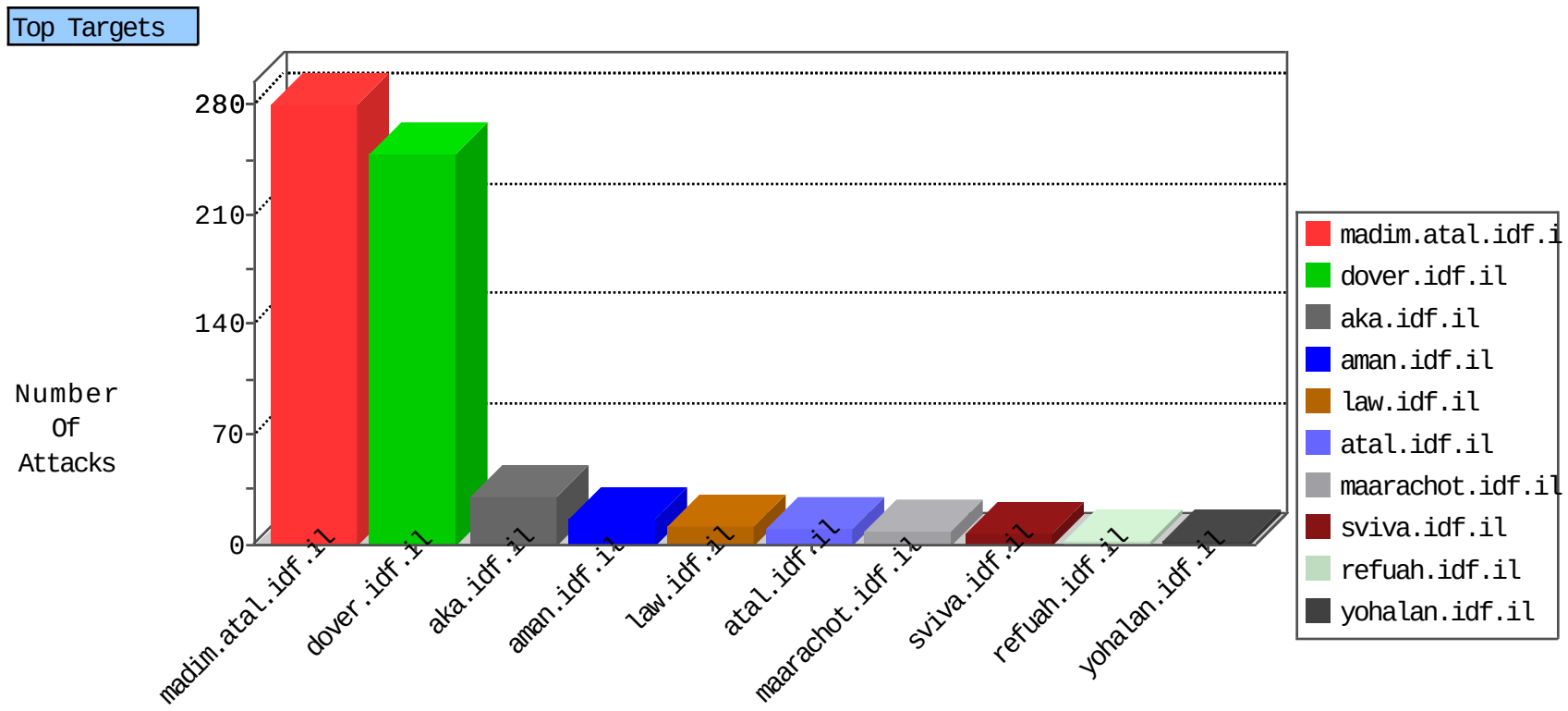
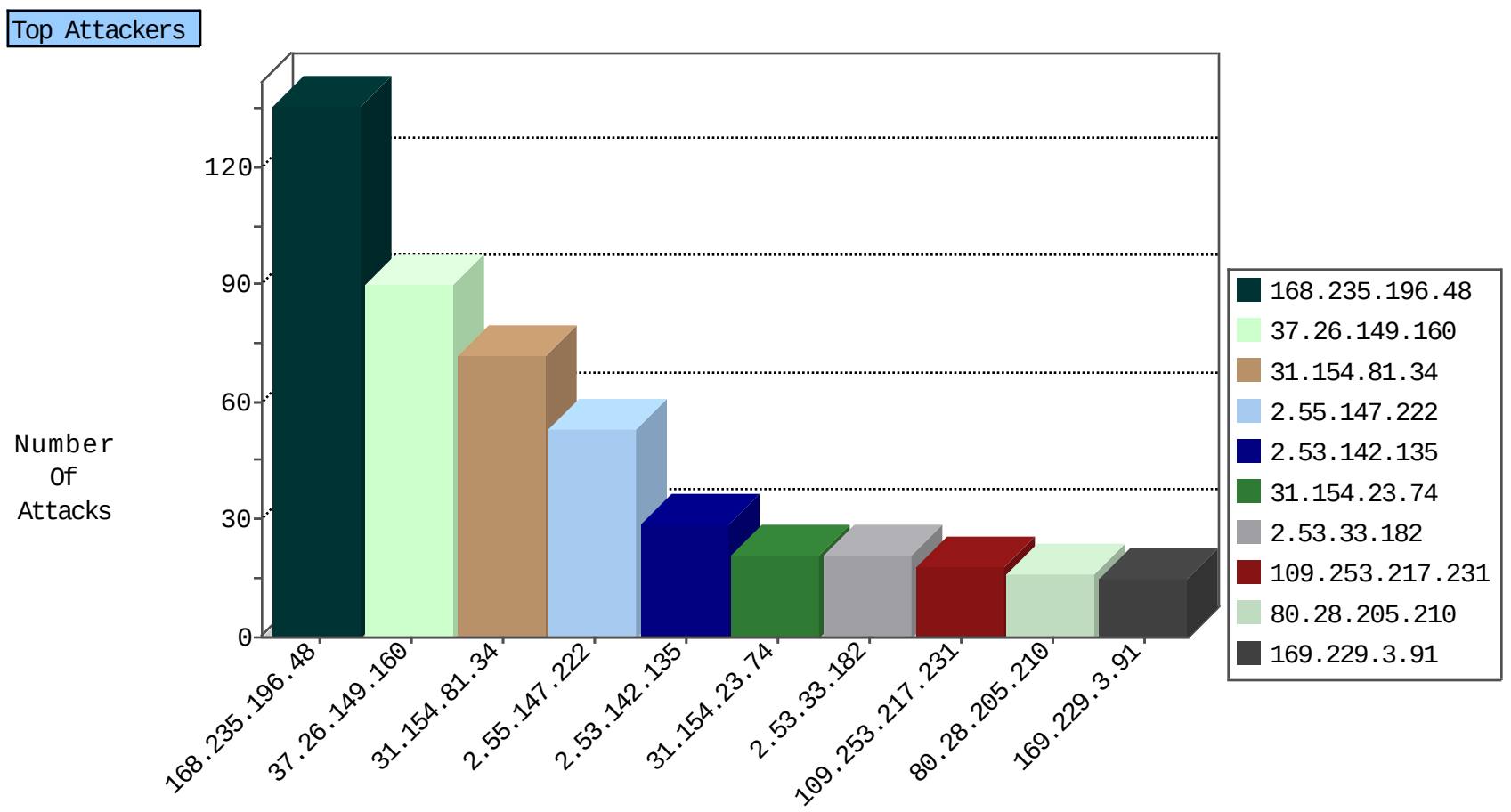
08-17-2016-10:04:06 to 08-17-2016-11:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-17-2016-10:04:06 to 08-17-2016-11:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
195.154.172.204	France	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
93.158.200.96	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
207.244.105.146	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
93.158.200.132	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
217.132.101.119	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.82.69.221	Netherlands	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
180.64.73.80	Korea, Republic of	147.237.77.235	sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

08-17-2016-10:04:06 to 08-17-2016-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
185.61.138.125	Ukraine	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
46.166.188.216	Netherlands	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-17-2016-10:04:06 to 08-17-2016-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.219.162.252	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	6
109.64.176.47	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
113.108.10.31	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.64.59.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.215.177	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.223.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.38.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.232.25.160	147.237.76.30	Colombia	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
194.90.66.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.57.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.11.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.215.177	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.215.177	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.168.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
72.252.249.125	147.237.76.38	Jamaica	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.168.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.71.251	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.176	United States	matpash.idf.il	ET DROP Dshield Block Listed Source	1
46.19.86.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.186.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.186.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-17-2016-10:04:06 to 08-17-2016-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.196.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
31.154.23.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
109.253.217.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.28.205.210	Spain	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.142.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.13.164.93	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
217.132.101.119	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	3
31.154.81.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
213.8.204.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.21.120.220	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.10.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
186.159.5.49	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.55.171.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.156.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
194.90.25.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.8.161	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
195.154.172.204	France	147.237.76.34	yohalan.idf.il	drop		drop	1
84.95.130.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.220.51	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
207.232.21.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.16.41	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
85.64.102.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.22.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.4.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.232.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.192.161	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
2.75.60.136	Kazakstan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
31.154.81.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
2.55.147.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
2.53.142.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.53.33.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
212.143.56.182	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	4
131.253.27.47	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.176.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
199.30.24.255	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
132.147.105.126	Singapore	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
77.124.60.168	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.124.60.168	Block	2
49.229.173.89	Thailand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	2
2.53.53.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
79.182.146.138	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Header Name [[#31]]?¾uÄ;ÀŒ¦ñ¤Óò	Block	1
62.219.165.75	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
109.67.16.20	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
37.26.149.183	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$ImageButton1.x in www.idf.il/1133-he/dover.aspx	Block	1
2.53.53.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/dover.aspx?searchtext='חיל התמודיעין	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in URL ~[[#16]]ke9]d	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ö<Ü¾m[[#14]]é[[#2]]×$È' in URL	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.102.195.68	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/wp-login.php	Block	1
80.178.201.104	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 80.178.201.104	Block	1
176.13.248.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.64.147	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
193.34.57.101	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xnklp/english	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/piwik.php	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Malformed URL ~[[#16]]ke9]d	Block	1
46.19.86.99	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1
109.65.165.252	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
31.154.81.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nzlvd/templates/navmenu/navmenu.css.aspx	Block	1
212.143.56.182	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 212.143.56.182	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
80.179.223.87	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method Fâ[[#29]]`>P†móV&«¹[[#29]]âŸ‹–æ›y~é][[#5]]3M	Block	1
66.249.76.56	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ses.20.8afc=*	Block	1
89.139.162.255	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	NULL Character in Method •ÿä]ÄÊêô[[#3]]ÆC¹r[[#0]][[#27]]¢Dñ°¦ØN	Block	1