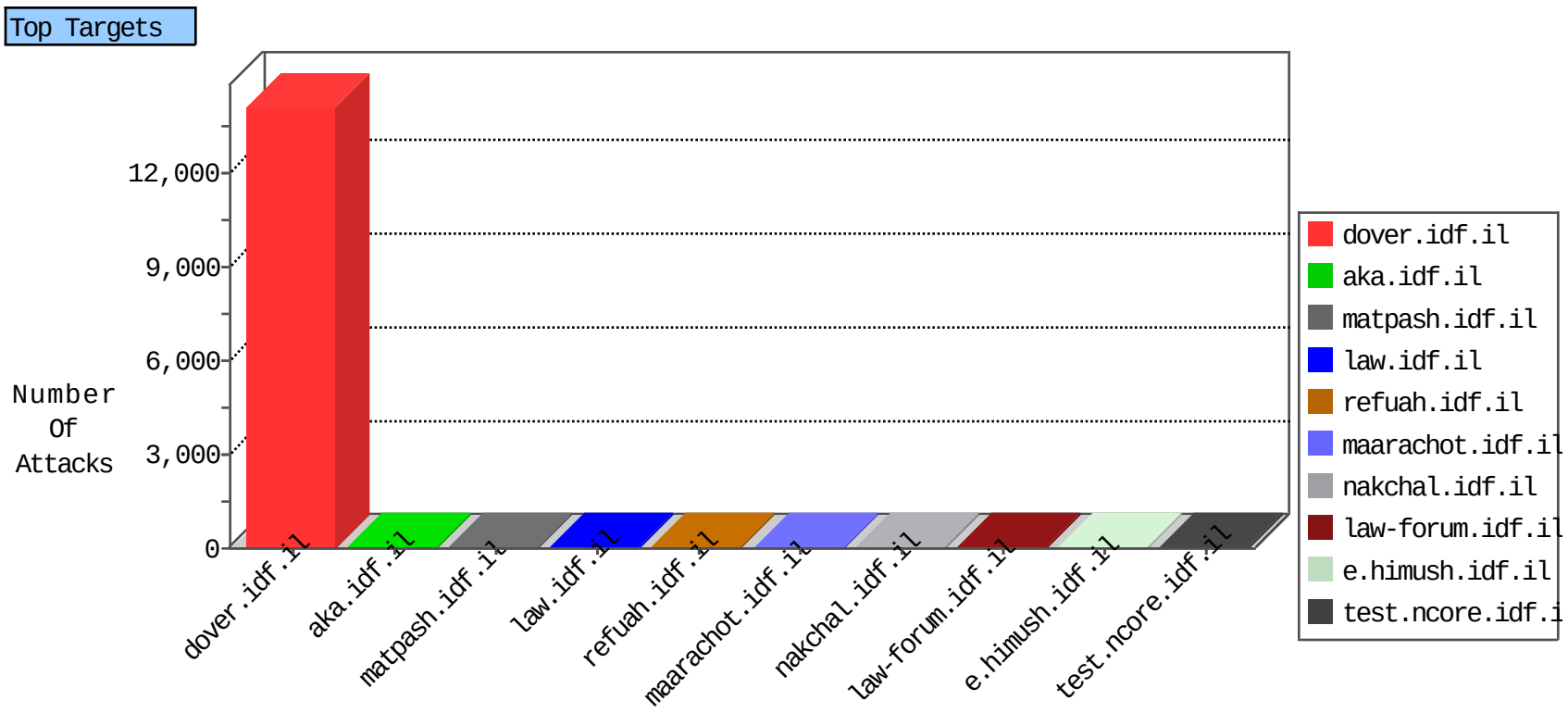
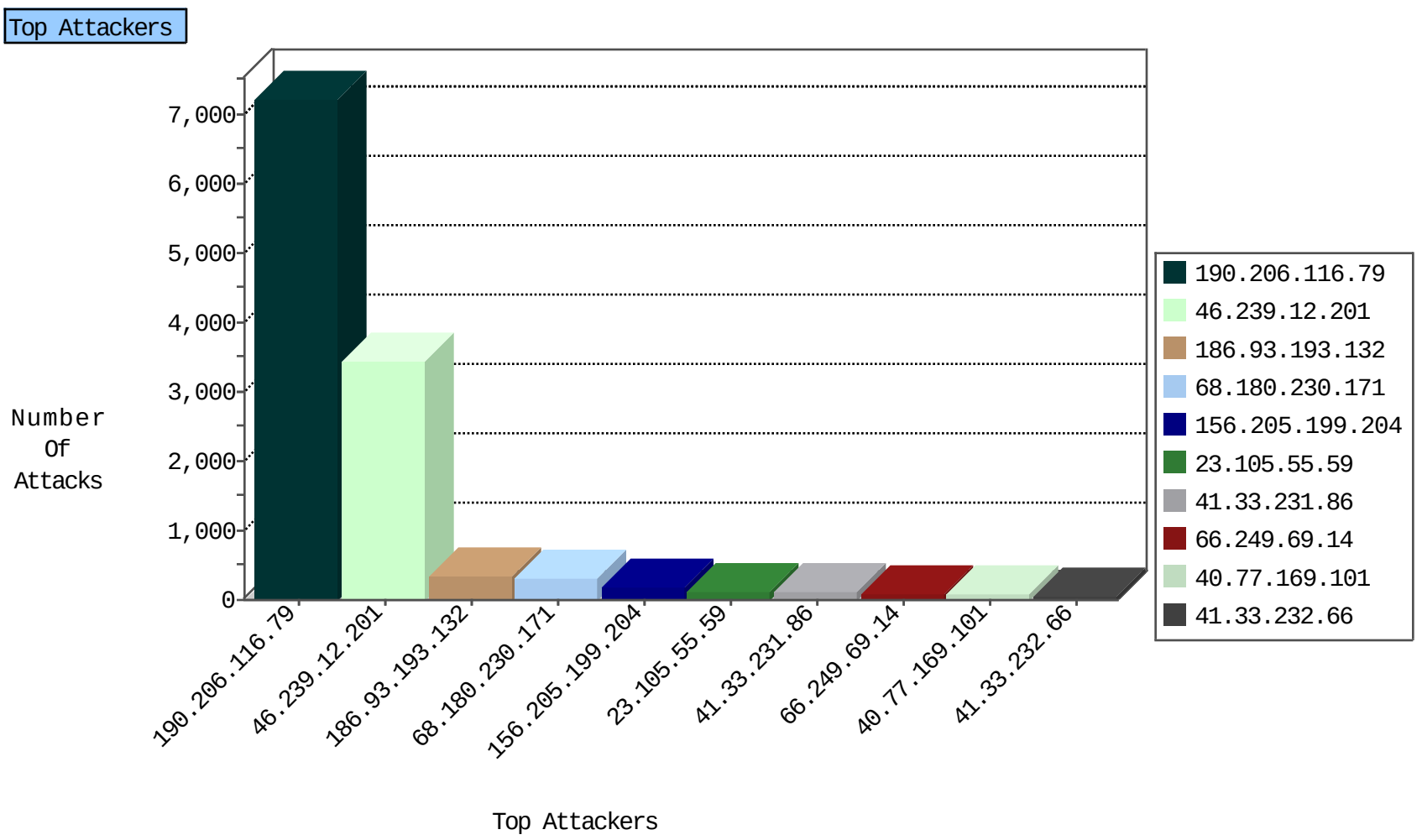
08-26-2016-05:04:05 to 08-26-2016-06:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-26-2016-05:04:05 to 08-26-2016-06:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	236132
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	53466
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	50944
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	34524
186.93.193.132	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	283
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	226
23.105.55.59	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	126
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	113
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	105
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	88
66.249.69.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	76
186.93.193.132	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	72
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	63
109.253.131.180	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	48
181.104.10.6	Argentina	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	46
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	41
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	35
73.4.190.189	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	32
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	30
40.77.169.101	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
79.178.61.177	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
81.218.33.77	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	26
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
66.249.69.18	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
197.40.130.130	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
40.77.169.100	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
66.249.69.14	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
159.220.75.3	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
136.160.90.51	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
66.249.85.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
40.77.169.99	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
208.96.180.225	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
159.220.75.2	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
66.249.91.8	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
40.77.167.66	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
40.77.169.100	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
176.13.13.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
107.10.132.61	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
212.76.114.247	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10

08-26-2016-05:04:05 to 08-26-2016-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.109.242.34	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.30.213.202	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
5.9.62.130	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
5.9.62.130	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
36.79.55.166	Indonesia	147.237.77.176	matpash.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

08-26-2016-05:04:05 to 08-26-2016-06:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.109.242.34	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	8
37.213.44.195	147.237.77.216	Belarus	dover.idf.il	Xenu Link Sleuth User Agent	4
36.79.55.166	147.237.77.170	Indonesia	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	3
36.79.55.166	147.237.76.42	Indonesia	refuah.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	3
36.79.55.166	147.237.77.176	Indonesia	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	2
36.79.55.166	147.237.77.74	Indonesia	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	2
201.238.202.219	147.237.0.35	Chile	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.49.77	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
94.102.48.195	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.38.14	147.237.77.227	Vietnam	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1

08-26-2016-05:04:05 to 08-26-2016-06:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3126
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	300
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	49
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	14
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
46.120.129.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.103	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
2.83.86.101	Portugal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.212.122.100	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.102	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.243.173.2	Russian Federation	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.103	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.99	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
141.212.122.99	United States	147.237.0.33	idf.il	drop		drop	1
183.129.160.229	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1

08-26-2016-05:04:05 to 08-26-2016-06:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.138.72.255	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
68.180.228.252	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
207.46.13.24	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
79.179.192.33	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
40.77.169.102	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL /1357-en/cogat.aspx#011200	Block	1
79.179.192.33	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.102.6.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

08-26-2016-05:04:05 to 08-26-2016-06:04:05