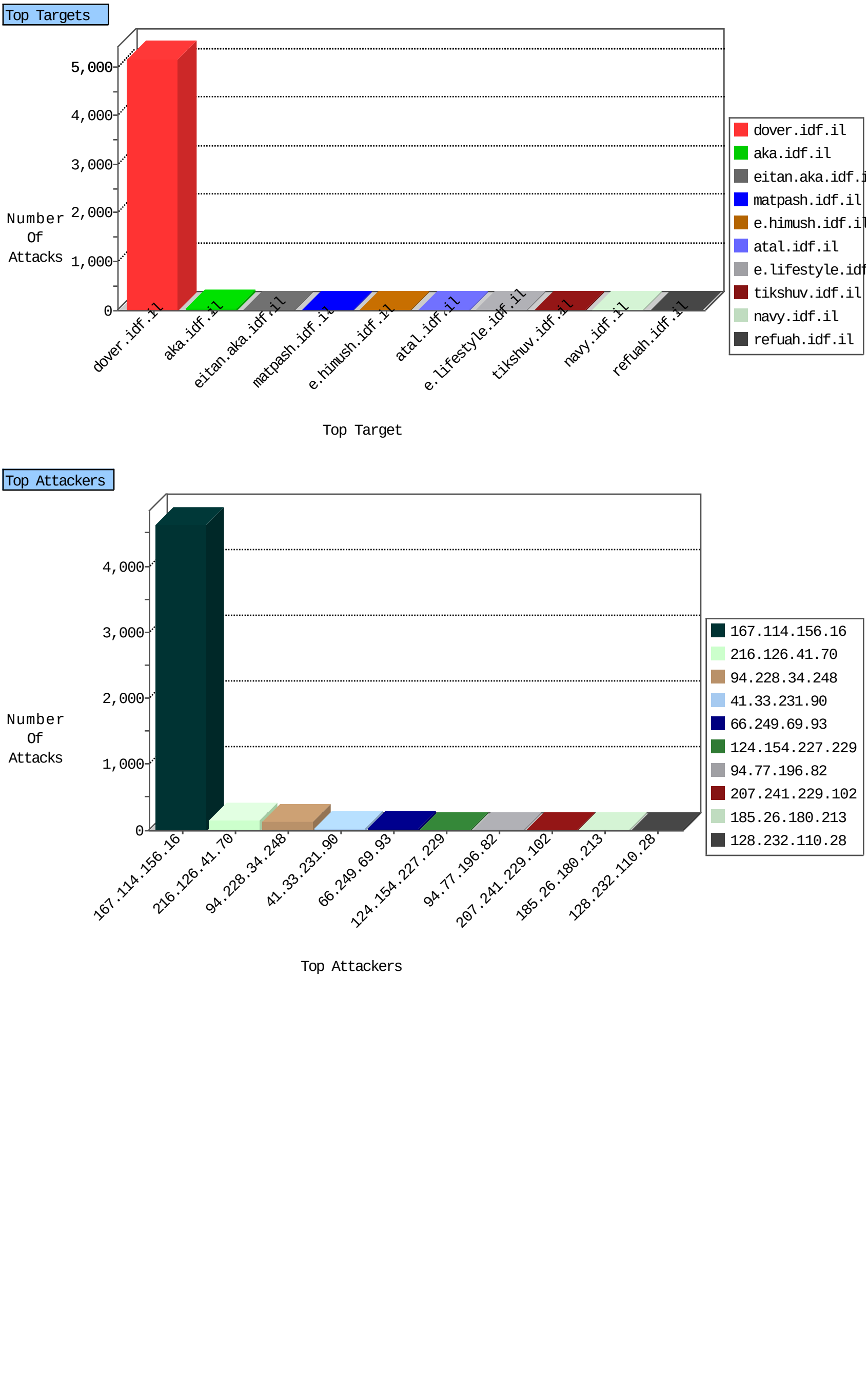
04-21-2016-04:04:02 to 04-21-2016-05:04:02

IDF Under Attack
Daily Report



04-21-2016-04:04:02 to 04-21-2016-05:04:02

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	6866
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2486
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1706
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	26
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
94.102.52.10	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
180.153.91.183	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.102.52.10	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-21-2016-04:04:02 to 04-21-2016-05:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-04:04:02 to 04-21-2016-05:04:02

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	3
122.173.18.8	147.237.0.19	India	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.240.250.154	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
58.218.205.69	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
93.180.66.29	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.205.69	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
202.67.237.220	147.237.77.216	Hong Kong	dover.idf.il	ET SCAN Potential SSH Scan	1

04-21-2016-04:04:02 to 04-21-2016-05:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3558
216.126.41.70	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	146
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
124.154.227.229	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
185.26.180.213	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.176.4.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
149.88.200.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
52.58.92.83	Germany	147.237.8.24	e.lifestyle.idf.	Geo-location enforcement	Geo-location inbound enforcement	drop	4
83.219.199.236	Sweden	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
66.249.69.175	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
46.166.190.181	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
103.234.89.116	Vietnam	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.126.85.176	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.25.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
156.208.73.29	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
8.37.70.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
156.208.73.29	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
173.252.90.97	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
204.79.180.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
190.43.254.237	Peru	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
141.212.122.220	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
204.79.180.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
198.50.200.139	Canada	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
185.26.180.213	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-21-2016-04:04:02 to 04-21-2016-05:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	3
124.154.227.229	Japan	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	2
107.200.54.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1280-	Block	1
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
106.38.241.149	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13077-en/dovera93f95ecb7909e49	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
144.76.93.46	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
107.200.54.76	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sa_swfobject.js	Block	1
198.58.103.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
65.158.81.132	United States	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

04-21-2016-04:04:02 to 04-21-2016-05:04:02