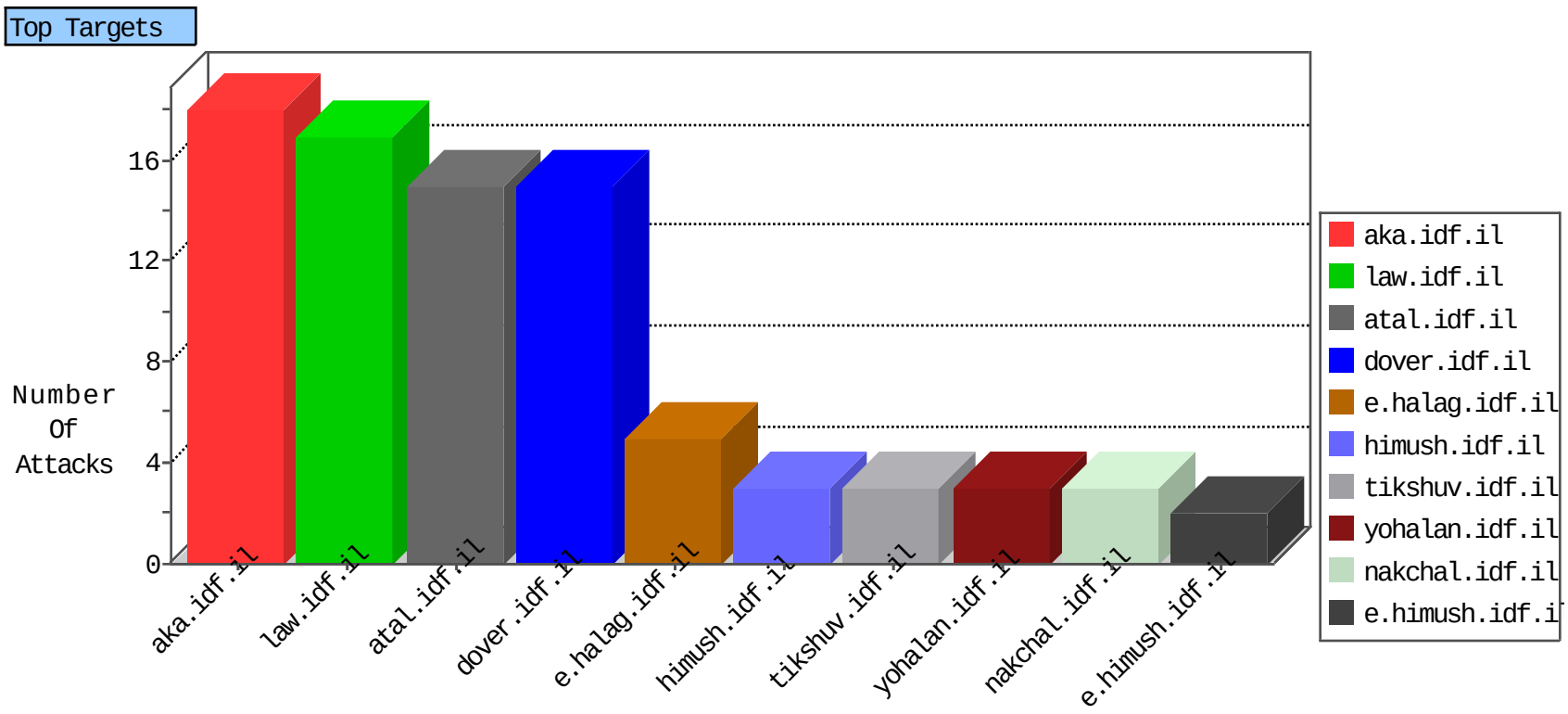
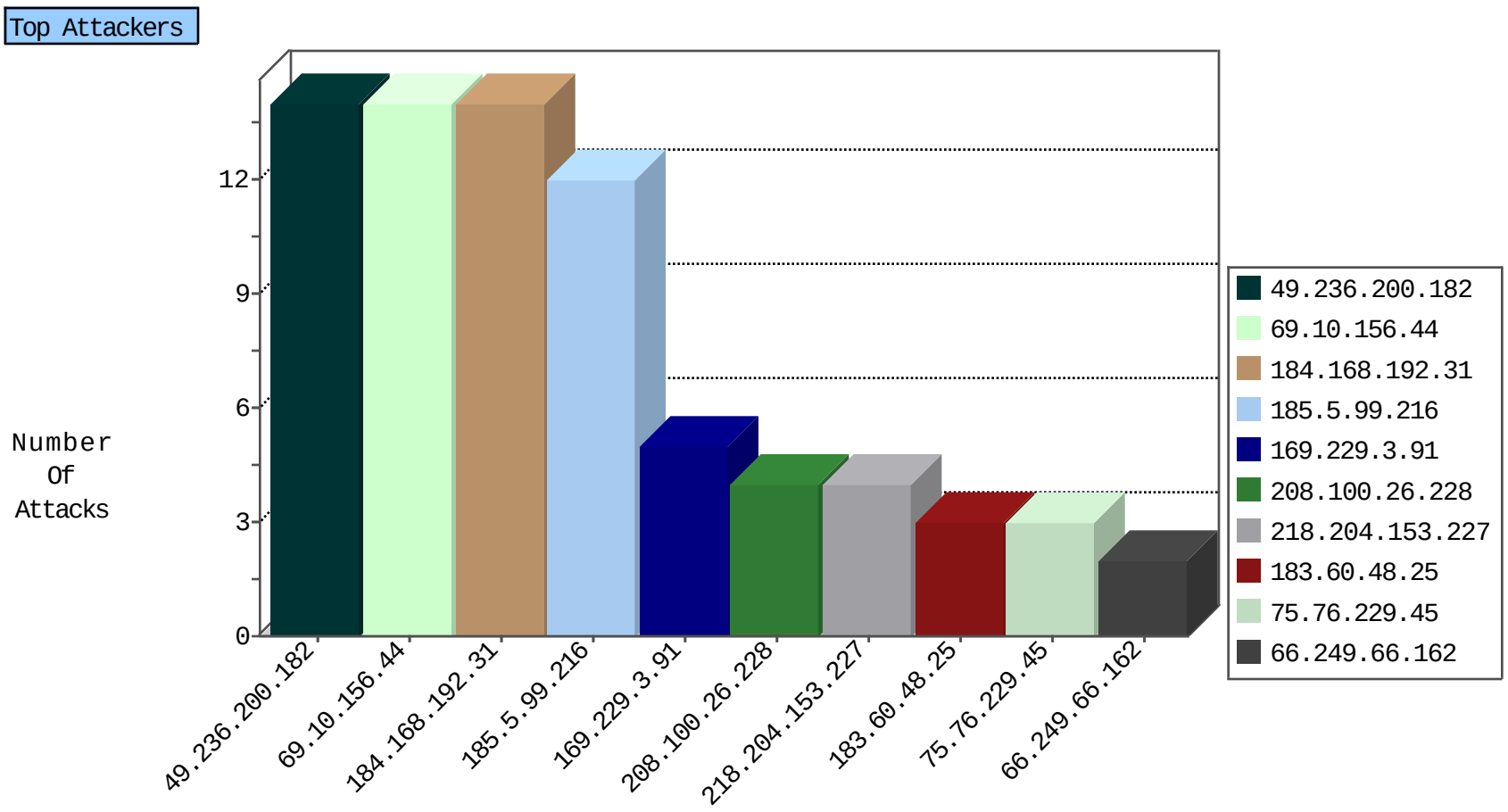
08-19-2016-02:04:00 to 08-19-2016-03:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-19-2016-02:04:00 to 08-19-2016-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.60.48.25	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
208.100.26.228	United States	147.237.76.86	navy.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
208.100.26.228	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

08-19-2016-02:04:00 to 08-19-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.168.192.31	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
49.236.200.182	Malaysia	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.10.156.44	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.30.198.202	United States	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
46.161.9.35	Russian Federation	147.237.77.74	law.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
151.80.31.172	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-19-2016-02:04:00 to 08-19-2016-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.168.192.31	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
69.10.156.44	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	8
49.236.200.182	147.237.72.166	Malaysia	aka.idf.il	SQL Injection - Select From	8
185.5.99.216	147.237.76.30	Poland	himush.idf.il	ET SCAN Potential SSH Scan	2
185.5.99.216	147.237.76.202	Poland	e.halag.idf.il	ET SCAN Potential SSH Scan	2
185.5.99.216	147.237.76.34	Poland	yohalan.idf.il	ET SCAN Potential SSH Scan	2
218.204.153.227	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
218.204.153.227	147.237.8.14	China	e.orchot.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
66.249.64.156	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
185.114.225.212	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 4096	1
54.153.99.128	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.5.99.216	147.237.76.199	Poland	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.5.99.216	147.237.76.176	Poland	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
185.5.99.216	147.237.76.39	Poland	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.204.153.227	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.20.183	147.237.77.226	Japan	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
218.204.153.227	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
186.116.70.97	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.97.8.128	147.237.76.31	India	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.5.99.216	147.237.76.197	Poland	e.himush.idf.il	ET SCAN Potential SSH Scan	1
41.249.55.253	147.237.76.30	Morocco	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.5.99.216	147.237.76.86	Poland	navy.idf.il	ET SCAN Potential SSH Scan	1
185.5.99.216	147.237.0.16	Poland	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

08-19-2016-02:04:00 to 08-19-2016-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.198	e.yohalan.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.227	e.hamaz.idf.il	drop	SAM rule	drop	1

08-19-2016-02:04:00 to 08-19-2016-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.76.229.45	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	3
213.151.38.122	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
74.64.44.168	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1/2871.ppt	Block	1
31.209.138.74	Iceland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.188	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
66.249.65.176	Israel	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to 147.237.76.31/1073-he/nakhal.aspx	Block	1
66.249.76.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
82.221.105.6	Iceland	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.162	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.164	United States	147.237.0.34	tikshuv.idf.i	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
5.102.195.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1

08-19-2016-02:04:00 to 08-19-2016-03:04:00