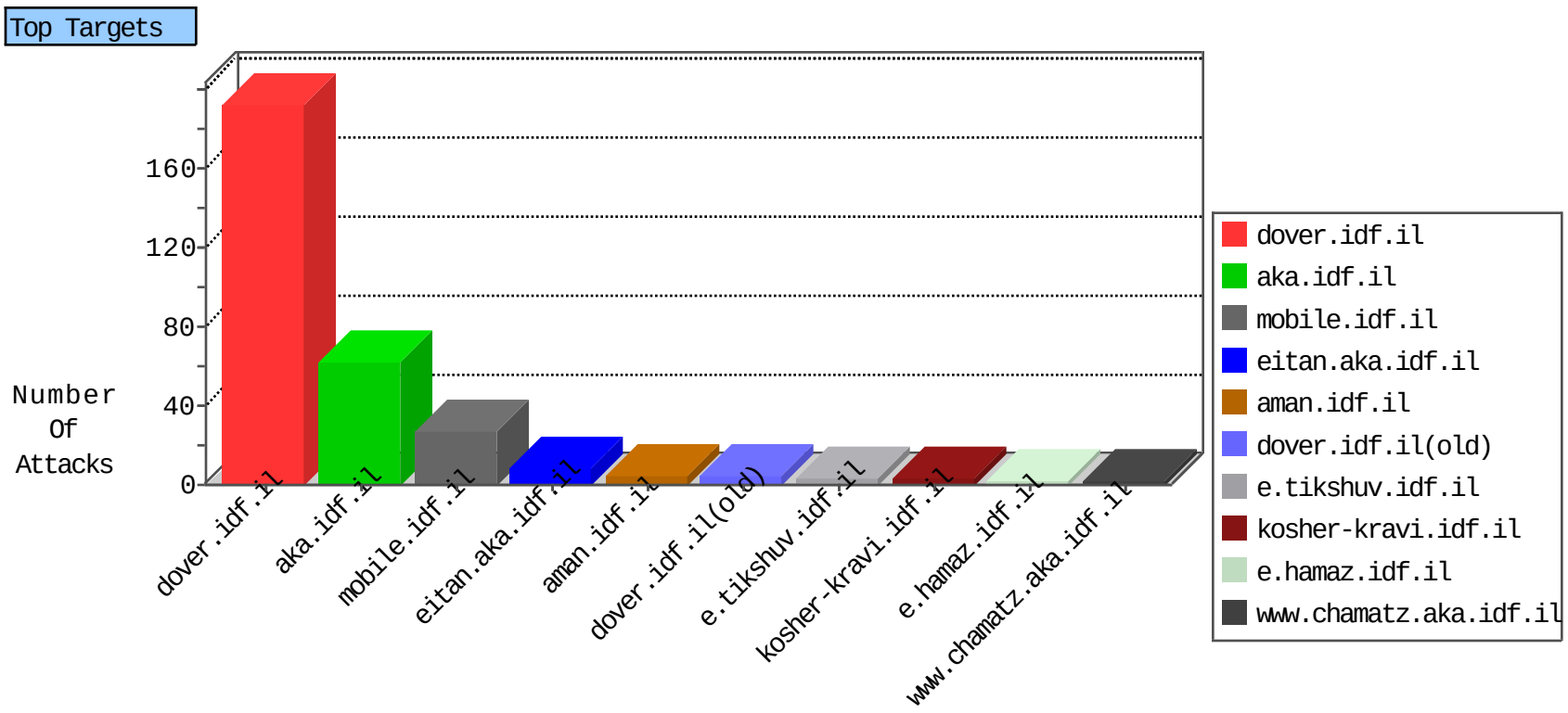
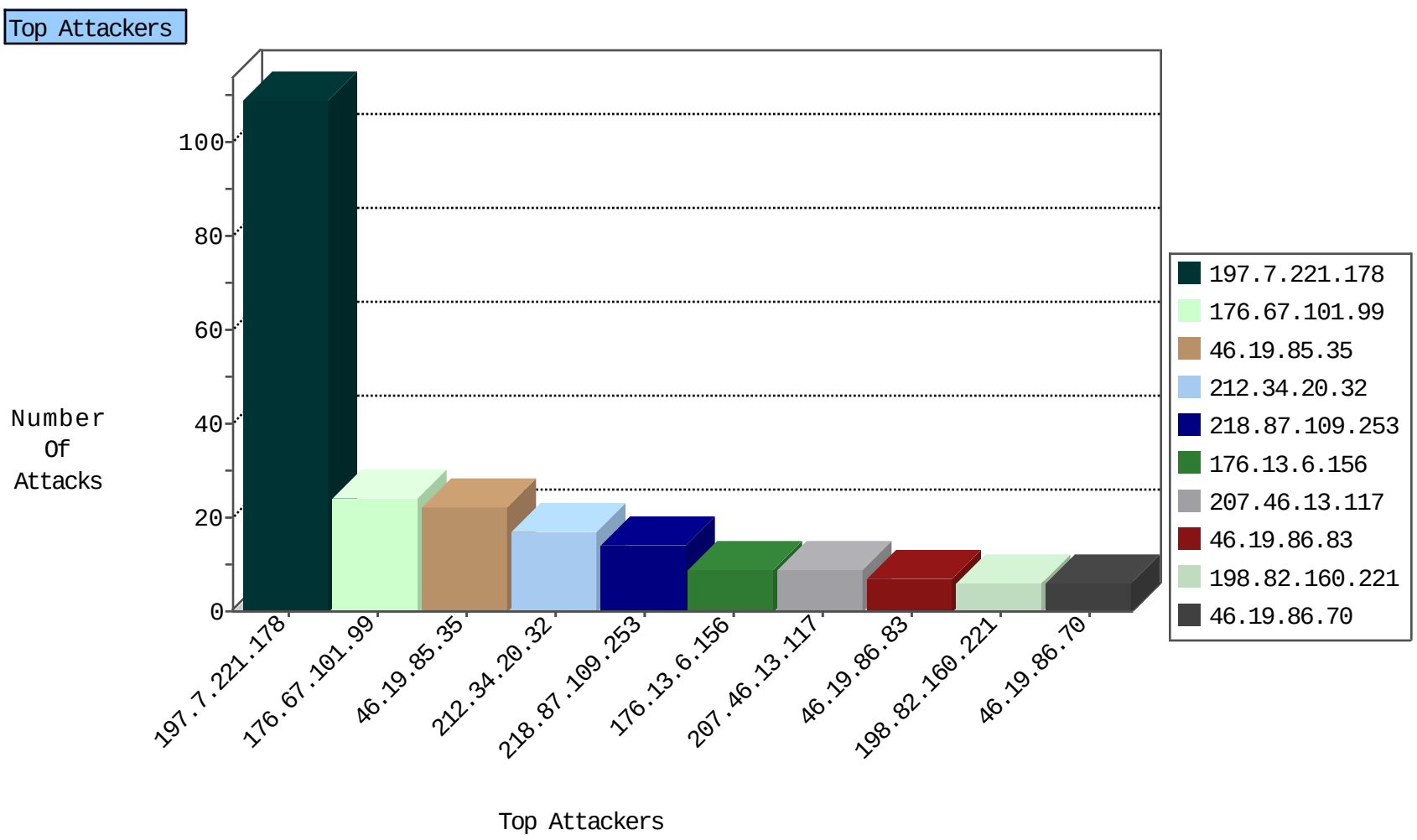
09-18-2016-02:04:02 to 09-18-2016-03:04:02

IDF Under Attack
Daily Report





09-18-2016-02:04:02 to 09-18-2016-03:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
130.194.252.8	Australia	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	3
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.33.90.68	Switzerland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.33.90.67	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
192.33.90.68	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
78.46.223.24	Germany	147.237.8.50	e.tikshuv.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-02:04:02 to 09-18-2016-03:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-18-2016-02:04:02 to 09-18-2016-03:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.87.109.253	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.0.15	Pakistan	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
218.87.109.253	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.193.74.175	147.237.77.235	Gibraltar	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
61.185.0.148	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
31.24.228.20	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
200.58.214.138	147.237.76.200	Colombia	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
221.7.36.78	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
139.162.13.205	147.237.76.38	Singapore	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.87.109.253	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
111.23.12.94	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.201	Ukraine	e.atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
218.87.109.253	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
80.246.136.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.185.0.148	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.24.228.20	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
200.58.214.138	147.237.76.200	Colombia	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1

09-18-2016-02:04:02 to 09-18-2016-03:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
176.67.101.99	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
207.46.13.117	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.6.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.70	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.34.20.32	Jordan	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.50	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
77.20.249.53	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.142.6.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.67.101.99	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
2.53.176.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.171	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
139.162.37.147	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.117.156.132	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.11	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.254.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.130.216.204	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
139.162.37.147	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.117.156.132	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.14.136.148	Romania	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	1
120.132.68.33	China	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.13.3.0	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.249.76.80	Israel	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
37.26.148.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.62.53.168	Russian Federation	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.59.54.147	China	147.237.0.35	akaws.idf.il	drop		drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
176.13.6.156	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
77.20.249.53	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.140	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
37.46.38.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.206.85.139	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-18-2016-02:04:02 to 09-18-2016-03:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.34.20.32	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.20.32	Block	4
212.34.20.32	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.20.32	Block	4
176.13.6.156	Israel	147.237.77.243	mobile.idf.i	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/61353.jpg	Block	1
212.34.20.32	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
212.34.20.32	Jordan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method =R3YOHNJYWGMHIJYK5AOC9K2EQ22FJTMAX5B5NHRIMJAOLYK03KAFYXC70JYFL4F2UBKC7SWNI5QPAETRH1BZJ7CZT454JCWI47U9&SessionCode=UP in URL www.idf.ilhttp/1.1	Block	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover	Block	1
212.34.20.32	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
88.102.37.253	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
212.34.20.32	Jordan	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
109.253.208.25	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.86.83	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	1

09-18-2016-02:04:02 to 09-18-2016-03:04:02