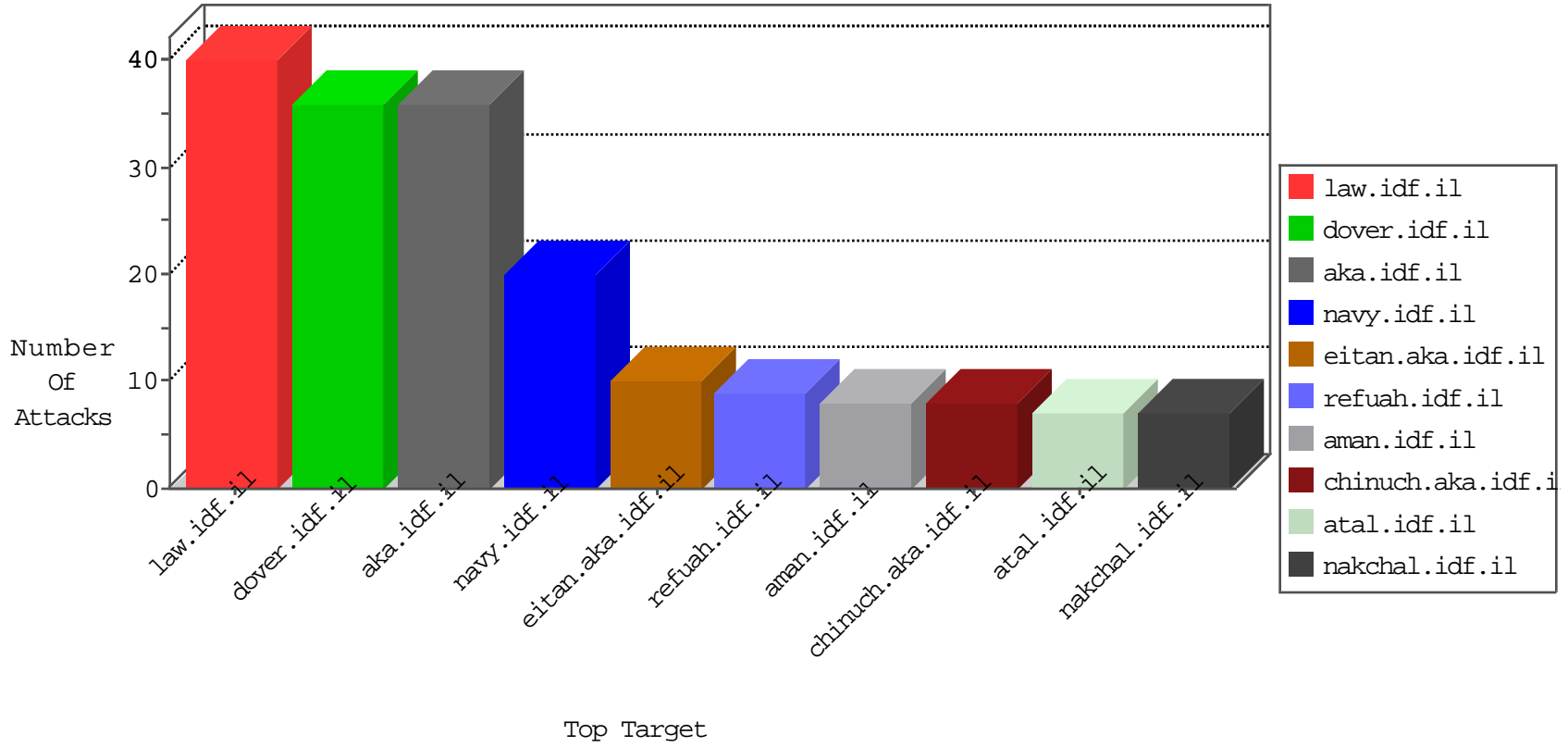


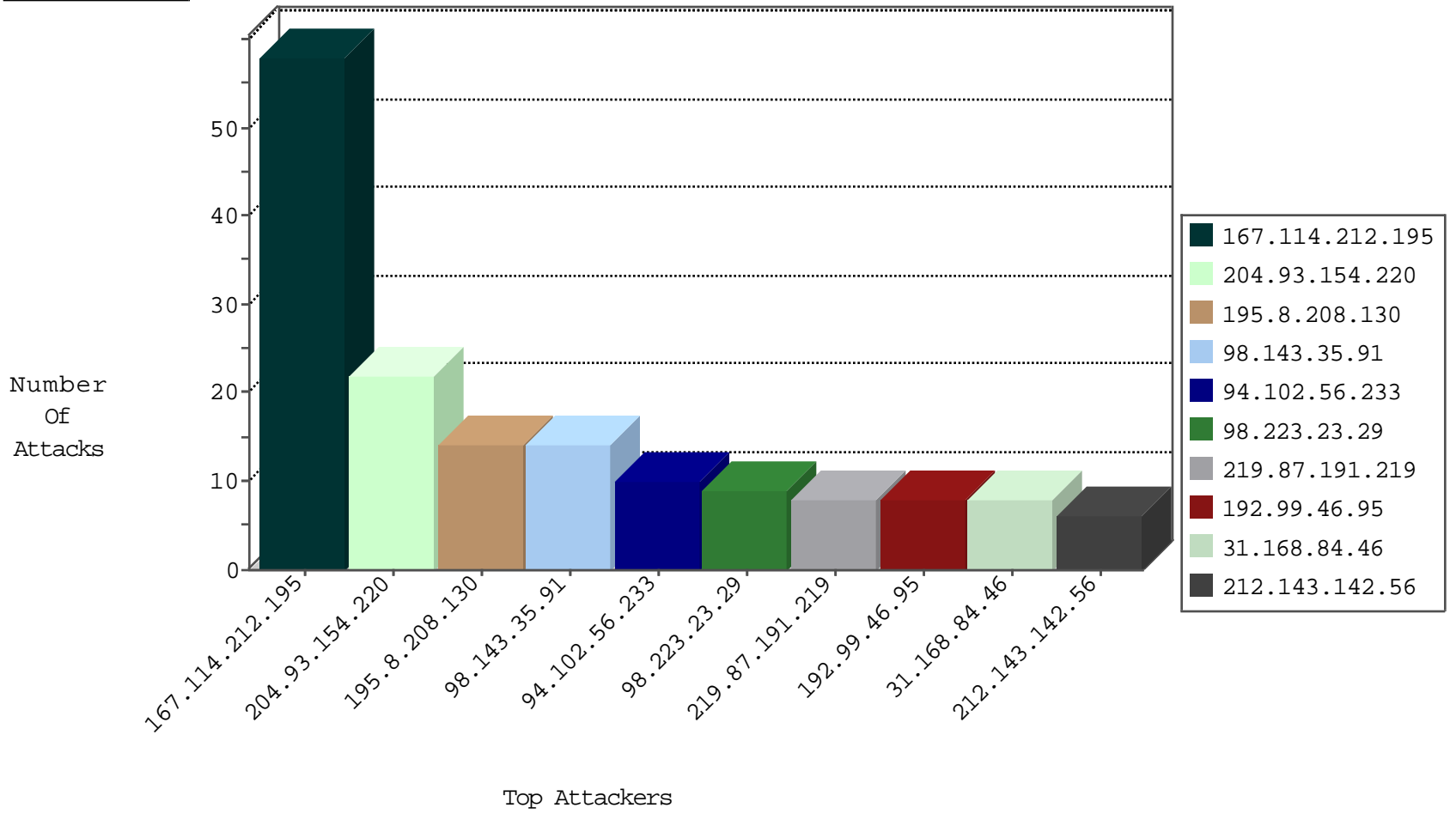
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.220	United States	147.237.77.74	law.idf.il	TCP Scan (vertical)	drop	175
209.126.136.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
158.217.165.220	Japan	147.237.77.205	prisha.idf.il	JIM_Purple_Con_Limit_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.8.208.130	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.154.73.125	France	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	4
111.202.102.66	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.8.208.130	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	8
158.217.165.220	147.237.77.235	Japan	sviva.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
158.217.165.220	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
150.242.238.99	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.233	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.196	Taiwan	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.176	Taiwan	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.38	Taiwan	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
158.217.165.220	147.237.77.227	Japan	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
158.217.165.220	147.237.76.147	Japan	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.39	Taiwan	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.34	Taiwan	yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.15	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	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
50.63.197.204	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
167.114.212.195	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
167.114.212.195	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
31.168.84.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
167.114.212.195	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
167.114.212.195	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
31.168.84.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
167.114.212.195	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
66.249.69.223	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.212.195	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
167.114.212.195	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
167.114.212.195	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
167.114.212.195	Canada	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
167.114.212.195	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
78.54.68.48	Germany	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.37.113	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
125.77.28.26	China	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
192.99.46.95	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
98.143.35.91	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.82	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.77.91.109	Turkey	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
98.143.35.91	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.69	United States	147.237.0.35	akaws.idf.il	drop		drop	1
167.114.212.195	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
65.55.218.40	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
131.253.24.150	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
98.143.148.107	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.212.195	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
192.99.46.95	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
98.143.35.91	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.73	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
78.54.68.48	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.34	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
125.77.28.26	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
167.114.212.195	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
192.99.46.95	Canada	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
98.143.35.91	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.82	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.77.91.109	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
98.143.35.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.70	United States	147.237.0.35	akaws.idf.il	drop		drop	1
65.55.218.58	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
131.253.24.151	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.223.23.29	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 98.223.23.29	Block	5
98.223.23.29	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	2
219.74.37.34	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
220.255.183.170	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.88.144	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
121.7.37.132	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
203.127.96.233	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/info.asp	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
204.79.180.223	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
66.249.88.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
66.249.88.143	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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/0/68320.doc	Block	1
109.64.25.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1