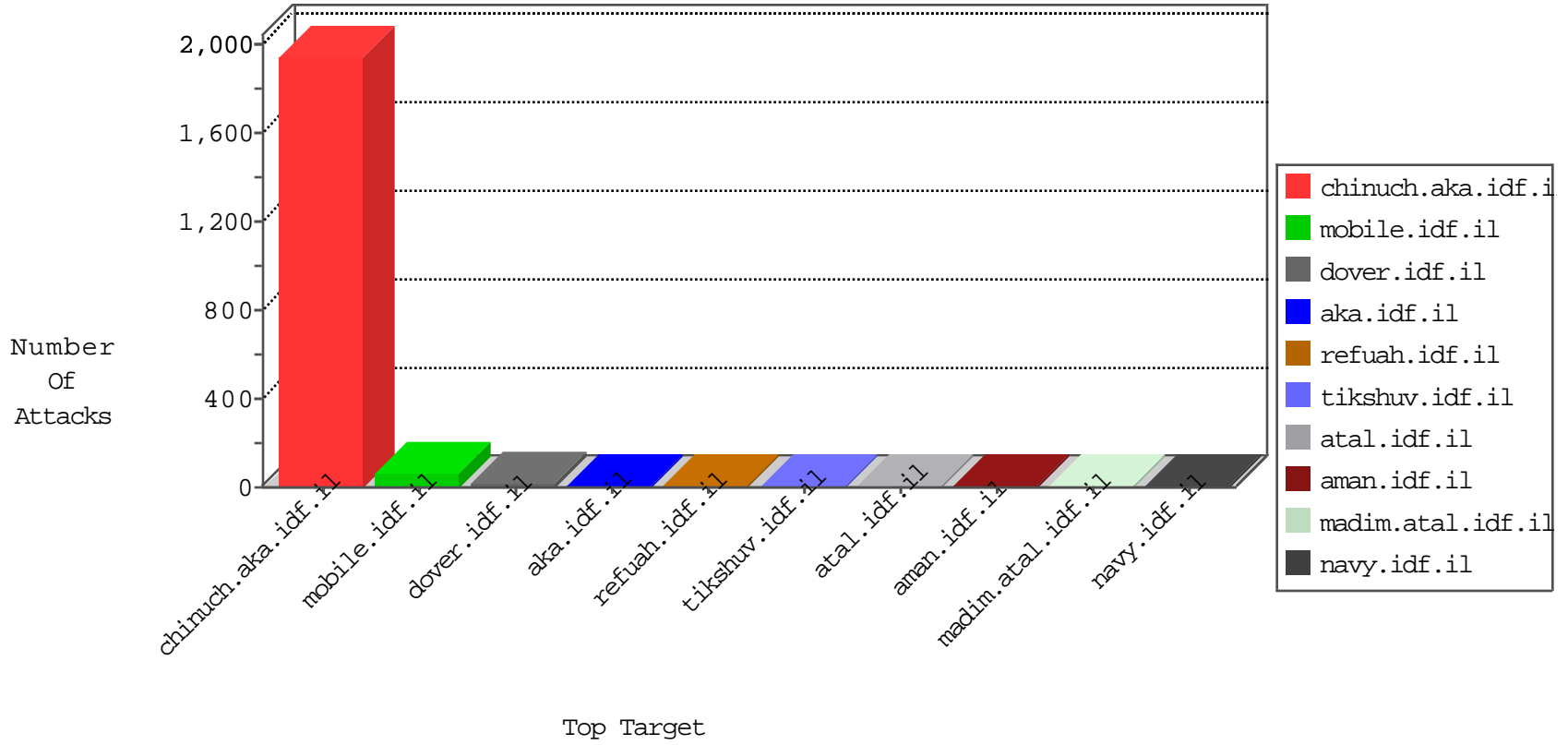


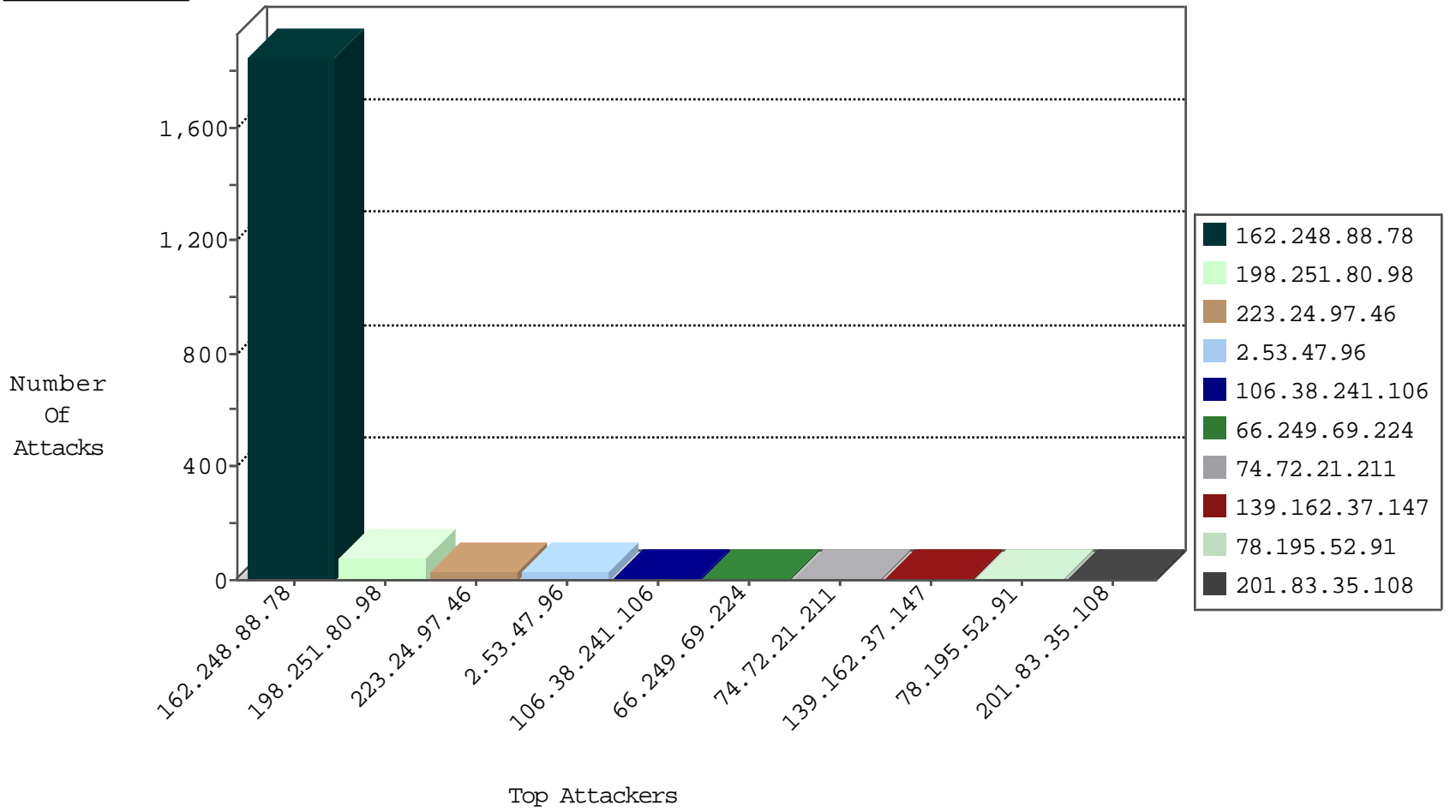
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.141.242.195	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	forward	2
204.12.220.85	United States	147.237.0.34	tikshuv.idf.il	block-sp-trafl	forward	1
45.63.53.164	United States	147.237.76.86	navy.idf.il	Black List	drop	1
191.96.249.34	Chile	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.111.84	147.237.77.216	France	dover.idf.il	Xenu Link Sleuth User Agent	2
177.189.209.160	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.129.15	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.8	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
46.183.223.228	147.237.0.34	Latvia	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
177.189.209.160	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
125.94.169.143	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.114.97.11	147.237.72.166	Portugal	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.161.40.17	147.237.77.243	Russian Federation	mobile.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
162.248.88.78	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1841
2.53.47.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
223.24.97.46	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	19
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
201.83.35.108	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
162.248.88.78	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
162.248.88.78	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
128.232.110.28	United Kingdom	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.122.53	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.176.119.184	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
68.8.187.154	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
176.228.158.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
139.162.37.147	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
78.195.52.91	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.54	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.201.154.142	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
74.72.21.211	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.95	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
78.195.52.91	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
37.49.225.180	Netherlands	147.237.72.167	ishurim.aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
109.253.136.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.72.21.211	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
216.218.206.94	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.200	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
78.195.52.91	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
46.19.86.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
125.77.28.26	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.72.21.211	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
216.218.206.108	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.248	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
78.195.52.91	France	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
46.19.86.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.72.21.211	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	7
77.138.154.52	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
89.138.176.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
24.5.58.234	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/library/generaldoc.asp	Block	1
180.76.15.5	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/atall/izkor/view_pictures.asp	Block	1
84.109.3.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/https://ww.idf.il/	Block	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/1133-16898-he/dover.aspx idf spokesperson	Block	1
216.244.66.231	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3288.jpg	Block	1
66.249.66.15	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/login/	Block	1
77.139.234.33	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/snalim/	Block	1
157.55.39.121	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/sip_storage/files/7/	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	1