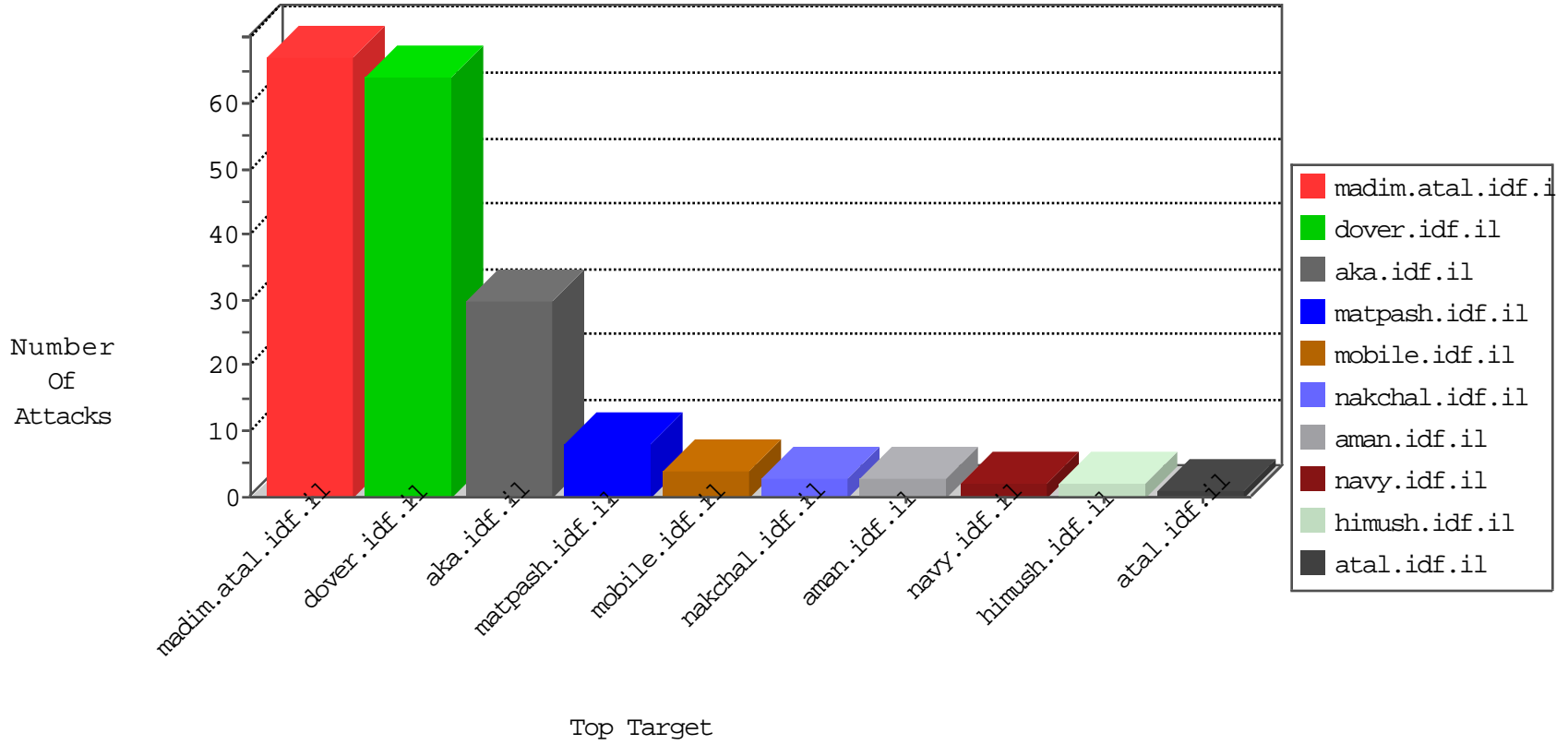


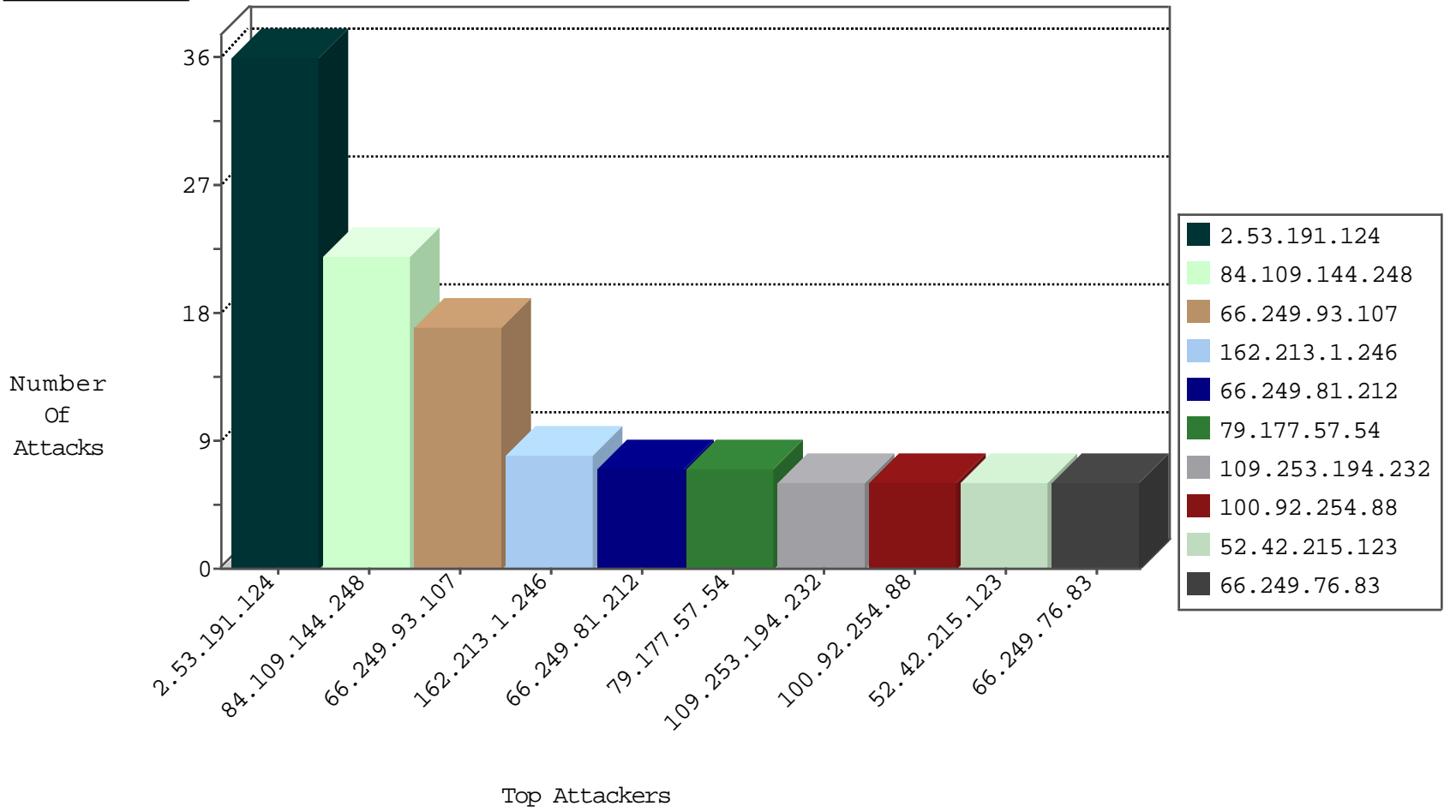
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	2
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	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	8
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
193.201.225.149	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -f -sS	1
177.17.159.76	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
142.54.108.92	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
79.177.57.54	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
52.42.215.123	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
100.92.254.88		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.248.143	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
173.255.134.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.128.48.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.186.77.41	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
176.13.14.53	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.110	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.126.67.48	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.19.37	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
104.24.103.87	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	1
5.11.43.184	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.243.142	Israel	147.237.72.166	aka.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
2.53.191.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
84.109.144.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	6
109.253.194.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.121.91.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.25.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
2.53.166.252	Israel	147.237.72.166	aka.idf.il	Malformed URL www.aka.idf.il	Block	1
213.8.204.58	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/kiosk/kiosk.aspx	Block	1
109.65.169.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authentication-service.aspx/getauthuser	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.77	Block	1
2.53.166.252	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Host: in URL www.aka.idf.il	Block	1
68.180.229.49	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
51.6.76.1	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
109.67.109.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.246.130.79	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.102.9.76	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
2.53.166.252	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
37.26.148.129	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.80.60.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1674	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.41	Block	1
2.53.166.252	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1