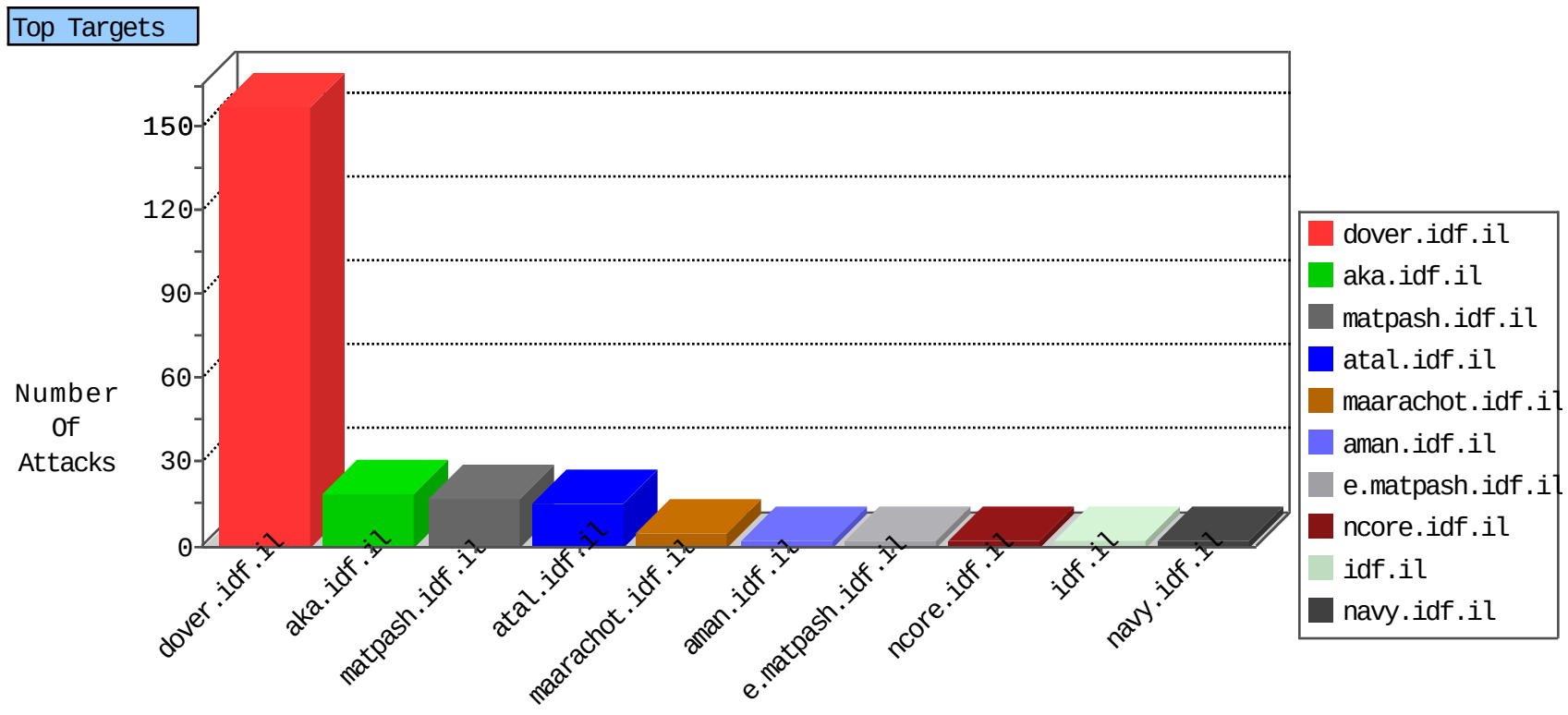
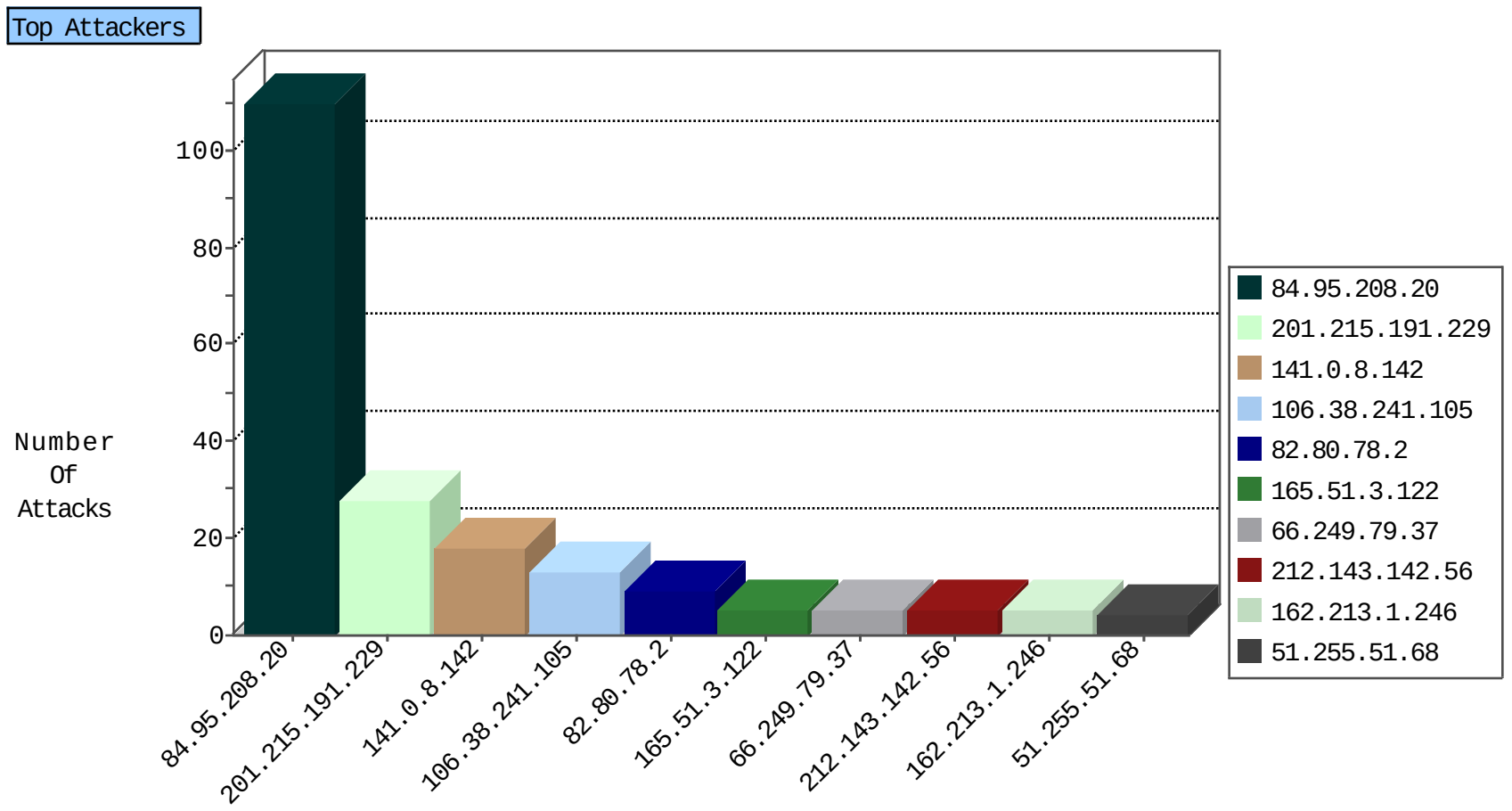
08-23-2016-04:04:01 to 08-23-2016-05:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-23-2016-04:04:01 to 08-23-2016-05:04:01

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	9
183.60.48.25	China	147.237.0.33	idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
138.59.16.54	Costa Rica	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
222.186.21.163	China	147.237.76.31	nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
104.237.48.102	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
138.59.16.55	Costa Rica	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
61.136.195.22	China	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
104.237.48.103	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
138.59.16.56	Costa Rica	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
61.136.195.22	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	1
104.237.48.105	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

08-23-2016-04:04:01 to 08-23-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.51.68	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.51.68	France	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2
78.142.19.172	Bulgaria	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
78.109.24.97	Ukraine	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-23-2016-04:04:01 to 08-23-2016-05:04:01

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
201.215.191.229	147.237.77.74	Chile	law.idf.il	ET SCAN Potential SSH Scan	2
201.215.191.229	147.237.76.201	Chile	e.atal.idf.il	ET SCAN Potential SSH Scan	2
201.215.191.229	147.237.76.177	Chile	ncore.idf.il	ET SCAN Potential SSH Scan	2
201.215.191.229	147.237.76.38	Chile	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
201.215.191.229	147.237.77.176	Chile	matpash.idf.il	ET SCAN Potential SSH Scan	2
201.215.191.229	147.237.76.86	Chile	navy.idf.il	ET SCAN Potential SSH Scan	2
201.215.191.229	147.237.77.178	Chile	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
180.97.75.130	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
112.124.10.141	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
201.215.191.229	147.237.76.197	Chile	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
27.100.198.60	147.237.8.14	Korea, Republic of	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.215.191.229	147.237.77.235	Chile	sviva.idf.il	ET SCAN Potential SSH Scan	1
201.215.191.229	147.237.76.44	Chile	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
201.215.191.229	147.237.77.227	Chile	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
201.215.191.229	147.237.77.216	Chile	dover.idf.il	ET SCAN Potential SSH Scan	1
195.88.208.193	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.75.130	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
201.215.191.229	147.237.77.121	Chile	e.navy.idf.il	ET SCAN Potential SSH Scan	1
201.215.191.229	147.237.77.61	Chile	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
201.215.191.229	147.237.76.198	Chile	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -f -sS	1
201.215.191.229	147.237.76.196	Chile	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
201.215.191.229	147.237.77.243	Chile	mobile.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.76.39	Czech Republic	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
201.215.191.229	147.237.77.233	Chile	atal.idf.il	ET SCAN Potential SSH Scan	1
201.215.191.229	147.237.76.39	Chile	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
201.215.191.229	147.237.77.226	Chile	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
195.88.208.193	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
186.170.245.255	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.215.191.229	147.237.77.170	Chile	maarachot.idf.il	ET SCAN Potential SSH Scan	1

08-23-2016-04:04:01 to 08-23-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.8.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
165.51.3.122	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.22.74	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
184.105.247.215	United States	147.237.0.35	akaws.idf.il	drop		drop	1
67.215.23.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-23-2016-04:04:01 to 08-23-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	95
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	5
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	5
77.138.153.228	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	3
77.138.247.127	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
66.249.73.209	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to chinuch.aka.idf.il/894-he	Block	1
157.55.39.21	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/1026-he/cogat.aspx	Block	1
72.82.254.244	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
64.137.244.235	Canada	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.137.244.235	Canada	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 64.137.244.235	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
207.46.13.126	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
77.138.247.127	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
64.137.244.235	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/admin/cms_wysiwyg/directive/index/	Block	1
66.249.79.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1

08-23-2016-04:04:01 to 08-23-2016-05:04:01