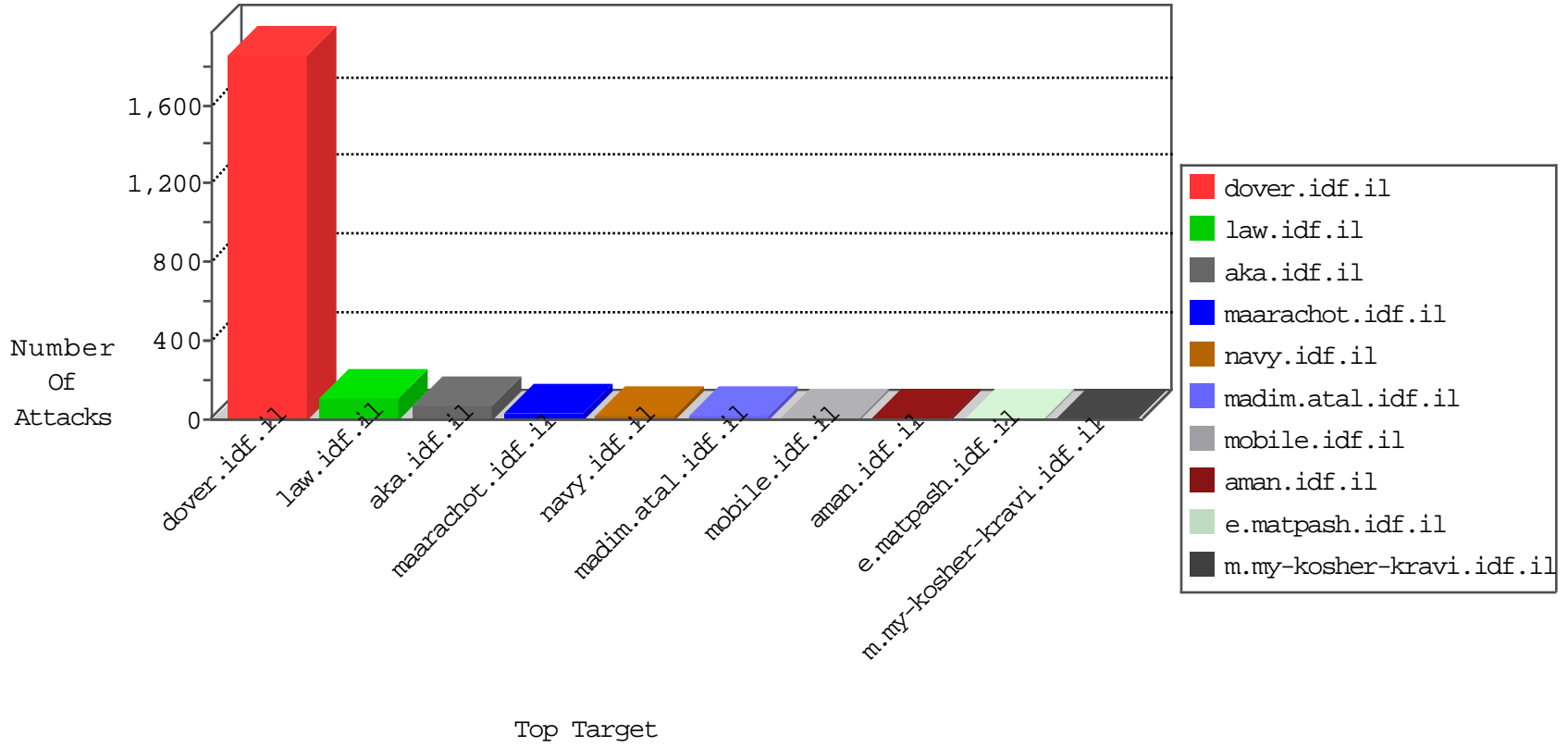


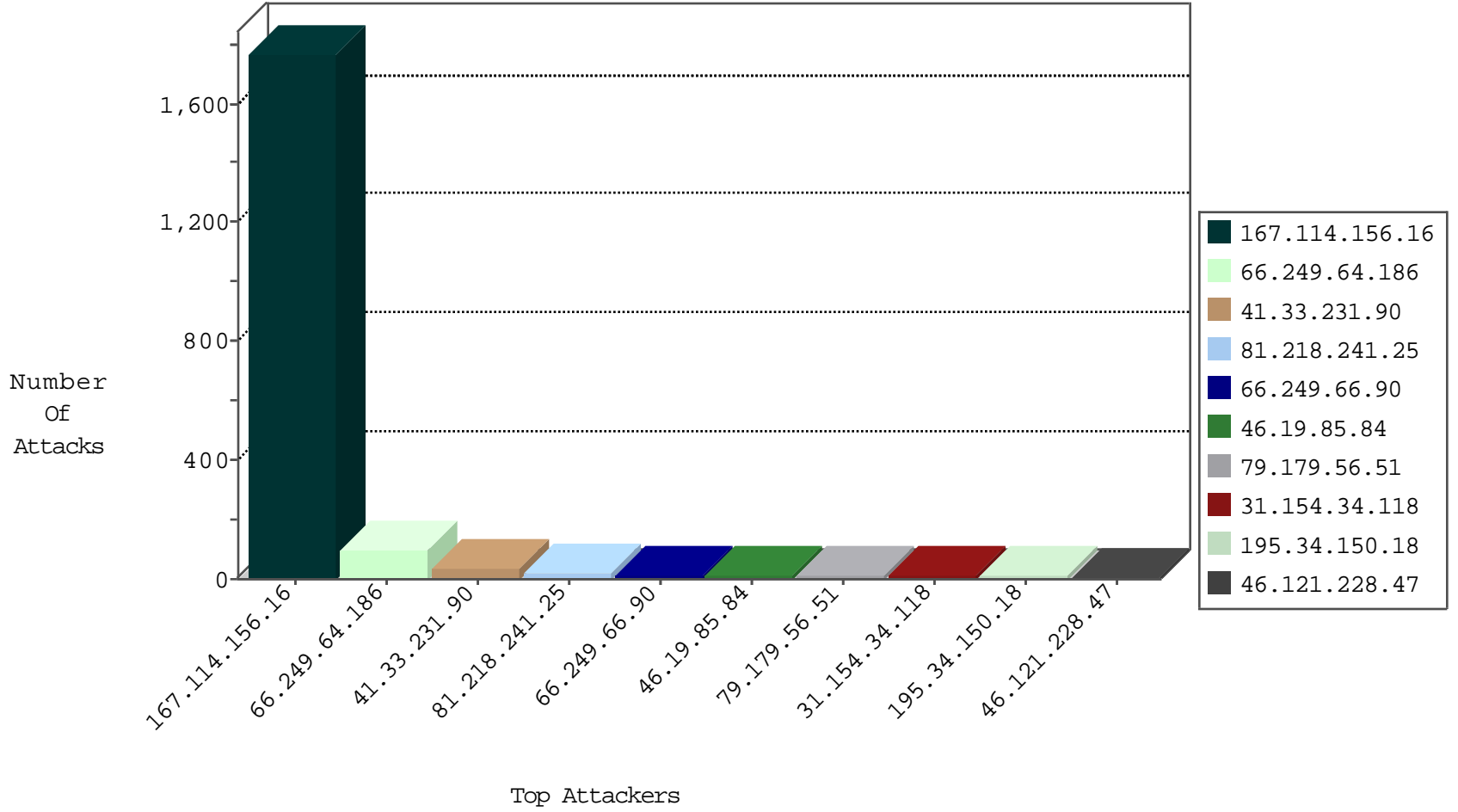
IDF Under Attack Daily Report



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	3331
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
208.67.1.60	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
125.31.154.18	Korea, Republic of	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
125.31.154.18	Korea, Republic of	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
199.99.200.64	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
125.31.154.18	Korea, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
199.99.200.64	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

01-03-2016-06:04:07 to 01-03-2016-07:04:07

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
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	98
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.165	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.76.201	United States	e.atal.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	36
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.179.56.51	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
31.154.34.118	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.241.25	Israel	147.237.72.166	aka.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	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.148.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.141.87	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	drop	First packet isn't SYN	drop	3
207.46.13.22	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.73.205.54	Ukraine	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.22.131.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.121.228.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
79.176.124.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.183.171.81	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
51.36.68.125	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
85.65.47.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.177.2.136	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
54.183.208.137	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
176.13.6.68	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
157.55.39.130	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.179.9.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.119	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.156	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
121.18.231.86	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.224		147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
74.82.47.42	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.96	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
168.62.238.153	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.237	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
96.56.10.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
184.105.139.119	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
121.18.231.86	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.224		147.237.77.178	e.matpash.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	6
87.69.211.182	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.69.211.182	Block	5
217.132.101.33	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 217.132.101.33	None	4
109.253.156.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.121.228.47	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1560	Block	3
46.121.228.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.44		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.198.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.169.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.160.149.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
157.55.39.130	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.155.236.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
67.19.79.218	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
109.201.152.248	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.69.211.182	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
157.55.39.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.251.27.99	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /robots.txt	Block	1
2.52.144.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.176.124.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.244.70.35	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
91.200.12.73	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/3916.pdf/trackback/	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/23012011masaiyot.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.66.127.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.68.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.101.33	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
109.253.221.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
104.155.236.4	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.155.236.4	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1