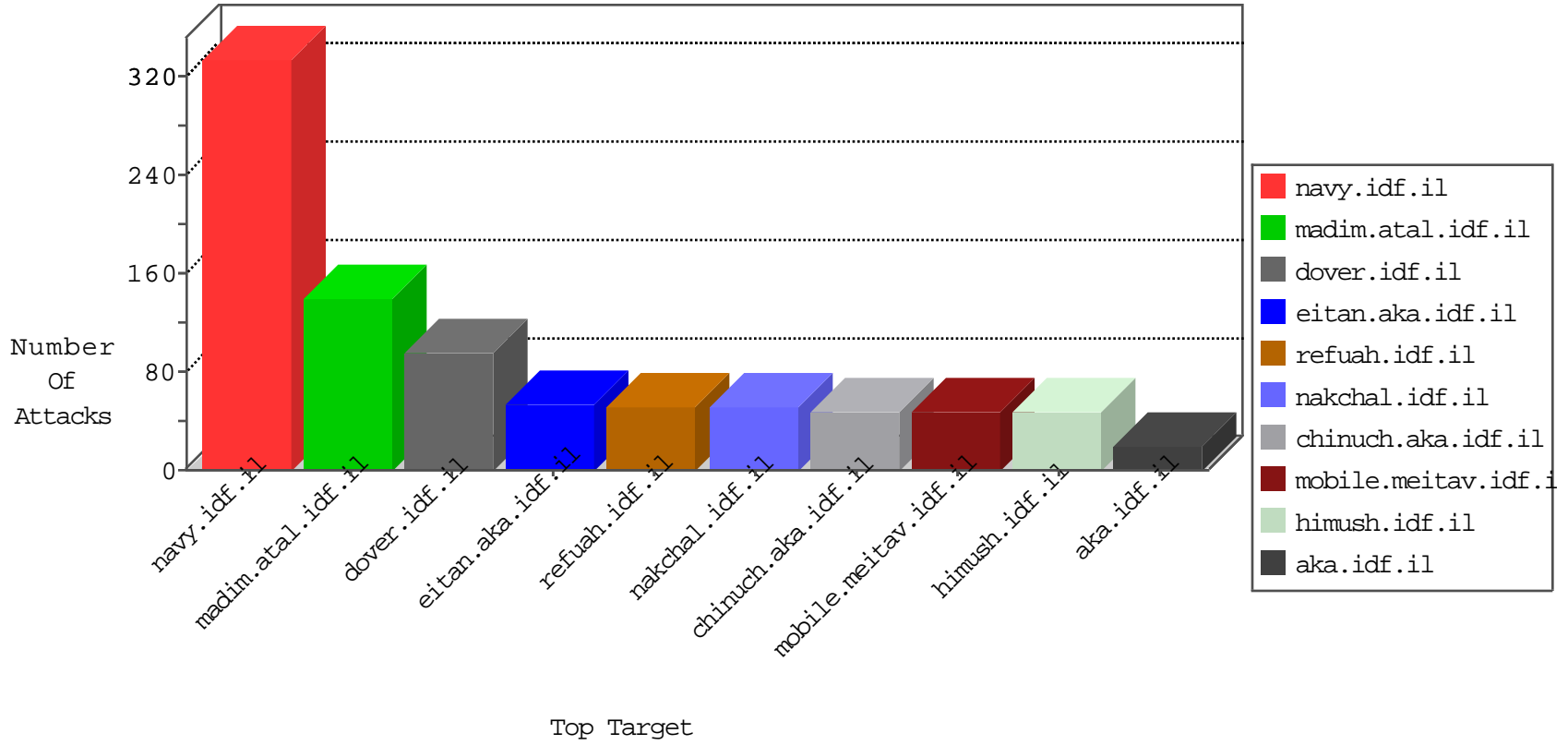


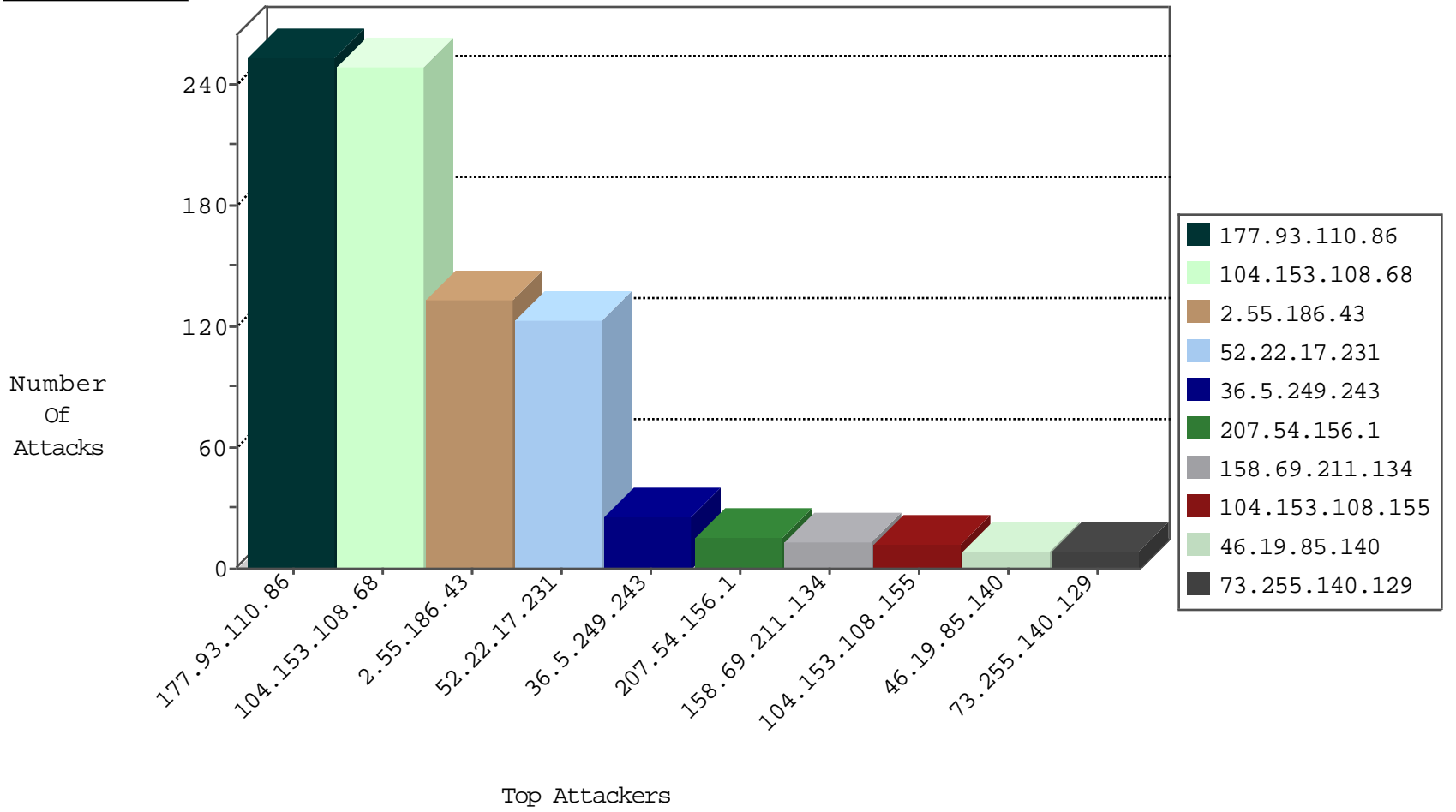
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.158.166	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
93.174.91.37	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
208.67.1.215	United States	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1

09-09-2016-06:04:03 to 09-09-2016-07:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.130	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.221.160	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
113.240.250.154	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.19	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
193.201.225.149	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
167.0.9.141	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
151.11.201.3	147.237.77.19	Italy	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
123.176.80.201	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
117.20.118.41	147.237.77.176	Cambodia	matpash.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.69.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
193.201.225.149	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.75.231	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.176.80.201	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
117.20.118.41	147.237.77.176	Cambodia	matpash.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.153.108.68	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	53
104.153.108.68	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
104.153.108.68	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	49
104.153.108.68	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	48
104.153.108.68	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	44
177.93.110.86	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	17
177.93.110.86	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	17
177.93.110.86	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
52.22.17.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
177.93.110.86	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
177.93.110.86	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
52.22.17.231	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
52.22.17.231	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
52.22.17.231	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
177.93.110.86	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
52.22.17.231	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
177.93.110.86	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
52.22.17.231	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
52.22.17.231	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
52.22.17.231	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
177.93.110.86	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
46.19.85.140	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
79.182.111.34	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.86	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
84.94.181.121	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
117.20.118.41	Cambodia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
66.249.76.2	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.33	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
73.255.140.129	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.153.108.155	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
104.153.108.155	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
73.255.140.129	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
104.153.108.155	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
104.153.108.155	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
73.255.140.129	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
109.253.218.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
93.172.147.113	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
73.222.149.91	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
104.153.108.155	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.29.73.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
73.255.140.129	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.186.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
36.5.249.243	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.5.249.243	Block	17
36.5.249.243	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
46.120.203.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.180.54.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
152.99.67.85	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.229.245	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
207.46.13.184	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/console/core/doc_mgr/null	Block	1
36.5.249.243	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
71.6.146.185	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/robots.txt	Block	1
37.46.41.154	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
76.175.69.112	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	1