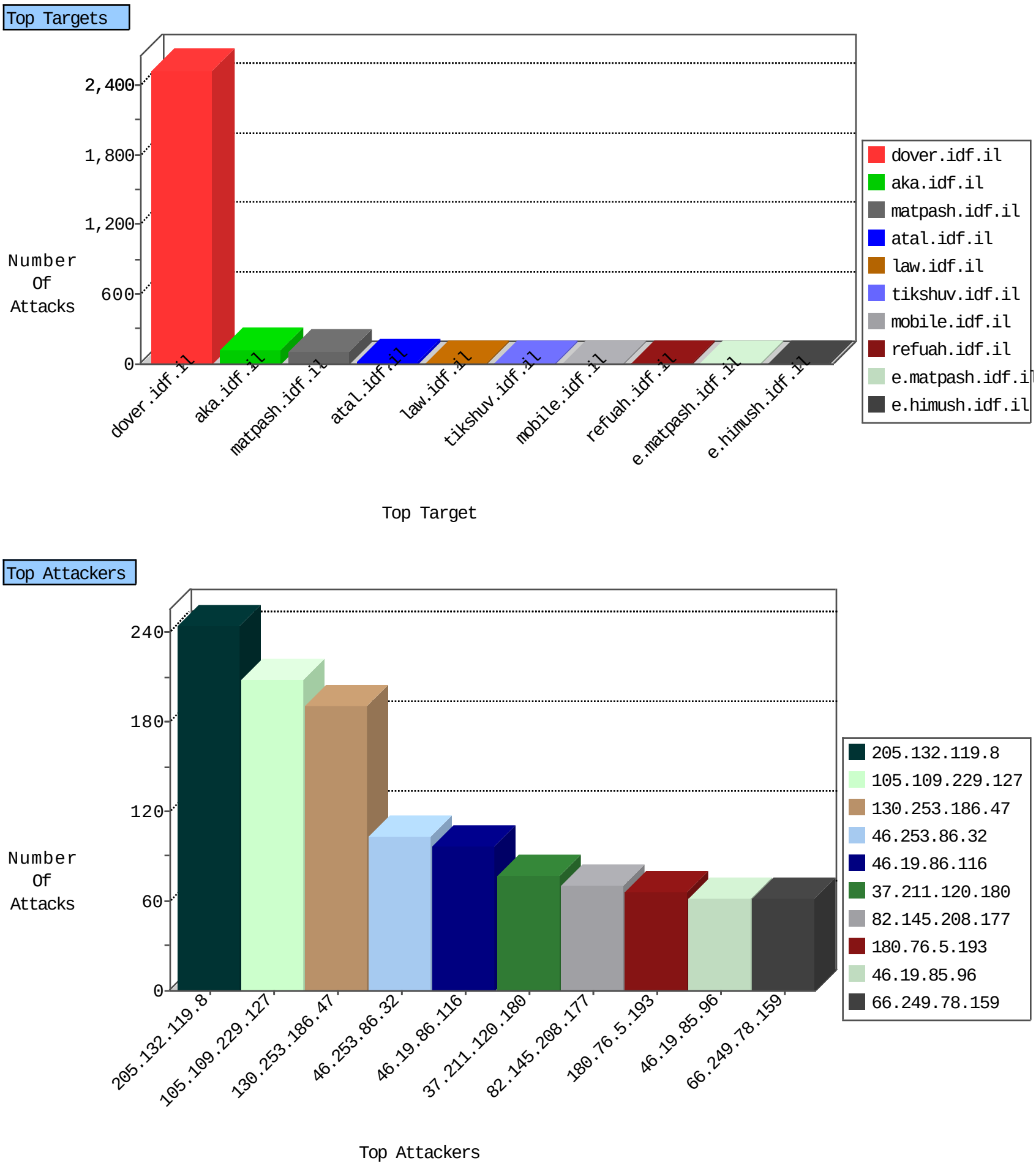
05-06-2015-00:03:00 to 05-06-2015-01:03:00

IDF Under Attack
05-06-2015-00:03:00



05-06-2015-00:03:00 to 05-06-2015-01:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.143	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	113
66.249.64.148	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
71.6.216.48	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
104.255.66.201		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

05-06-2015-00:03:00 to 05-06-2015-01:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	66
79.182.25.175	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	3
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.24	e.lifestyle.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
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
105.109.229.127	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.0.200	m4u.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	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
109.67.33.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
213.57.214.141	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.86	navy.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
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1

05-06-2015-00:03:00 to 05-06-2015-01:03:00

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	5
5.29.100.123	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.81.208.80	United Kingdom	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
104.128.144.130		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
182.254.226.90	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
175.136.197.37	Malaysia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.166.125	Canada	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
144.0.0.60	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
141.212.121.167	United States	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.130		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
183.136.216.3	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.3	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
175.136.197.37	Malaysia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
31.184.194.114	Russian Federation	147.237.77.74	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.248.166.125	Canada	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
218.77.79.43	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
144.0.0.60	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
121.88.5.177	Korea, Republic of	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
121.88.5.177	Korea, Republic of	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

05-06-2015-00:03:00 to 05-06-2015-01:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
205.132.119.8	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	245
130.253.186.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	191
105.109.229.127	Algeria	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	140
46.19.86.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	97
46.253.86.32	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	88
37.211.120.180	Qatar	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
82.145.208.177	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
46.19.85.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
130.253.34.98	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
93.172.163.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
105.109.229.127	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
50.244.45.237	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
130.245.197.174	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
69.171.231.195	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
79.179.131.199	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
154.98.7.14	Sudan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
212.179.213.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
217.195.174.96	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
5.22.135.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
109.253.143.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
70.177.87.27	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
176.12.146.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
37.26.147.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
69.171.231.193	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
69.171.231.194	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
5.41.4.81	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
182.249.247.150	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
84.108.49.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
37.26.146.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
176.58.78.36	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
99.238.140.17	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.253.86.32	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
85.250.140.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
2.54.28.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
73.219.99.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
174.48.175.144	United States	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	12
37.26.148.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
178.152.208.182	Qatar	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	29
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	27
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	26
164.138.115.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
79.183.31.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ giyus	Block	3
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	2
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.152.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/doctrine/doctrine.stm	Block	1
109.186.173.48	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
41.252.244.159	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/il	Block	1
84.108.65.245	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
180.76.6.140	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/reka1.stm	Block	1
66.249.67.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
87.81.208.80	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/skira/default.asp	None	1
208.186.96.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
78.131.32.191	Hungary	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.131.32.191	Block	1
164.138.121.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19478-he/idfgdover.aspx	Block	1
66.249.64.235	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6396-he/patzar.aspx	Block	1
42.118.233.128	Vietnam	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1283-15565-en/dover.aspx	Block	1
84.228.79.152	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
185.32.178.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/sitemap	Block	1
66.249.67.147	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
105.109.229.127	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	1
2.54.171.231	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
217.132.78.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
78.131.32.191	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/6_s3_	Block	1
173.252.114.119	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/chinuch/klali	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-18773-en/dover.aspx	Block	1
66.249.64.240	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74//templates/getfile/getfile.aspx	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.229.164.113	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/×œ×›×ª×‘×″×″+×″×žœ×?×″	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
188.165.15.230	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8763-he/refuah.aspx	Block	1
157.55.39.164	United States	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.67.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1216-he/refuah.aspx	Block	1
107.168.64.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.41.4.81	Romania	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
79.181.179.46	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/938-he/atal.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

05-06-2015-00:03:00 to 05-06-2015-01:03:00