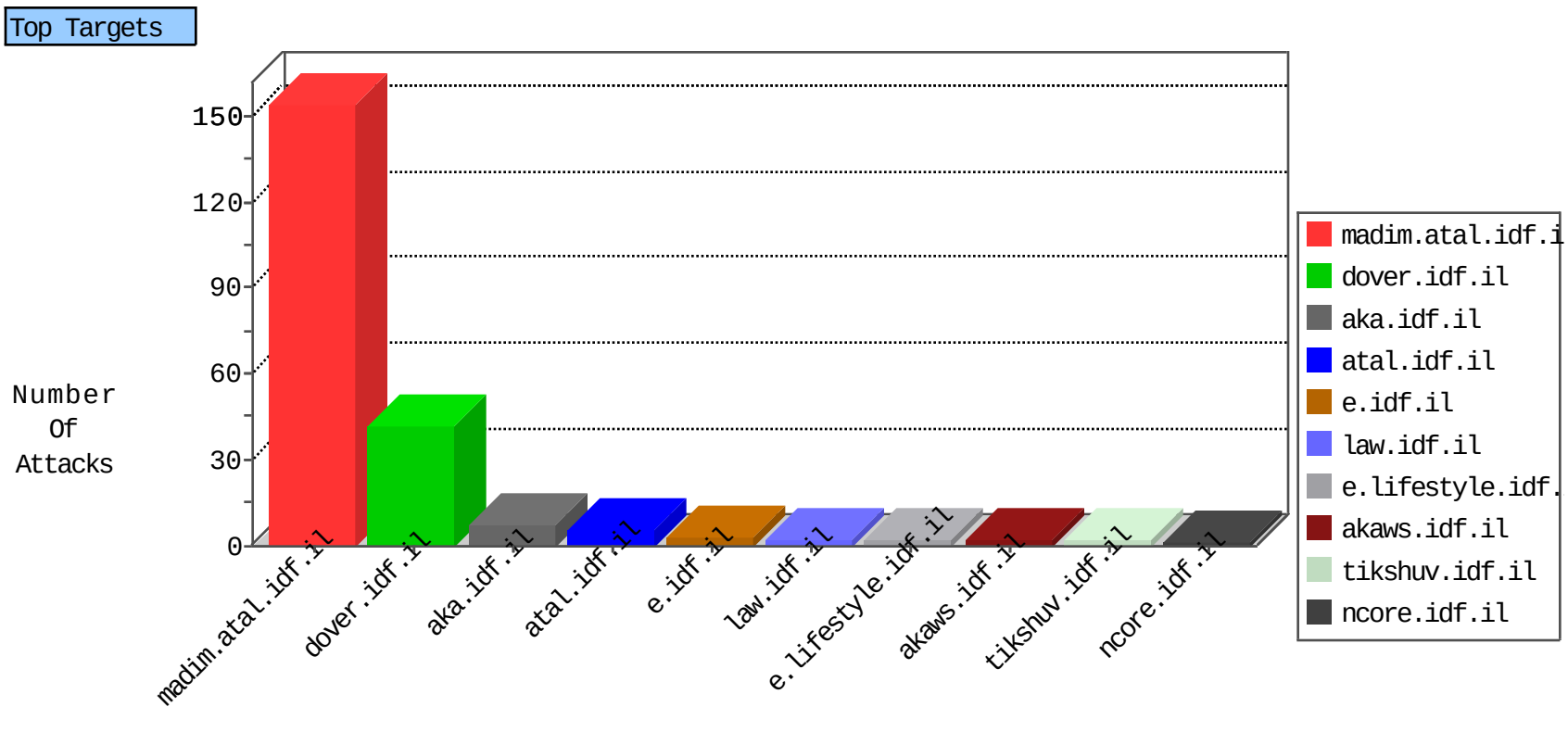
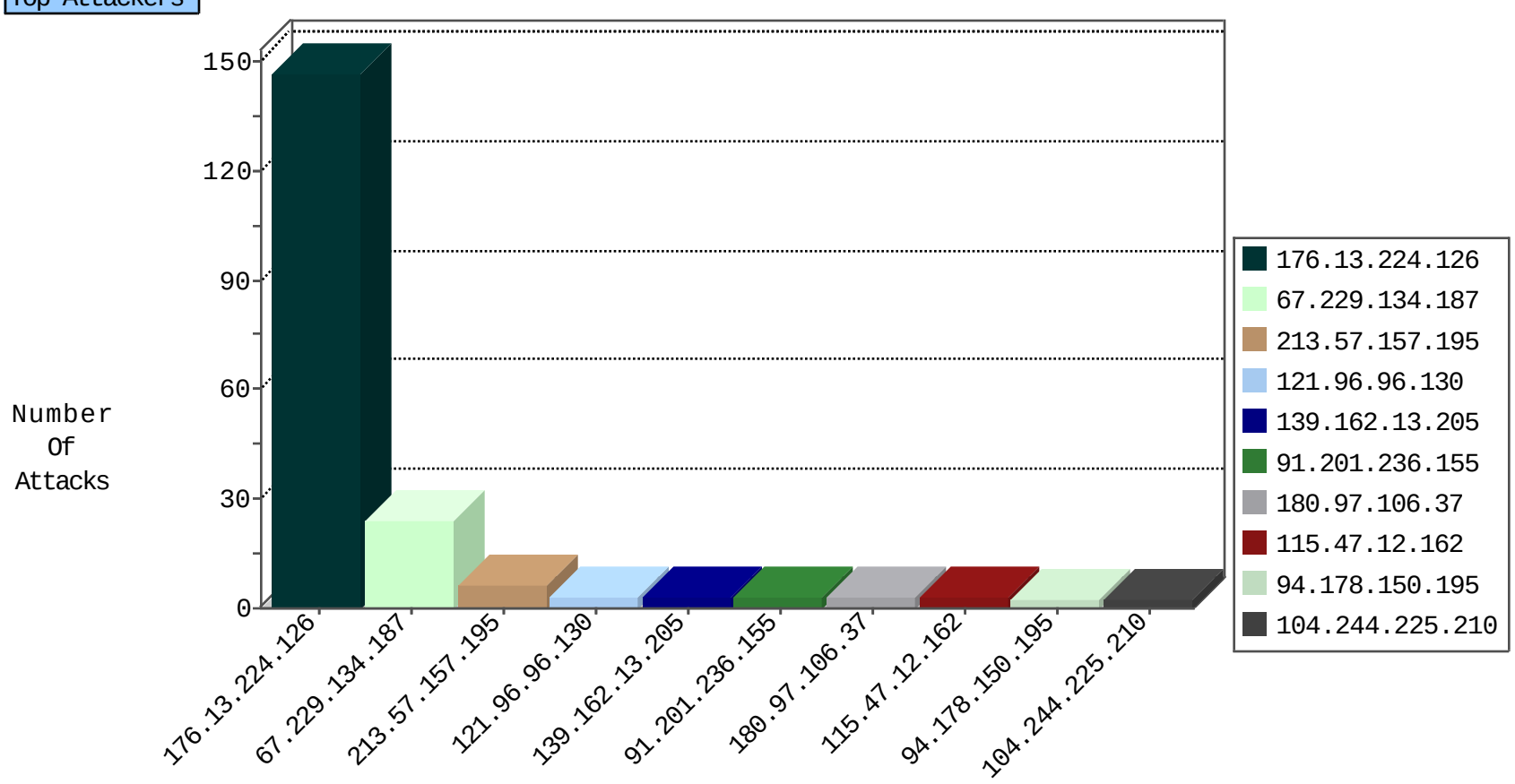
08-18-2016-06:04:08 to 08-18-2016-07:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-18-2016-06:04:08 to 08-18-2016-07:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
154.16.199.47	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
176.13.224.126	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
89.248.171.2	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
115.47.12.162	China	147.237.8.24	e.lifestyle.idf.i	JLM_Purple_Con_Limit_Tcp	drop	1

08-18-2016-06:04:08 to 08-18-2016-07:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.6.167.142	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-18-2016-06:04:08 to 08-18-2016-07:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.48.195	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
89.33.246.121	147.237.0.15	Romania	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
66.151.255.234	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
216.196.194.170	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
139.162.13.205	147.237.77.233	Singapore	atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
115.47.12.162	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.92	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.72.217	Ukraine	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.66.185	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
5.255.90.133	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
190.229.161.133	147.237.0.34	Argentina	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.47.12.162	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
113.108.10.31	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

08-18-2016-06:04:08 to 08-18-2016-07:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
121.96.96.130	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
104.244.225.210	Jamaica	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
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
184.105.139.80	United States	147.237.0.35	akaws.idf.il	drop		drop	1
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
184.105.247.207	United States	147.237.0.33	idf.il	drop		drop	1
113.108.10.31	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
180.97.106.37	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
176.13.240.89	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.76	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-18-2016-06:04:08 to 08-18-2016-07:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.224.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	146
67.229.134.187	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 67.229.134.187	Block	17
213.57.157.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
67.229.134.187	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
94.178.150.195	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
157.55.39.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
64.62.219.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
67.229.134.187	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
99.225.173.240	Canada	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
64.62.219.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.17.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
77.139.176.29	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus	Block	1
139.162.13.205	Singapore	147.237.77.233	atal.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.109.244.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
139.162.13.205	Singapore	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
192.243.55.136	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhllytaxltawms5kb2m=&infocenteritem=true	Block	1
84.229.18.175	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.116.86.138	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

08-18-2016-06:04:08 to 08-18-2016-07:04:08