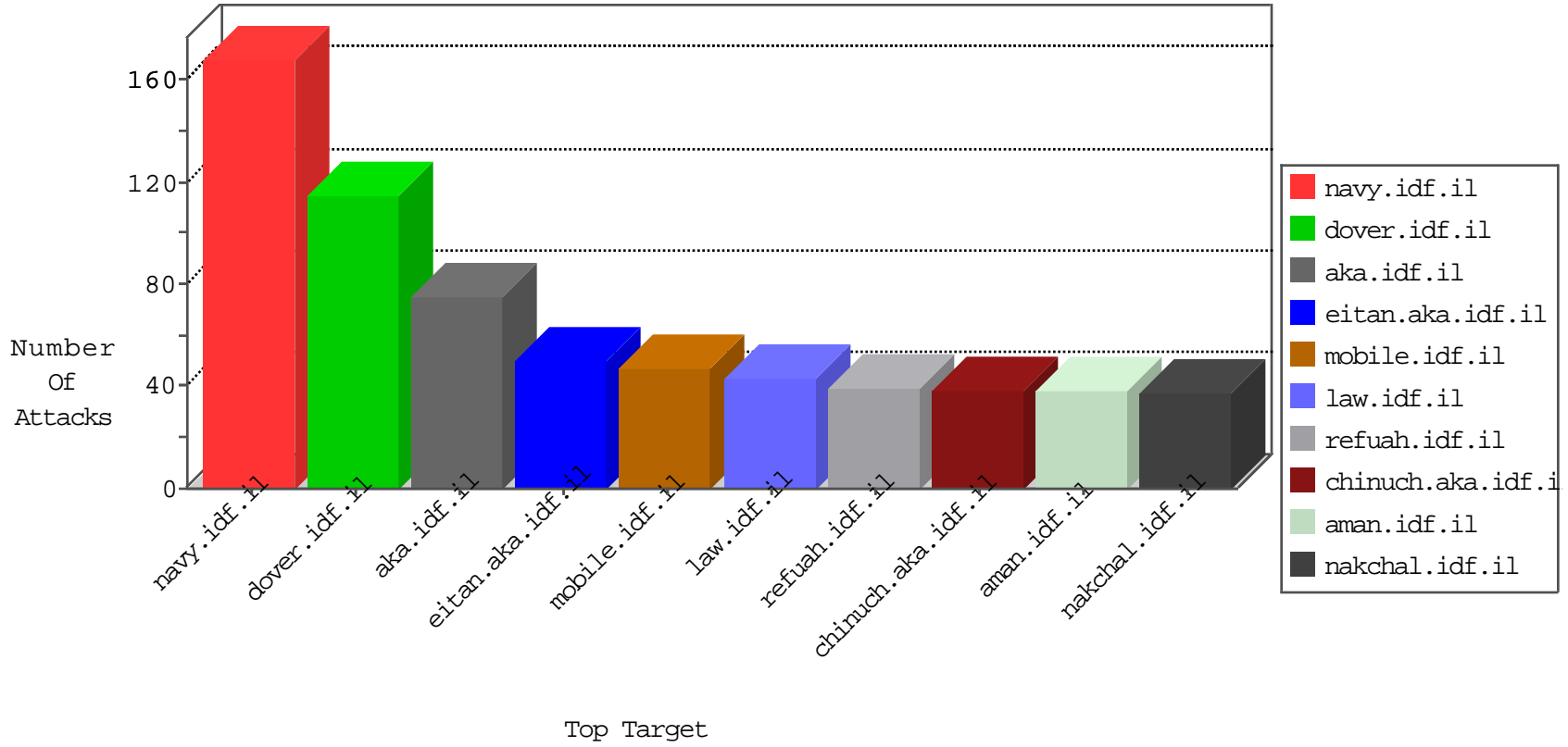


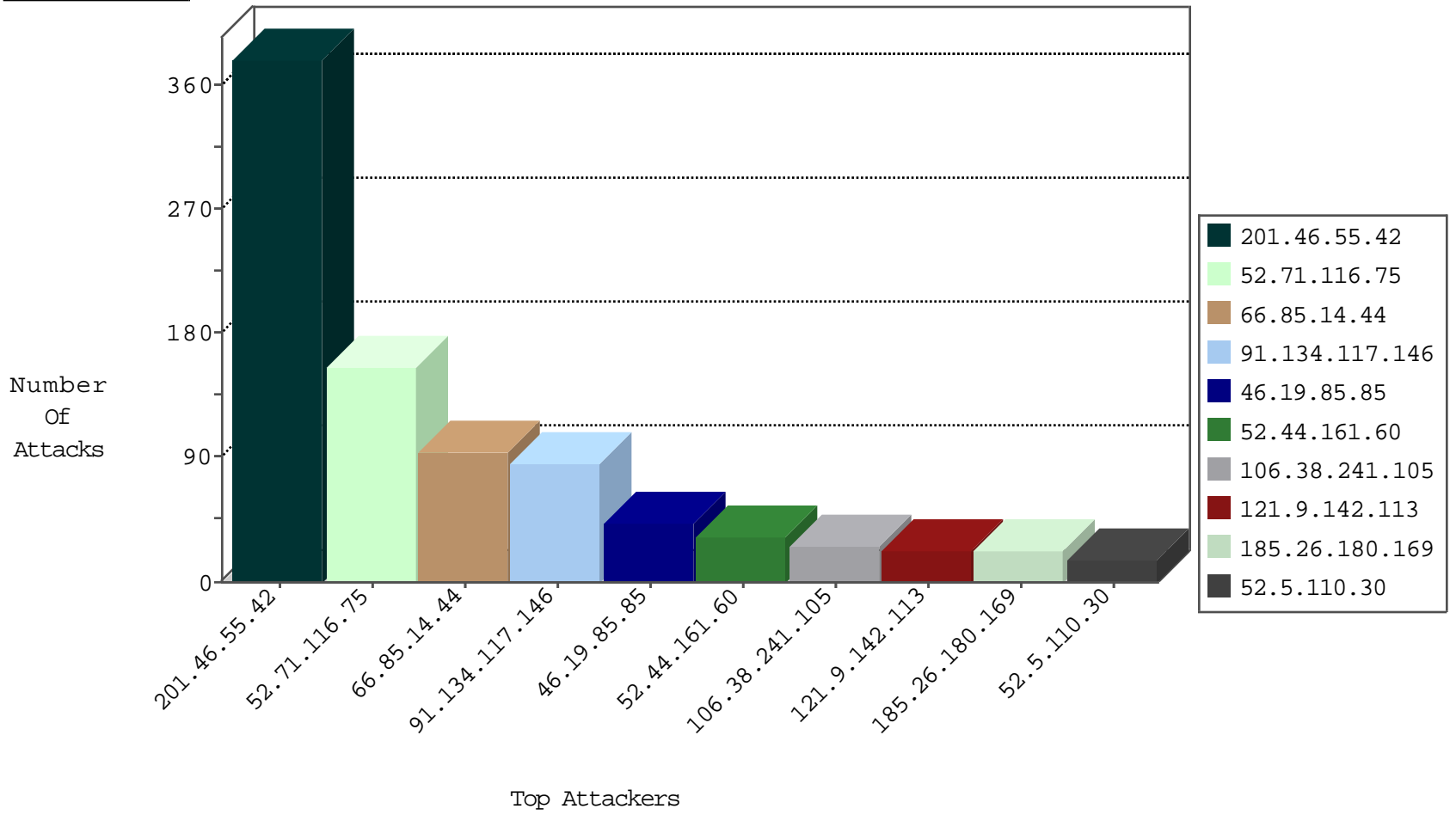
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
123.59.59.52	China	147.237.77.176	matpash.idf.il	block-sp-trafl	forward	2
149.202.57.201	France	147.237.76.177	ncore.idf.il	Black List	drop	1
93.174.93.156	Netherlands	147.237.76.42	refuah.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	21
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
151.80.31.182	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.75.46	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
42.116.29.68	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
195.88.208.193	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
42.116.29.68	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
191.109.221.33	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.129.15	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
195.88.208.193	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
42.116.29.68	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.76.197	Canada	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.147	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
66.85.14.44	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	22
185.26.180.169	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
66.85.14.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
5.10.231.162	Iraq	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
2.53.59.40	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
66.85.14.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
71.170.15.211	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
66.190.183.33	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.42	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
52.71.116.75	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
52.71.116.75	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
52.71.116.75	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
52.71.116.75	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
52.71.116.75	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
52.71.116.75	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
52.71.116.75	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.42	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
52.71.116.75	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
52.71.116.75	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
52.71.116.75	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
52.71.116.75	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
52.71.116.75	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
52.71.116.75	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
52.71.116.75	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.9.142.113	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 121.9.142.113	Block	17
121.9.142.113	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
80.246.136.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.64.220	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/724-5764-he/patzar.aspx	Block	1
204.79.180.82	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
92.75.237.172	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.4.74.42	Block	1
157.55.39.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/&sa=u&ved=0ahukewj-ienfrp_jahvdtbqkhd8_cw0qf ggkmag&sig2=lfjvi6ayozbqh88tgi4jzq&usg=afqjcnhcyyg7wlcq-yhd5_ammz oyodtwa	Block	1
66.249.64.224	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/881-he/patzar.aspx	Block	1
106.38.241.105	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10670-en	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
157.55.39.74	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
66.249.64.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1444-he/atal.aspx	Block	1
109.67.33.248	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
46.101.147.179	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/default.asp	Block	1
185.27.105.92	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
68.180.228.29	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/general.aspx	Block	1
185.89.217.231	Netherlands	147.237.77.74	law.idf.il	Distributed URL is Above Root Directory	Block	1