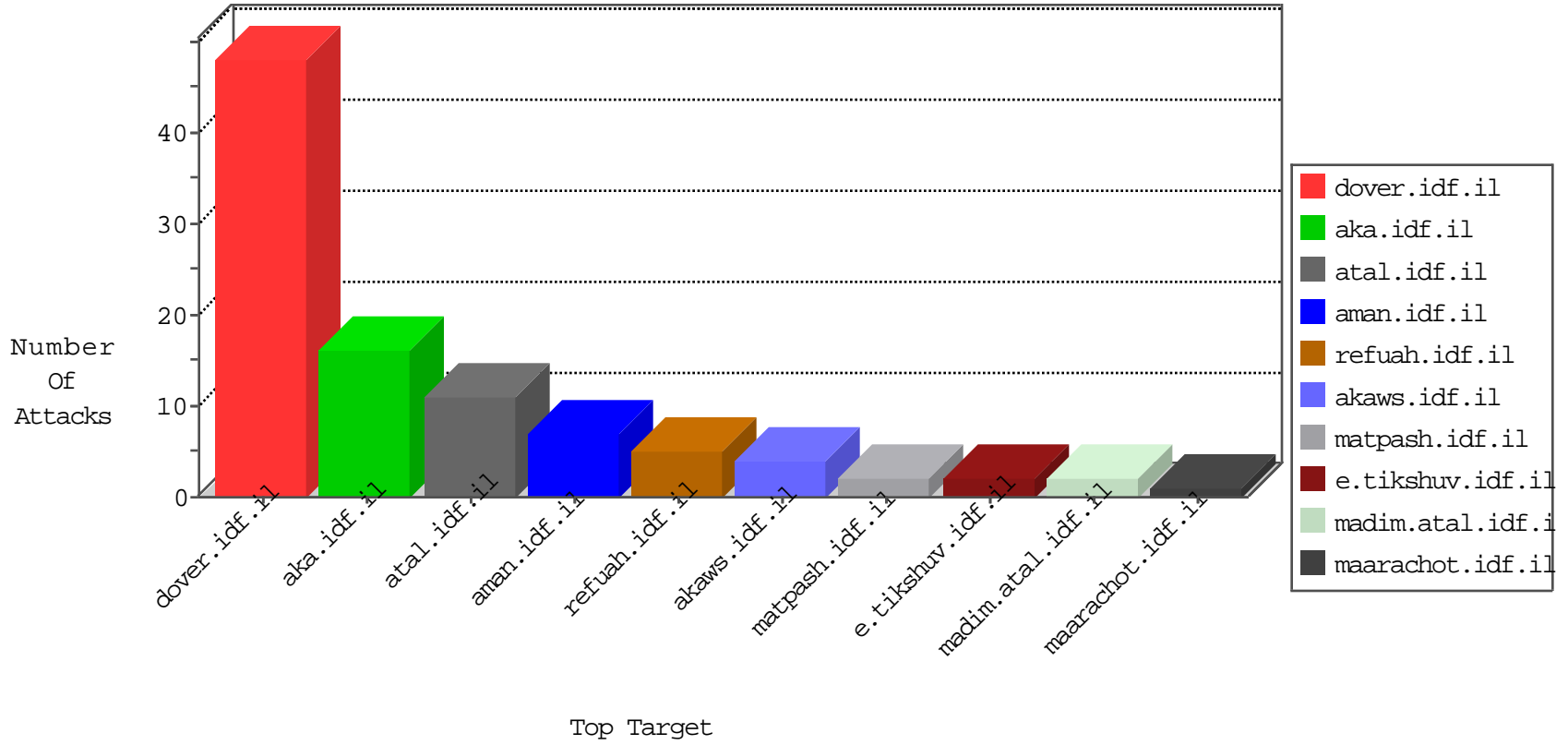


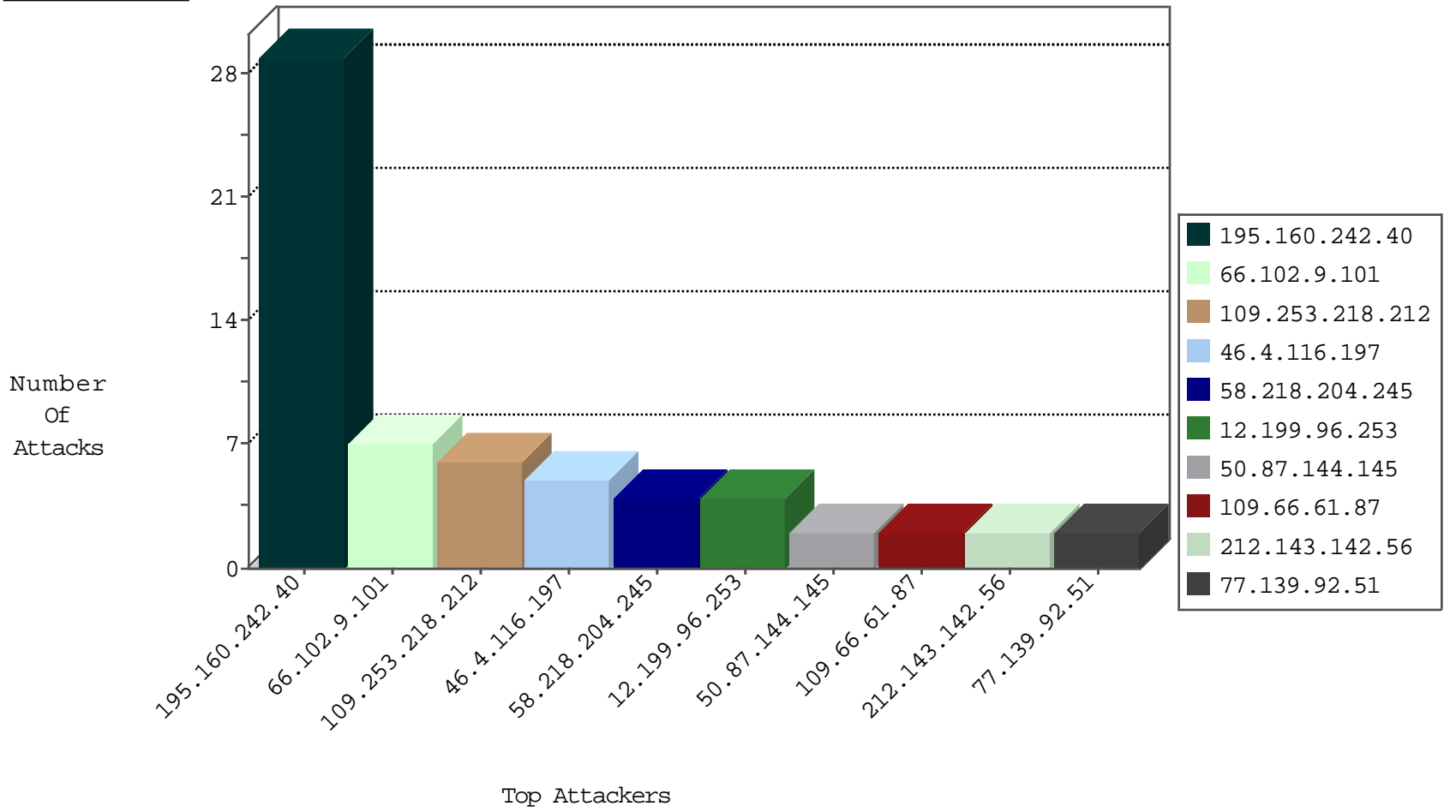
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.116.197	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.116.197	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
187.58.159.163	147.237.0.200	Brazil	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.76.52	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
66.102.9.111	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.65	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
173.208.249.36	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
66.151.255.234	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.177	China	ncore.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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.102.9.101	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
109.253.218.212	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
68.180.228.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.125.32.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	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
85.130.229.121	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
176.13.235.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
95.35.228.8	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
177.67.92.11	Brazil	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.133	United States	147.237.0.35	akaws.idf.il	drop		drop	1
2.55.128.152	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
82.166.235.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.134	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
12.199.96.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.206.85	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
77.139.92.51	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.92.51	Block	1
46.19.86.247	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
93.172.230.97	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.9.95	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
24.24.221.165	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
77.139.92.51	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim	Block	1
62.219.142.66	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 62.219.142.66	Block	1
109.65.69.239	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
31.15.133.102	Slovenia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus	Block	1
79.178.111.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.219.142.66	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.55.133.247	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
109.66.61.87	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
37.26.148.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.158.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	1
63.116.61.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.22.134.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
109.111.112.73	Andorra	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
77.125.55.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.85.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
89.139.158.79	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
66.102.9.54	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1