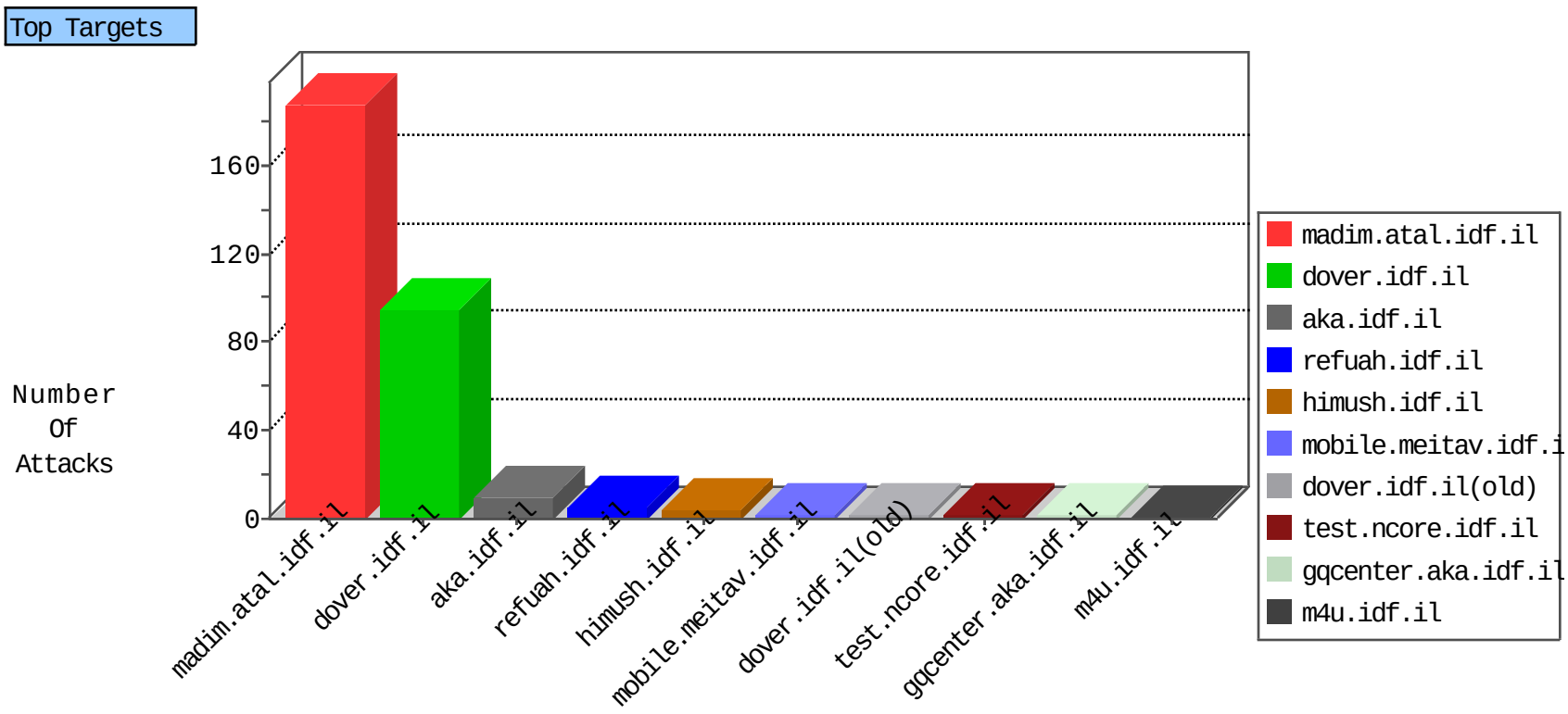
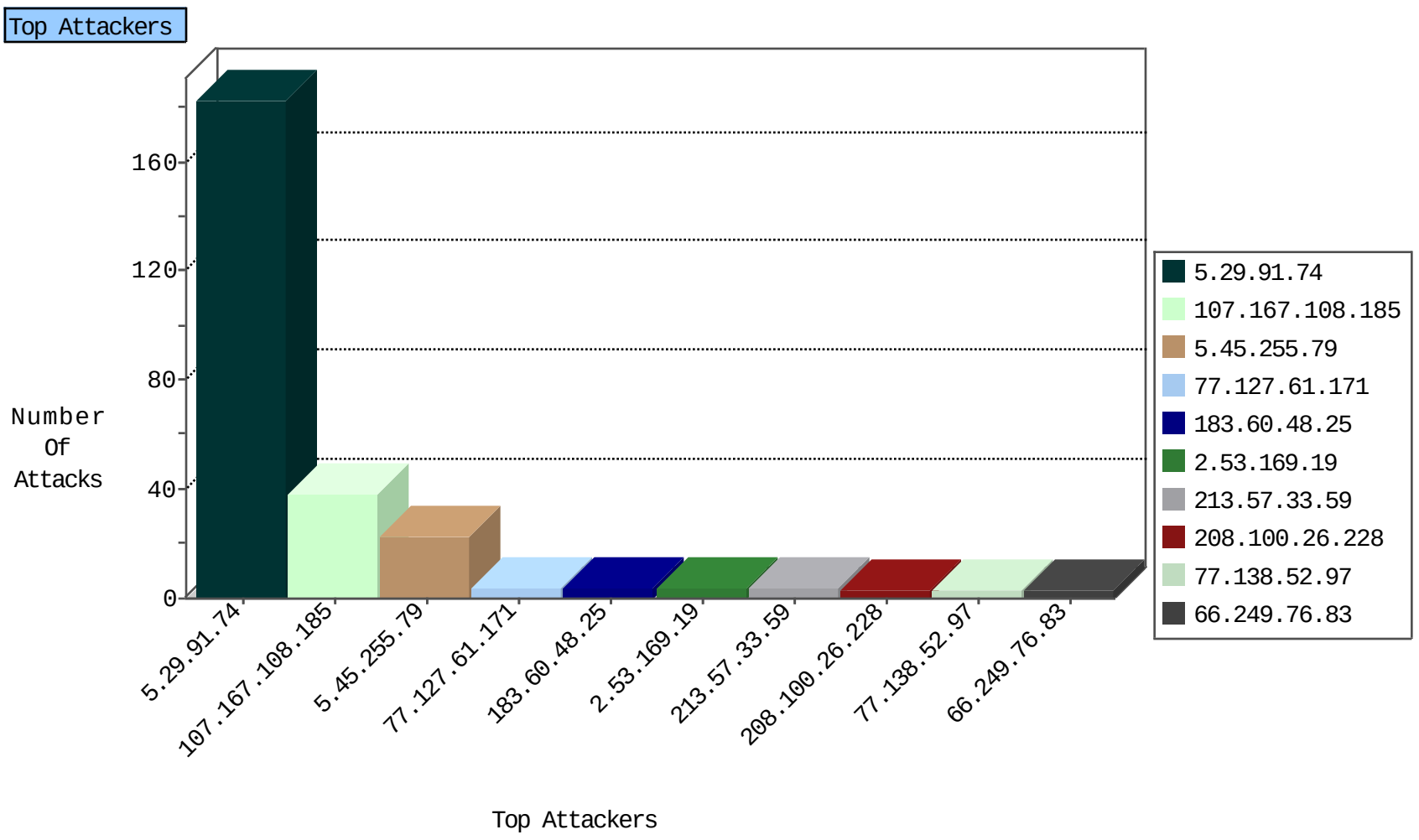
08-20-2016-09:04:04 to 08-20-2016-10:04:04

IDF Under Attack Daily Report





08-20-2016-09:04:04 to 08-20-2016-10:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.186.21.56	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	1
208.100.26.228	United States	147.237.76.30	himush.idf.il	Black List	drop	1
108.61.220.78	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1

08-20-2016-09:04:04 to 08-20-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-20-2016-09:04:04 to 08-20-2016-10:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
148.245.192.248	147.237.77.243	Mexico	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.72.14	Ukraine	dover.idf.il(old	ET SCAN NMAP -sS window 3072	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
5.255.90.133	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
185.93.185.235	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
179.43.141.228	147.237.76.199	Switzerland	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
123.123.119.180	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.72.14	Ukraine	dover.idf.il(old	ET SCAN NMAP -sS window 1024	1
49.145.237.179	147.237.0.33	Philippines	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
182.64.187.79	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-20-2016-09:04:04 to 08-20-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.167.108.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
5.45.255.79	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
77.127.61.171	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.169.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
208.6.46.45	United States	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	2
93.80.51.201	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.204.55.52	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
139.162.37.147	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.28	United States	147.237.0.200	m4u.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
40.77.167.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-20-2016-09:04:04 to 08-20-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.91.74	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	178
5.29.91.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
79.176.119.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.33.59	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
84.109.118.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.126.111	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.116.37.11	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
207.46.13.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.76.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/main792b.html	Block	1
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	1
66.249.73.174	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/m/	Block	1
213.57.33.59	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 213.57.33.59	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
40.77.167.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12535-he/dov	Block	1
94.228.3.110	Spain	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.73.198	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/mobile/	Block	1
213.57.33.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/6/	Block	1
68.180.229.49	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1233-he/atal.aspx	Block	1
46.116.37.11	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
139.162.13.205	Singapore	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/שקופית12	Block	1

08-20-2016-09:04:04 to 08-20-2016-10:04:04