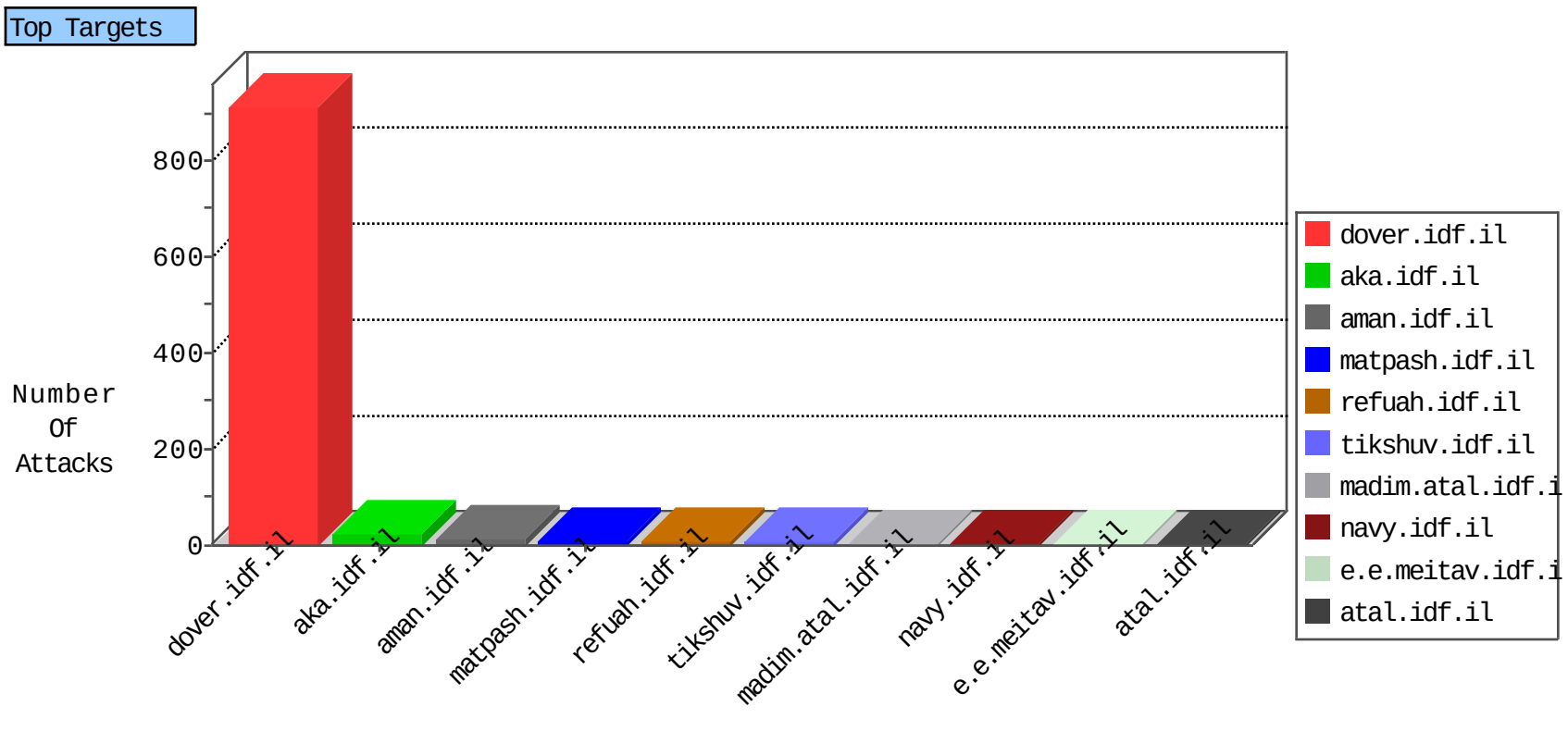
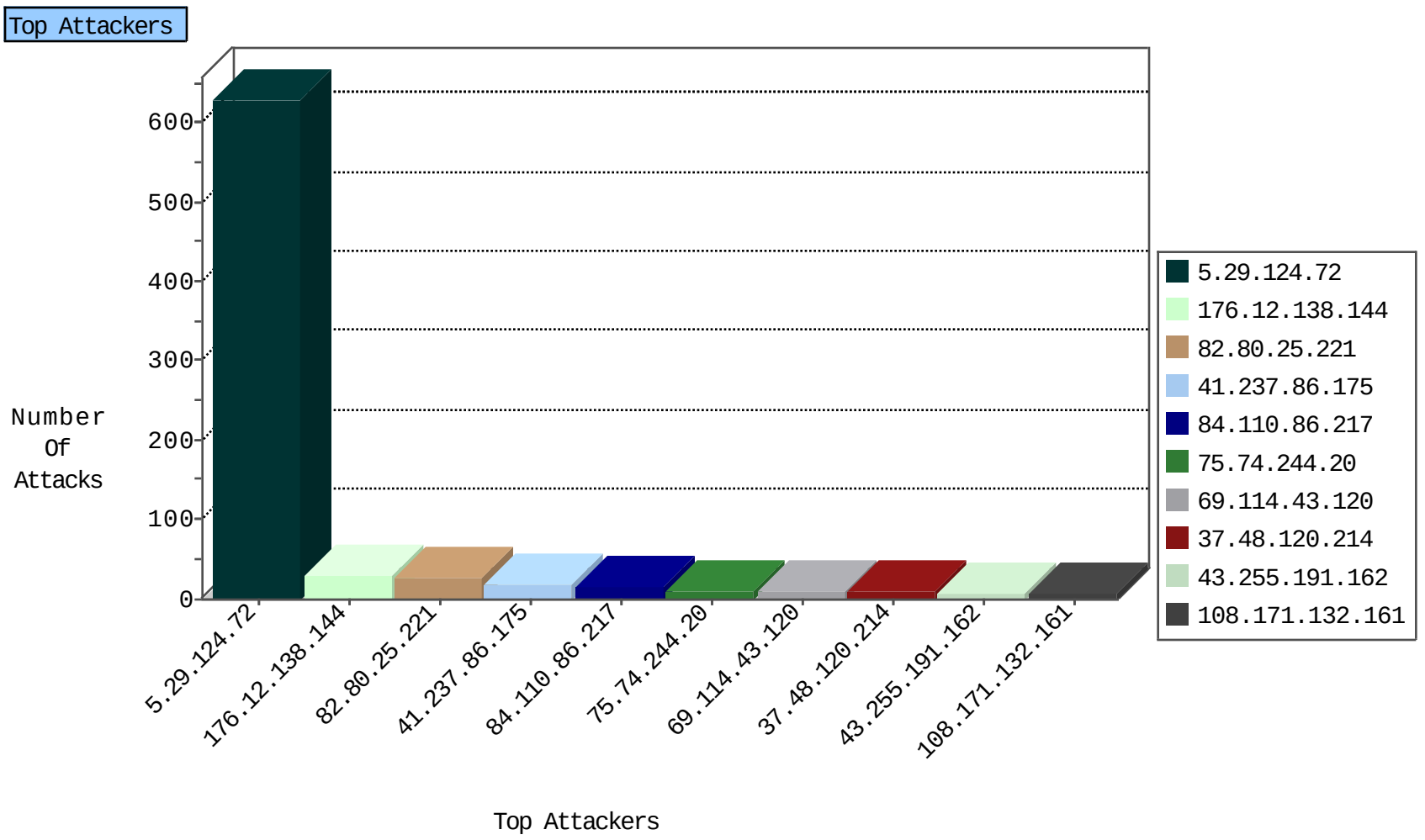
04-24-2015-23:03:04 to 04-25-2015-00:03:04

IDF Under Attack
04-24-2015-23:03:04

Top Targets



Top Attackers



04-24-2015-23:03:04 to 04-25-2015-00:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
176.12.148.33	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7978
10.0.0.10		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5056
157.55.39.59	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1171
84.110.86.217	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
188.103.6.210	Germany	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	13
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3
79.176.216.221	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
83.130.99.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.93.164	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-24-2015-23:03:04 to 04-25-2015-00:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.34.12.177	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.66.146.133	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.72	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
212.34.12.167	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.70.114	United States	147.237.76.202	e.halag.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
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
88.241.130.228	Turkey	147.237.77.216	dover.idf.il	13328: HTTP: Microsoft Internet Explorer Information Disclosure Vulnerability	Permit	1
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
88.241.130.228	Turkey	147.237.77.216	dover.idf.il	13894: HTTP: Apache Struts 2 ClassLoader Security Bypass Vulnerability	Permit	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.i	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
88.241.130.228	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-23:03:04 to 04-25-2015-00:03:04

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	28
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.79.74	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
66.249.81.144	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.110	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
2.54.23.189	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.162	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
188.95.158.198	Ukraine	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.194.115	Russian Federation	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.194.115	Russian Federation	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
92.50.82.18	Germany	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
61.16.232.231	India	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
31.184.194.115	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.16.232.231	India	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
89.40.71.178	Romania	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
88.241.130.228	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	1
43.255.191.162	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
31.184.194.115	Russian Federation	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
104.245.99.48		147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.194.115	Russian Federation	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.194.115	Russian Federation	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.231.192.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.16.232.231	India	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
89.40.71.178	Romania	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
88.241.130.228	Turkey	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	1
43.255.191.162	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1

04-24-2015-23:03:04 to 04-25-2015-00:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.29.124.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	630
176.12.138.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
41.237.86.175	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
75.74.244.20	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	9
69.114.43.120	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
176.12.138.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.26.146.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
85.64.156.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
108.171.132.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.176.216.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
89.139.170.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.121.79.0	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.0.55	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	3
84.109.184.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
208.92.134.60	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
81.218.136.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.150.178.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.117.251.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.58.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
94.159.233.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
213.8.129.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
130.166.109.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.29.26.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
94.249.98.208	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.148.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.178.118.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.103	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
62.90.184.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.111.22.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
70.55.204.222	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.178.128.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.157.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
213.57.189.156	Israel	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	1
141.212.122.149	United States	147.237.76.200	eitan.aka.idf.i		drop	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
121.54.58.225	Philippines	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
84.228.227.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.126.191.66	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
149.78.72.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
81.218.142.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.93.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.12.146.151	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-24-2015-23:03:04 to 04-25-2015-00:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.29.12.34	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
79.183.1.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	3
108.169.73.18	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/11â€‹33-19857-hâ€‹e/dover.asâ€‹px	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
88.241.130.228	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/0108	Block	1
50.207.2.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter catID in www.aka.idf.il/yohalan/home/home.asp	None	1
79.178.196.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/default.aspx 	Block	1
89.138.243.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.81.202	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/sachar/	Block	1
62.90.184.90	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1
157.55.39.127	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
66.249.75.72	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
24.77.236.141	Canada	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.153.8.126	Ukraine	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.81.239	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/894-he/himush.aspx	Block	1
62.219.62.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-index05.stm	Block	1
84.109.185.165	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1770-he/refuah.aspx	Block	1
46.19.85.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.233.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/090a.stm	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
66.249.65.15	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
84.228.195.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	1
46.117.98.67	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.65.39	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1

04-24-2015-23:03:04 to 04-25-2015-00:03:04