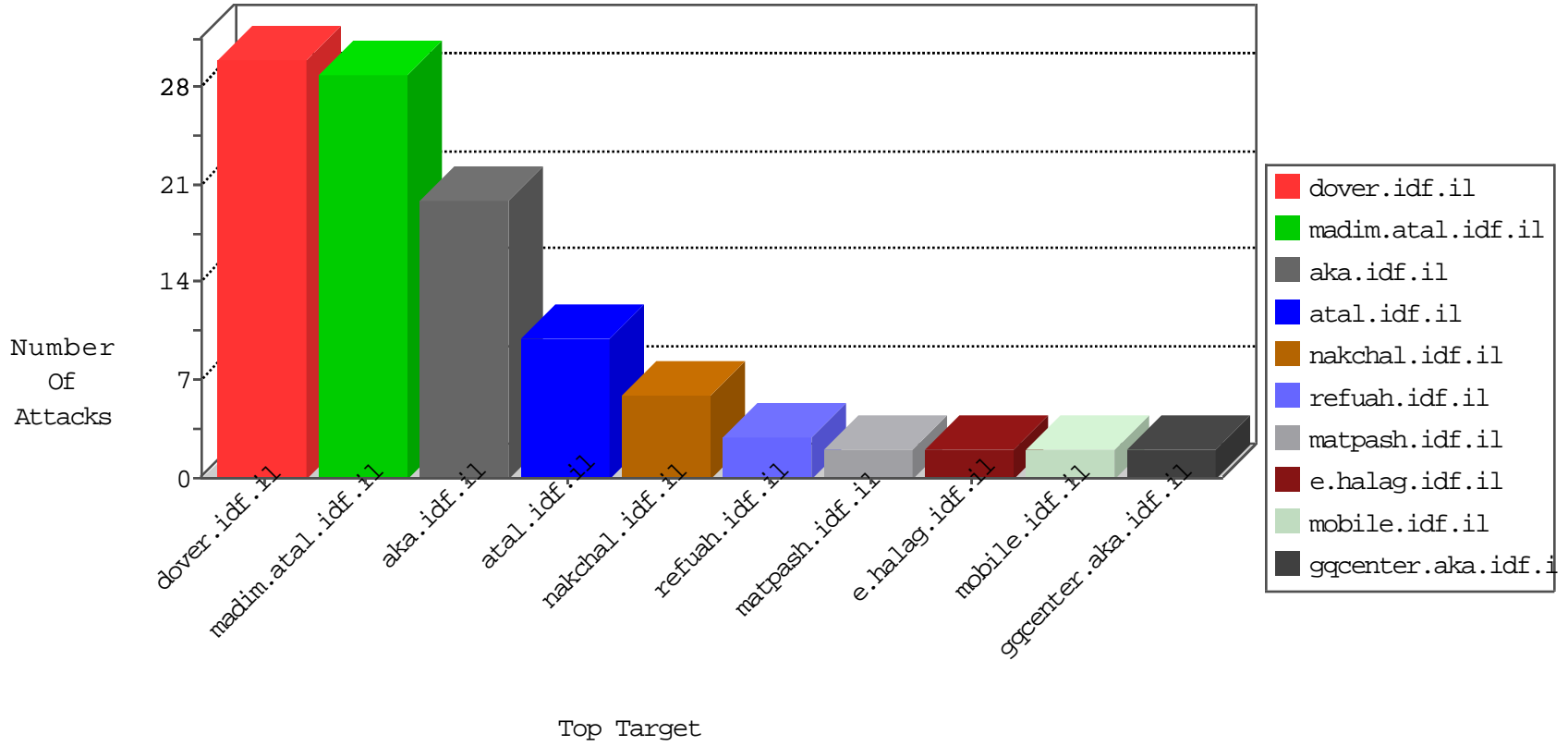


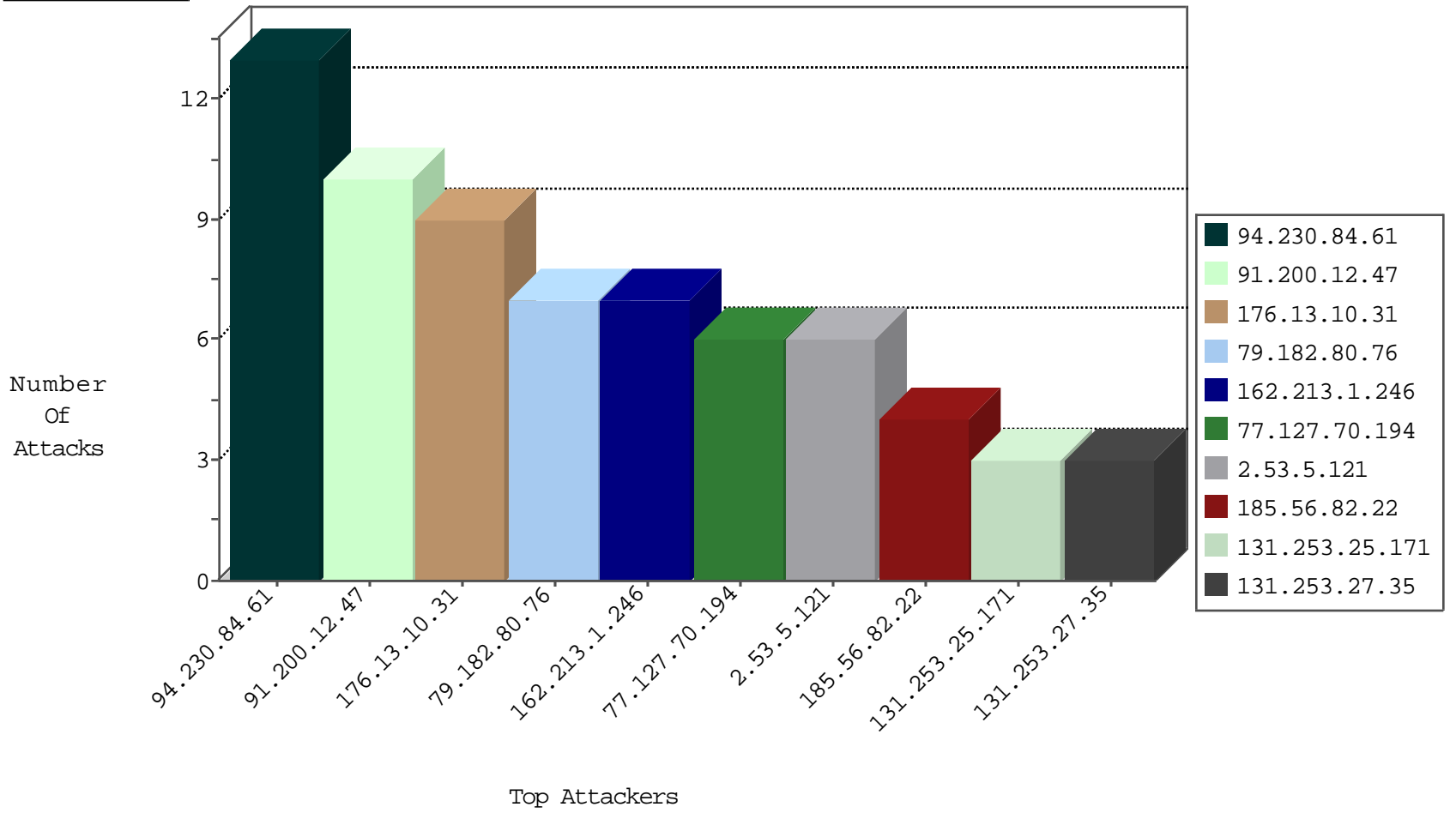
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
185.94.111.1	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Permit	8
71.6.167.142	United States	147.237.76.177	ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
86.186.225.159	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

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	7
185.56.82.22	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.56.82.22	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.242.213.18	147.237.0.19	Kazakstan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
58.218.204.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
50.244.232.141	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.56.82.22	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.137.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.204.245	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
54.80.32.24	147.237.76.42	United States	refuah.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.80.76	Israel	147.237.72.166	aka.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	3
46.19.86.87	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
109.253.156.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
120.132.68.73	China	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.16.20	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.204	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.230.84.61	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	13
176.13.10.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.53.5.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.127.70.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
131.253.25.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
131.253.27.35	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.230.141	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
199.30.24.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.139.137.155	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/pniot.aspx	Block	2
92.1.172.190	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
89.248.172.16	Netherlands	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.127.70.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/sip_storage/files/2/	Block	1
66.102.9.54	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
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.102.9.85	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
207.46.13.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/11	Block	1
84.108.85.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
66.249.65.163	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
212.235.16.21	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21587-he/idfgdover.aspx	Block	1
2.53.30.46	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
84.229.43.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
217.132.247.34	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
2.53.49.198	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
176.228.158.248	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1