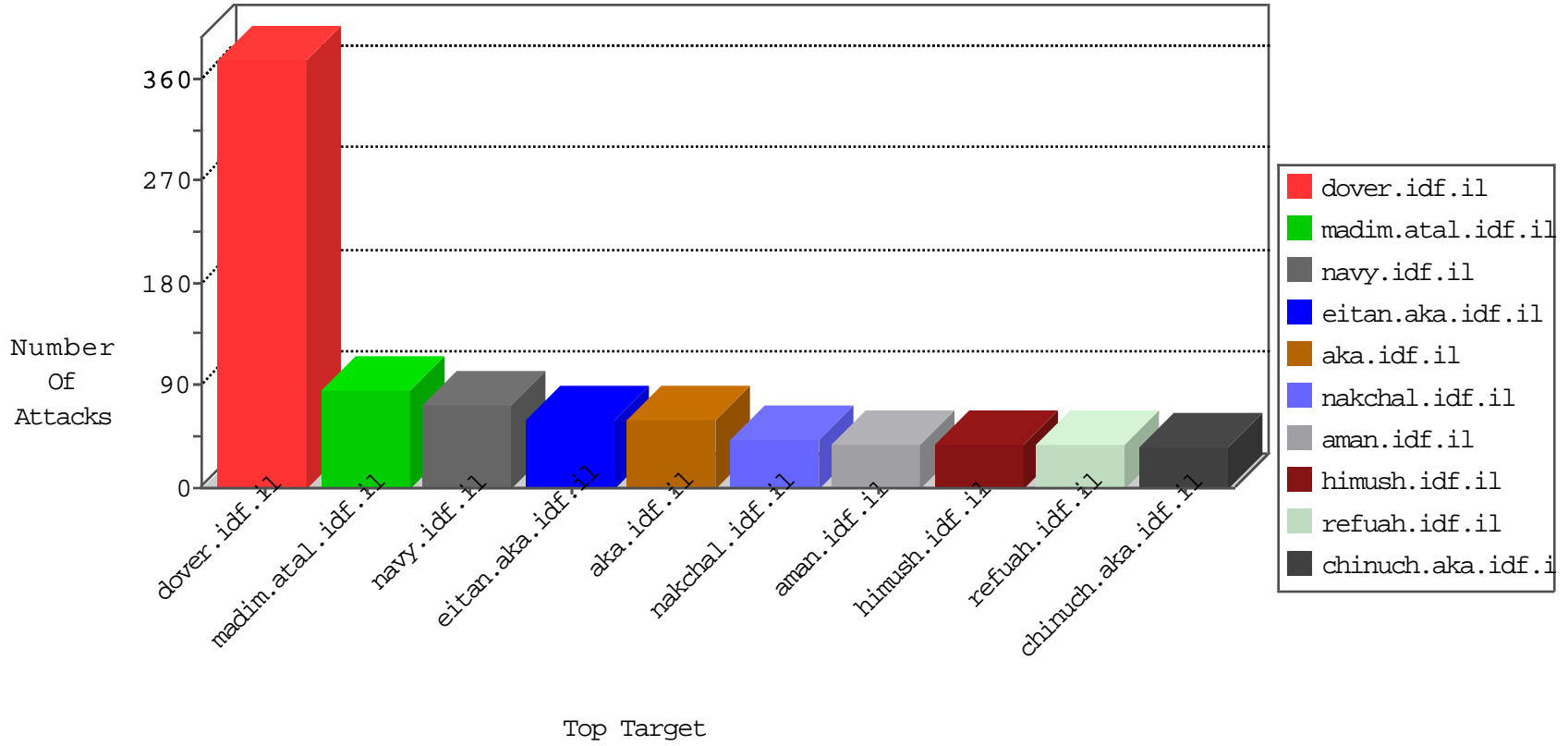


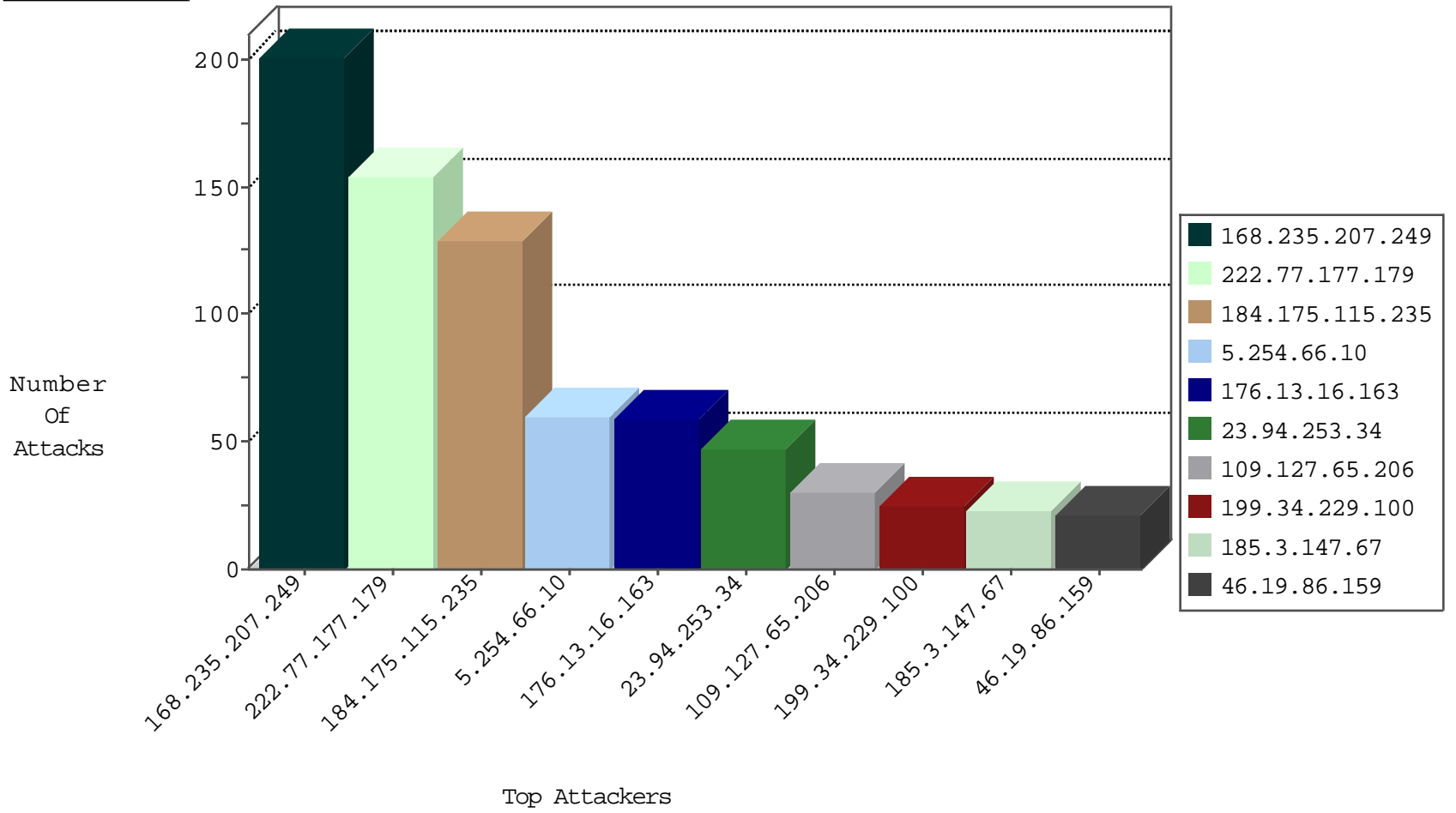
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.207.249	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
207.46.13.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.240.219.146	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
71.6.216.49	United States	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.209	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.20.69.74	United States	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
91.121.136.34	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
45.56.96.80	147.237.77.216	United States	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
150.242.238.99	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.20	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.20	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.165.189	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
65.23.114.140	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
179.33.73.139	147.237.77.216	Colombia	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.192.0.22	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.20	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
65.23.114.140	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
65.23.114.140	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
198.20.69.74	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.207.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
168.235.207.249	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	59
199.34.229.100	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
184.151.179.68	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
185.3.147.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
176.13.15.247	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.29.114.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
5.254.66.10	Romania	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
5.254.66.10	Romania	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
222.77.177.179	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
222.77.177.179	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
222.77.177.179	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
5.254.66.10	Romania	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
184.175.115.235	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
222.77.177.179	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
185.3.147.67	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
222.77.177.179	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
184.175.115.235	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
84.109.18.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
184.175.115.235	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
5.254.66.10	Romania	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
5.254.66.10	Romania	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
184.175.115.235	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
5.254.66.10	Romania	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
184.175.115.235	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
184.175.115.235	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
5.254.66.10	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
184.175.115.235	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
222.77.177.179	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
222.77.177.179	China	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
62.219.137.5	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
184.175.115.235	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
222.77.177.179	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.64.39.127	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
222.77.177.179	China	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
184.175.115.235	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
222.77.177.179	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
222.77.177.179	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
23.94.253.34	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
23.94.253.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
184.175.115.235	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.182.23.21	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
5.254.66.10	Romania	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
141.0.13.241	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
184.175.115.235	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
184.175.115.235	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
176.13.244.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
45.56.96.80	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
77.139.59.223	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	2
37.26.147.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.63.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.224	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	1
66.249.64.228	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Malformed HTTP Header Line 2	Block	1
89.138.165.189	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy.	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
40.77.167.52	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62048	Block	1
185.27.105.82	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
109.253.200.63	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	1
46.117.179.84	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
45.56.96.80	United States	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
204.79.180.50	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluum/templates/inner.asp	Block	1
66.249.69.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	1
157.55.39.253	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.45	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
45.56.96.80	United States	147.237.77.216	dover.idf.il	Unauthorized Method OPTIONS for /	Block	1
213.151.35.221	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/default.asp	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed URL from 45.79.71.122	Block	1