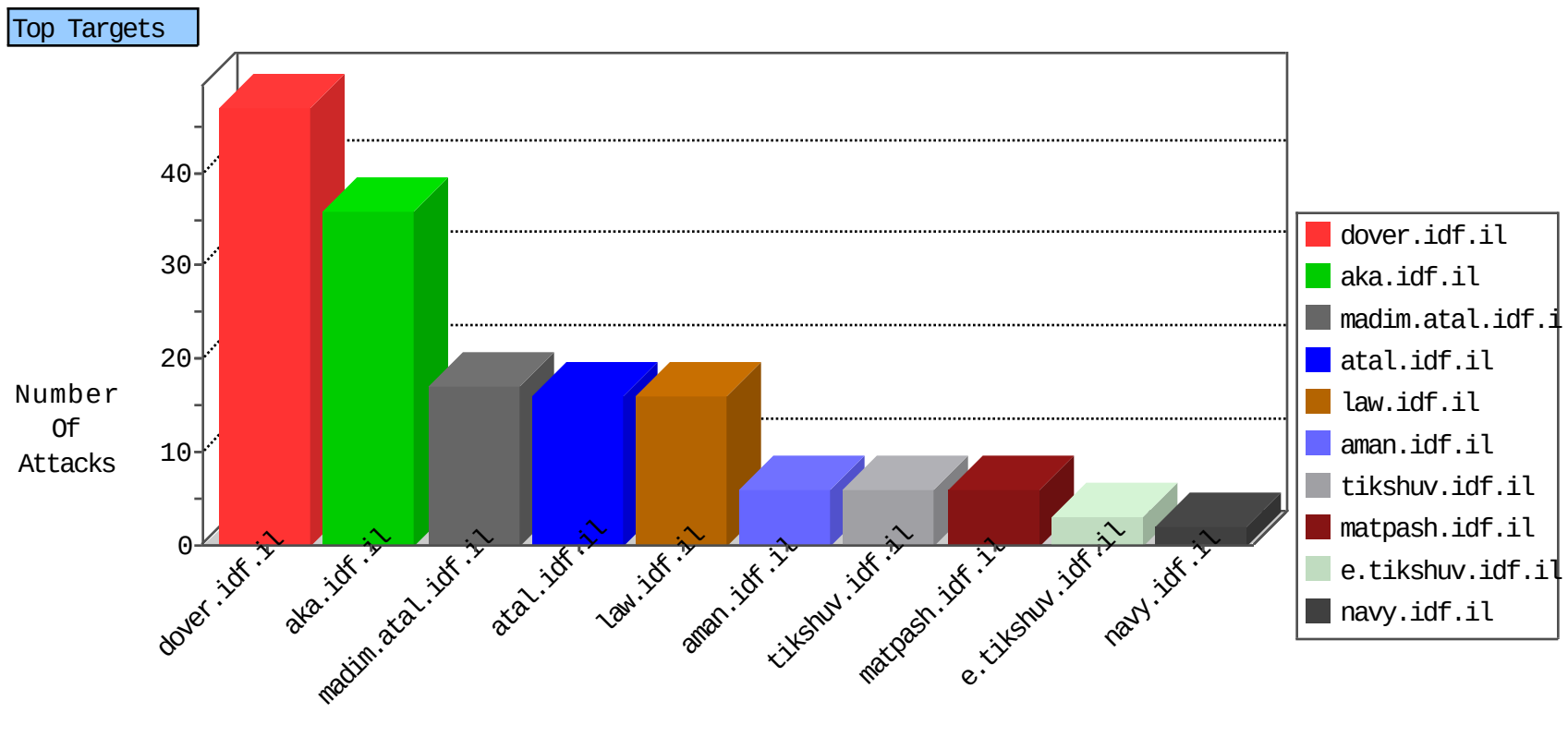
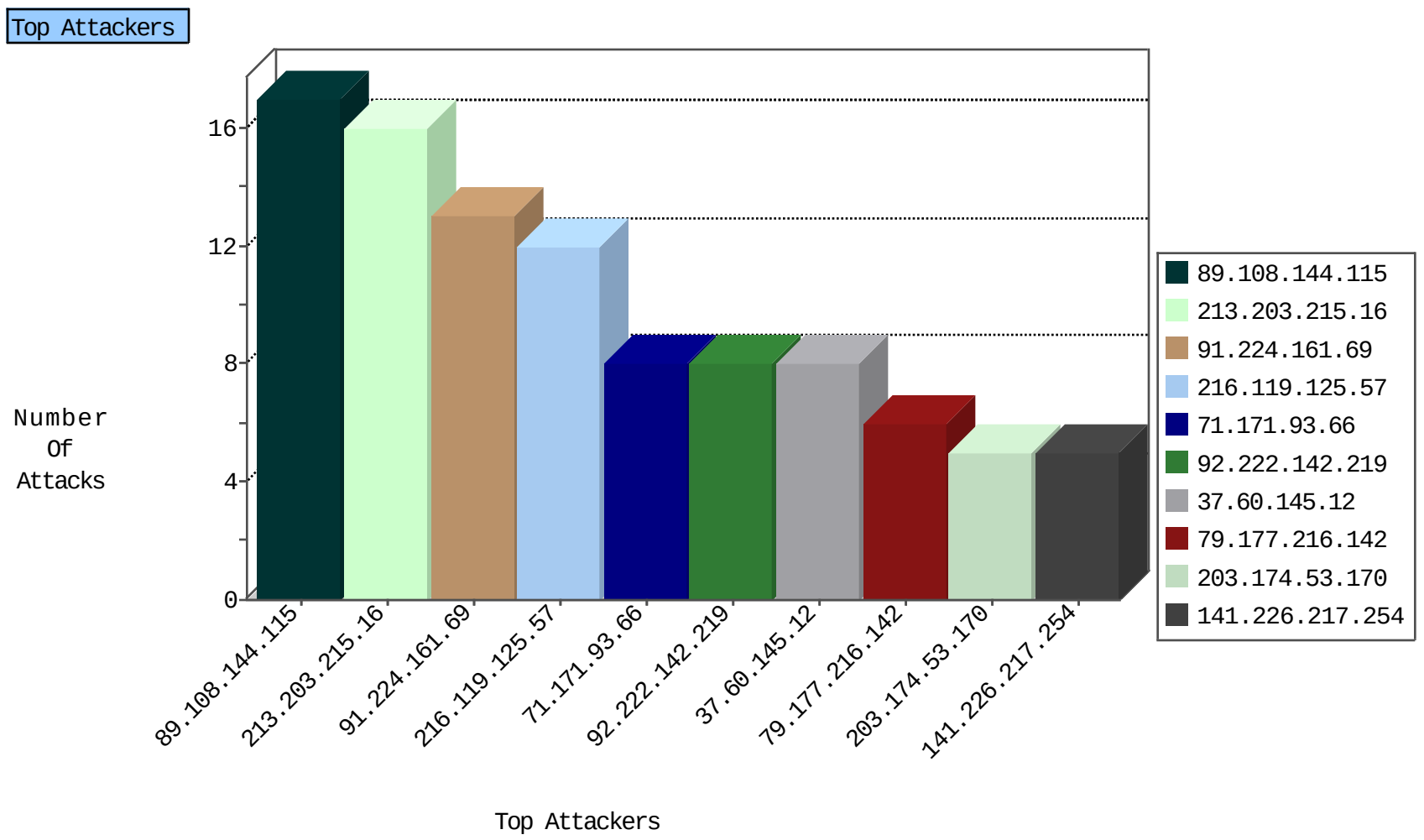
09-03-2016-11:04:09 to 09-03-2016-12:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-03-2016-11:04:09 to 09-03-2016-12:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-11:04:09 to 09-03-2016-12:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-11:04:09 to 09-03-2016-12:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.203.215.16	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	16
216.119.125.57	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	12
92.222.142.219	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	8
71.171.93.66	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
91.224.161.69	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	2
175.142.129.124	147.237.77.216	Malaysia	dover.idf.il	Xenu Link Sleuth User Agent	2
91.224.161.69	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
189.83.227.63	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.161.69	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
122.224.250.234	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.179.62.193	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
103.207.36.84	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
5.255.90.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
103.207.36.84	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

09-03-2016-11:04:09 to 09-03-2016-12:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.108.144.115	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
141.226.217.254	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
37.60.145.12	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
37.60.145.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
217.132.102.181	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
188.225.150.184	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
188.225.150.184	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
223.24.78.12	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.0.200	m4u.idf.il	drop		drop	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.120.124.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
213.233.203.110	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-03-2016-11:04:09 to 09-03-2016-12:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.216.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.178.83.207	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
203.174.53.170	Hong Kong	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	4
85.65.5.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
85.65.79.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.65.4.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.245.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.120.124.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
77.138.80.126	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
176.13.251.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.64.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
77.138.94.85	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
79.180.118.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
77.138.229.34	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
194.72.238.241	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
78.46.84.199	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
5.22.135.203	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
203.174.53.170	Hong Kong	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.218.101.207	Switzerland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1380-21438-he/dover.aspx	Block	1
79.177.19.1	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter WT.mc_id in www.aka.idf.il/ishurim/main	None	1
37.26.147.140	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.94.123.127	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.69.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/masaiyot04012011.aspx	Block	1
66.249.76.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19883-he/idfgdover.aspx	Block	1

09-03-2016-11:04:09 to 09-03-2016-12:04:09