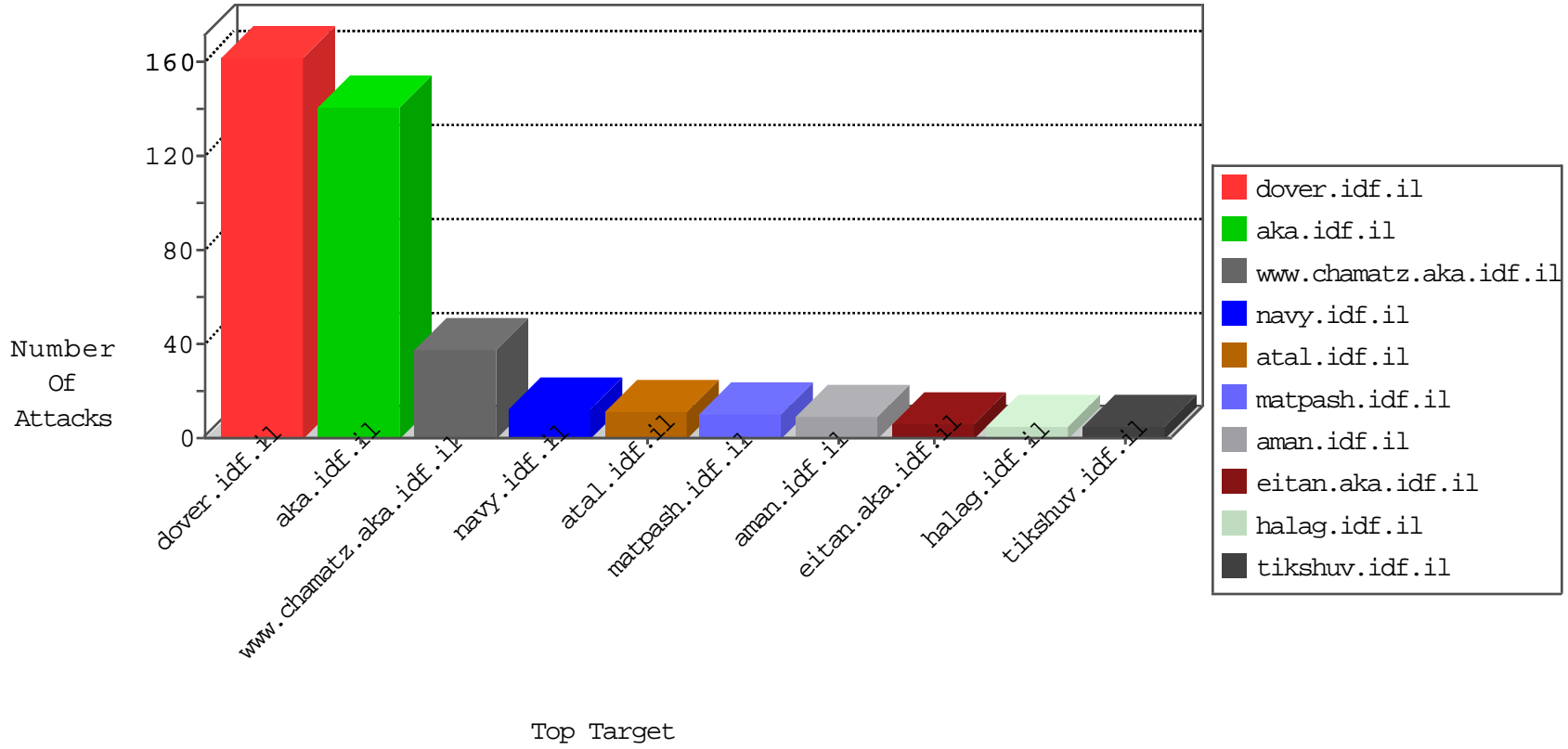


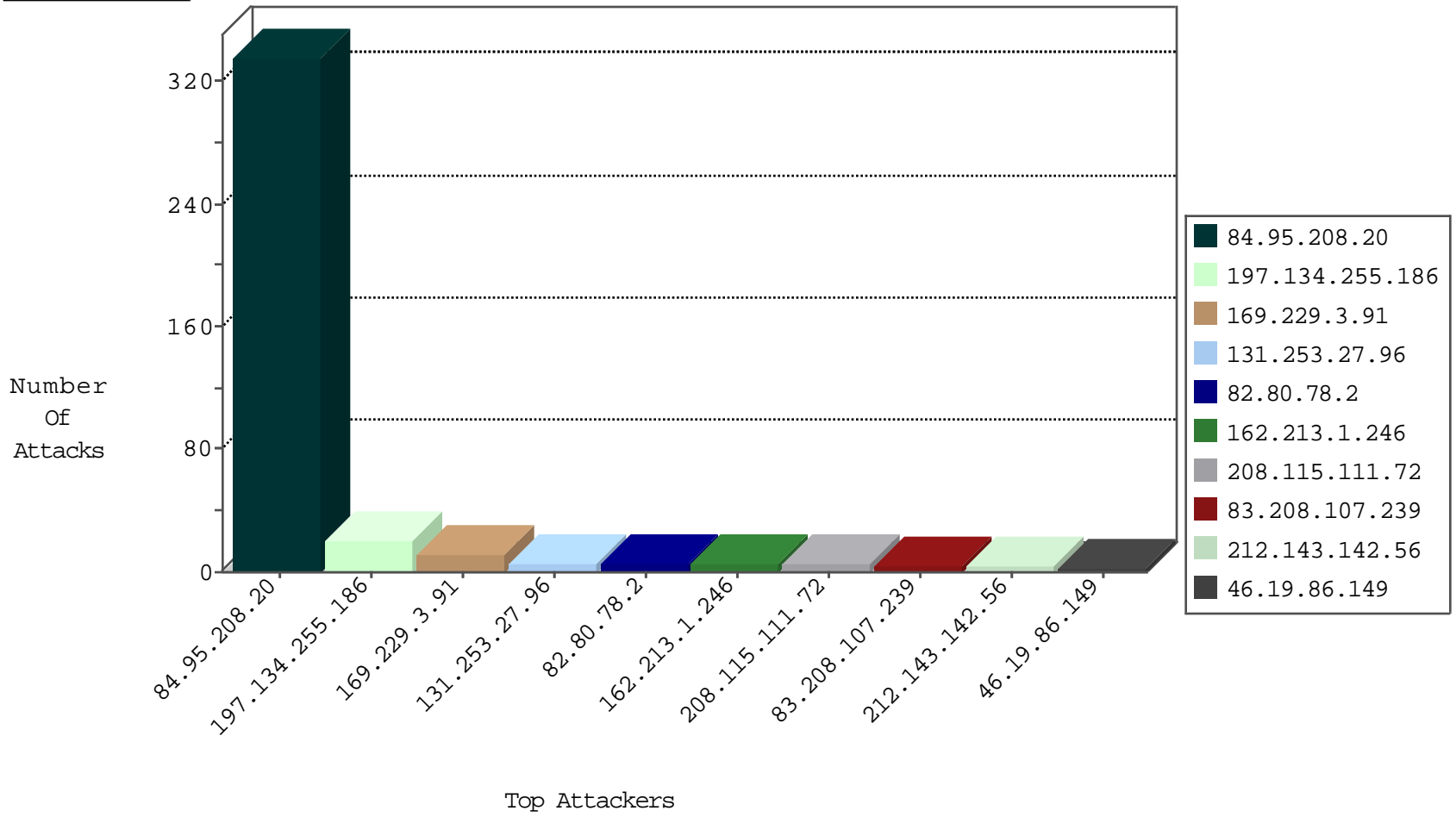
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
113.105.82.158	China	147.237.72.14	dover.idf.il(old)	Invalid TCP Flags	drop	1
84.108.92.237	Israel	147.237.76.31	nakchal.idf.il	network flood IPv4 TCP-RST	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
78.174.112.116	Turkey	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Permit	1
78.174.112.116	Turkey	147.237.77.176	matpash.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

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
151.80.40.87	147.237.77.176	France	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.134.255.186	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
83.208.107.239	Czech Republic	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.184.12.134	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
176.106.47.169	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.33	idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
141.212.122.27	United States	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1
141.212.122.28	United States	147.237.0.33	idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	134
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	104
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	27
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	13
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	10
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
131.253.27.96	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/gyus/forum/asp/showforum.asp	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
162.219.173.228	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
193.252.118.176	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
46.229.164.102	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-22850-he/dover.aspx	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
207.46.13.39	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/slider.js	Block	1
131.253.27.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1