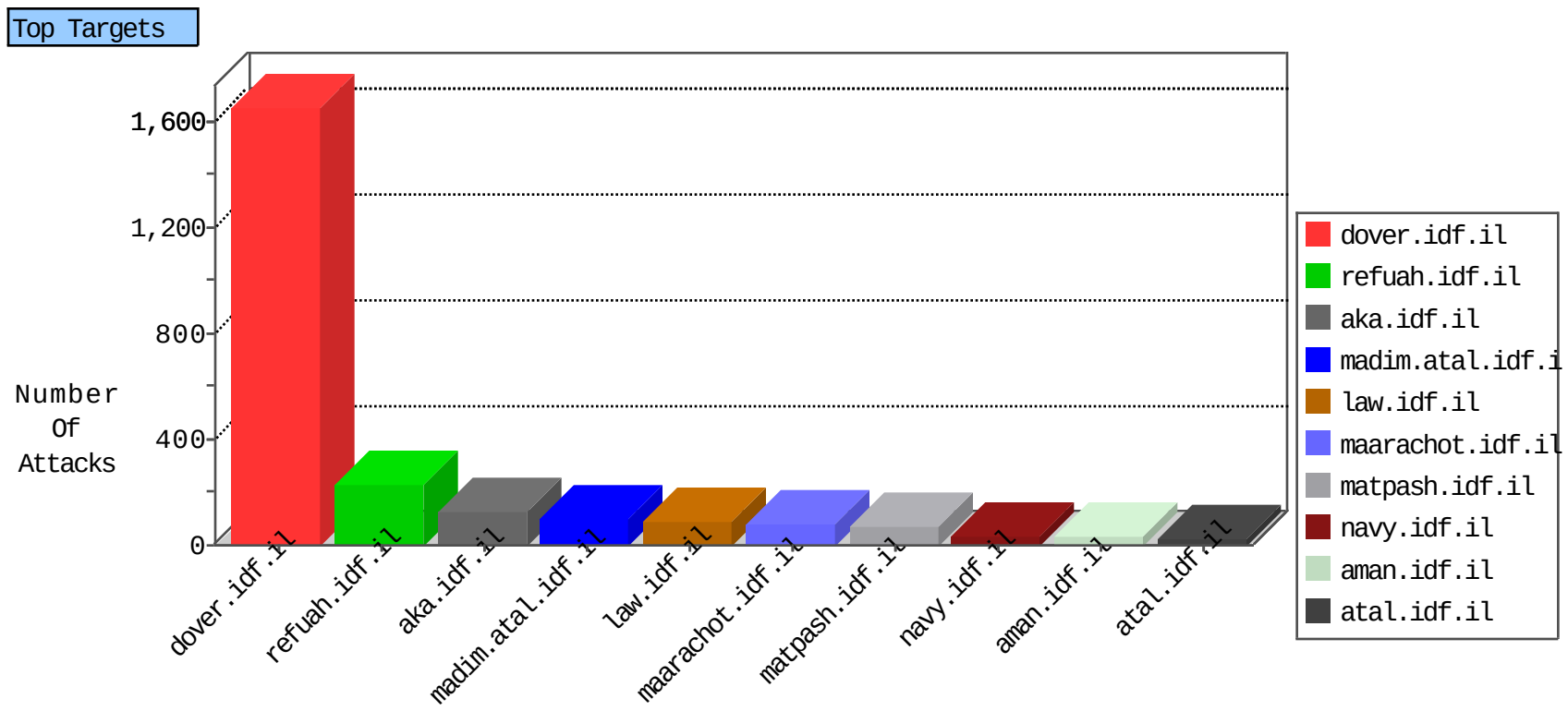
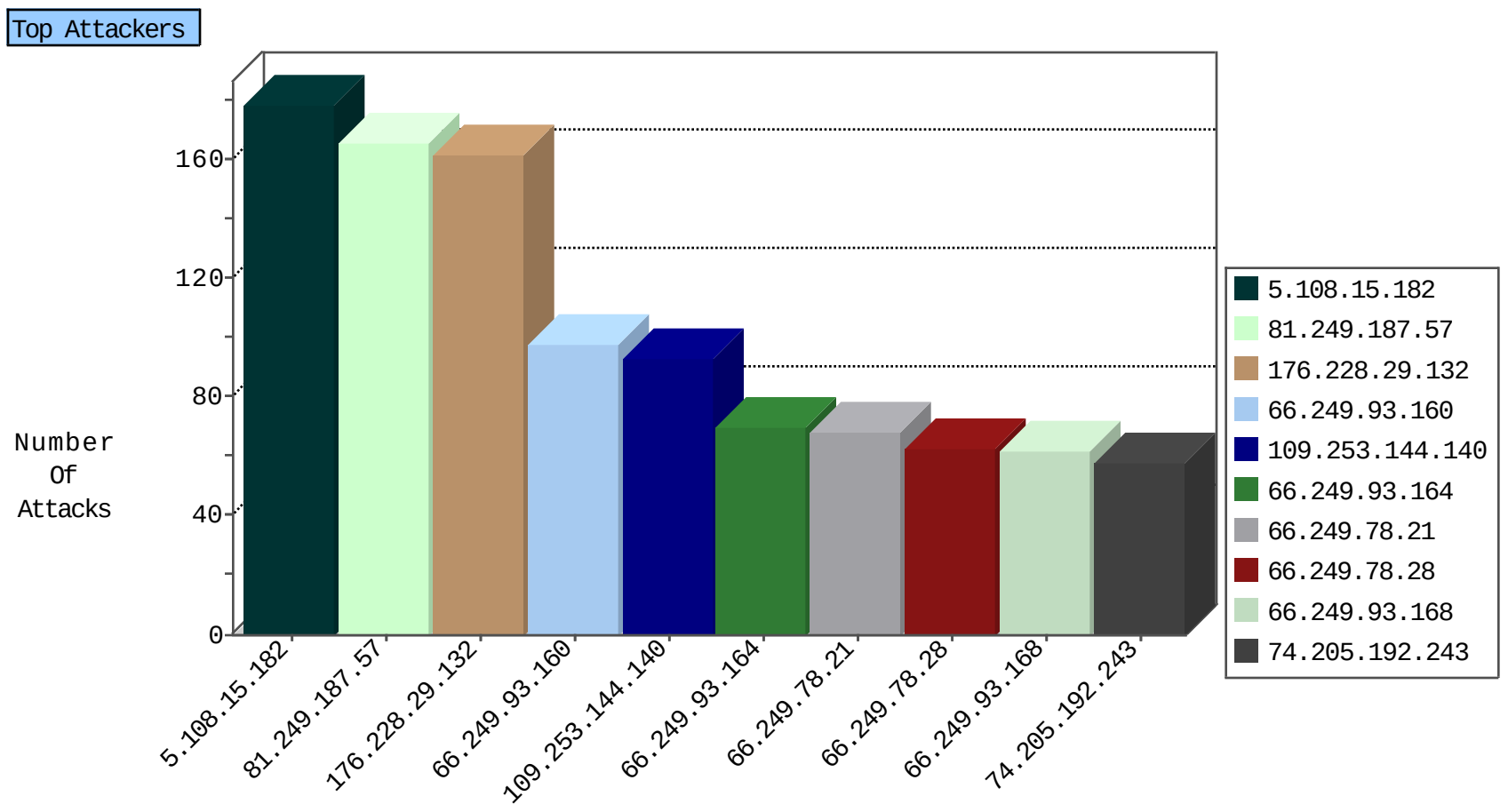
04-12-2015-01:03:04 to 04-12-2015-02:03:04

IDF Under Attack
04-12-2015-01:03:04

Top Targets



Top Attackers



04-12-2015-01:03:04 to 04-12-2015-02:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
81.249.187.57	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	962
204.93.154.220	United States	147.237.77.233	atal.idf.il	TCP Scan (vertical)	drop	170
74.205.192.243	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	146
79.176.177.7	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	103
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	98
109.253.129.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	81
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	70
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	68
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	63
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	62
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	49
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	24
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	24
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	23
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	22
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	21
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	21
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	19
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	18
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	17
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.93.200	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
66.249.64.155	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	14
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	13
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.64.79	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	8
66.249.64.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	7
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.67.1	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.67.153	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.93.204	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.93.208	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	5

04-12-2015-01:03:04 to 04-12-2015-02:03:04

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
37.142.3.56	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
67.180.158.88	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
197.178.125.86	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-12-2015-01:03:04 to 04-12-2015-02:03:04

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	26
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
79.183.15.63	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
101.226.2.99	China	147.237.72.217	e.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.76	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
54.172.240.102	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	1
122.228.207.76	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.165.220.215	Germany	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
46.162.115.130	Sweden	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
118.69.174.89	Vietnam	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
101.226.2.99	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.76	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
46.165.220.215	Germany	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.165.220.215	Germany	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
118.69.174.89	Vietnam	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
118.69.174.89	Vietnam	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1

04-12-2015-01:03:04 to 04-12-2015-02:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.108.15.182	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	179
176.228.29.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	162
81.249.187.57	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	130
74.205.192.243	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
79.176.177.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
95.86.74.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
89.139.185.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
197.46.70.84	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
89.136.137.149	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
134.0.98.202	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
157.55.39.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
95.86.120.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
79.182.205.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
176.12.145.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
37.142.227.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
176.12.142.113	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
79.178.97.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.138.96	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
217.129.211.145	Portugal	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
81.110.87.149	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
177.17.88.85	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
46.19.85.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
80.230.19.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
77.30.107.158	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
188.120.133.211	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
85.65.99.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
81.57.81.41	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
108.94.109.15	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
100.2.74.188	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.241.237.105	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.46.13.82	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
85.64.76.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
109.64.150.85	Israel	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
85.65.3.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
157.55.39.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
212.76.127.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
92.154.19.194	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
84.228.144.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
69.57.225.245	Antigua and Barbuda	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4

04-12-2015-01:03:04 to 04-12-2015-02:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.144.140	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.144.140	Block	92
109.253.134.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
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
192.77.254.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/1.stm	Block	1
67.180.158.88	United States	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$rbSearchSites in aka.idf.il/main/sachar/	None	1
37.142.3.69	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
178.137.153.122	Ukraine	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
79.182.205.1	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/site/	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
157.55.39.66	United States	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/english/history/humanitarian.stm	Block	1
46.19.86.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.255.87.242	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
109.67.144.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113535.pdf.	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
2.52.22.189	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
157.55.39.121	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
70.190.60.243	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
46.116.131.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.6.21	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/901-7740-he/tikshuv.aspx	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.115.187.54	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
70.190.60.243	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
46.117.62.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
188.165.15.75	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9641-he/refuah.aspx	Block	1
109.253.144.140	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
67.180.158.88	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/forgotpassword.aspx	None	1
37.142.3.56	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
176.222.143.221	Kazakstan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1513-en/dover.aspx	Block	1
46.210.213.129	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan/pazan.stm	Block	1

04-12-2015-01:03:04 to 04-12-2015-02:03:04