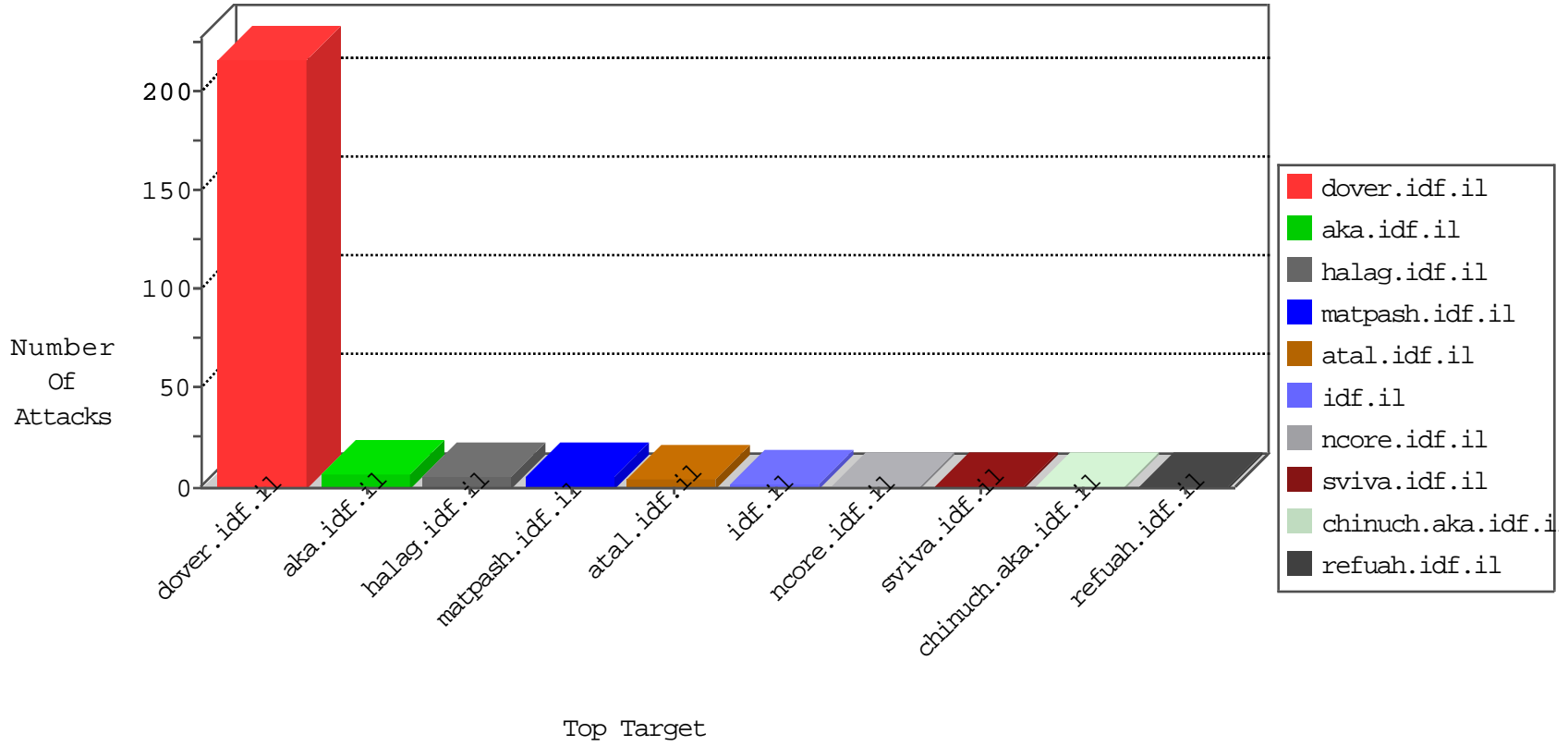


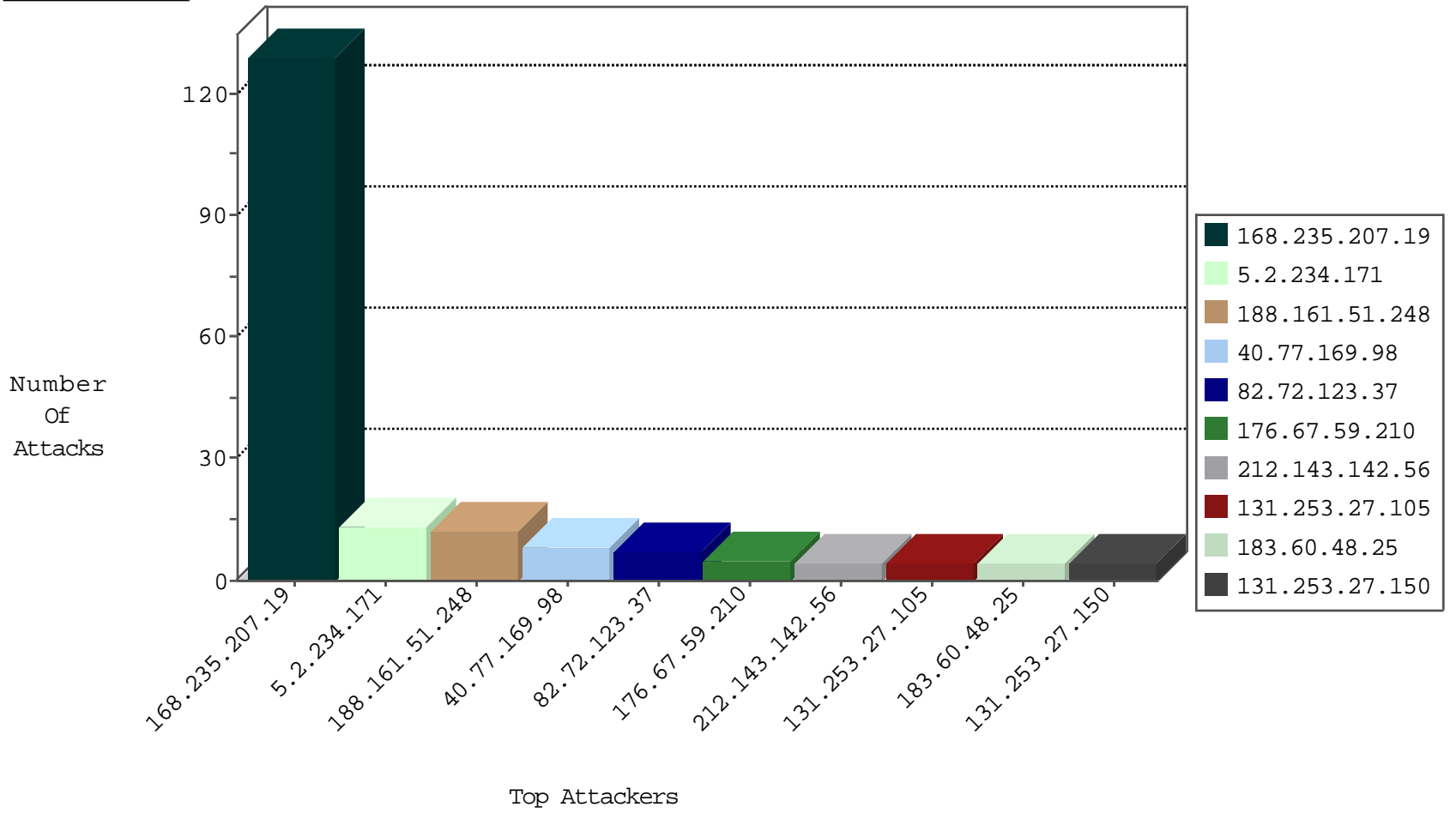
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.207.19	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3

08-25-2016-00:04:00 to 08-25-2016-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.65.32	France	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.125.184.101	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
133.242.4.52	147.237.77.121	Japan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.3.168	147.237.72.217	Japan	e.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.160.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
133.242.4.52	147.237.77.234	Japan	halag.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.3.168	147.237.77.235	Japan	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.212	Japan	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.202.219	147.237.77.205	Chile	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.207.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	126
5.2.234.171	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
188.161.51.248	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
82.72.123.37	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.67.59.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
107.170.101.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.108.25.33	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.13.102.117	Ireland	147.237.77.216	dover.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
176.67.59.210	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
31.13.102.126	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
49.145.208.40	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
129.56.2.38	Nigeria	147.237.0.33	idf.il	drop		drop	1
31.13.102.118	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
202.155.58.28	Indonesia	147.237.76.34	yohalan.idf.il	drop		drop	1
66.249.65.50	Israel	147.237.0.33	idf.il	drop		drop	1
212.76.110.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.27.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	4
131.253.27.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
5.29.164.247	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.97.106.162	China	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.229.38.15	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.228	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1877	Block	1
204.79.180.248	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/portalmilium/templates/inner.asp	Block	1
68.180.229.49	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.19.86.184	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
180.97.106.162	China	147.237.77.176	matpash.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
89.138.149.242	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
31.154.81.25	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	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
77.125.81.135	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.116.33.231	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
192.243.55.135	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem	Block	1
109.65.80.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct163 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.75.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22805-he/idfgdover.aspx	Block	1
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
176.13.15.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
77.138.146.47	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.105	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
199.80.248.1	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.27.5	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.75.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
176.54.161.146	Turkey	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.58.247.99	Italy	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.29.105.23	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
199.80.248.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1