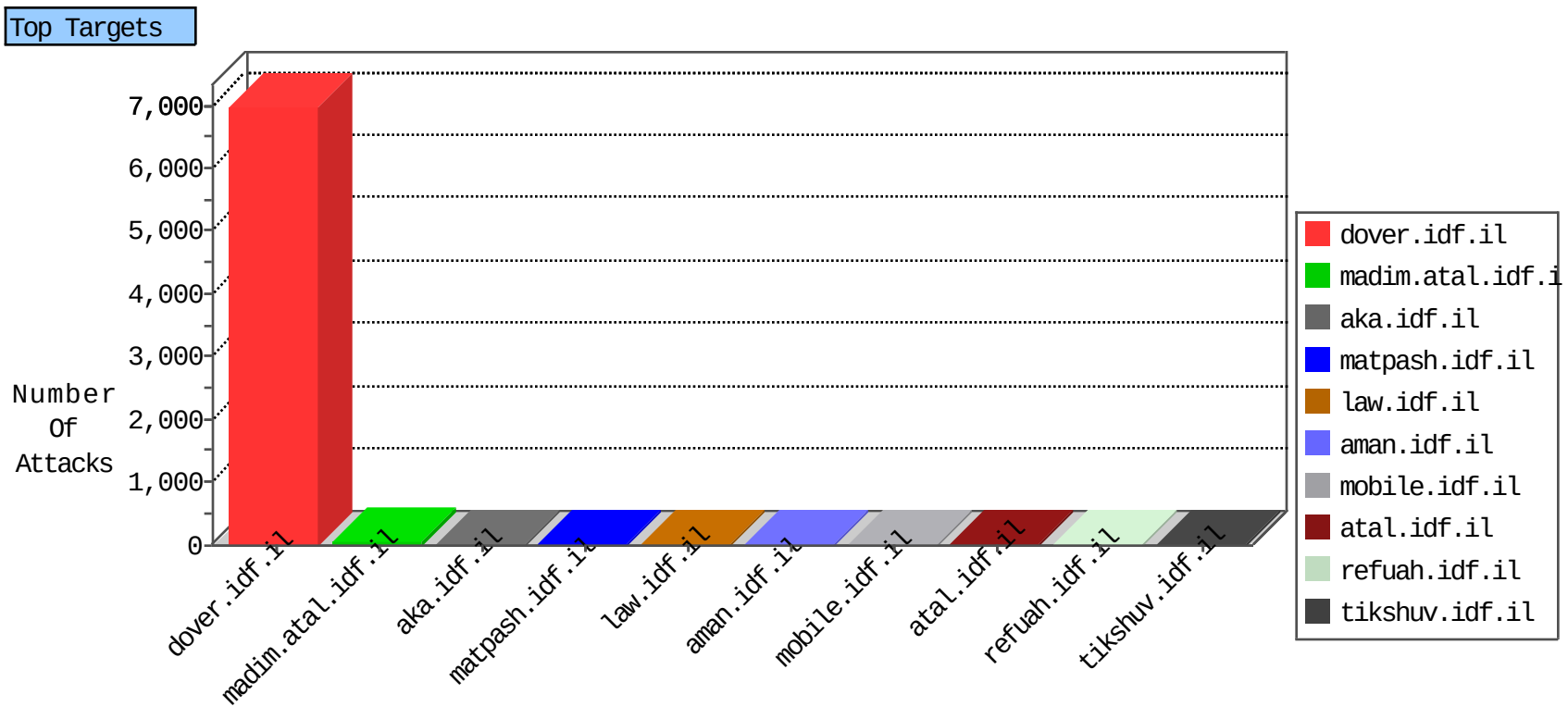
08-28-2016-00:04:01 to 08-28-2016-01:04:01

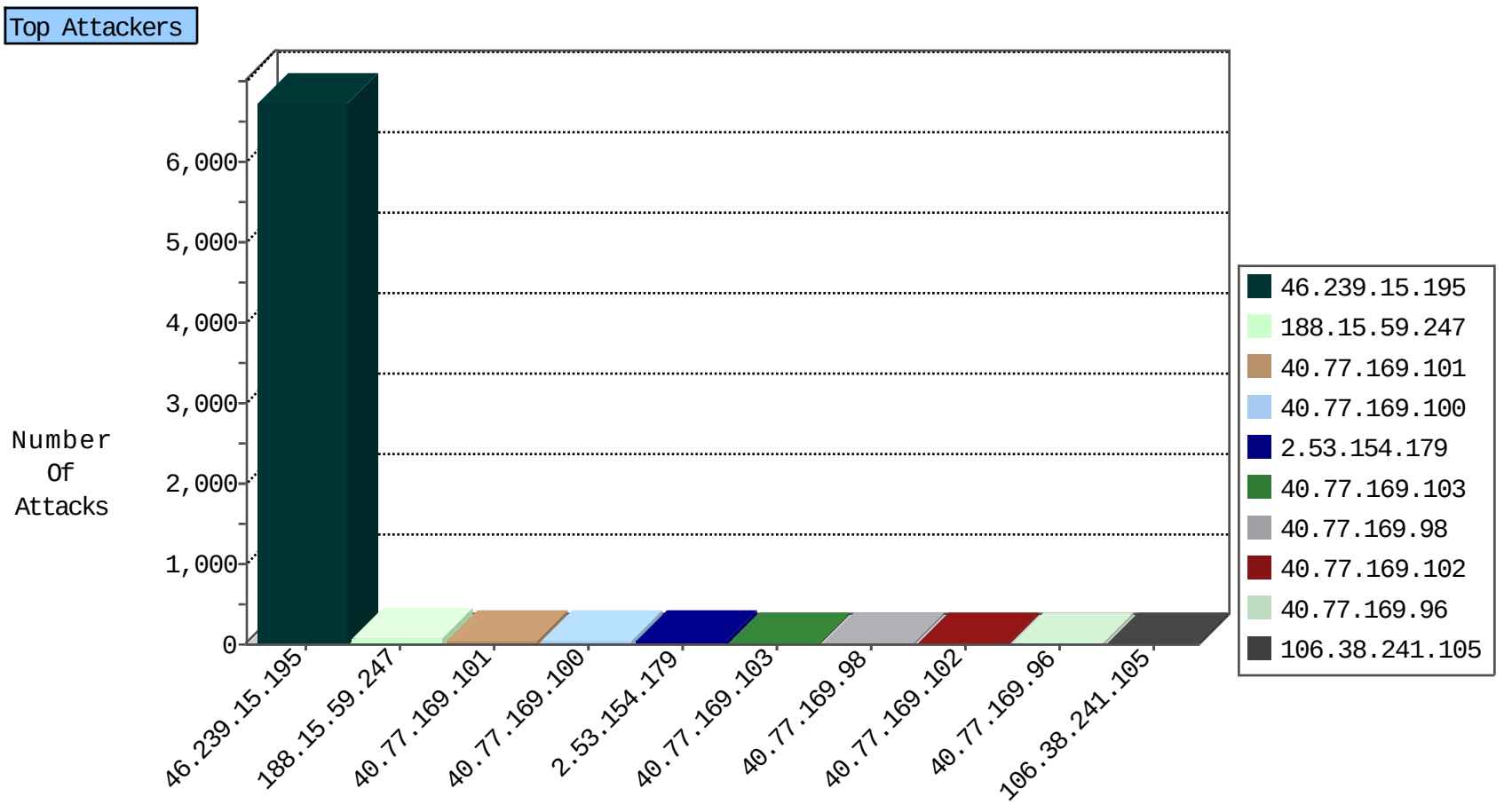
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-28-2016-00:04:01 to 08-28-2016-01:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2

08-28-2016-00:04:01 to 08-28-2016-01:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-28-2016-00:04:01 to 08-28-2016-01:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.218.140.63	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	8
188.0.236.165	147.237.0.33	Moldova, Republic of	idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
154.16.199.47	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
83.130.65.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
154.16.199.47	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.189	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
154.16.199.47	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
202.83.21.48	147.237.76.197	India	e.himush.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
202.83.21.48	147.237.76.38	India	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.168.69.86	147.237.77.216	India	dover.idf.il	portscan: TCP Distributed Portscan	1
202.83.21.48	147.237.0.33	India	idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
188.0.236.165	147.237.0.35	Moldova, Republic of	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
188.0.236.165	147.237.0.15	Moldova, Republic of	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -f -sS	1
154.16.199.47	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.111	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
154.16.199.47	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
202.83.21.48	147.237.76.39	India	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.83.21.48	147.237.0.34	India	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.64.143.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.103.31.165	147.237.8.50	Venezuela	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

08-28-2016-00:04:01 to 08-28-2016-01:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6753
188.15.59.247	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
40.77.169.98	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	7
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
79.182.97.170	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
40.77.169.98	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
79.182.92.8	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
40.77.169.101	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	4
109.253.135.46	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
151.49.82.3	Italy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.97	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
40.77.169.104	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.12.180	Israel	147.237.72.166	aka.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
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
105.225.240.248	South Africa	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
188.207.65.163	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
217.92.51.75	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.206.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-28-2016-00:04:01 to 08-28-2016-01:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.154.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.53.50.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
185.120.125.101	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.193.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.139.118.13	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.162.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.138.9.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.102.207.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.151.35.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
46.19.86.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
46.121.63.50	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
94.102.49.193	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20581-he/dover.aspx	Block	1
213.57.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.106.109	Block	1
80.230.220.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.236	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1726	Block	1
2.55.33.44	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
189.232.178.86	Mexico	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
105.225.240.248	South Africa	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
82.239.56.57	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
189.232.178.86	Mexico	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
109.64.13.10	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/faq.aspx	None	1
157.55.2.169	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.109.80.156	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.233	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to chinuch.aka.idf.il/894-he	Block	1
5.22.135.109	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
199.30.25.151	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.92.32	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.181.12.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
166.137.139.127	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
5.29.141.208	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
212.76.116.195	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.64.92.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
80.230.220.211	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1

08-28-2016-00:04:01 to 08-28-2016-01:04:01