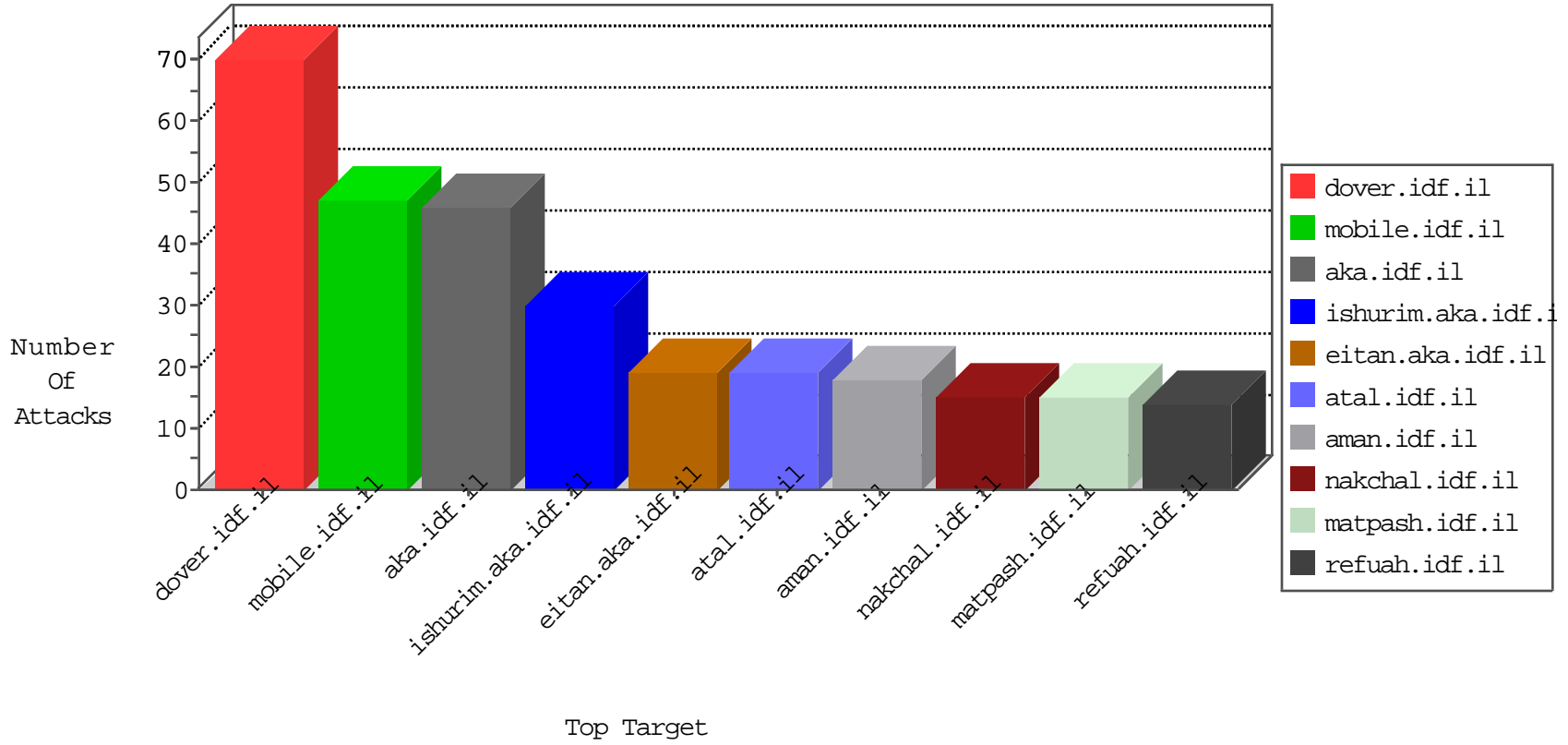


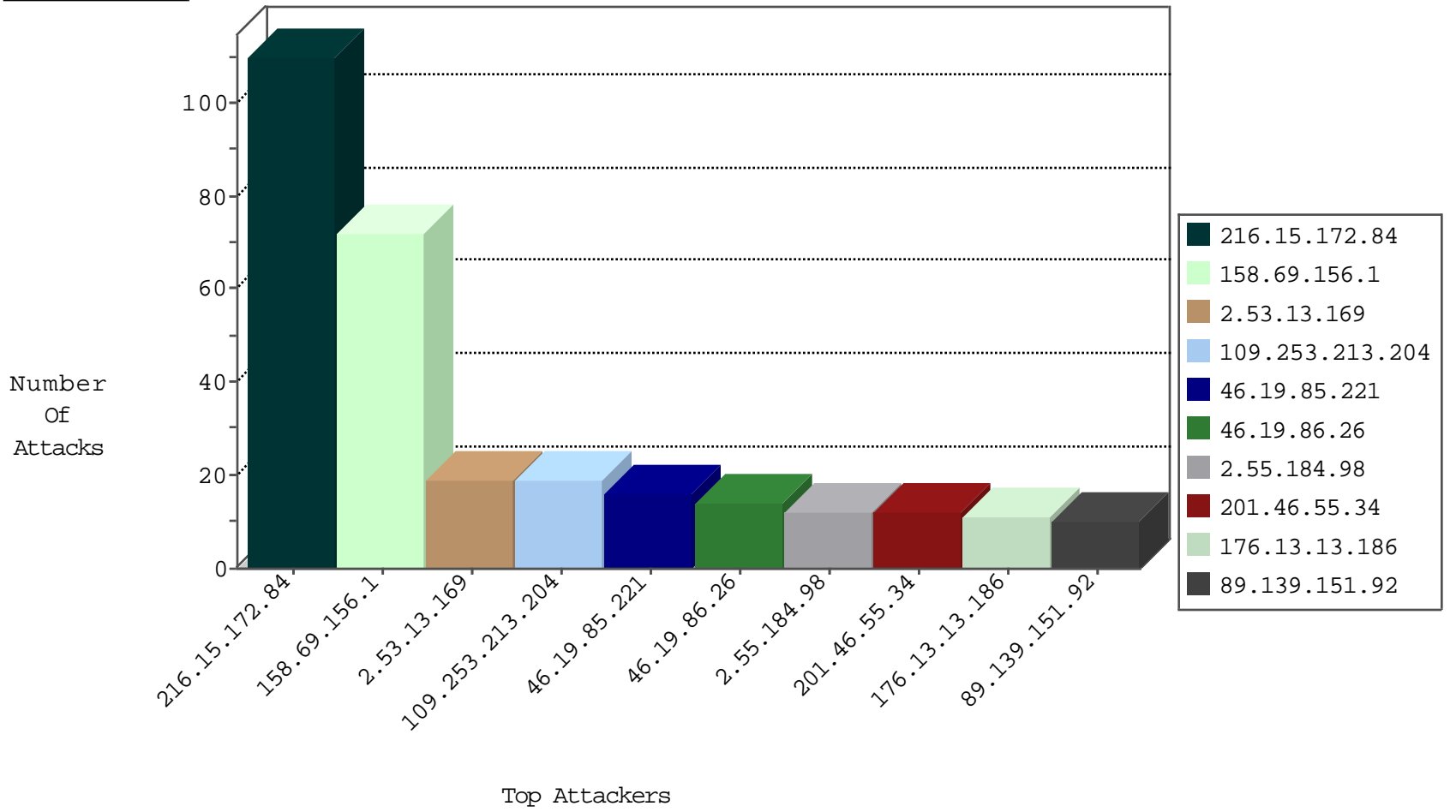
# IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.230.121.156	Ukraine	147.237.76.30	himush.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.51.26	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.51.26	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.213.204	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
46.120.122.219	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	2
221.204.249.157	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
197.221.50.66	147.237.77.205	South Africa	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
180.213.5.204	147.237.72.217	China	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.200.192.50	147.237.76.148	Brazil	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.245.143.138	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
211.141.78.56	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
197.221.50.66	147.237.77.205	South Africa	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
177.200.192.50	147.237.76.148	Brazil	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
177.200.192.50	147.237.76.148	Brazil	ggcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
50.245.143.138	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
50.245.143.138	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.13.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.55.184.98	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.13.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
2.100.56.154	United Kingdom	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
216.15.172.84	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
216.15.172.84	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
216.15.172.84	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
216.15.172.84	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
216.15.172.84	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.116.21.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
216.15.172.84	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.3.147.205	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
216.15.172.84	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
216.15.172.84	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
216.15.172.84	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
216.15.172.84	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
216.15.172.84	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
216.15.172.84	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
216.15.172.84	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
216.15.172.84	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
216.15.172.84	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
216.15.172.84	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.156.1	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
216.15.172.84	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
158.69.156.1	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
158.69.156.1	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
216.15.172.84	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
158.69.156.1	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
88.202.218.230	United Kingdom	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
216.15.172.84	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
158.69.156.1	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.213.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
158.69.156.1	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
158.69.156.1	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
216.15.172.84	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
208.54.90.164	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
216.15.172.84	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
158.69.156.1	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
158.69.156.1	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.156.1	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.156.1	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.156.1	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.156.1	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
216.15.172.84	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.46.41.201	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
2.53.13.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.242.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.52.181	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
77.139.21.104	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.97	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.116.116.18	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_bottom.asp	Block	1
37.142.67.35	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.120.122.219	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/894-he/eitan.aspx	None	1
79.180.93.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/70284.pdf	Block	1
37.142.67.35	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
180.76.15.10	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	1
66.249.64.139	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
80.246.130.56	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/7	Block	1
185.24.207.122	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
66.249.64.144	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
88.202.218.230	United Kingdom	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/iturimpages.asp	Block	1
46.116.21.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
76.17.81.122	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chinuch/klali/default.asp	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1