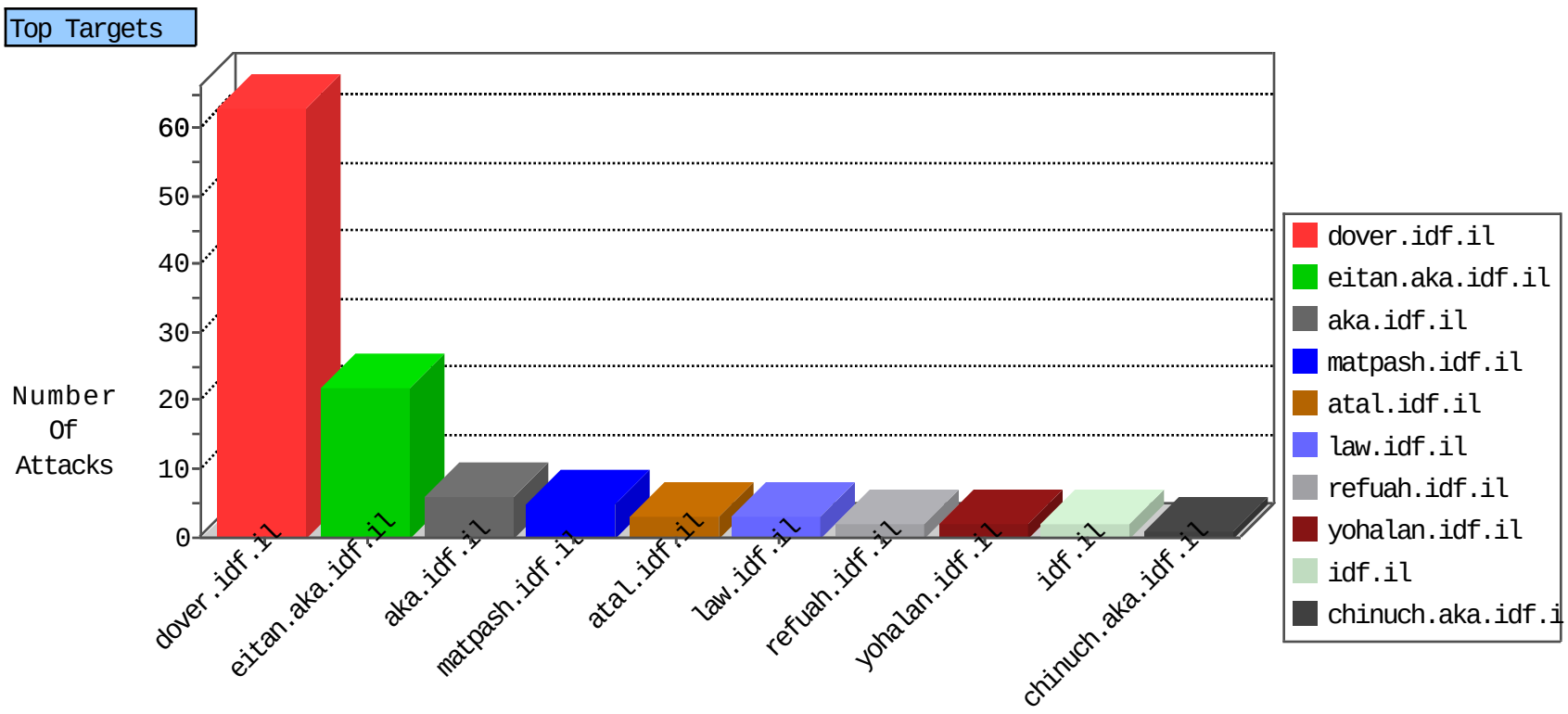
08-22-2016-05:04:02 to 08-22-2016-06:04:02

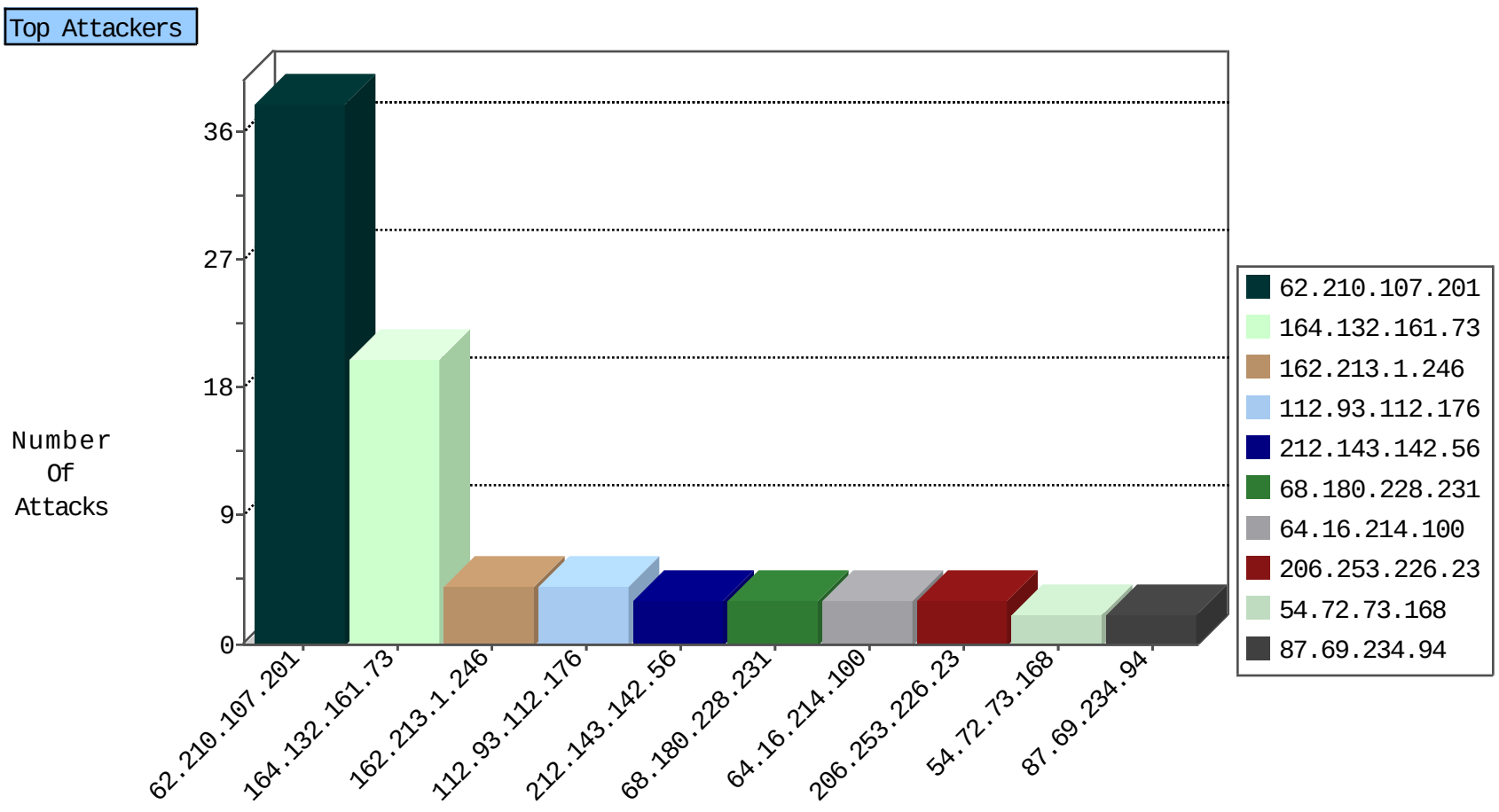
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-22-2016-05:04:02 to 08-22-2016-06:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.132.161.73	Italy	147.237.76.200	eitan.aka.idf.il	TCP handshake violation, first packet not syn	drop	14938
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
209.126.136.2	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	1

08-22-2016-05:04:02 to 08-22-2016-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.107.201	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	36
62.210.107.201	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
82.221.105.7	Iceland	147.237.76.197	e.himush.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
51.255.65.36	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.73	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.61	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-22-2016-05:04:02 to 08-22-2016-06:04:02

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	4
162.250.190.142	147.237.77.216	Canada	dover.idf.il	Xenu Link Sleuth User Agent	2
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1

08-22-2016-05:04:02 to 08-22-2016-06:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.118.73.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.226.144.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.80.14.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.91	United States	147.237.0.33	idf.il	drop		drop	1
61.148.115.22	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.92	United States	147.237.0.33	idf.il	drop		drop	1
64.16.214.100	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
64.16.214.100	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
177.11.161.136	Brazil	147.237.76.34	yohalan.idf.il	drop		drop	1
45.79.156.96	United States	147.237.0.200	m4u.idf.il	drop		drop	1

08-22-2016-05:04:02 to 08-22-2016-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
112.93.112.176	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.93.112.176	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
87.69.234.94	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1764	Block	1
206.253.226.23	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
112.93.112.176	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
206.253.226.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
68.180.228.99	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
206.253.226.23	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
40.77.167.66	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
149.56.223.98	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/blog/	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1962-he/cogat.aspx	Block	1
217.132.37.157	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in refua.atal.idf.il/938-he/refuah.aspx	Block	1
87.69.234.94	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
64.16.214.100	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to /phpmyadmin/scripts/setup.php	Block	1
172.91.159.183	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1

08-22-2016-05:04:02 to 08-22-2016-06:04:02