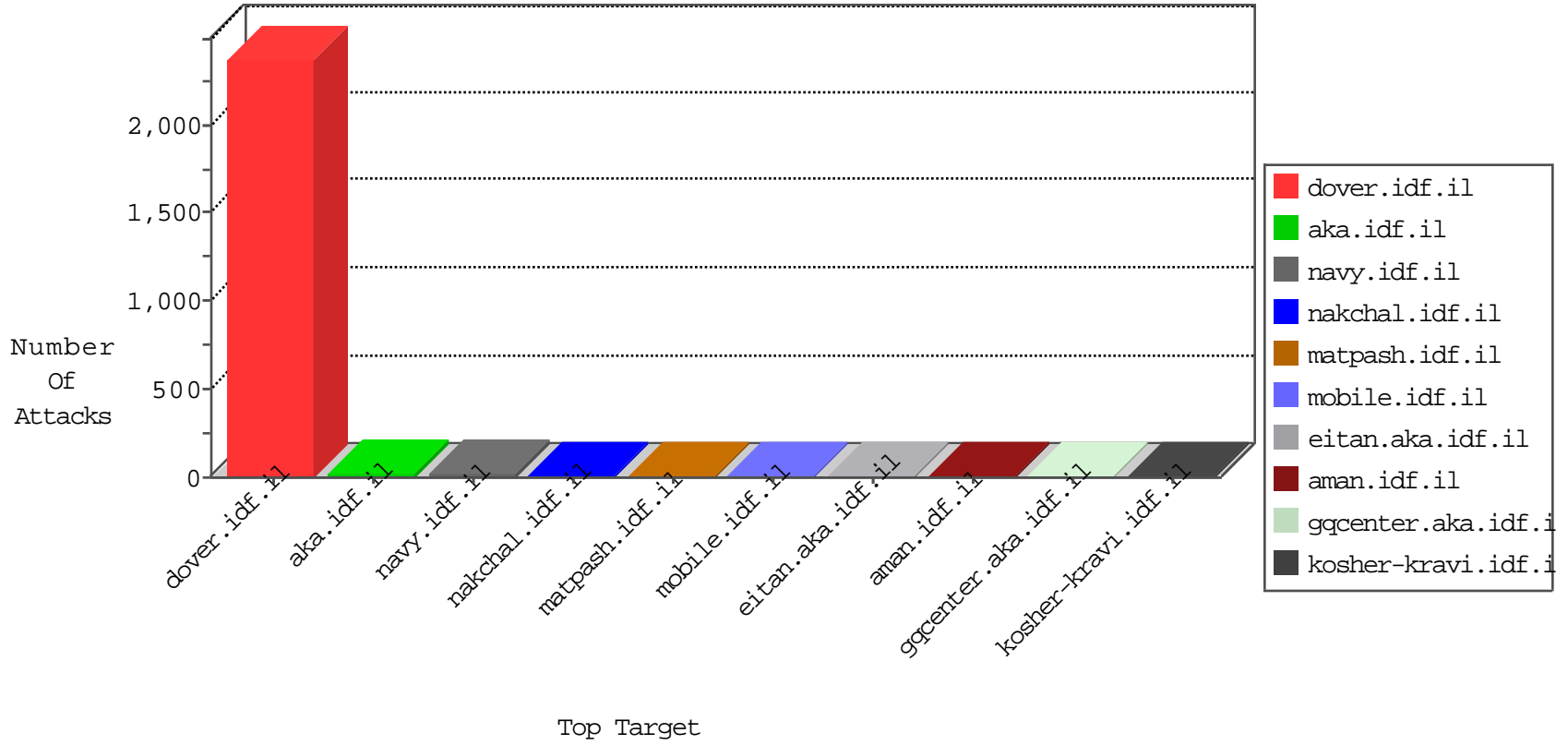


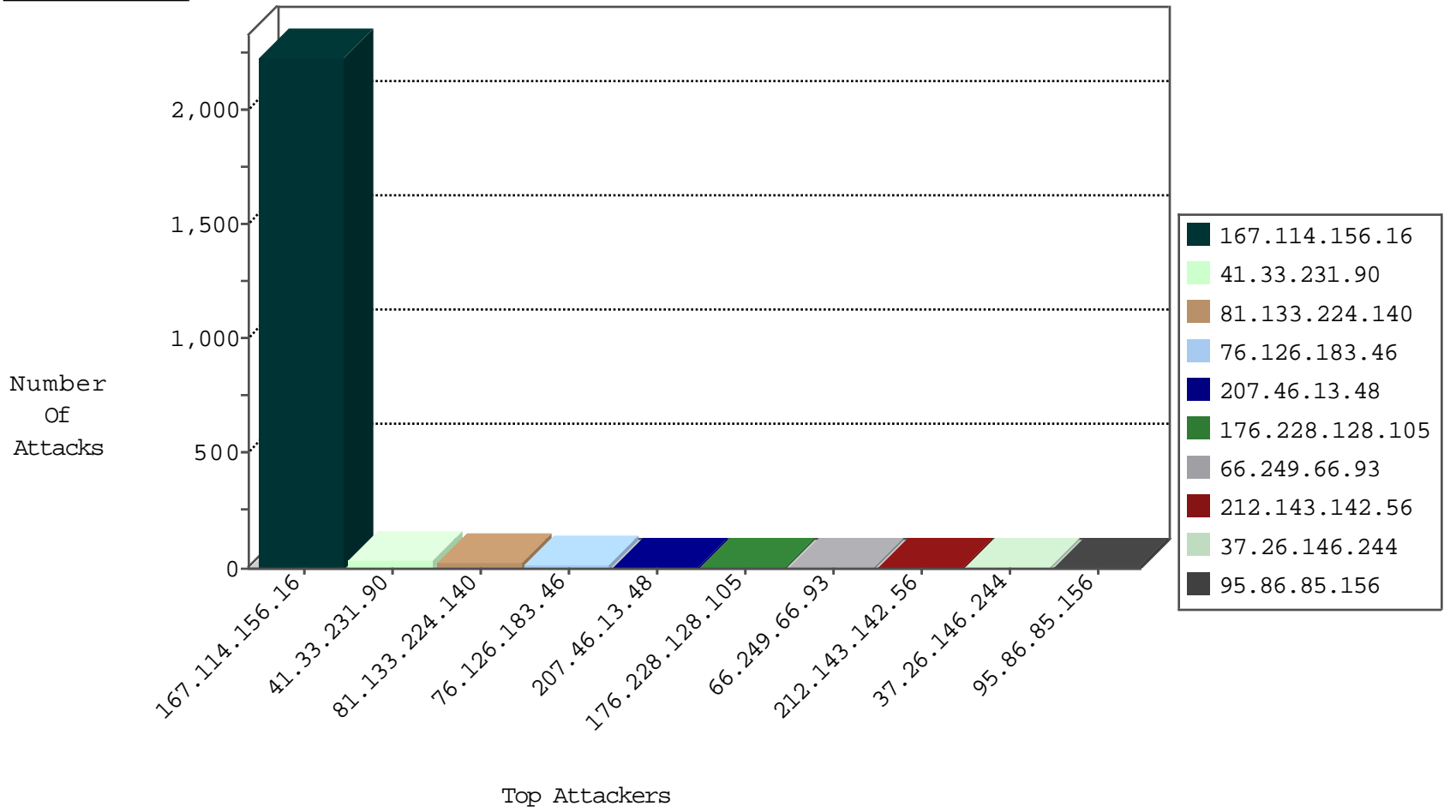
# IDF Under Attack Daily Report



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	3420
66.249.66.26	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	3177
81.133.224.140	United Kingdom	147.237.77.216	dover.idf.il	I4 Source or Dest Port Zero	drop	7
218.6.155.58	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
115.231.222.40	China	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.122	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
61.189.228.178	China	147.237.76.34	ychalan.idf.il	Block_Udp_All_Nets	drop	1

12-13-2015-04:04:07 to 12-13-2015-05:04:07

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	5
94.102.48.195	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
24.149.125.48	147.237.72.14	United States	dover.idf.il(olc	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
24.149.125.48	147.237.72.156	United States	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	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	36
81.133.224.140	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
76.126.183.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.48	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	8
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.228.128.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.77	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
46.19.85.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.159.211.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
199.30.24.211	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.149.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.167.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
95.86.124.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.5	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.155	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
94.75.220.155	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.76.15.19	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.210.105.116	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.206	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.6.155.58	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
203.133.168.147	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
185.101.107.189		147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.195	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
94.75.220.155	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
199.203.206.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.17.31.10	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.124	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.249.64.74	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.207	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
204.85.191.30	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
50.186.128.54	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.195	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.84	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.75.220.155	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
200.108.244.122	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.232	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.85.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
95.86.85.156	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.85.156	Block	2
66.249.66.32	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
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
185.101.107.189		147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
89.138.217.165	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	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
66.249.66.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.66.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.56.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
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	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/1133-18719-he/dover.aspx	Block	1
37.8.47.98	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
157.55.39.173	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jenin.stm" target="_blank	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9032-he/refuah.aspx	Block	1
184.105.247.196	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1930-he/cogat.aspx	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1415	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/20032011yezu.aspx	Block	1
66.249.65.122	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/404.aspx	Block	1