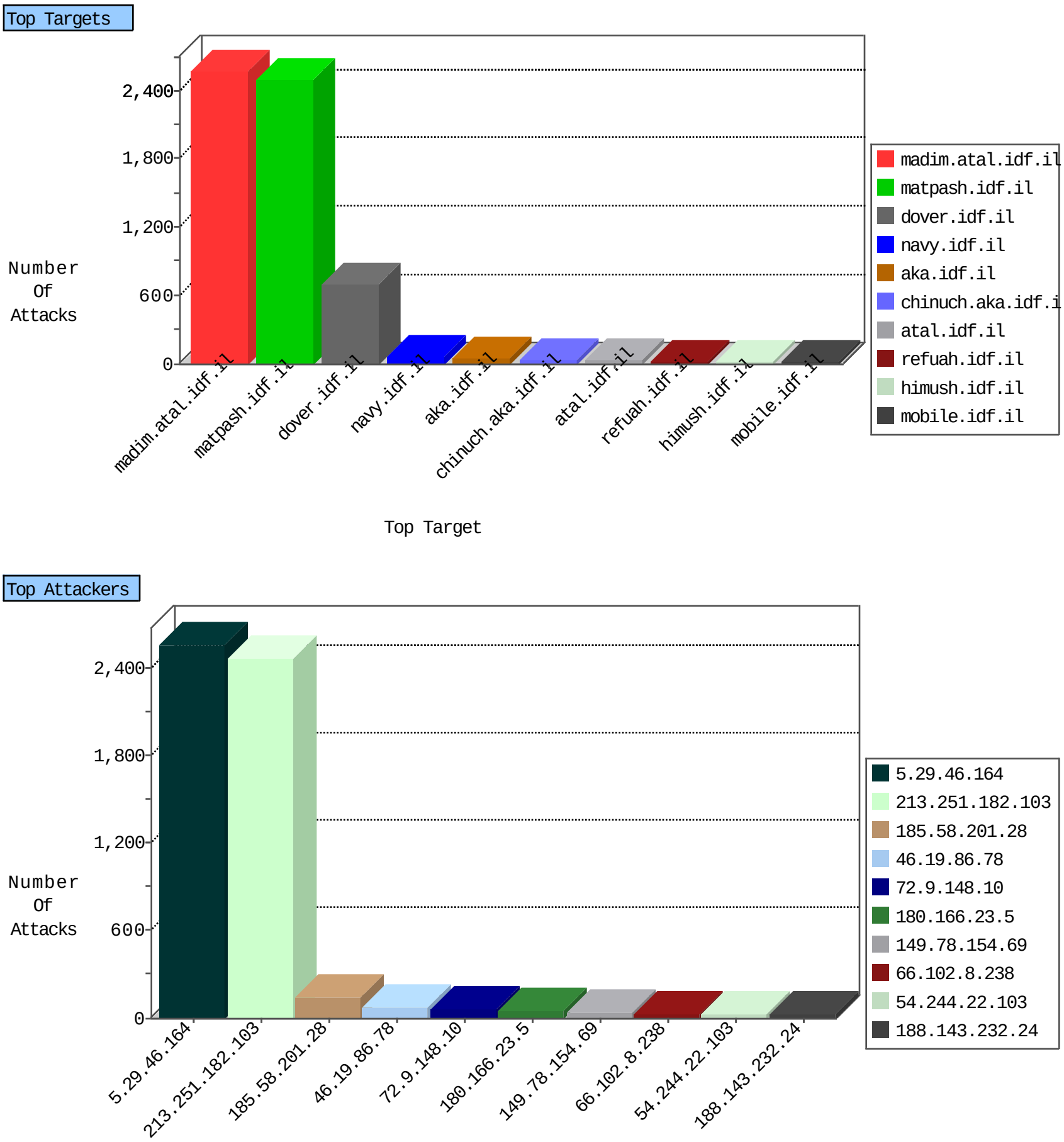
10-20-2015-06:04:01 to 10-20-2015-07:04:01

IDF Under Attack Daily Report



10-20-2015-06:04:01 to 10-20-2015-07:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.135.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
79.177.159.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
114.112.90.54	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

10-20-2015-06:04:01 to 10-20-2015-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-20-2015-06:04:01 to 10-20-2015-07:04:01

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	12
180.251.134.114	147.237.77.216	Indonesia	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
198.154.241.142	147.237.72.166	United States	aka.idf.il	SERVER-WEBAPP backup access	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
77.236.96.52	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
50.242.74.241	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
14.169.162.22	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
210.61.150.154	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
165.228.233.142	147.237.76.86	Australia	navy.idf.il	ET SCAN NMAP -sS window 3072	1
50.242.74.241	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
5.39.222.253	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

10-20-2015-06:04:01 to 10-20-2015-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
46.19.86.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
180.166.23.5	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.102.8.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
108.231.90.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
71.191.246.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.165.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
80.246.130.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
203.116.59.35	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
128.180.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
93.172.135.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.242.246.30	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.245	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
202.232.11.178	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.66.200.212	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.177.159.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.67.102.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.232.143.127	Egypt	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
176.13.12.6	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
5.9.36.66	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	3
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.58.201.28	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
46.19.85.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
173.252.73.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.29.176.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
153.168.28.68	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.58.201.28	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2

10-20-2015-06:04:01 to 10-20-2015-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.46.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2564
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	2464
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	52
157.55.39.211	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	26
31.193.51.80	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
188.143.232.24	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.24	Block	13
79.176.202.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
157.55.39.131	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/70344.jpg	Block	13
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	13
188.143.232.24	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	13
80.246.136.233	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	13
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
207.46.13.88	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	13
84.108.237.116	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/images/1.he/email/mail_link.gif	Block	13
2.54.165.73	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	13
180.153.180.92	China	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../shared/clientscripts/jquery.plugins/jquery.charts.js	Block	13
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
207.46.13.126	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	13
106.185.54.59	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/shared/usercontrols/headerupper/	Block	13
185.58.201.28	Lebanon	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	13
207.46.13.187	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	13
109.65.211.30	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	13

10-20-2015-06:04:01 to 10-20-2015-07:04:01