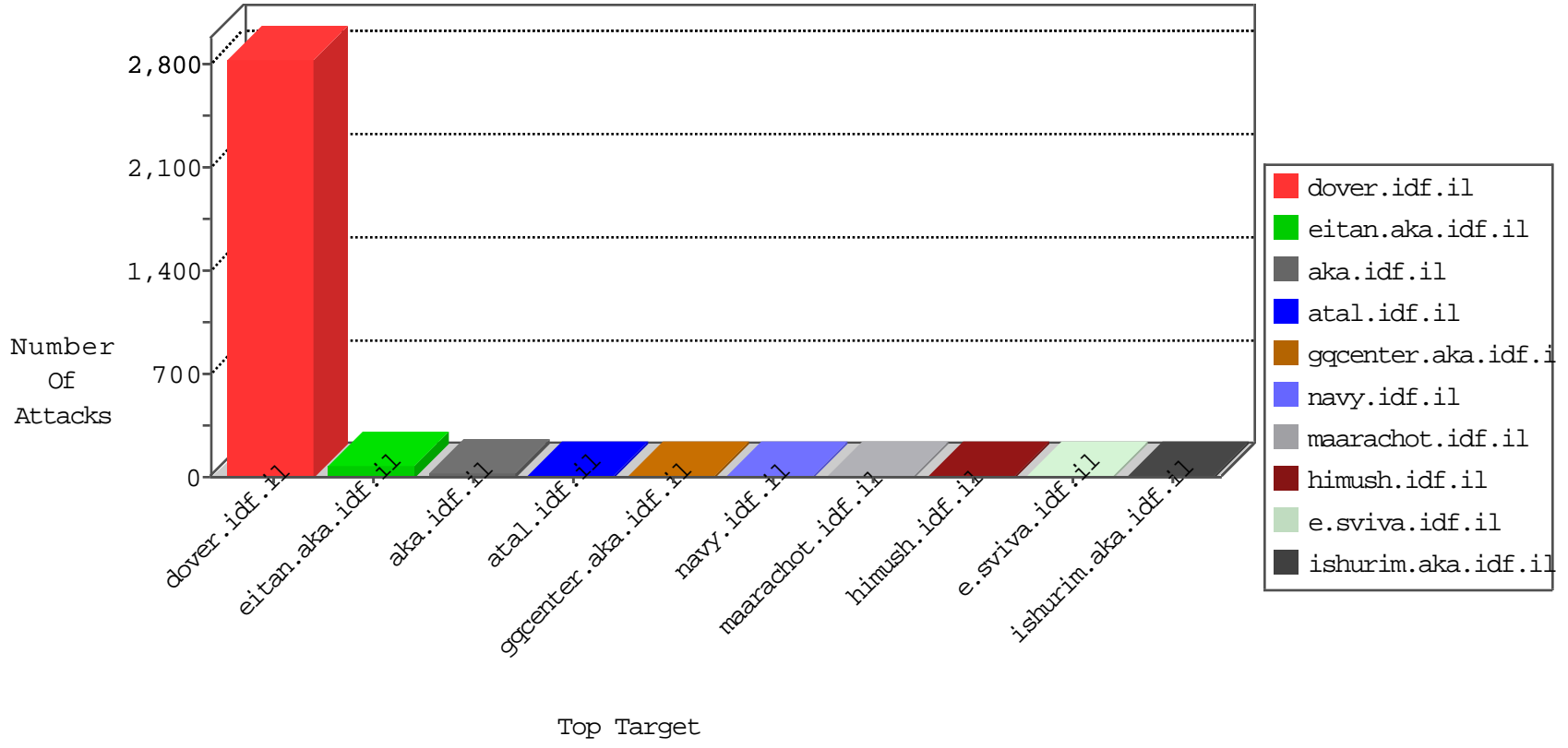


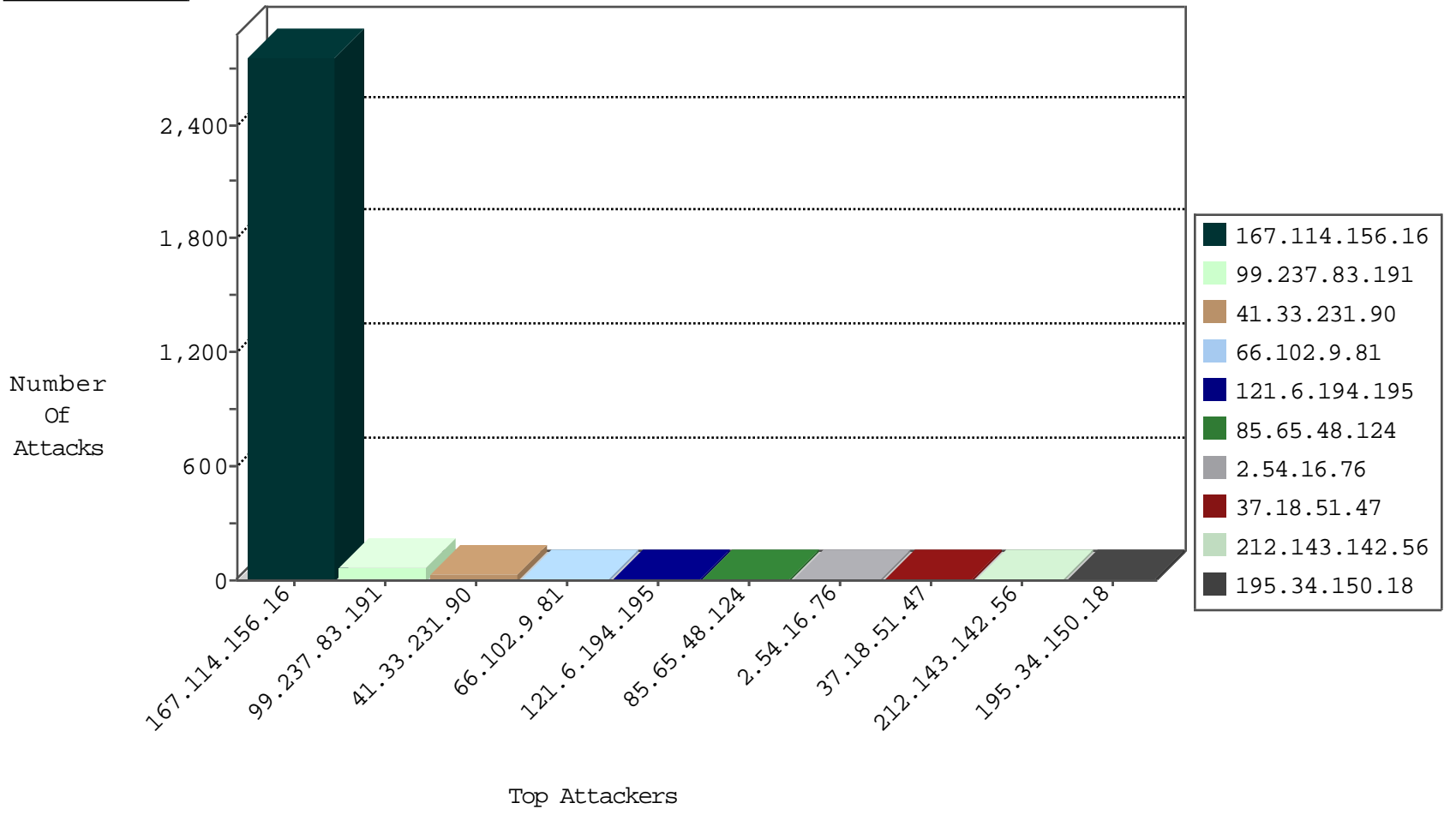
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3565
222.186.21.75	China	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
202.112.51.96	China	147.237.77.176	matpash.idf.il	block-sp-trafl	drop	1

12-05-2015-07:04:00 to 12-05-2015-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
122.114.17.100	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
138.121.34.52	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
31.148.219.86	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
208.69.30.8	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.176	Sweden	test.noore.idf.il	ET SCAN NMAP -sS window 1024	1
189.220.51.154	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.114.17.100	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
201.173.220.93	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.105.134.220	147.237.77.212	Sweden	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.39	Sweden	mobile.meitav.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
66.102.9.81	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.16.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.48.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.18.51.47	Russian Federation	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.66.179.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.29.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.154.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.159.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
121.6.194.195	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
121.6.194.195	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
121.6.194.195	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.105.106.67	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
121.6.194.195	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.25.7	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
121.6.194.195	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
84.228.54.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.234.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.69.124.80	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.59	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.153.186.23	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.64	United States	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
85.64.150.67	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.84	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.176	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
87.69.124.80	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.77	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.64.150.67	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.186	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
79.180.136.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.78	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.11	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.187	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.133.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.211	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
86.123.240.150	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.82.47.12	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.116.147	United States	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
37.153.186.23	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.121.191	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 99.237.83.191	Block	56
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1134-he/dover.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/may/bethlehem2.stm" target="_blank	Block	1
82.160.134.5	Poland	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp/wp-admin/	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71919-he/maarachot.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1158-he/dover.aspx	Block	1
197.37.37.121	Egypt	147.237.76.30	himush.idf.il	PHP Attempt	Block	1
85.25.236.165	Germany	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2349.jpg	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
197.37.37.121	Egypt	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/xmlrpc.php	Block	1
85.65.48.124	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 85.65.48.124	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2277.jpg	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/gyus/general.aspx	Block	1
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.170.44.126	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
66.249.66.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/gyus/general.aspx	Block	1