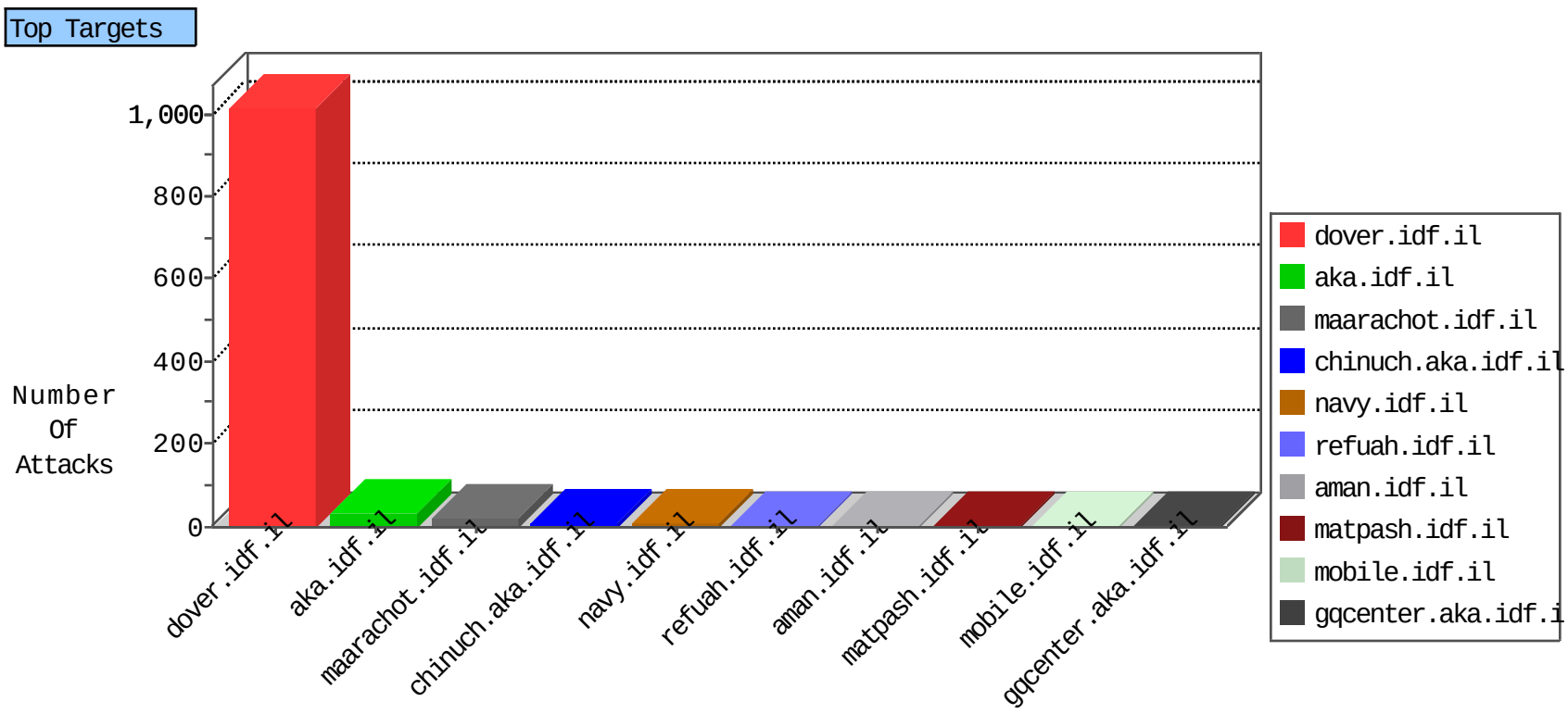
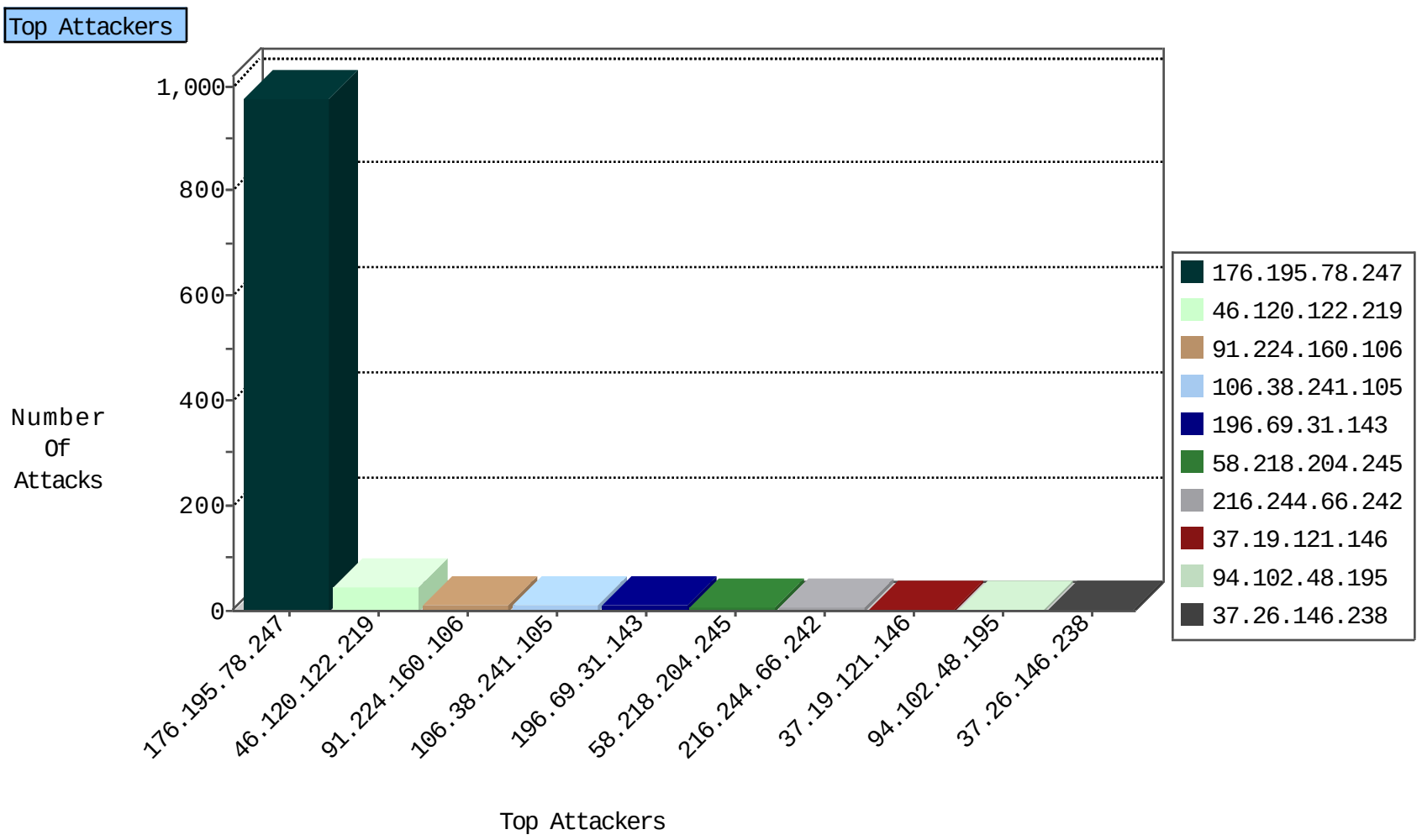
08-30-2016-03:04:01 to 08-30-2016-04:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-30-2016-03:04:01 to 08-30-2016-04:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
89.248.167.131	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

08-30-2016-03:04:01 to 08-30-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
52.41.116.86	United States	147.237.72.166	aka.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
61.135.189.120	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
141.95.0.58	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
71.6.135.131	United States	147.237.76.177	ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-30-2016-03:04:01 to 08-30-2016-04:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	18
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	12
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.76.147	Israel	chinuch.aka.idf.il	Xenu Link Sleuth User Agent	4
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	2
162.250.190.142	147.237.77.216	Canada	dover.idf.il	Xenu Link Sleuth User Agent	2
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
64.137.171.55	147.237.76.86	Canada	navy.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	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
58.218.204.245	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1

08-30-2016-03:04:01 to 08-30-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.195.78.247	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	978
196.69.31.143	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
178.140.10.121	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.92.32.107	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
151.25.249.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.228.35.111	Russian Federation	147.237.77.216	dover.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
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
46.120.12.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.176	test.ncore.idf.il	drop	First packet isn't SYN	drop	1
66.249.64.111	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1

08-30-2016-03:04:01 to 08-30-2016-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	7
37.19.121.146	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
216.244.66.242	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 216.244.66.242	Block	4
31.168.13.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.238	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
109.65.33.6	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
41.97.96.105	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
81.218.229.198	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.229.198	Block	1
66.249.65.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9841-he/refuah.aspx	Block	1
157.55.39.16	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.120.122.219	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method HEAD for www.chinuch.aka.idf.il/	None	1
216.244.66.242	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/library/library.asp	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.69.92	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1
157.55.39.175	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/klali/default.asp	None	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
65.55.210.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
220.255.145.120	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
66.249.73.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
203.127.96.214	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.222.181	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/portalmiluim/templates/inner.asp	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
220.255.148.68	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
203.127.96.247	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.229.198	Israel	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 81.218.229.198	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
157.55.39.14	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/rabanut/general.aspx	None	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1

08-30-2016-03:04:01 to 08-30-2016-04:04:01