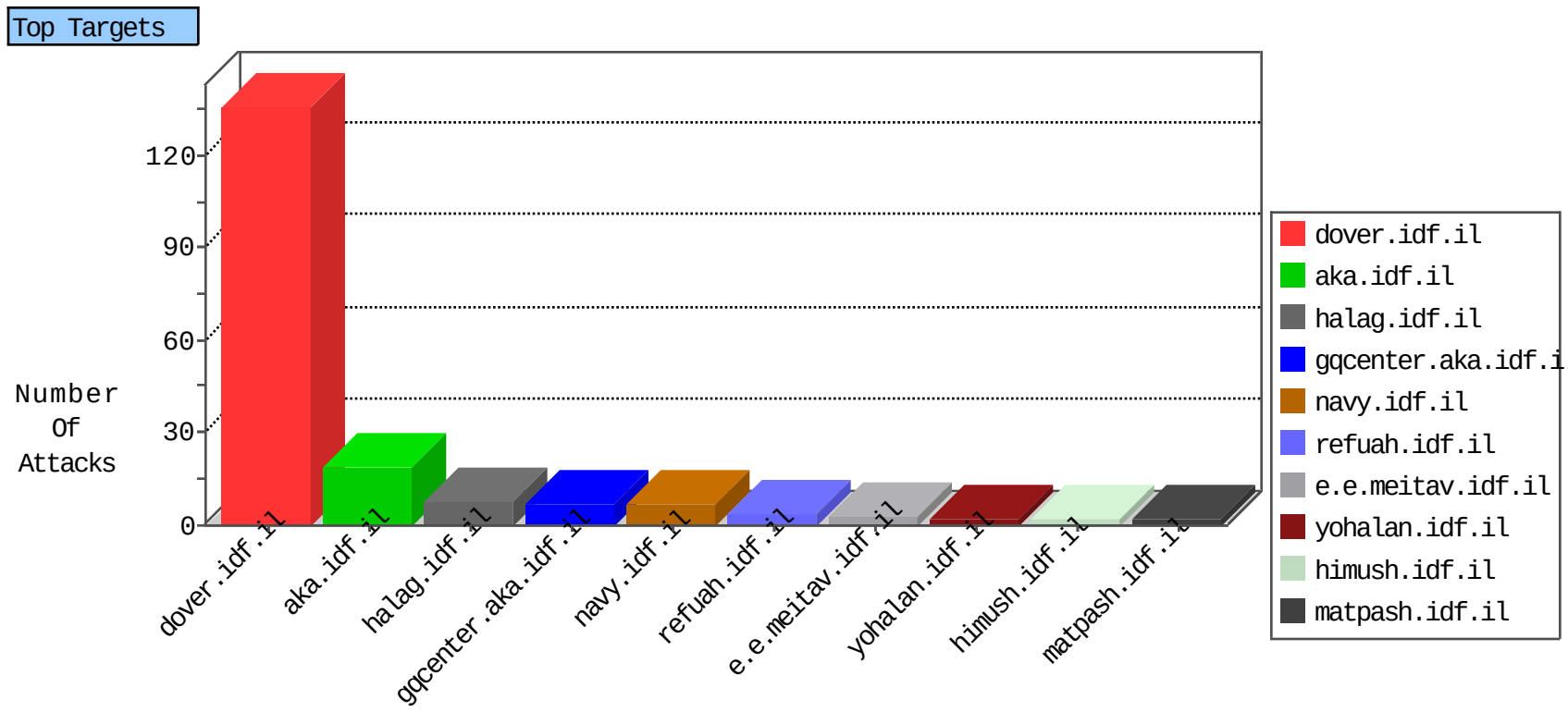
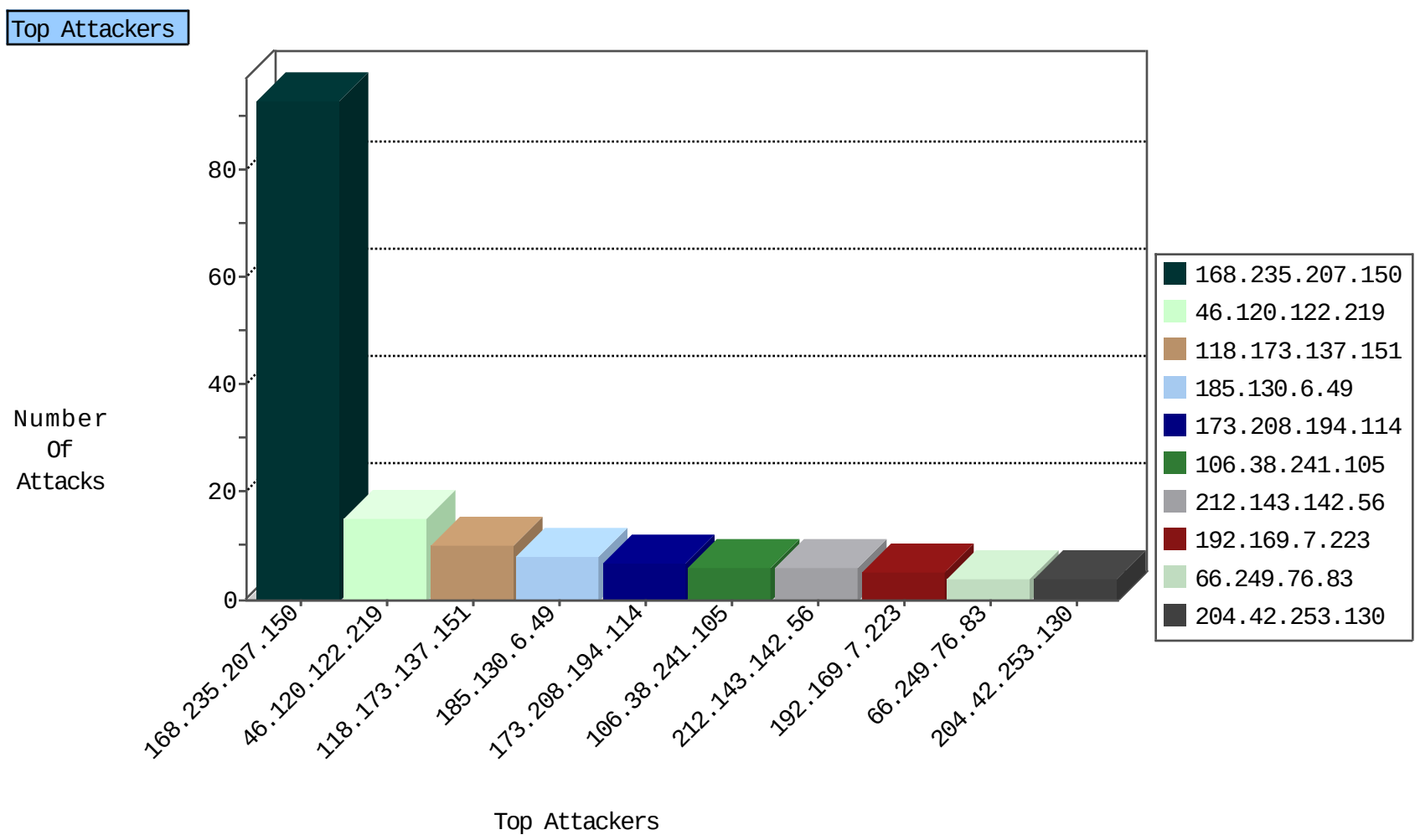
08-30-2016-04:04:01 to 08-30-2016-05:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-30-2016-04:04:01 to 08-30-2016-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.207.150	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	78
168.235.207.150	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	34
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.207.150	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
8.21.198.22	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
204.42.253.130	United States	147.237.76.30	himush.idf.il	Black List	drop	2
204.42.253.130	United States	147.237.76.34	yohalan.idf.il	Black List	drop	2
209.126.136.2	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

08-30-2016-04:04:01 to 08-30-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.208.194.114	United States	147.237.77.234	halag.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
106.38.241.105	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
98.218.34.60	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
173.208.194.114	United States	147.237.77.234	halag.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

08-30-2016-04:04:01 to 08-30-2016-05:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	8
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	3
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	2
87.236.194.161	147.237.76.38	Czech Republic	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.165.253.25	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
173.208.194.114	147.237.77.234	United States	halag.idf.il	ET WEB_SERVER Muieblackcat scanner	1
111.91.163.205	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.236.194.161	147.237.77.212	Czech Republic	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
217.118.23.124	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

08-30-2016-04:04:01 to 08-30-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.207.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
118.173.137.151	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.130.6.49	Lithuania	147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
37.247.36.119	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
185.130.6.49	Lithuania	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
185.130.6.49	Lithuania	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
185.130.6.49	Lithuania	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
185.130.6.49	Lithuania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
185.130.6.49	Lithuania	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
185.130.6.49	Lithuania	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
185.130.6.49	Lithuania	147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
5.102.195.62	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1

08-30-2016-04:04:01 to 08-30-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
131.253.25.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
178.137.164.171	Ukraine	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 178.137.164.171	Block	2
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	2
207.46.13.149	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.64.19.77	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
5.28.181.114	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
66.249.76.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/iaf7	Block	1
157.55.39.101	United States	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to 147.237.76.31/	Block	1
66.102.6.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
199.30.25.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/reserve/	Block	1
157.55.39.240	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
5.15.15.185	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
178.137.164.171	Ukraine	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1

08-30-2016-04:04:01 to 08-30-2016-05:04:01