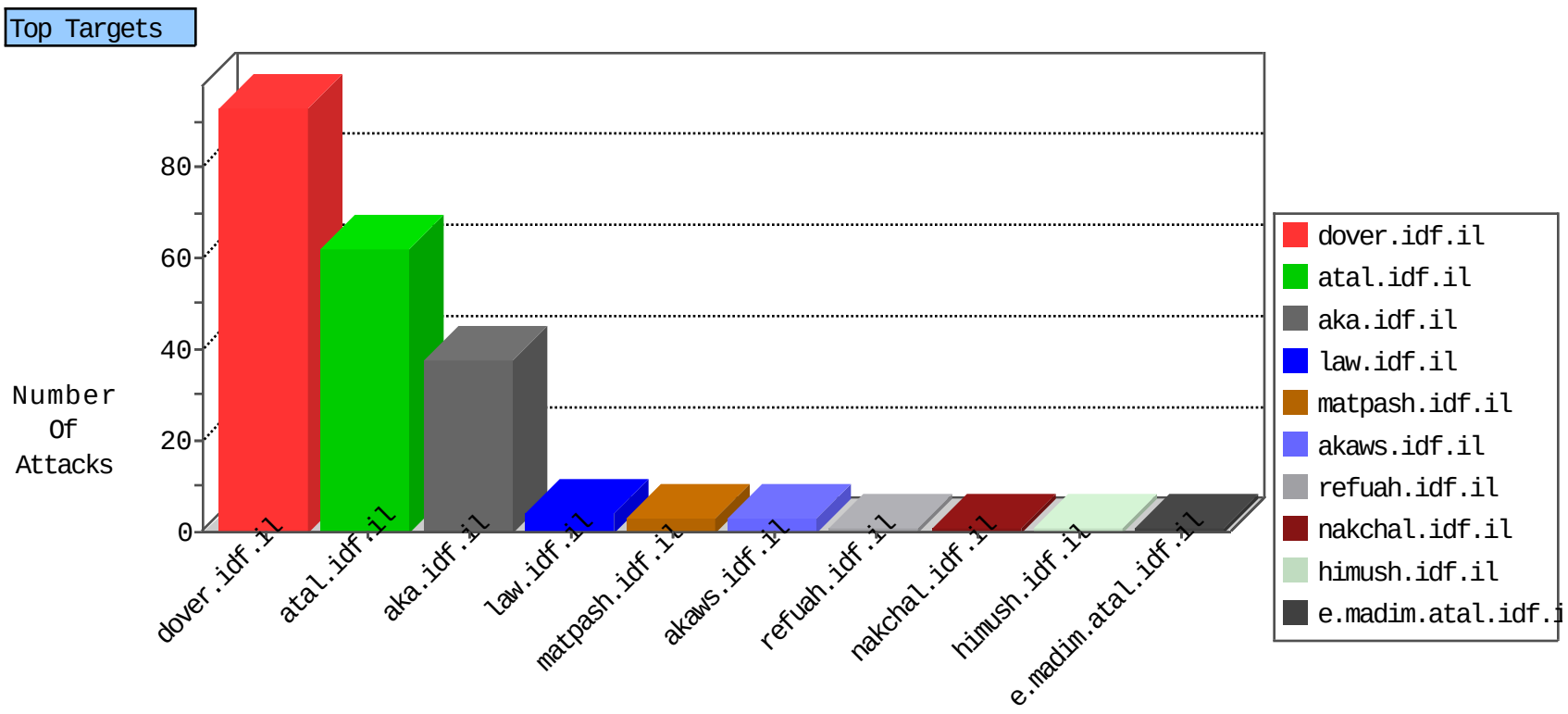
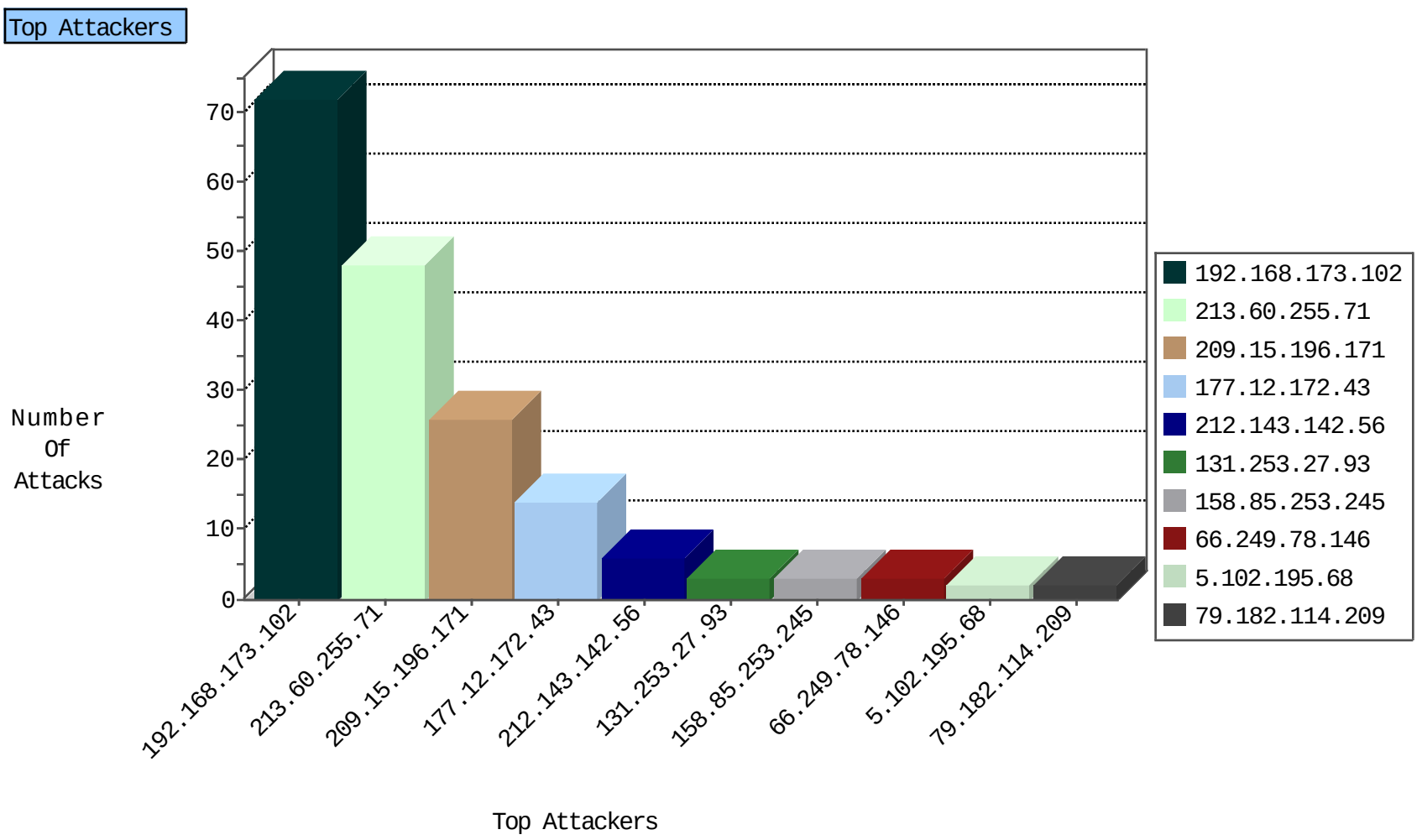
08-17-2016-05:04:04 to 08-17-2016-06:04:04

IDF Under Attack
Daily Report





08-17-2016-05:04:04 to 08-17-2016-06:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1

08-17-2016-05:04:04 to 08-17-2016-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.15.196.171	Canada	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
213.60.255.71	Spain	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
177.12.172.43	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.171	Canada	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
158.85.253.245	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
158.85.253.245	United States	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
69.163.163.224	United States	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-17-2016-05:04:04 to 08-17-2016-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.60.255.71	147.237.77.233	Spain	atal.idf.il	SQL Injection - Select From	36
177.12.172.43	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	8
209.15.196.171	147.237.72.166	Canada	aka.idf.il	SQL Injection - Select From	6
200.118.123.46	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.139.132.252	147.237.8.27	Malaysia	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.64.147	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1

08-17-2016-05:04:04 to 08-17-2016-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	72
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
186.43.168.219	Ecuador	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
61.3.107.240	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
69.63.188.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
137.116.71.170	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.204	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.114	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.219	United States	147.237.0.200	m4u.idf.il	drop		drop	1

08-17-2016-05:04:04 to 08-17-2016-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.27.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.101	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.182.114.209	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.102.195.68	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/שקופית4	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59268&docid=65415	Block	1
79.182.114.209	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
66.249.64.144	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/602-2265-he/patzar.aspx - paragraph_12	Block	1
190.24.58.229	Colombia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/	Block	1
66.249.83.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.136.198	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 80.246.136.198 (Open Mode)	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
68.180.229.116	United States	147.237.76.31	nakchal.idf.i	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	1
80.246.136.198	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/selectusertype.asp	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=4&catid=22705&docid=58728	Block	1
71.6.135.131	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
5.102.195.68	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.108.48.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter reffer in www.aka.idf.il/ishurim/main	None	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1

08-17-2016-05:04:04 to 08-17-2016-06:04:04