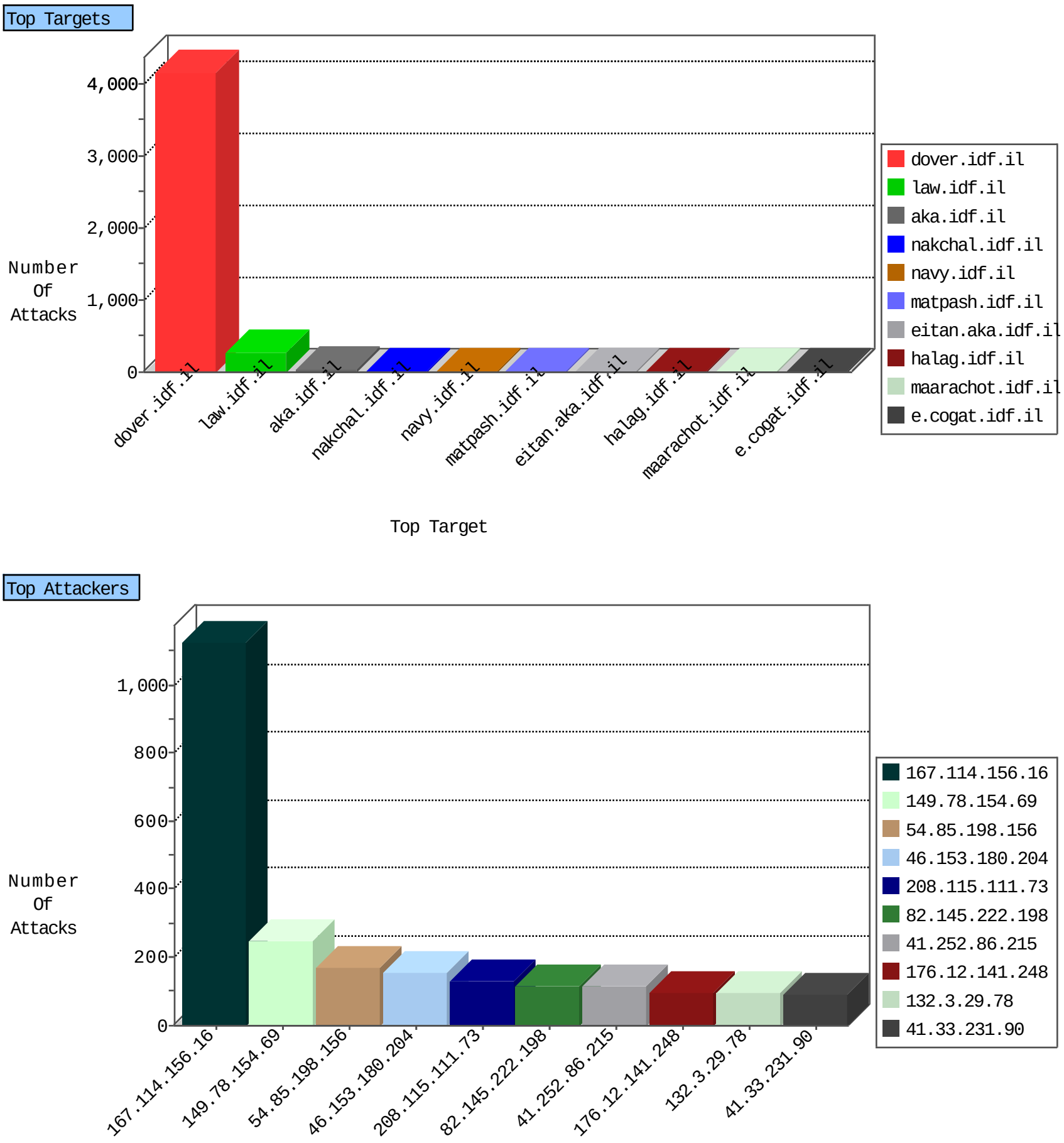
11-06-2015-02:04:06 to 11-06-2015-03:04:06

IDF Under Attack Daily Report



11-06-2015-02:04:06 to 11-06-2015-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2047
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	739
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	99
176.12.141.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
31.210.187.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
176.12.141.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
69.27.76.49	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
180.97.106.36	China	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1

11-06-2015-02:04:06 to 11-06-2015-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.252.86.215	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	3909: HTTP: Cross Site Scripting (Alert function)	Block	1

11-06-2015-02:04:06 to 11-06-2015-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.73.191	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-WEBAPP login.htm access	4
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-WEBAPP admin.php access	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	Admin login page scan - Havij	1
222.186.34.158	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
210.61.150.154	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
173.0.51.225	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
173.0.51.225	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
210.61.150.154	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
210.61.150.154	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
188.138.9.51	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
173.0.51.225	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.192	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
41.252.86.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SQL Injection - Select From	1

11-06-2015-02:04:06 to 11-06-2015-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	250
54.85.198.156	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	168
46.153.180.204	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	153
82.145.222.198	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	115
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	115
132.3.29.78	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	98
41.252.86.215	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
100.13.41.137	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	86
140.241.253.162	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	82
198.217.26.198	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	81
52.7.46.16	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	76
176.12.141.248	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	72
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	70
31.210.187.160	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
132.3.29.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
198.251.52.101	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
132.3.29.79	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
64.233.172.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
66.249.93.196	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
79.177.55.37	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
69.27.76.49	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.249.93.192	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
132.3.29.80	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
46.19.86.217	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
66.249.93.200	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
178.63.55.202	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
212.117.149.162	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
157.55.39.115	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
66.249.69.34	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
198.58.103.102	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
5.141.231.100	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
198.58.99.82	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
75.82.50.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
198.58.103.114	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.69.42	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.158	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
107.170.62.43	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
37.26.146.147	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12

11-06-2015-02:04:06 to 11-06-2015-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.252.86.215	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.252.86.215	Block	13
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	7
41.252.86.215	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
54.173.113.175	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 54.173.113.175	Block	2
79.178.50.199	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.17	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71786-he/maarachot.aspx	Block	1
141.212.122.64	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on /x	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
41.252.86.215	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nosuchpage123	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
85.65.98.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
149.88.158.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
66.249.67.217	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
104.33.97.119	United States	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/info.asp	Block	1
157.55.39.181	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1514-en/dover.aspx.	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
62.210.88.201	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
104.33.97.119	United States	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
207.46.13.182	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf×•Â»Â¢×“×ŸÂ¿Â½Â»×“×ŸÂ¿Â½Â»-×“×ŸÂ¿Â½Â»×“×ŸÂ¿Â½Â»×•Â»Â¢×“×ŸÂ¿Â½Â»×“×ŸÂ¿Â½Â»	Block	1
69.95.110.175	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
62.210.88.201	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
141.212.122.64	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /x	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1

11-06-2015-02:04:06 to 11-06-2015-03:04:06