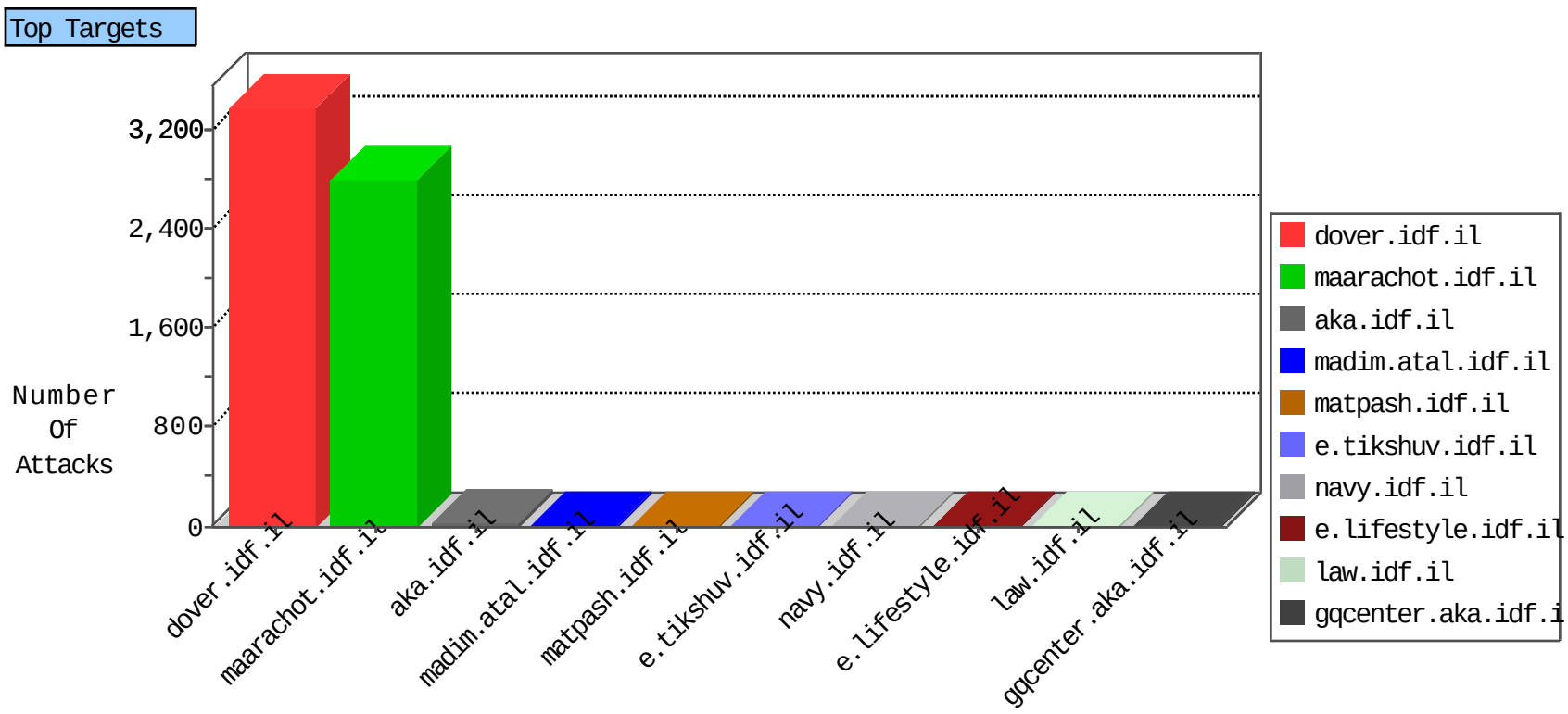
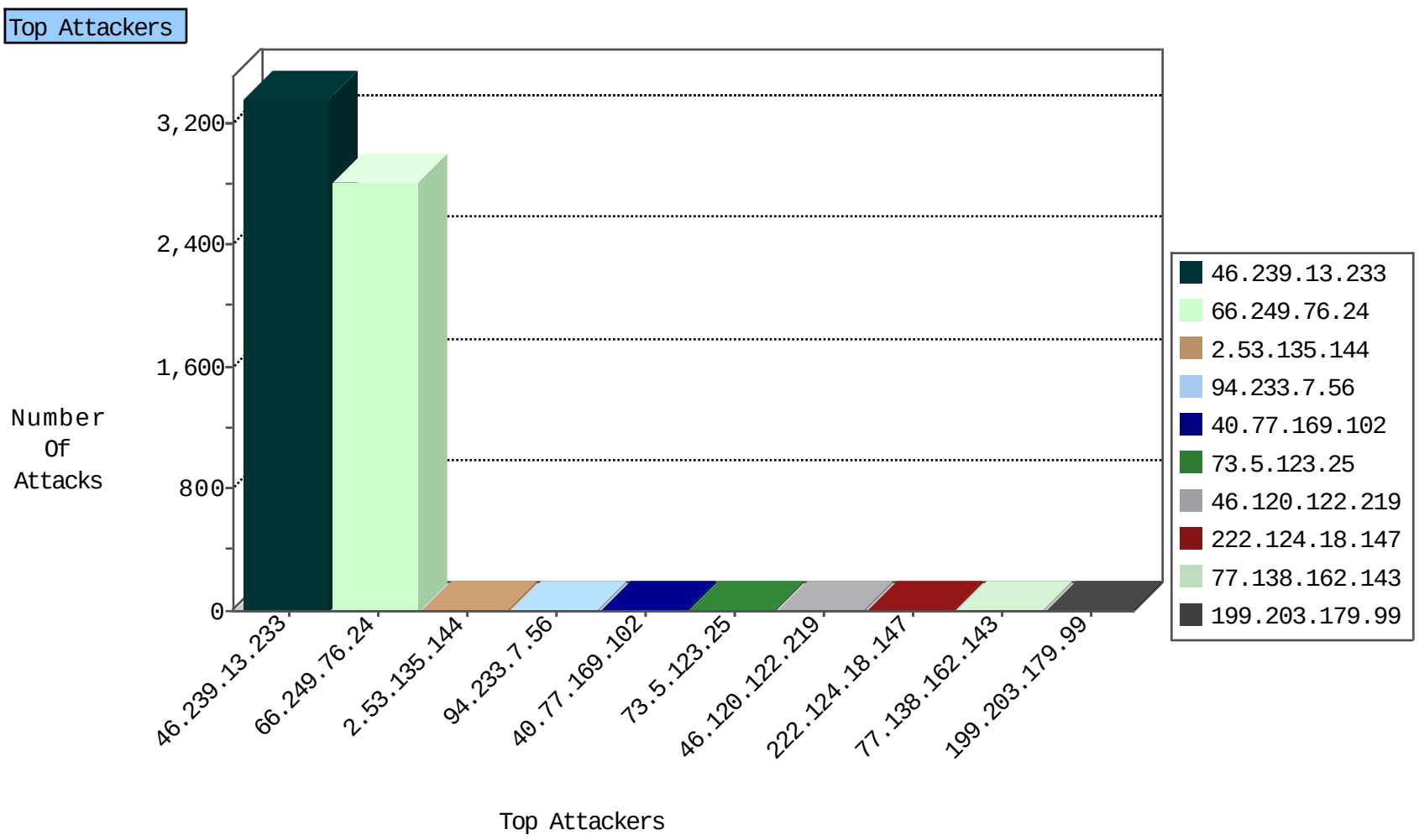
08-29-2016-05:04:09 to 08-29-2016-06:04:09

IDF Under Attack Daily Report





08-29-2016-05:04:09 to 08-29-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
218.205.132.103	China	147.237.0.15	kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	1
123.59.59.52	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1
5.189.136.84	Germany	147.237.76.86	navy.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1

08-29-2016-05:04:09 to 08-29-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.123.116	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
93.180.64.135	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-29-2016-05:04:09 to 08-29-2016-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.76.24	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2806
104.232.98.38	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
94.233.7.56	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
94.233.7.56	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
222.124.18.147	147.237.76.34	Indonesia	yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.233.7.56	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
222.124.18.147	147.237.72.166	Indonesia	aka.idf.il	ET SCAN Potential SSH Scan	1
94.233.7.56	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
222.124.18.147	147.237.0.33	Indonesia	idf.il	ET SCAN Potential SSH Scan	1
94.233.7.56	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.187	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
161.18.109.133	147.237.77.216	Colombia	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.68.210.118	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.38	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
13.68.210.118	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
94.233.7.56	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
94.233.7.56	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
222.124.18.147	147.237.76.86	Indonesia	navy.idf.il	ET SCAN Potential SSH Scan	1
94.233.7.56	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	1
222.124.18.147	147.237.72.217	Indonesia	e.idf.il	ET SCAN Potential SSH Scan	1
94.233.7.56	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.124.18.147	147.237.72.14	Indonesia	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
94.233.7.56	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.149	147.237.77.74	Ukraine	law.idf.il	ET SCAN NMAP -sS window 1024	1
94.233.7.56	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
161.18.141.140	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
13.68.210.118	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1

08-29-2016-05:04:09 to 08-29-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3156
46.239.13.233	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	200
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	9
46.120.122.219	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
199.203.179.99	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	4
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		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
199.58.86.211	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
162.243.71.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
107.77.160.30	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
46.120.122.219	Israel	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
109.253.212.75	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
46.120.122.219	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
40.77.167.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.50	e.tikshuv.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

08-29-2016-05:04:09 to 08-29-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.135.144	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	13
77.138.162.143	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar	Block	5
73.5.123.25	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 73.5.123.25	Block	4
73.5.123.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
194.242.174.233	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
37.26.148.236	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
100.37.104.248	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
207.46.13.153	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/forums/forums.asp	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
37.142.0.148	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
131.253.25.199	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.229.35.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-23183-he/dover.aspx	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
91.200.12.60	Ukraine	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.88.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
37.26.148.140	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
100.37.104.248	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 100.37.104.248	Block	1
73.5.123.25	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1

08-29-2016-05:04:09 to 08-29-2016-06:04:09