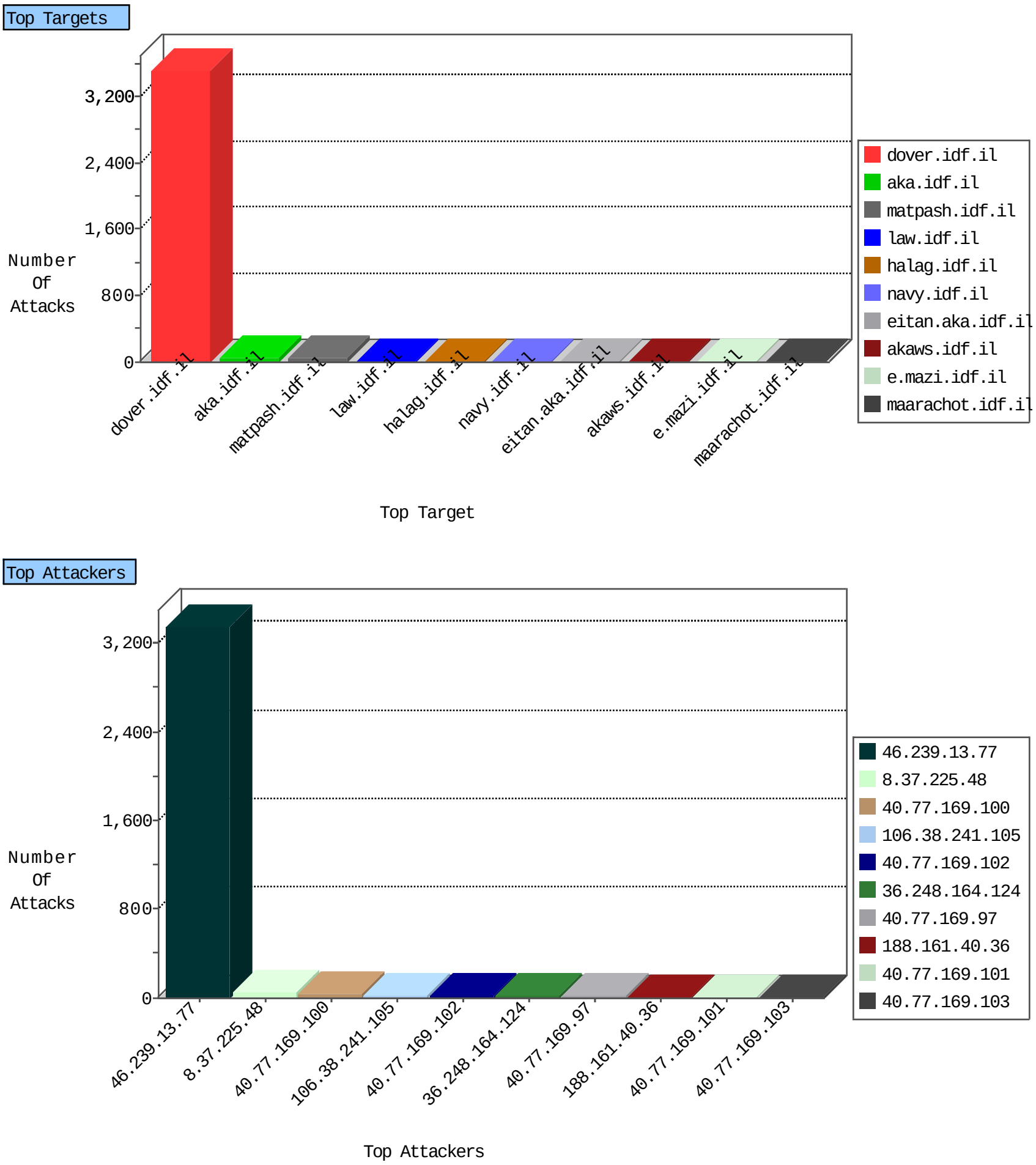
08-27-2016-05:04:05 to 08-27-2016-06:04:05

IDF Under Attack Daily Report



08-27-2016-05:04:05 to 08-27-2016-06:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
206.40.102.223	United States	147.237.76.86	navy.idf.il	Black List	drop	1
104.148.35.34	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
104.148.35.34	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
104.148.35.34	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
63.135.128.2	United States	147.237.76.86	navy.idf.il	Black List	drop	1

08-27-2016-05:04:05 to 08-27-2016-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	23
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	5
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
37.187.129.166	France	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-27-2016-05:04:05 to 08-27-2016-06:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.230	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
52.166.246.229	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
202.83.21.48	147.237.76.202	India	e.halag.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
134.226.55.214	147.237.76.200	Ireland	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
120.236.19.10	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
120.236.19.2	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
81.168.91.95	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
52.166.246.229	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
46.172.71.251	147.237.77.74	Ukraine	law.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.244.89	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
134.226.55.214	147.237.76.202	Ireland	e.halag.idf.il	ET SCAN Potential SSH Scan	1
120.236.19.10	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
120.236.19.2	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

08-27-2016-05:04:05 to 08-27-2016-06:04:05

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	3353
8.37.225.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
188.161.40.36	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	12
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
167.220.232.104	Japan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
185.130.6.49	Lithuania	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
40.77.169.99	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	4
40.77.169.101	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	4
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
40.77.169.102	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	3
190.18.171.40	Argentina	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.139.67	United States	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
141.212.122.70	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.71	United States	147.237.0.35	akaws.idf.il	drop		drop	1
187.101.67.189	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
158.130.6.191	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-27-2016-05:04:05 to 08-27-2016-06:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.248.164.124	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 36.248.164.124	Block	15
36.248.164.124	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
131.253.25.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
40.77.169.96	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 40.77.169.96	Block	3
131.253.25.206	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.25.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.70	Block	1
36.248.164.124	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
40.77.169.96	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in URL from 40.77.169.96	Block	1
66.249.76.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
207.46.13.24	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/english/about/doctrine/ethics	Block	1
207.46.13.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1

08-27-2016-05:04:05 to 08-27-2016-06:04:05