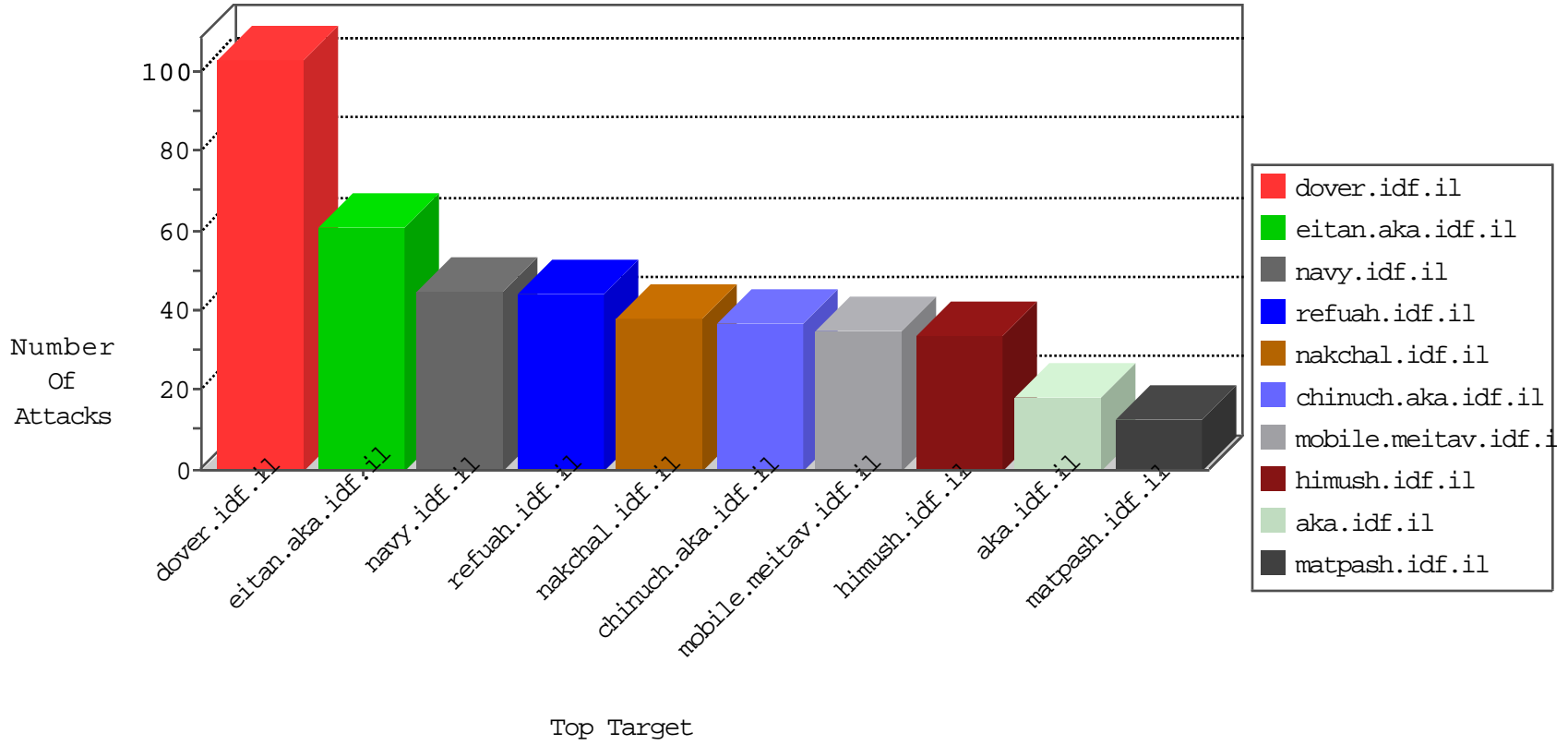


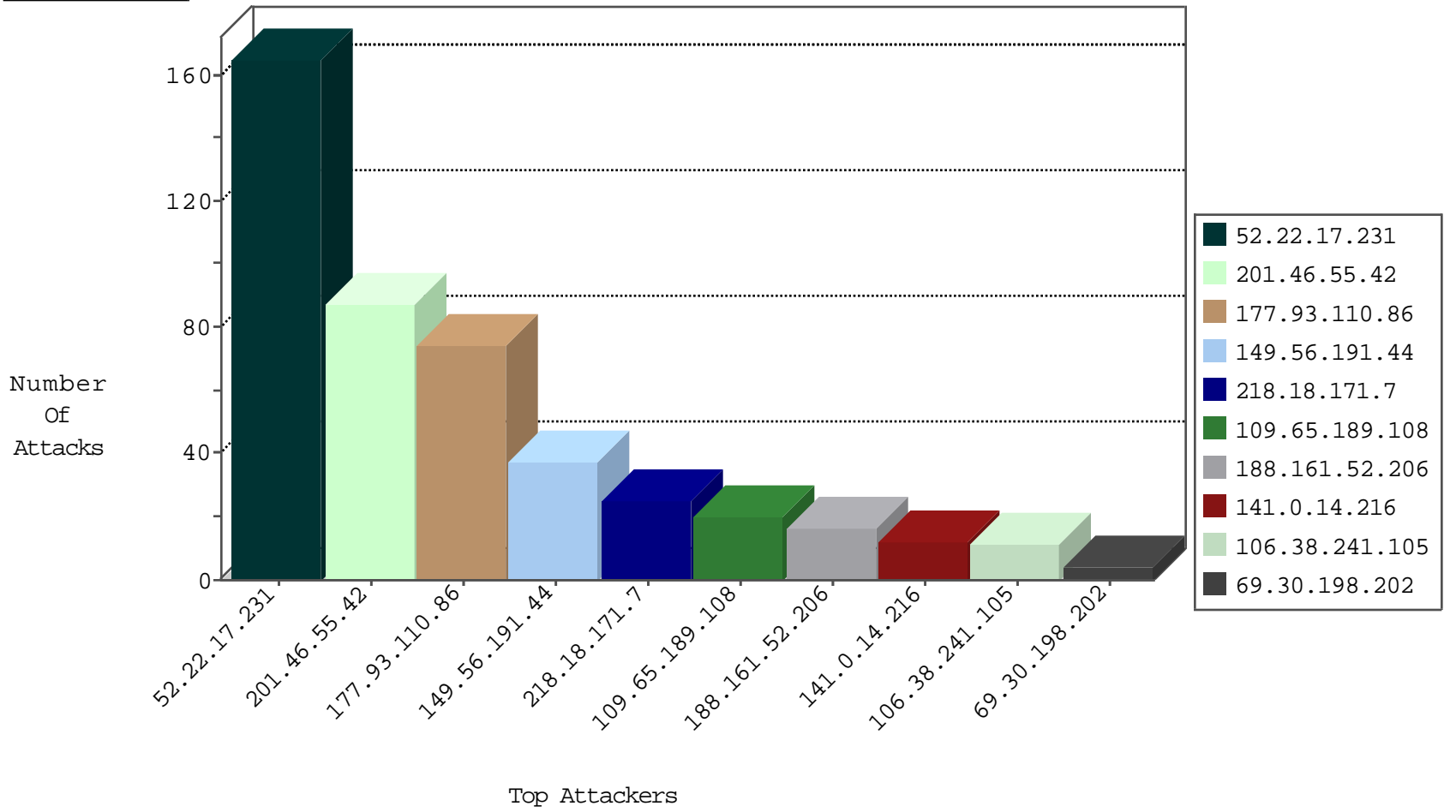
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	2
58.218.200.137	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
71.6.158.166	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
137.226.113.7	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
146.0.79.172	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	11
162.210.196.130	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
103.207.37.81	147.237.76.42	Vietnam	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
85.14.42.2	147.237.77.179	Bulgaria	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
80.87.205.120	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
220.242.82.131	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -f -sS	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
195.88.208.193	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.149	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.94.130	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
120.236.19.10	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
120.236.19.2	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
85.14.42.2	147.237.77.179	Bulgaria	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
85.14.42.2	147.237.77.179	Bulgaria	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
220.242.82.131	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
80.87.205.120	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
211.141.78.56	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
193.201.225.149	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.94.130	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
193.201.225.149	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.94.130	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -f -sS	1
120.236.19.10	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
120.236.19.2	147.237.0.16	China	my-kosher-kravi.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
52.22.17.231	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
52.22.17.231	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
52.22.17.231	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
52.22.17.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
52.22.17.231	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
109.65.189.108	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
52.22.17.231	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
52.22.17.231	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
52.22.17.231	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
141.0.14.216	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
188.161.52.206	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
188.161.52.206	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
177.93.110.86	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
177.93.110.86	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
177.93.110.86	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
177.93.110.86	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
177.93.110.86	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
177.93.110.86	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
177.93.110.86	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
177.93.110.86	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
54.234.131.192	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
177.93.110.86	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
177.93.110.86	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
177.93.110.86	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
177.93.110.86	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
177.93.110.86	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
177.93.110.86	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
177.93.110.86	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
177.93.110.86	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
177.93.110.86	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
109.253.218.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
177.93.110.86	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
69.30.198.202	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
69.30.198.202	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
218.18.171.7	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.18.171.7	Block	17
218.18.171.7	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.174	Block	1
107.77.219.27	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
66.249.69.134	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding 82G013ebf[{}u@oTlGh8I]nprO in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
157.55.39.241	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-8504/tikshuv.aspx	Block	1
218.18.171.7	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
157.55.39.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
71.195.0.165	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	1
192.169.7.223	United States	147.237.0.19	madim.atal.idf.il	Unauthorized Method HEAD for 147.237.0.19/	Block	1
73.128.133.27	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1