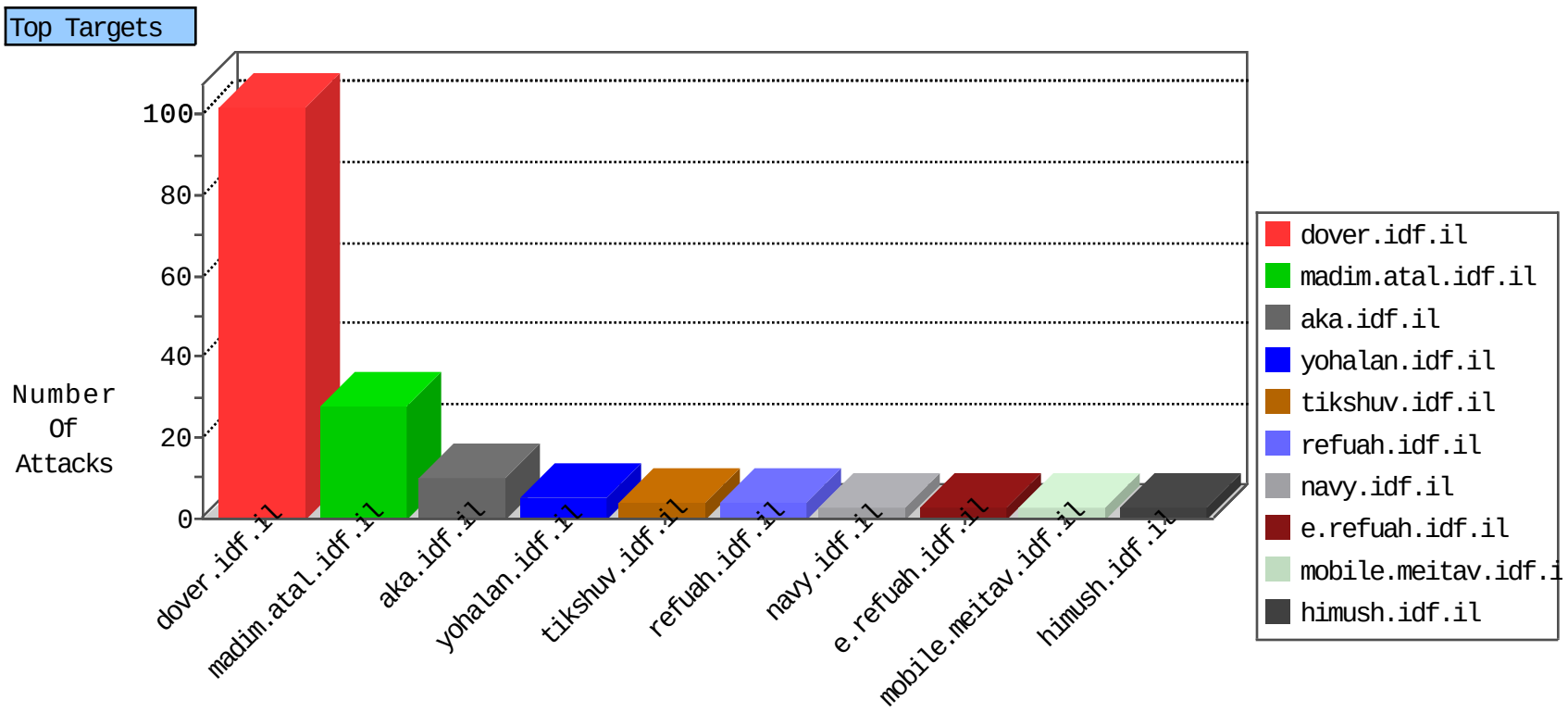
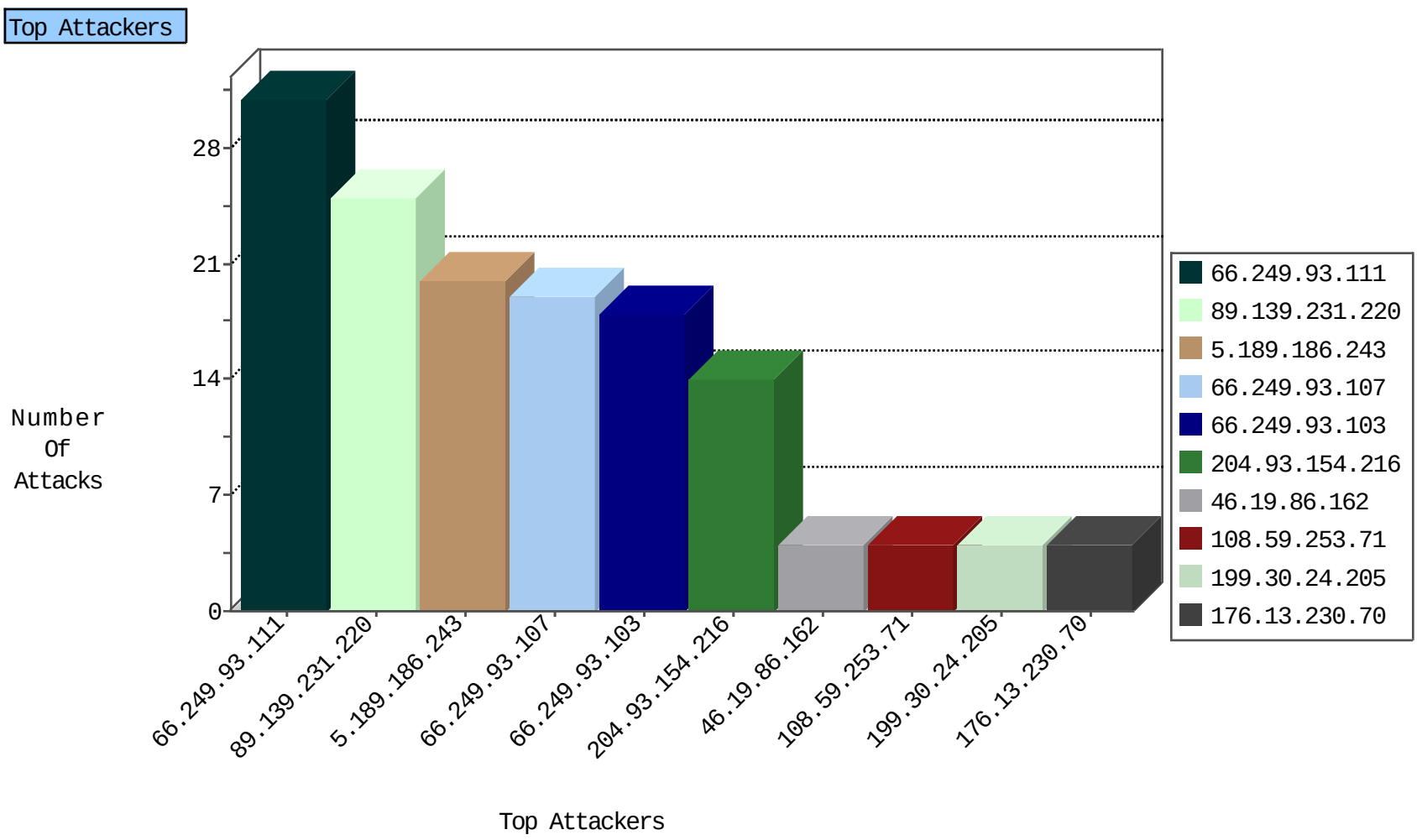
09-02-2016-01:10:13 to 09-02-2016-02:10:13

IDF Under Attack Daily Report





09-02-2016-01:10:13 to 09-02-2016-02:10:13

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	179
199.30.24.205	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
108.59.253.71	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
5.189.186.243	Germany	147.237.76.86	navy.idf.il	Black List	drop	3
66.249.93.111	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
5.189.186.243	Germany	147.237.76.38	e.e.meitav.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
66.249.93.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
5.189.186.243	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	1
217.23.9.123	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.30	himush.idf.il	Black List	drop	1
110.173.16.166	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
5.189.186.243	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.176	test.ncore.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.31	nakchal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.42	refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.177	ncore.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

09-02-2016-01:10:13 to 09-02-2016-02:10:13

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-01:10:13 to 09-02-2016-02:10:13

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
204.93.154.216	147.237.77.216	United States	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
190.252.36.163	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.224.250.234	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
110.173.16.166	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
217.165.67.151	147.237.72.167	United Arab Emirates	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
122.224.250.234	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
110.173.16.166	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
217.165.67.151	147.237.72.167	United Arab Emirates	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1

09-02-2016-01:10:13 to 09-02-2016-02:10:13

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	26
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	18
66.249.93.103	Europe	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	15
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
81.18.218.190	Poland	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
89.139.212.12	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
176.221.173.252	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
141.212.122.59	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
119.105.137.31	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.249.93.103	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
183.129.160.229	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.58	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

09-02-2016-01:10:13 to 09-02-2016-02:10:13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.231.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
176.13.230.70	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 176.13.230.70	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	2
180.76.15.32	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.162	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
188.162.229.197	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	1
41.226.107.226	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
128.232.110.28	United Kingdom	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
46.19.86.162	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method /Style/1.HE/960.css in URL www.tikshuv.idf.ilhttp/1.1	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.19.85.139	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers Referer	Block	1
176.13.230.70	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
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.162	Israel	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
204.93.154.216	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Distributed URL is Above Root Directory	Block	1
46.19.86.162	Israel	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version	Block	1

09-02-2016-01:10:13 to 09-02-2016-02:10:13