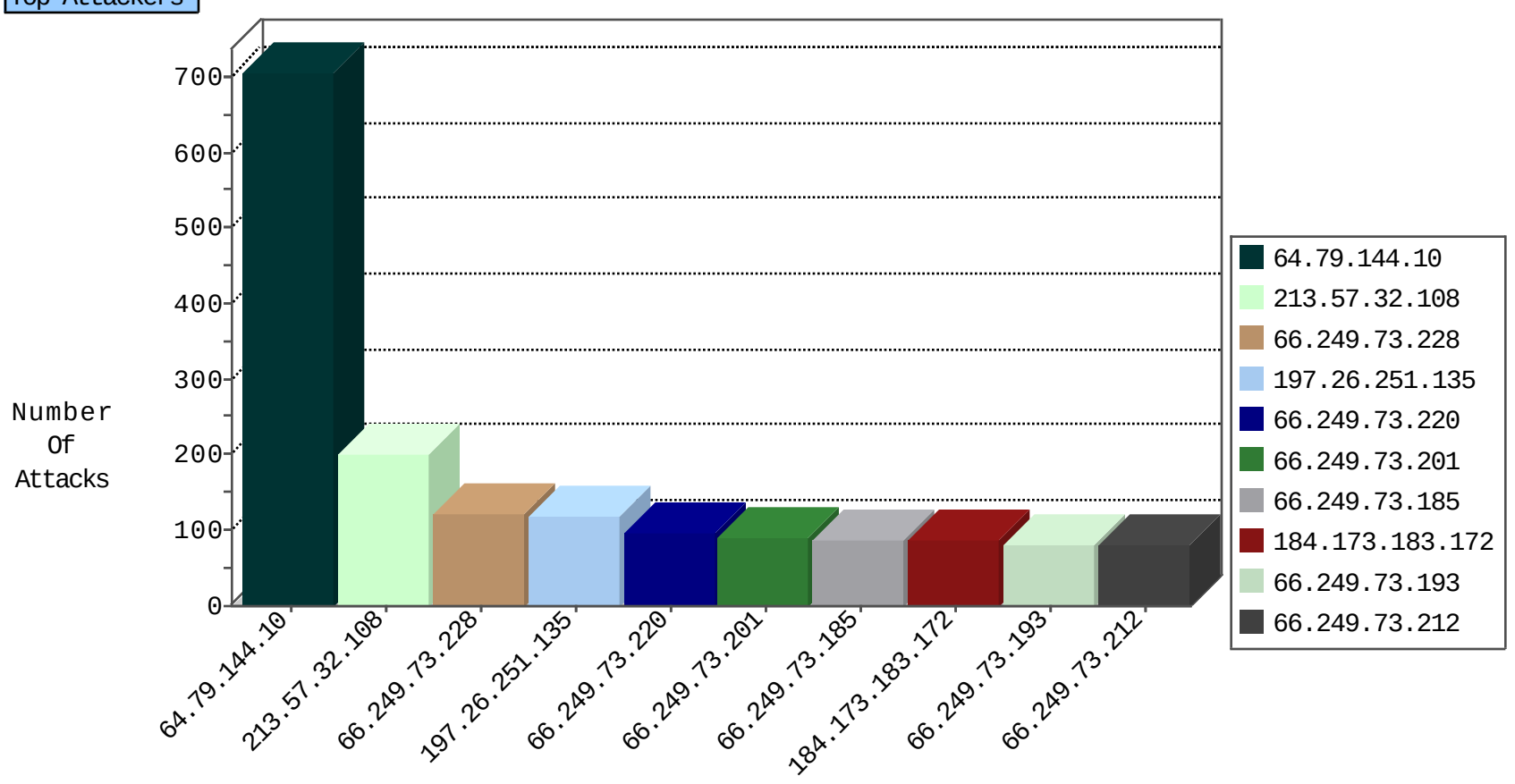
04-09-2015-19:03:05 to 04-09-2015-20:03:05

IDF Under Attack
04-09-2015-19:03:05

Top Targets



Top Attackers



04-09-2015-19:03:05 to 04-09-2015-20:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.103	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	377
176.12.141.45	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	168
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	122
66.249.73.220	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	97
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	89
66.249.73.185	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	88
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	82
66.249.73.193	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	82
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	82
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	80
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	72
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	70
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	34
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	31
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	24
220.181.108.154	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	22
66.249.93.196	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.93.204	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	18
66.249.93.200	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.81.206	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.81.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.93.144	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
66.249.81.212	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.93.136	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.75.95	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.93.140	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.73.223	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.81.130	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.93.159	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.64.8	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
2.54.170.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5

04-09-2015-19:03:05 to 04-09-2015-20:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
64.79.144.10	United States	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	707
213.57.32.108	Israel	147.237.76.86	navy.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	100
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	87
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.181.169.99	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-09-2015-19:03:05 to 04-09-2015-20:03:05

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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
2.54.140.158	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.165.138	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
222.69.94.13	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.66	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.77	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
122.228.207.77	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.77	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
198.89.108.125	United States	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
95.242.63.20	Italy	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.231	Netherlands	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
79.182.32.74	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.77	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1

04-09-2015-19:03:05 to 04-09-2015-20:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
197.26.251.135	Tunisia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	119
76.164.218.178	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
212.179.61.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
76.164.218.182	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
105.156.45.169	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
37.26.148.240	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
2.54.170.69	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
98.125.88.106	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
85.64.203.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
41.73.125.236	Mali	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
46.19.86.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
185.5.153.49	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
46.19.85.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
79.181.104.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
109.253.149.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
76.100.105.46	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
79.182.54.147	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	21
93.172.60.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
109.253.138.8	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.140.213	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
197.41.202.99	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
79.176.130.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
79.183.147.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
46.19.86.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
69.167.57.80	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
109.64.186.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
98.245.207.64	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.147.230	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
84.109.185.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
176.12.144.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
217.9.101.140	Germany	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10
5.22.130.30	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
176.12.141.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
37.26.148.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
37.26.147.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
99.238.32.134	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
85.64.136.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
178.61.176.122	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
85.65.14.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.120.47.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

04-09-2015-19:03:05 to 04-09-2015-20:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.32.108	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized HTTP Method	Block	102
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
85.204.74.16	Romania	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
77.125.74.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.y in aka.idf.il/main/sachar/	None	1
5.28.168.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.25	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
85.64.204.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatzhelp	Block	1
41.238.249.161	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//qar/	Block	1
167.114.119.188	United States	147.237.77.176	matpash.idf.il	Malformed URL www.cogat.idf.il	Block	1
2.54.2.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
87.69.152.39	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
77.127.113.88	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
5.29.123.97	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forgotpassword.aspx	Block	1
85.204.74.16	Romania	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
46.121.77.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00_ctl00_ScriptManager1_HiddenField in www.aka.idf.il/main/sachar/	None	1
167.114.119.188	United States	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method Host: in URL www.cogat.idf.il	Block	1
2.54.2.255	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
109.66.48.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.160.140	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.123.97	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding www.aka.idf.il/main/giyus/userdetails/function () { var = math.round(this[2] / 100 * 255); if (this[1] == 0) { return [c, c, c]; } else { var a = this[0] r 360; var e = a e 60; var g = math.round((this[2] * (100 - this[1])) / 10000 * 255); var d = math.round((this[2] * (6000 - this[1] * e)) / 600000 * 255); var b = math.round((this[2] * (6000 - this[1] * (60 - e))) / 600000 * 255); switch (math.floor(a / 60)) { case 0: return	Block	1
157.55.39.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
85.204.74.16	Romania	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1113-1.stm	Block	1
180.76.4.27	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
2.54.177.164	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
112.111.188.90	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp/trackback/	Block	1
79.182.54.147	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.182.54.147	Block	1
37.59.29.19	France	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	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.204.74.16	Romania	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
5.28.168.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
136.243.36.88	Germany	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 136.243.36.88	Block	1
79.183.28.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
38.117.200.18	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
167.114.119.188	United States	147.237.77.176	matpash.idf.il	Illegal HTTP Version	Block	1

04-09-2015-19:03:05 to 04-09-2015-20:03:05