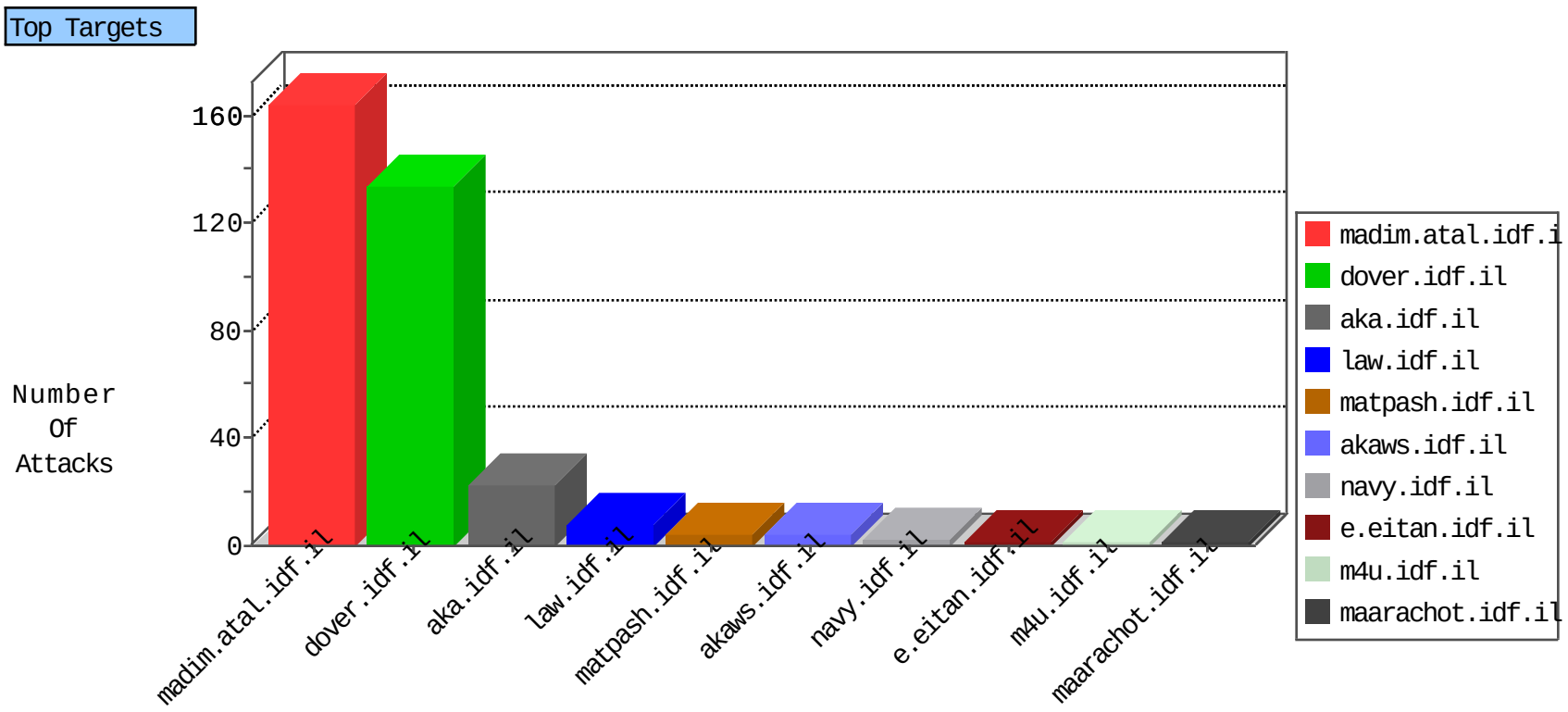
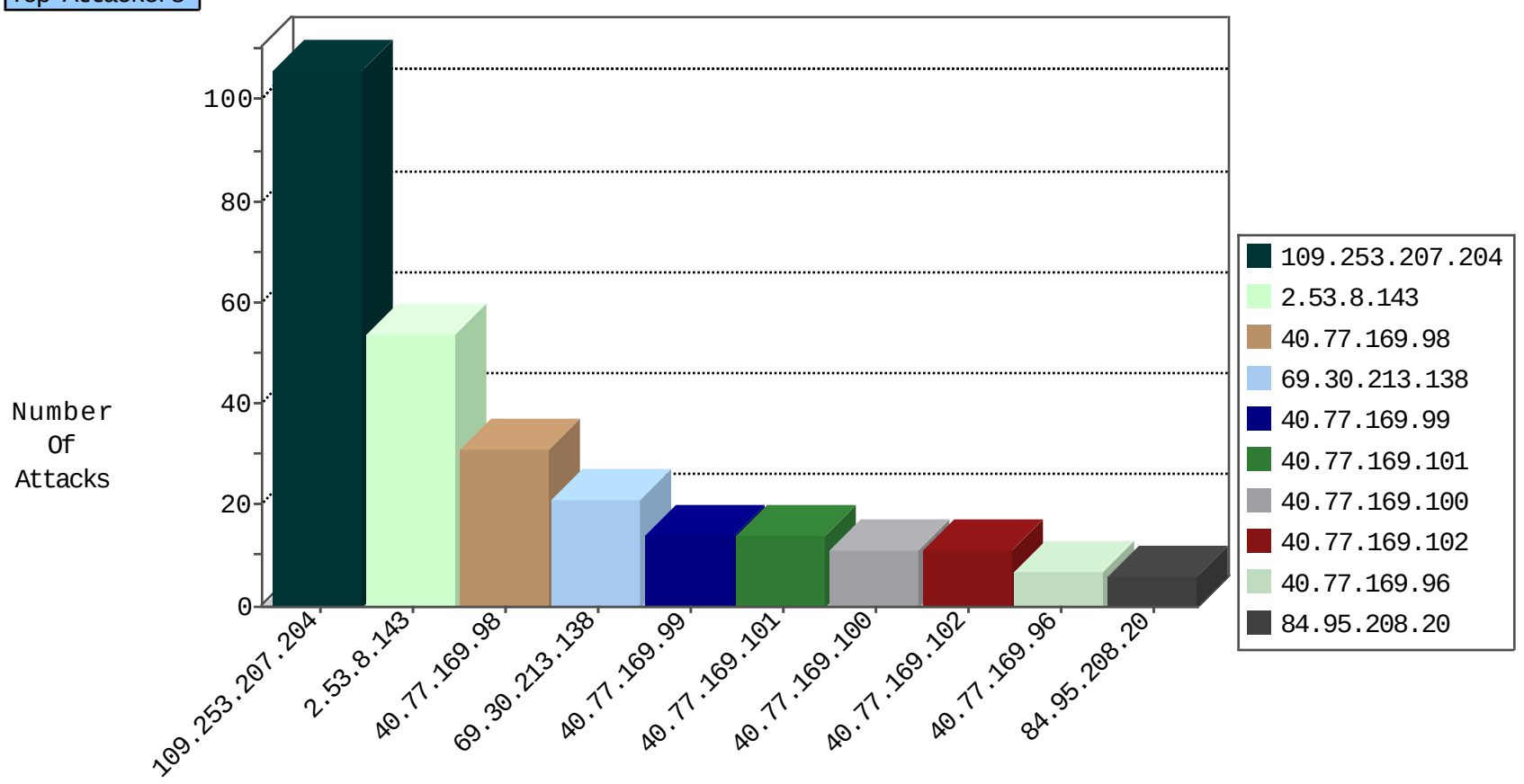
08-23-2016-06:04:02 to 08-23-2016-07:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-23-2016-06:04:02 to 08-23-2016-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.177.160.214	Romania	147.237.76.42	refuah.idf.il	Black List	drop	1
96.55.69.67	Canada	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
66.240.219.146	United States	147.237.76.86	navy.idf.il	Black List	drop	1
71.6.146.185	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1

08-23-2016-06:04:02 to 08-23-2016-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.213.138	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	19
62.210.148.246	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.213.138	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-23-2016-06:04:02 to 08-23-2016-07:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
186.114.96.119	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.227.112.24	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1
14.211.210.76	147.237.8.45	China	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.88.208.193	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.106	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1

08-23-2016-06:04:02 to 08-23-2016-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
74.82.47.34	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
192.40.95.3	Finland	147.237.0.35	akaws.idf.il	drop		drop	1
200.0.33.82	Brazil	147.237.0.200	m4u.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.93	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.78	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.94	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-23-2016-06:04:02 to 08-23-2016-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.207.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
2.53.8.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	8
40.77.169.96	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
2.53.149.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
156.202.64.19	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 156.202.64.19	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.99	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	2
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
31.154.5.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
207.46.13.18	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.177.62.59	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.85.158	Block	1
212.150.214.90	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	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
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/redirects/ssl-redirect.html	Block	1
40.77.169.96	United States	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
207.46.13.39	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
84.94.181.163	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 84.94.181.163 (Open Mode)	None	1
62.90.49.16	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
212.150.214.90	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
103.63.24.177	India	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
207.46.13.126	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/klali/default.asp	None	1
84.94.181.163	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
62.90.49.16	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	1
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.78	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
40.77.169.100	United States	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
31.154.5.181	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.138.69.154	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/giyus/	Block	1
40.77.169.104	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1226-	Block	1
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	1

08-23-2016-06:04:02 to 08-23-2016-07:04:02