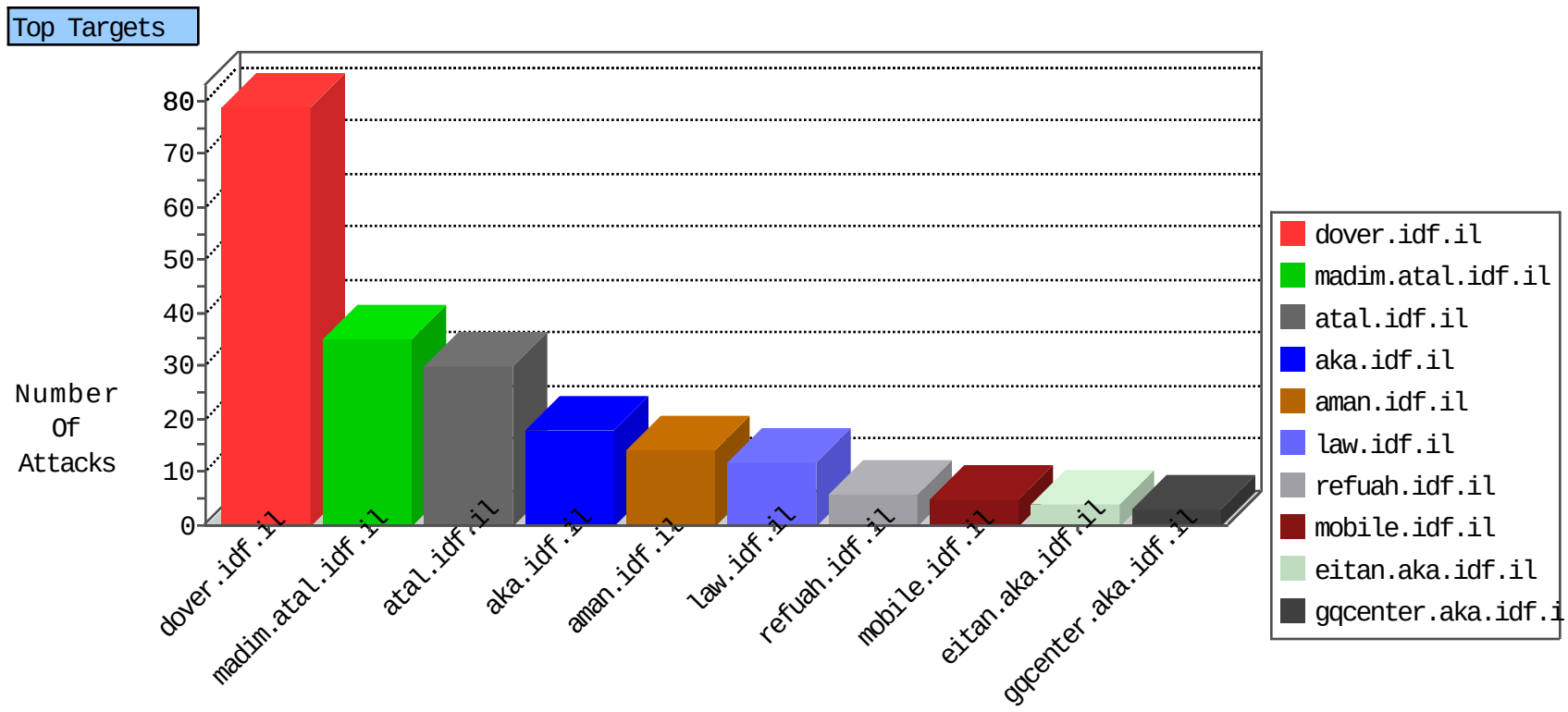
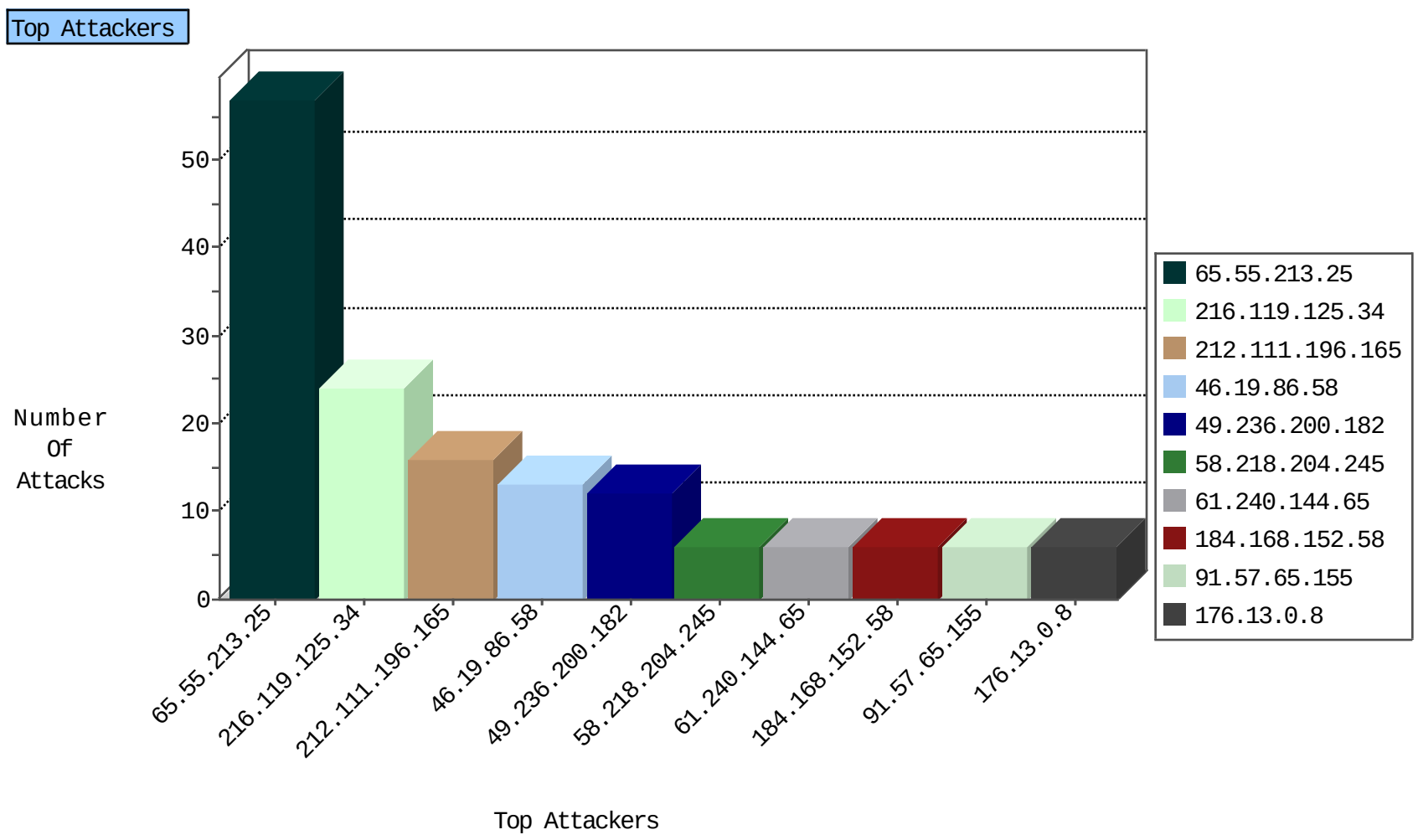
08-20-2016-22:04:09 to 08-20-2016-23:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-20-2016-22:04:09 to 08-20-2016-23:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
104.148.55.162	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
58.218.204.245	China	147.237.8.14	e.orchot.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1

08-20-2016-22:04:09 to 08-20-2016-23:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.119.125.34	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
49.236.200.182	Malaysia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
51.255.65.6	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.87	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
85.248.227.165	Slovakia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-20-2016-22:04:09 to 08-20-2016-23:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.125.34	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
49.236.200.182	147.237.77.74	Malaysia	law.idf.il	SQL Injection - Select From	6
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
212.111.196.165	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
62.215.175.27	147.237.76.30	Kuwait	himush.idf.il	ET SCAN NMAP -sS window 1024	1
212.111.196.165	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.205	China	prisha.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
212.111.196.165	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
212.111.196.165	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
212.111.196.165	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.147	United States	chinuch.aka.idf.il	ET DROP Dshield Block Listed Source	1
58.218.204.245	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
212.111.196.165	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
141.136.228.42	147.237.76.199	Croatia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
212.111.196.165	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN Potential SSH Scan	1
123.206.73.185	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.111.196.165	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.82.194	147.237.72.166	Asia/Pacific Region	aka.idf.il	ET SCAN NMAP -sA (2)	1
212.111.196.165	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.243	China	mobile.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
212.111.196.165	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
212.111.196.165	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
212.111.196.165	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
212.111.196.165	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
212.111.196.165	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.111.196.165	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
141.136.228.42	147.237.76.176	Croatia	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
212.111.196.165	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.72.217	Germany	e.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1

08-20-2016-22:04:09 to 08-20-2016-23:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
184.168.152.58	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
91.57.65.155	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.0.8	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
176.13.229.89	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	5
95.86.122.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.26	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
176.13.17.90	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
95.242.180.23	Italy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
197.123.99.232	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
5.22.131.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.180.154.239	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.144	United States	147.237.0.35	akaws.idf.il	drop		drop	1
40.77.167.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.239.207	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
89.138.121.108	Israel	147.237.72.156	aman.idf.il	drop	Virtual defragmentation error: Timeout	drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
141.212.122.159	United States	147.237.0.35	akaws.idf.il	drop		drop	1
46.32.213.111	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1

08-20-2016-22:04:09 to 08-20-2016-23:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
65.55.213.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	57
46.19.86.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	3
87.71.4.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.131.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.215.209	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	2
46.19.86.226	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
109.253.243.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.39.224.85	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
141.226.145.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.247.5	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
2.53.44.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
31.168.189.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.174	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/robots.txt	Block	1
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21587-he/idfgdover.aspx	Block	1
109.64.118.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.102.7.136	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
157.55.39.228	United States	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 157.55.39.228	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
5.29.165.67	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/70014.doc	Block	1
157.55.39.228	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
76.99.203.193	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
5.29.228.154	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/archive	Block	1
46.19.85.13	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
207.46.13.53	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
87.65.92.97	Belgium	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
46.120.229.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

08-20-2016-22:04:09 to 08-20-2016-23:04:09