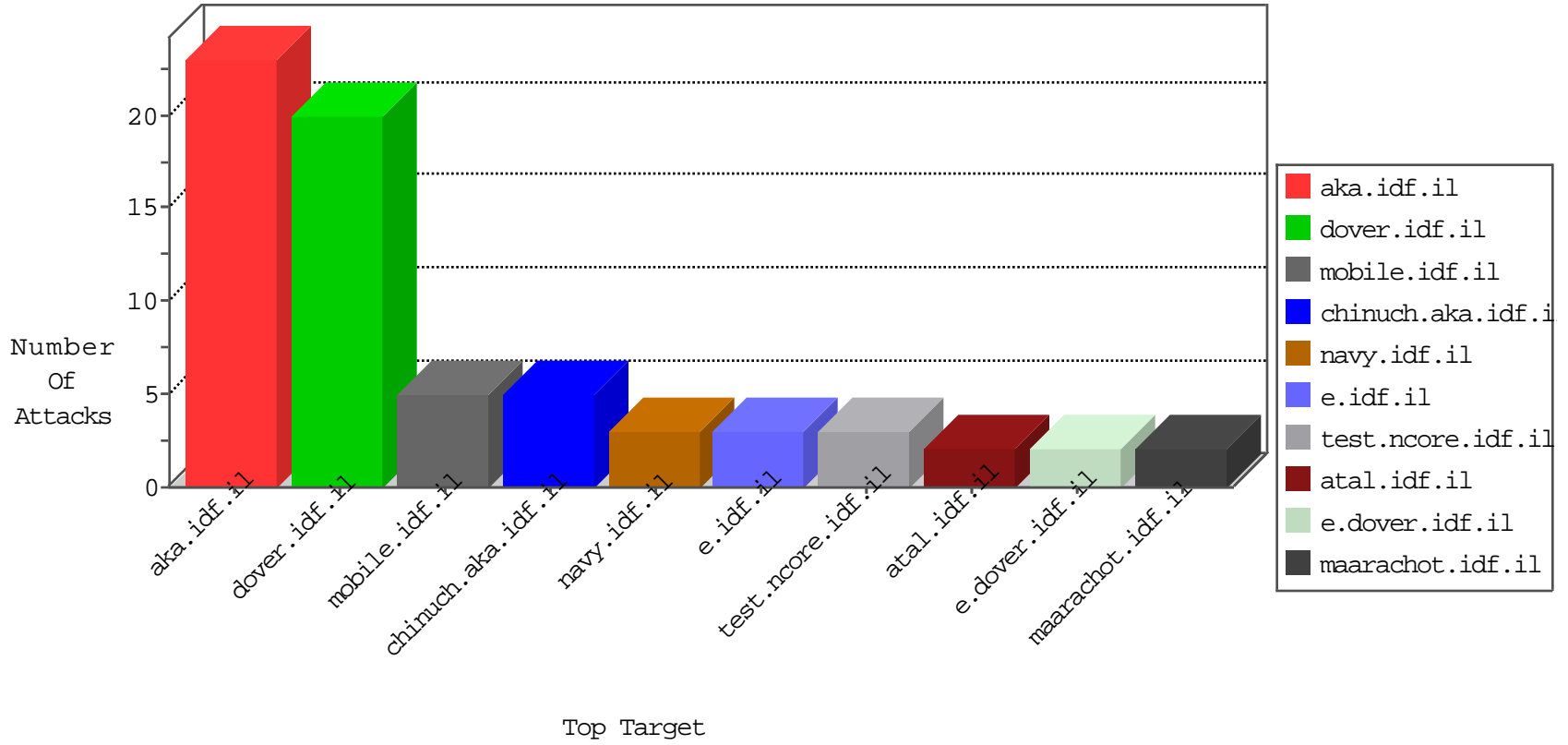


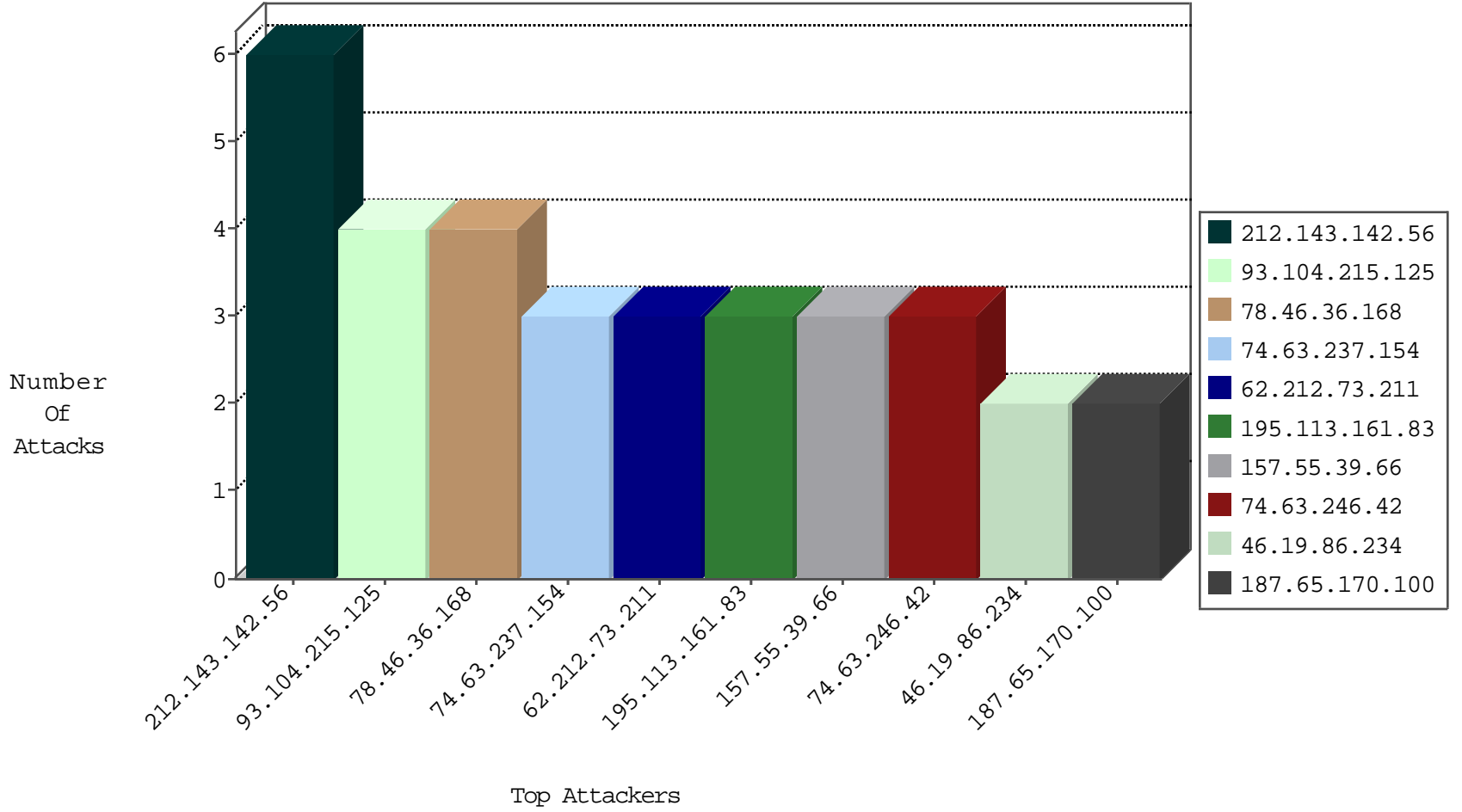
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.62.53.168	Russian Federation	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1
128.223.8.112	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.197	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
121.32.129.130	147.237.77.212	China	e.dover.idf.il	GPL SCAN nmap TCP	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
74.63.246.42	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
74.63.237.154	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
54.249.13.70	147.237.77.170	Japan	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.120.149	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
74.63.246.42	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.79.99	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
41.248.236.112	147.237.77.235	Morocco	sviva.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.66	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.104.215.125	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
187.65.170.100	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
93.104.215.125	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
154.105.120.245	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
78.46.36.168	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
213.57.165.175	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
154.105.120.245	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
78.46.36.168	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.237.154	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
78.46.36.168	Germany	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.57	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.237.154	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
78.46.36.168	Germany	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.58	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.246.42	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
100.2.212.58	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	2
46.19.86.234	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
195.62.53.168	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
207.46.13.1	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
157.55.39.173	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/main/giyus	Block	1
67.170.100.194	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
191.101.153.146	United States	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
191.101.153.146	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/wp/wp-login.php	Block	1
109.63.232.247	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1