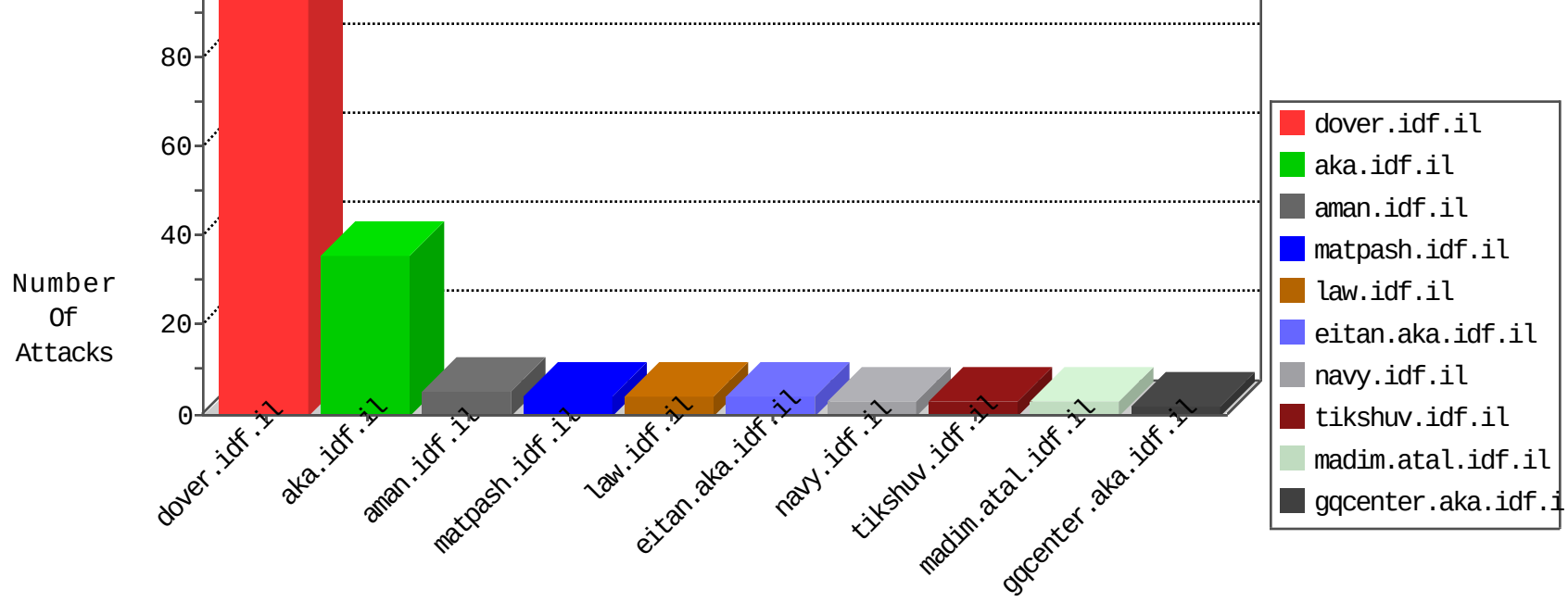
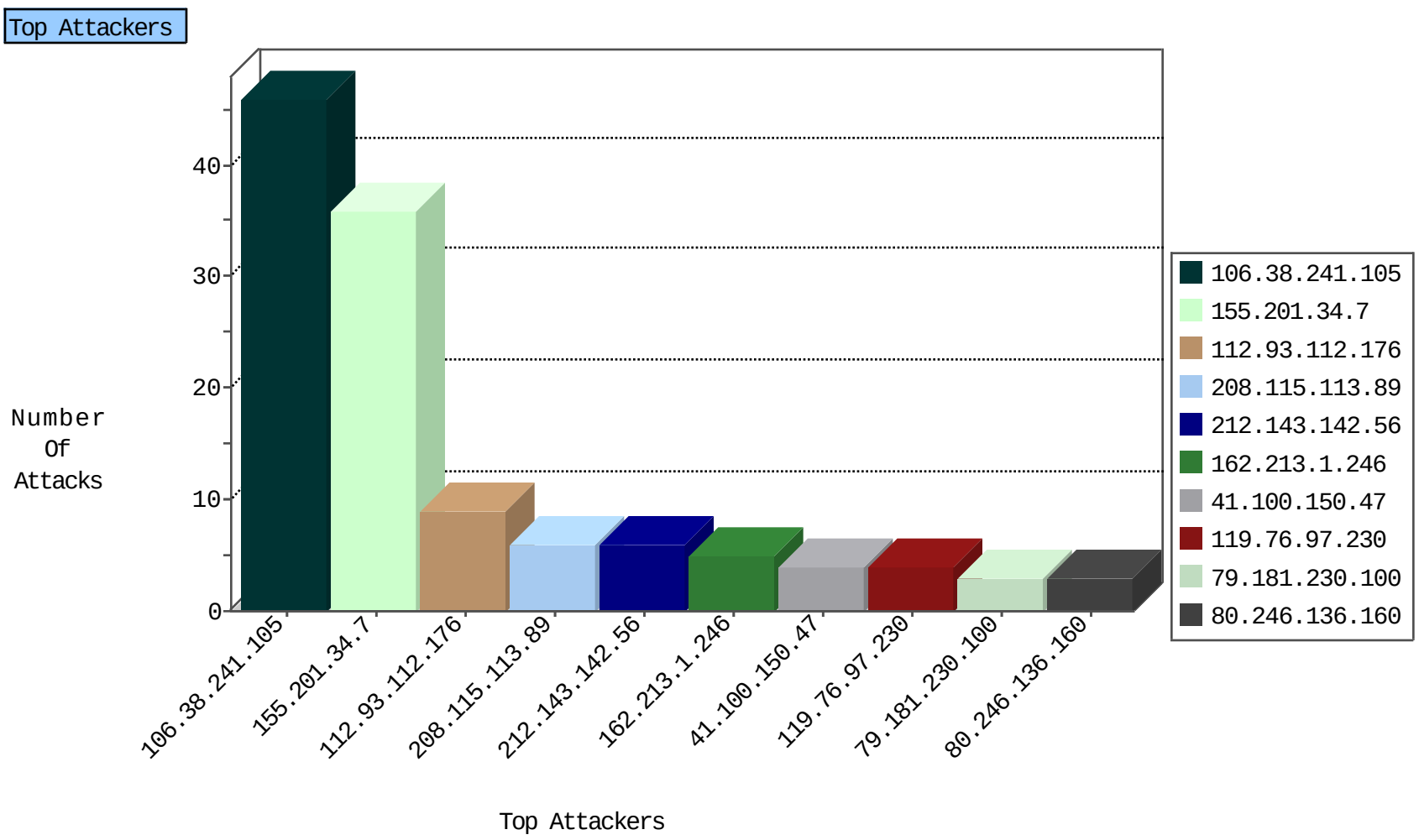
08-22-2016-06:04:08 to 08-22-2016-07:04:08

IDF Under Attack Daily Report





08-22-2016-06:04:08 to 08-22-2016-07:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.218.204.245	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
177.0.38.147	Brazil	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
41.100.150.47	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
103.29.5.8	Indonesia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
119.110.80.21	Indonesia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
89.248.168.21	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1

08-22-2016-06:04:08 to 08-22-2016-07:04:08

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	28
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.76.200	eitan.aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
151.80.31.163	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.155	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.55	France	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-22-2016-06:04:08 to 08-22-2016-07:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.i	Tehila - Perl LWP with fake user agent	5
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
79.181.230.100	147.237.77.216	Israel	dover.idf.i	WEB-FRONTPAGE /_vti_bin/ access	1

08-22-2016-06:04:08 to 08-22-2016-07:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
155.201.34.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
119.76.97.230	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.100.150.47	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
112.93.112.176	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.179.1.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.164.204.105	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
107.77.160.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.193.230	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-22-2016-06:04:08 to 08-22-2016-07:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
112.93.112.176	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.93.112.176	Block	5
80.246.136.160	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
112.93.112.176	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
24.205.246.229	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	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
180.76.15.136	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
79.181.230.100	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.181.230.100	Block	1
27.153.170.175	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
79.181.230.100	Israel	147.237.77.216	dover.idf.il	Multiple _vti_ from 79.181.230.100	Block	1
27.153.170.175	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
75.82.117.252	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
207.46.13.9	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
66.249.69.249	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
131.253.27.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
77.138.122.10	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
2.55.24.208	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
207.46.13.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.30	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
111.69.70.18	New Zealand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1

08-22-2016-06:04:08 to 08-22-2016-07:04:08