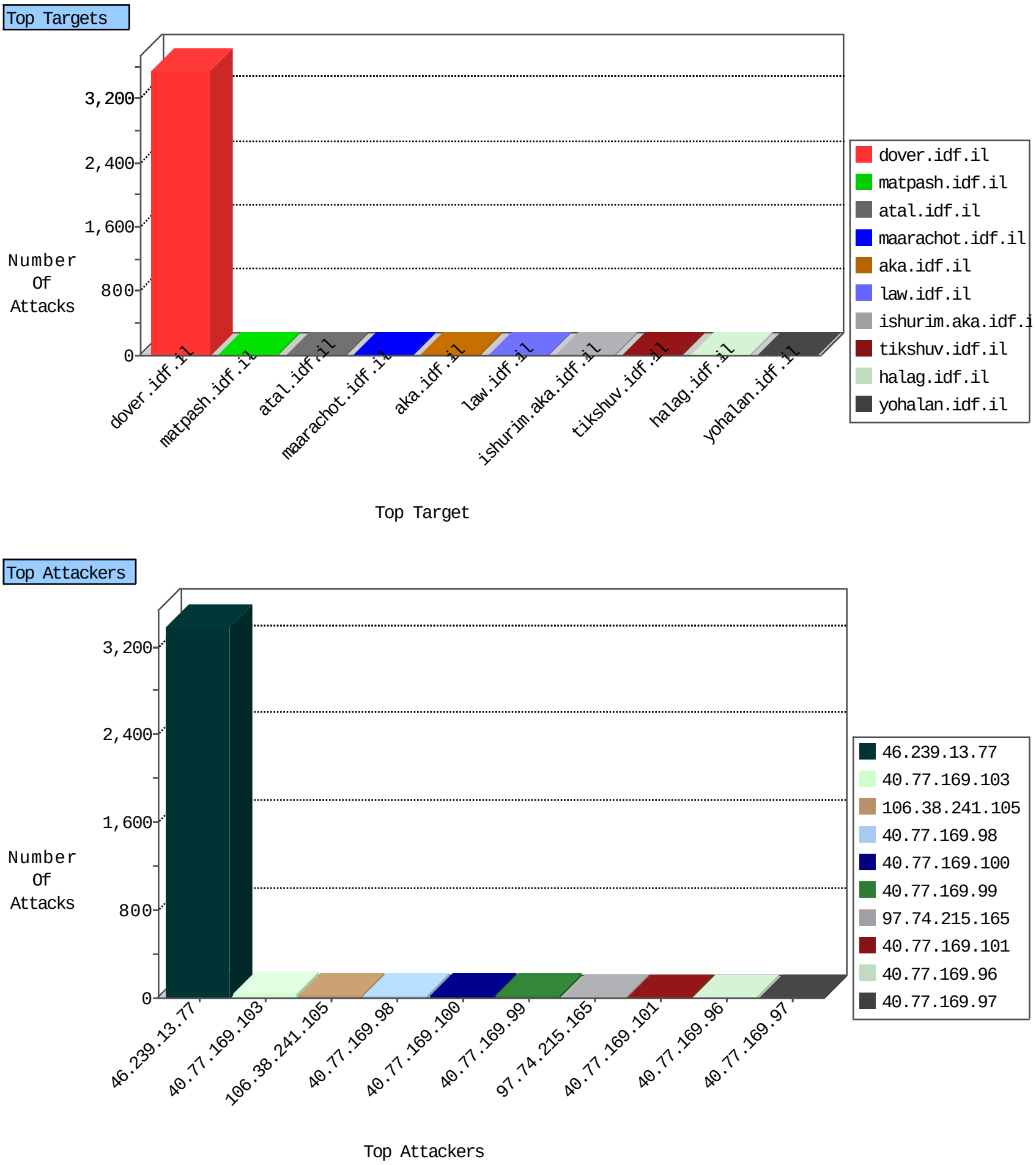
08-27-2016-06:04:09 to 08-27-2016-07:04:09

IDF Under Attack Daily Report



08-27-2016-06:04:09 to 08-27-2016-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.192.138	United States	147.237.76.30	himush.idf.il	Black List	drop	1
94.102.49.190	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
104.148.35.34	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1

08-27-2016-06:04:09 to 08-27-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.32.139.10	Italy	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	8
97.74.215.165	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
46.4.123.172	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-27-2016-06:04:09 to 08-27-2016-07:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
97.74.215.165	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
163.172.169.150	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.169.150	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.37.81	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
92.87.20.104	147.237.0.35	Romania	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -f -sS	1
163.172.169.150	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

08-27-2016-06:04:09 to 08-27-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3241
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	150
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	7
40.77.169.101	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	7
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	7
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	7
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
40.77.169.96	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	6
168.144.249.54	Canada	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
40.77.169.99	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
40.77.169.99	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
118.173.188.156	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
69.197.177.50	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
69.197.177.50	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
162.210.196.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
69.197.177.50	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
88.198.230.79	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
156.196.99.37	Egypt	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
104.158.35.213	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.88	United States	147.237.0.200	m4u.idf.il	drop		drop	1
37.247.36.82	Netherlands	147.237.0.200	m4u.idf.il	drop		drop	1
158.130.6.191	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
184.105.139.96	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.121.183	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.121.184	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.121.189	United States	147.237.0.200	m4u.idf.il	drop		drop	1
184.105.139.67	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
64.95.102.36	United States	147.237.0.33	idf.il	drop		drop	1

08-27-2016-06:04:09 to 08-27-2016-07:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.25.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.164	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
62.219.78.155	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
158.130.6.191	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/images/	Block	1
2.53.140.40	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
199.30.24.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-15505-en/dover.aspx	Block	1
64.62.219.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
158.130.6.191	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/images/	Block	1
66.249.64.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1248-he/atal.aspx	Block	1
12.28.167.226	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
64.62.219.89	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
158.130.6.191	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/images/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.65.178.25	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/newsarchive.aspx	Block	1
64.62.219.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.169.102	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /1283-12388-en/dover.aspx#011404	Block	1
158.130.6.191	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/images/	Block	1
65.55.210.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

08-27-2016-06:04:09 to 08-27-2016-07:04:09