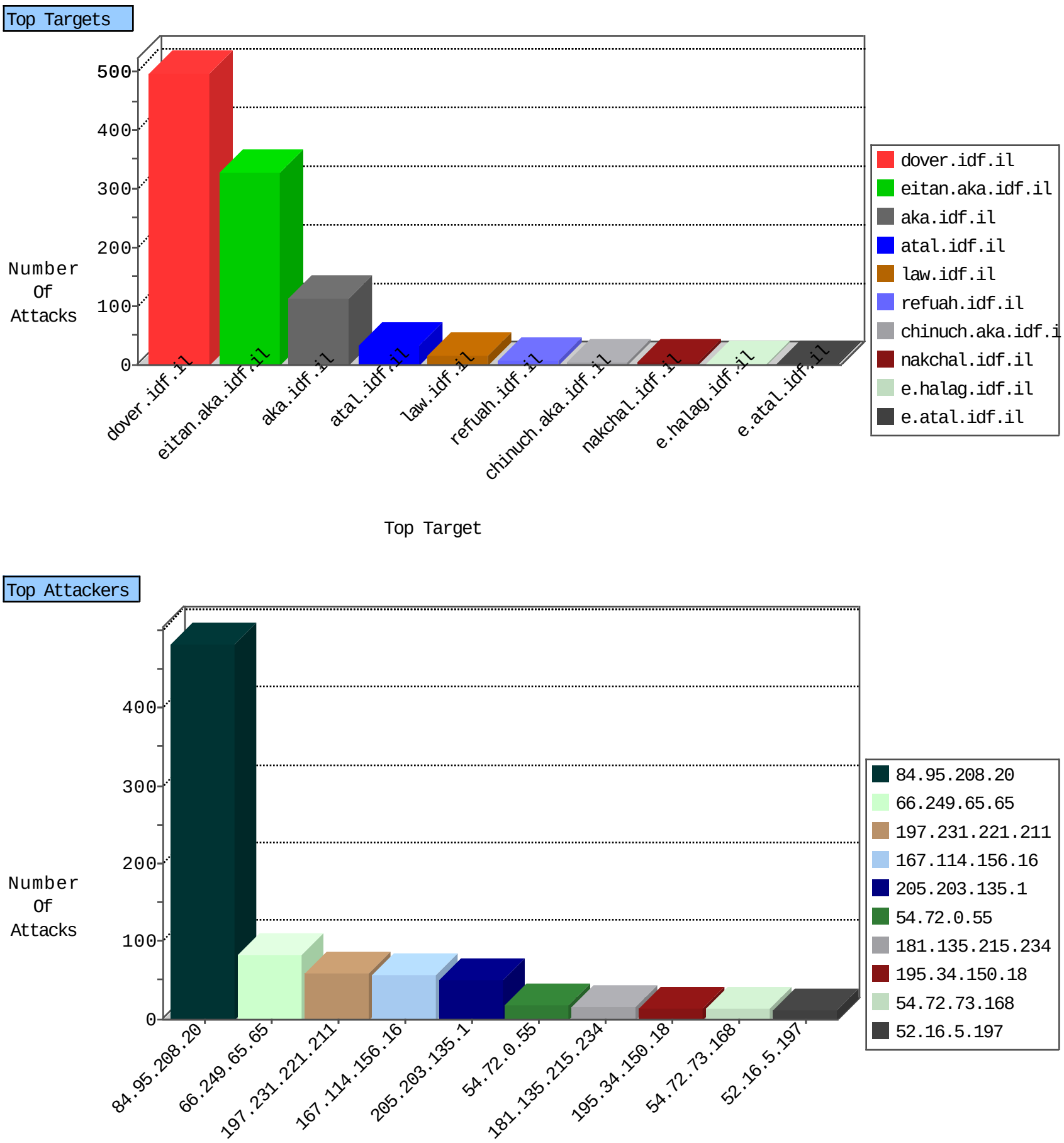
05-04-2016-04:04:03 to 05-04-2016-05:04:03

IDF Under Attack Daily Report



05-04-2016-04:04:03 to 05-04-2016-05:04:03

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	HTTP-POST-Segmented-DoS	dest-reset	2723
69.197.185.18	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
66.249.65.18	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
107.150.32.58	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
107.150.32.61	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.39	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
107.150.46.37	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
198.55.103.222	United States	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1

05-04-2016-04:04:03 to 05-04-2016-05:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-04:04:03 to 05-04-2016-05:04:03

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
200.195.135.82	147.237.77.243	Brazil	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
112.169.100.157	147.237.76.202	Korea, Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
112.169.100.157	147.237.76.147	Korea, Republic of	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
91.197.232.40	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
13.82.25.17	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
200.195.135.82	147.237.77.243	Brazil	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
112.169.100.157	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Potential SSH Scan	1
112.169.100.157	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
13.82.25.17	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

05-04-2016-04:04:03 to 05-04-2016-05:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
84.95.208.20	Israel	147.237.77.233	atal.idf.il	drop	SAM rule	drop	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
181.135.215.234	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
84.95.208.20	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	15
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	drop	SAM rule	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.218.151.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
36.110.147.67	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
67.82.229.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
121.54.54.53	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
104.154.75.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.73.243	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.9.122.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.53.168.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.176	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
189.61.88.40	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
121.54.54.134	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.70.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.138.192.35	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
164.132.161.91	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.234.93.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
186.80.37.111	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
199.30.24.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	98
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
121.54.54.131	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/mobile	Block	2
51.255.65.36	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/11.asp	Block	1
104.139.37.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9698-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;h in www.aka.idf.il/main/giyus/captcha.ashx	None	1
69.197.185.18	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.defences1.com/	Block	1
66.249.73.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
79.178.159.101	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.178.159.101 (Open Mode)	None	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2799.jpg	Block	1
79.178.159.101	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.55.128.243	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.89	Block	1