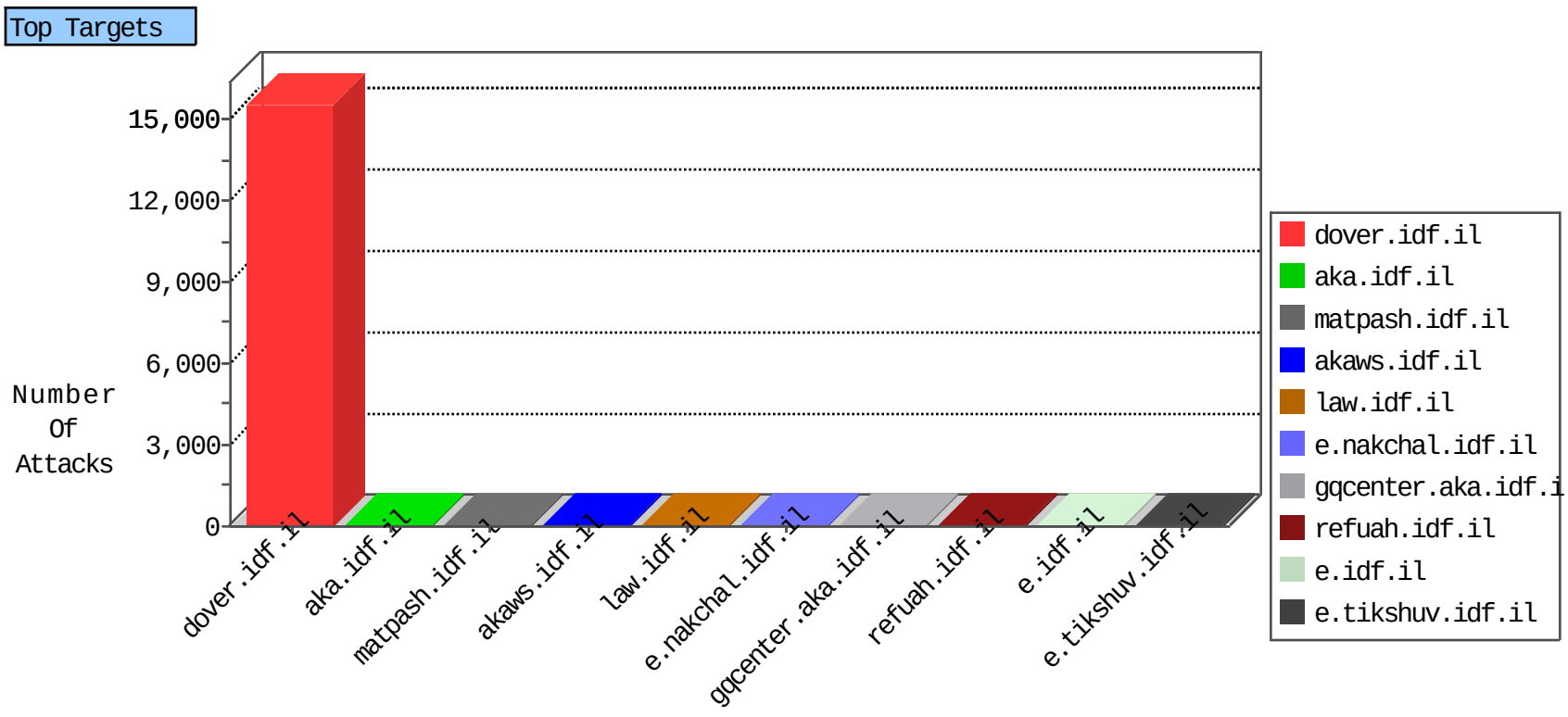
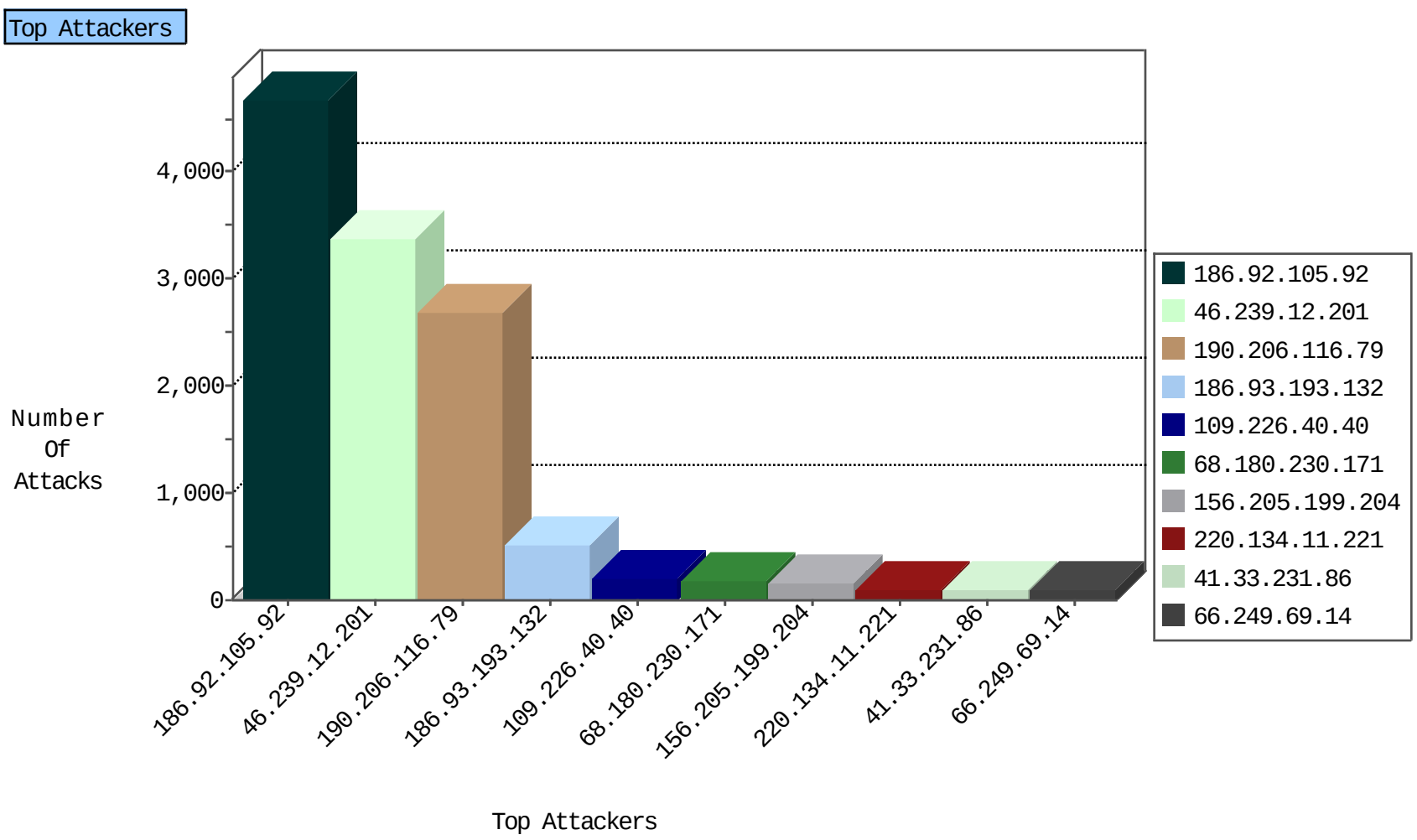
08-26-2016-03:04:06 to 08-26-2016-04:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-26-2016-03:04:06 to 08-26-2016-04:04:06

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	network flood IPv4 TCP-FIN-ACK	drop	2161996
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	302928
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2746
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	2211
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1634
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1065
186.93.193.132	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	459
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	205
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	125
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	87
220.134.11.221	Taiwan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	84
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	79
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	79
139.162.216.112	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	79
66.249.69.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	78
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	72
136.160.90.51	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	62
186.93.193.132	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	55
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	50
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	47
104.249.236.166	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	43
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	39
79.180.29.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	35
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	30
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
79.180.209.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
157.55.39.93	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
157.55.39.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
186.204.199.86	Brazil	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
109.65.67.225	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
80.246.133.132	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
109.65.175.187	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
66.249.69.18	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
109.66.102.209	Israel	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 out of context	drop	20
84.109.193.55	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
220.134.11.221	Taiwan	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
79.178.2.141	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
46.116.193.240	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
179.115.31.7	Brazil	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
64.62.219.94	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
176.12.160.4	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
64.62.219.150	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
202.36.244.4	New Zealand	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
73.172.17.229	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
159.220.75.3	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
64.62.219.153	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
64.62.219.79	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
64.62.219.164	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15

08-26-2016-03:04:06 to 08-26-2016-04:04:06

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	19

08-26-2016-03:04:06 to 08-26-2016-04:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
201.238.202.219	147.237.76.44	Chile	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.75.130	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.75.130	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.74	Japan	law.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.105	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
203.4.240.101	147.237.72.217	Australia	e.idf.il	ET SCAN NMAP -sS window 1024	1
186.112.64.25	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.75.130	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
123.206.73.185	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.148.91	147.237.77.74	France	law.idf.il	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
203.4.240.101	147.237.72.217	Australia	e.idf.il	ET SCAN Potential SSH Scan	1

08-26-2016-03:04:06 to 08-26-2016-04:04:06

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	3386
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
109.201.133.100	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
188.247.78.163	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
167.220.232.104	Japan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
46.120.129.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.103	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
188.247.78.163	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.9.10.227	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
157.55.39.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
141.212.122.165	United States	147.237.0.35	akaws.idf.il	drop		drop	1
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
141.212.122.166	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.50	e.tikshuv.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
141.212.122.76	United States	147.237.0.35	akaws.idf.il	drop		drop	1
162.216.46.173	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
141.212.122.77	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-26-2016-03:04:06 to 08-26-2016-04:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.4.15.197	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
80.246.136.236	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.64	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.75.174	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
207.46.13.89	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
87.68.55.56	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
40.77.169.100	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL /1328-en/cogat.aspx#011404	Block	1
77.138.166.226	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
87.68.55.56	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
40.77.169.100	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in URL from 40.77.169.100	Block	1
77.139.183.8	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1

08-26-2016-03:04:06 to 08-26-2016-04:04:06