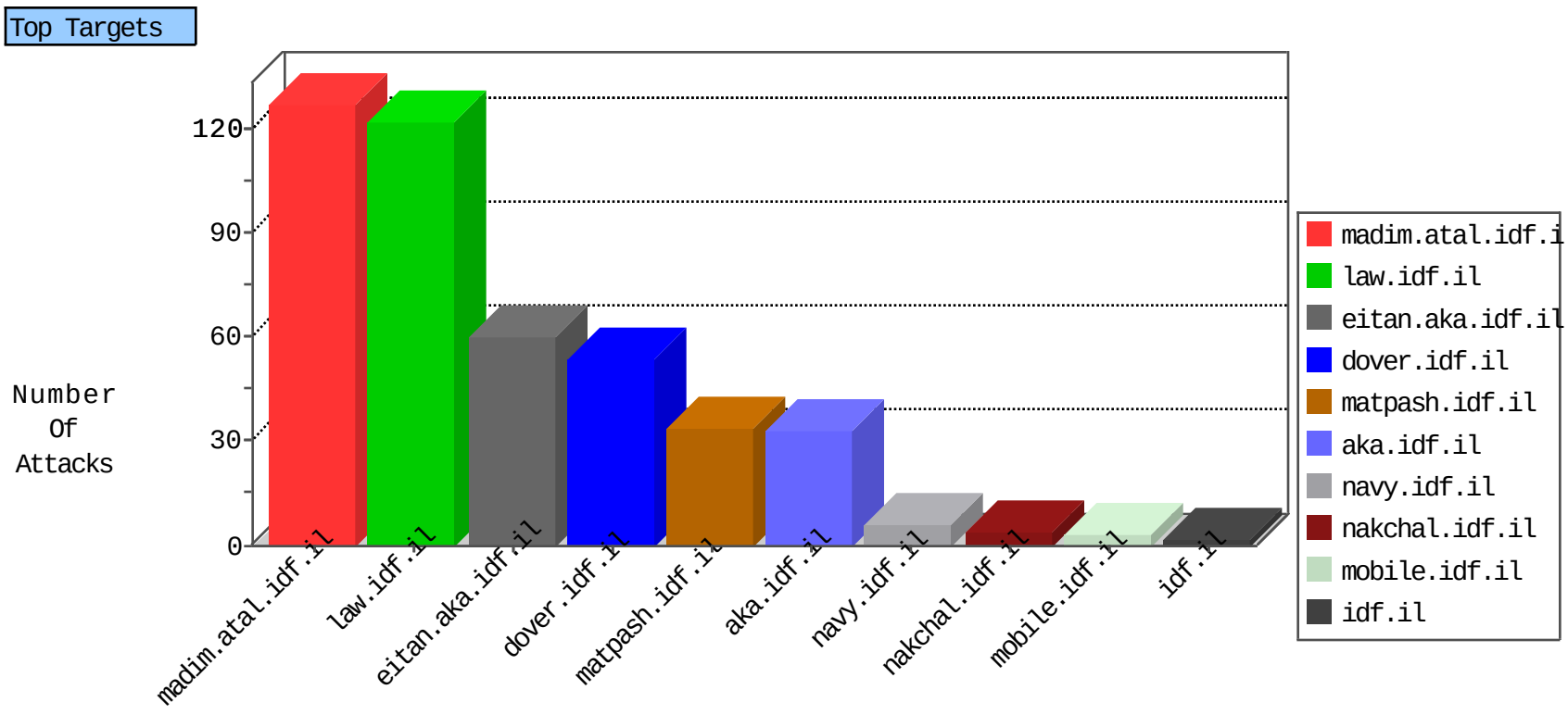
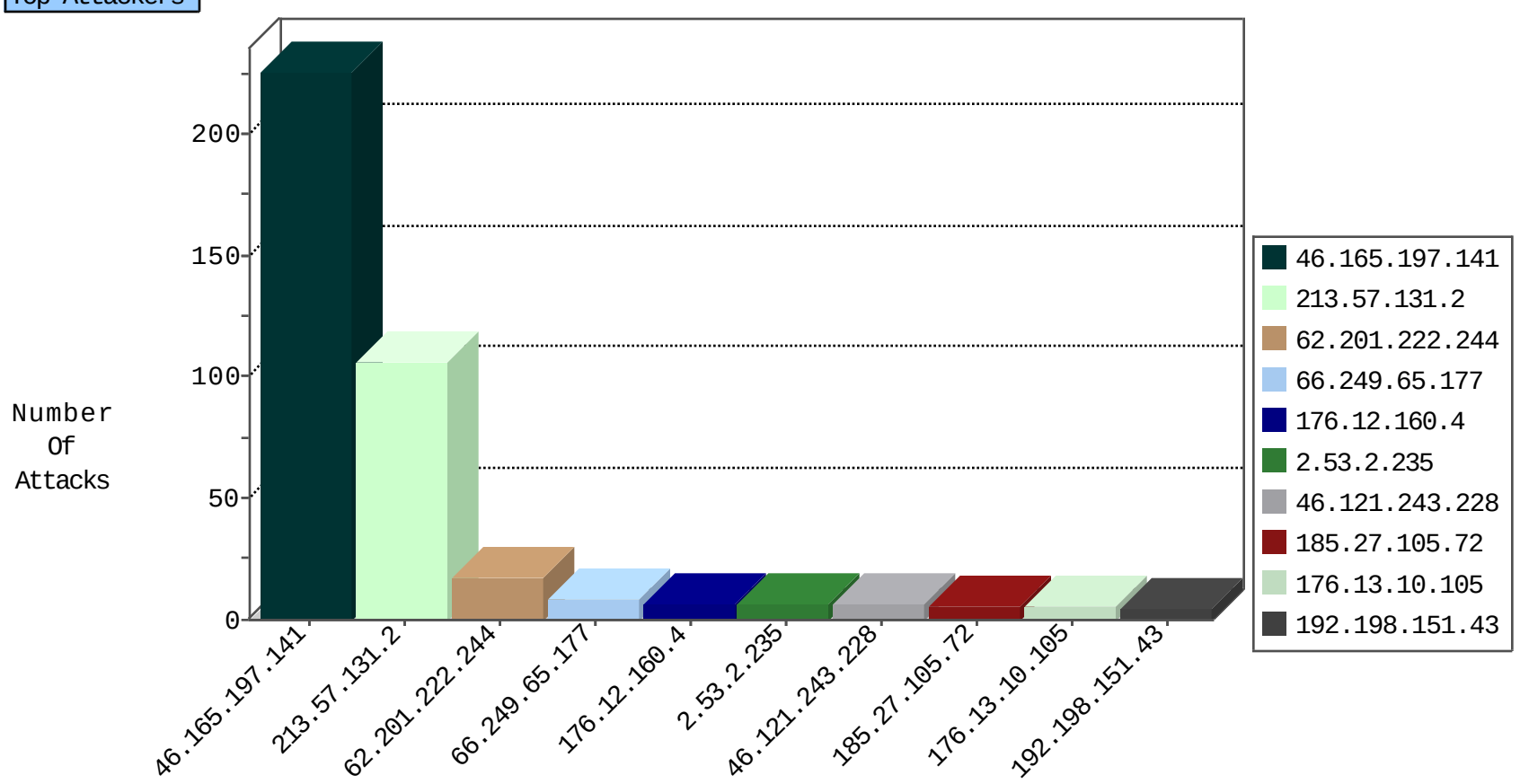
08-20-2016-21:04:03 to 08-20-2016-22:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-20-2016-21:04:03 to 08-20-2016-22:04:03

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	2
93.158.200.86	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
94.177.160.214	Romania	147.237.76.30	himush.idf.il	Black List	drop	1
222.187.223.120	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
89.248.168.21	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1

08-20-2016-21:04:03 to 08-20-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.165.197.141	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	122
46.165.197.141	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	60
46.165.197.141	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	31
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
46.165.197.141	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	6

08-20-2016-21:04:03 to 08-20-2016-22:04:03

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
61.240.144.65	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
189.107.104.45	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
129.56.2.38	147.237.8.27	Nigeria	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
66.249.66.16	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
193.201.225.138	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
129.56.2.38	147.237.8.24	Nigeria	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

08-20-2016-21:04:03 to 08-20-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.201.222.244	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
176.12.160.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.27.105.72	Israel	147.237.77.216	dover.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	2
176.13.10.105	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
66.249.69.113	Israel	147.237.0.33	idf.il	drop		drop	1
176.13.242.240	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
129.56.2.38	Nigeria	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.247.14	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
173.255.244.48	United States	147.237.0.35	akaws.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.131.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
2.53.2.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.121.243.228	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.243.228	Block	5
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	4
2.53.40.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
157.55.39.176	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.10.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.148.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
131.253.25.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	3
77.138.95.49	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
217.132.135.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.139.36.160	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.125.73.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	2
5.22.134.217	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
207.46.13.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
89.237.66.68	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
46.121.243.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
151.237.143.96	Bulgaria	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.182.142.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
5.22.135.174	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
95.86.93.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
54.174.51.78	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15144-he/dover.aspxjump	Block	1
80.246.139.141	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71679.pdf	Block	1
213.57.131.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
45.33.143.54	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
107.178.41.32	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
77.139.226.251	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
66.249.64.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/14112010dohoctober.aspx	Block	1
2.55.11.34	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 2.55.11.34 (Open Mode)	None	1
84.94.66.20	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.125.73.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.125.73.159	Block	1
213.57.186.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.222.60	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.206.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.55.183.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/haredim/general.aspx	Block	1
79.178.12.8	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1

08-20-2016-21:04:03 to 08-20-2016-22:04:03