Brutal Gift

Version 5.0ß9
Coded by DCHKG
Released by the UGMPT

Brutal Gift is a new Mac OS X program coded by DCHKG (active member of the Underground Mac Programming Team) and inspired by Forced Entry 2.0 (on Mac OS 9). Actually it's a powerful FTP, POP3, Oscar (AIM/ICQ2000), Hotline, Hotmail/Passport (MSN), web form and internet account brute force cracker. This means it is able to connect to a server and test a selected list of passwords for a specified username. **Brutal Gift** can open up to 500 connections at the same time. It detects any time-out error or misconnection in order to immediately reconnect the matching socket. **Brutal Gift** adds a fast word list generator. When an attack is launched, a specific window opens so that you can follow what occurs on the server side. If you are not familiar to cracking, don't be worry since an interactive help will solve all the problems you'll encounter.

DISCLAIMER

* Don't pay for Brutal Gift 5.0b.

* I made a program called HellRaiser that is a trojan. When I code a trojan, I call it a trojan. Brutal Gift is not a trojan.

* If you have no idea of the target password, don't expect getting it with Brutal Gift. It's a question of probability.

* It's almost no use trying to brute force Hotmail or MSN with Brutal Gift, because of MSN security. Read the Known Issues note below for further information. The video from YouTube showing Brutal Gift cracking a MSN account is actually fake a little bit.

* With "web form" as target, in order determine if sent form is valid, Brutal Gift search into the received page every specified "failure meaning expression". If Brutal Gift doesn't find it, it considers sent form was valid. This explains why you could get weird results with "web form" cracking.

* Brutal Gift does not work on some web forms. It does not mean this feature doesn't work at all.

* If a website requires a type of challenge-response test to ensure that the response is not generated by a computer (Captcha features) you can not crack it with Brutal Gift. Captchas are commonly shown after some invalid authentication attempts. So, check that before loosing your time.

* Brutal Gift works great on these targets : FTP, POP3, Oscar, Hotline, Webmail/IMAP.

* If you wish to use sock servers, be aware that good free sock servers have become very rare. In addition, a sock server may not be compatible with all targets. Test them with ProxyM8, a program of mine.

HOW TO USE

Let's take an example : you want to crack a FTP account.

This account is owned by a server, it's the "Address" field inside the "Server" group box (eg. "ftp.yahoo.com"). This server has a opened port for the FTP service, it's the "Port :" field inside the "Server" group box and for ftp it's pretty sure that it's "21".

To complete the ftp identification process and then access to the account you need two values that are sent to the server at the beginning of the connection : the USERNAME and the PASSWORD. If those values are correct then access is granted but if they're not in this case access is denied. In the most common cases it's not hard to get the USERNAME of the account you want to crack... For instance if the address for the ftp account's matching website is "http://www.yahoo.com/devil/index.html" then the USERNAME must be "devil" (but sometime for a better security it can be different !).

If you miss both the USERNAME and the PASSWORD or just one of them, then **Brutal Gift** will send variable strings to the server until access is granted. So for both the USERNAME and the PASSWORD you have to choose one of these following options : "custom (specified)", "dictionary (word list)" or "random characters". Let's call the USERNAME or the PASSWORD a variable.

- custom (specified) : the variable will be constant during the attack and this constant is the string you specified in the edit field at the right of the matching pop up menu ;
- dictionary (word list) : the variable will be (really) variable during the attack and this variable will be read from a word list specified in the "Dictionary" panel. Actually each line of the selected word list constitute a potential variable for the cracking process ;
- random characters : the variable is randomly generated, according to the Word List Lab settings or the ADVANCED MODE (of the Word List Lab) settings depending on what strategy option is selected.

Please note you are never sure (at all) you'll get the right password before the word list is finished... That's why it's better to know the people you want to hack, to have an idea of kind of PASSWORD they may choose.

KNOWN ISSUES

Brutal Gift 5.0 does not support cracking of Captchas (image verification systems) (eg. Google's Gmail).

WHEN BRUTE FORCING HOTMAIL/MSN, AFTER 10 BAD ATTEMPTS IT WILL TELL YOU THE PASSWORD IS WRONG WHETHER IT'S VALID OR NOT, DURING A CERTAIN AMOUNT OF TIME.

THIS IS A LIMITATION OF MSN ITSELF THAT YOU CAN NOT BYPASS (OR AT LEAST I CAN'T SEE HOW TO). **BRUTAL GIFT** VERSIONS FURTHER 5.0B6 WILL WARN YOU AT THE POINT WHEN GOING ON ATTACK IS USELESS (THAT SEEMS TO ME THAT B2 WON'T).

AS A RESULT THE PROBLEM IS TO KNOW HOW LONG YOU HAVE TO WAIT BEFORE BEING AUTHORIZED AGAIN BY MSN TO TRY OTHER PASSWORDS. THAT'S THE PURPOSE OF THE "STRATEGY" : "ARBITRATION" OPTION IN **BRUTAL GIFT**.

SO YOU HAVE TO SET THE "DELAY BETWEEN SERIES" PARAMETER. I DON'T KNOW THE RIGHT VALUE OF THAT PARAMETER FOR MSN/HOTMAIL. ONE WAY TO GET IT COULD BE TO MAKE ATTEMPTS MANUALLY. ENTER 10 BAD PASSWORDS IN HOTMAIL AND THEN WAIT 1 HOUR (THEN 2, 3, ETC.) UNTIL YOU GET IT. I TRIED TO DO THAT ONCE BUT GOT BORED AND ABORTED BEFORE DISCOVERING THE VALUE. FOR MSN/HOTMAIL, THE VALUE OF "LOGIN ATTEMPTS PER SERIES" SHOULD BE SET TO 9.

VERSION HISTORY

- **Version 5.0ß9** :
  - [feature added] : Hotmail/MSN via POP3 brute forcing ;
  - [feature added] : IMAP brute forcing ;
  - [feature added] : SSL option for FTP and POP3 ;
  - [bug fixed] : word list lab preferences saving ;
  - [bug fixed] : fake user-agent preferences saving.

- **Version 5.0ß8** :
  - [bug fixed] : MSN protocol changed a very little bit in August 2008.

- **Version 5.0ß7** :
  - [feature improved] : about web form, the "failure meaning expressions" interface has been improved ;
  - [feature added] : about web form, the "fake user-agent" option makes brute cracking possible with web servers that require a compatible web browser.

- **Version 5.0ß6** :
  - [feature improved] : universal binary release ;
  - [feature improved] : major improvements of web form support ;
  - [feature improved] : about web form, the GUESS method has been improved ;
  - [feature added] : cookie support ;
  - [feature added] : you are able to debug sockets with TextEdit ;
  - [feature added] : about web form, you are able to check the received page with TextEdit.

- **Version 5.0ß5** :
  - [feature improved] : huge work into advanced managing with the nasty MSN protocol which is really hard to crack unless you have an idea of the targeted password ;
  - [feature added] : with MSN as target, ability to wait a specified time after a specified number of login attempts ;
  - [feature added] : about web form, ability to capture forms from clipboard with the GUESS method ;
  - [bug fixed] : about web form, the GUESS method sometimes returned bad form urls ;
  - [bug fixed] : Hotmail/Passport support has been fixed to bound with upgraded anti-brute security (10 maximum attempts) ;
  - [bug fixed] : closing attack progress window while cracking web forms now really aborts the cracking progress with Hotmail/Passport and web form targets ;
  - [bug fixed] : warnings relative to attack power fixed ;
  - [bug fixed] : minor bugs fixed.

- **Version 5.0ß4** :
  - [bug fixed] : support for HTTP status 301 and 302 fixed ;
  - [bug fixed] : web form user interface fixed ;
  - [feature added] : the application opens when clicking on its related documents ;
  - [feature added] : "Software Update" menu and "Check For Update..." menu item.

- **Version 5.0ß3** :
  - [bug fixed] : "&" was not replaced by "&" in the form action ;
  - [bug fixed] : many others ;
  - [feature added] : HTTP secure brute forcing ;
  - [feature added] : the choice to specify several failure meaning expressions (eg. "Invalid ID or password" and "This ID is not yet taken") ;
  - [feature added] : new text converter feature called "add at end of each word", useful to build email word lists (eg. add "@hotmail.com" to each word of the English dictionary).

- **Version 5.0ß2** :
  - [feature added] : support added to web form cracking for HTTP status 302 (object moved) : Brutal Gift now automatically moves to moved object. This feature is essential to HTTP brute forcing process ;
  - [feature added] : support added to web form cracking for attack resuming.

- **Version 5.0ß** :
  - [feature added] : web form brute cracking !!! NEEDS TO BE BETA TESTED, PLEASE GIVE ME FEEDBACK ;
  - [bug fixed] : some interface-related bugs have been fixed. One of them could make the cracking process stuck, keeping sending the same username/password pair.

- **Version 4.9** :
  - [bug fixed] : the "Invalid nick or password" Oscar event now makes next tested username/password pair changed ;
  - [bug fixed] : "use only one wingate" is disabled but remains checked when selecting "Oscar" as target, if checked before, what freezes the cracking process ;
  - [feature added] : wingate support (proxy/sock) for Oscar ;
  - [feature improved] : user interface "smart" enabling/disabling system improved.

- **Version 4.8** :
  - [feature added] : Oscar cracking support, protocol used by AIM (iChat) and ICQ2000 ;
  - [feature added] : reconnection delay (after invalid tested account or time-out events) setting option.

- **Version 4.5** :
  - [bug fixed] : if target is FTP, POP3 or Hotline and if username (or password) is [custom] or [random characters] and password (or username) is [dictionary (word list)] then the program crashes at the end of the wordlist with a NilObjectException ;
  - [bug fixed] : abusive showing of the time-out alert window during the attack.

- **Version 4.3f** :
  - [MAJOR bug fixed] : the application do not succeed to reconnect or to get a stable connection after an "eof" socket status (meaning that one of the wordlist is done) ;
  - [feature added] : hotmail cracking support : works well (but not perfect maybe) with 1 socket only connection ! (that's why you can not select more connections). Actually, hotmail seems to "bug" while multiconnecting ; it will never say a wrong password is valid but it does not always accept the valid password. Strange...

- **Version 4.3b** :
  - [feature added] : hotline cracking support ;
  - [bug fixed] : the application crashes after having recovered a valid account ;
  - [bug fixed] : the application crashes at the end of the cracking process.
- **Version 4.0.1** :
  - the application has been built with a new version of RB that is not buggy ;
  - word lists like "aaa, aab, aac, etc." can be created thanks to the extended "in order" Word List Lab option ;
  - a few bug has been fixed.

- **Version 4.0rc** :
  - the source code has been cleaned ;
  - word lists are handled in a better way during the attack : first or last words of a word list will no longer risk of being skipped ;
  - "resume attack" system has been fixed and improved ;
  - "attack power" assessment system has been fixed ;
  - a bug regarding hostname solving has been fixed ;
  - new "drag & drop" abilities : "for username" edit field, "for password" edit field ;
  - a disclosure triangle has been added to the "Attack Progress" window in case you want to reduce its size ;
  - **Brutal Gift** is capable of reading the "UGMPT/DCHKG - WINGATE LIST" file created by **ProxyM8** in order to gets valid proxy/sock servers' addresses ;
  - the attack log ("Attack Progress" window) is now able to purge automatically in order to avoid memory wasting and attack slowdowns when the process is long.

- **Version 4.0b** : many new options added, the proxy managing part of **Brutal Gift** is now a separated application called **ProxyM8**, some option windows changed into sheet windows, new iTunes like list boxes. A new target mode, the "Internet account" mode has been added. It aims to crack or simply get a free internet access account. To use this mode you'll need a valid phone number of a true ISP. A bug that could trigger a OutOfBoundsException error on process

initiation has been fixed. Another one that made **Brutal Gift** crash when password is recovered has been eradicated too.

• **Version 3.8** : application's default language has been set to English and some bugs have been corrected.

• **Version 3.7** : the code now fits with the new development tool's version. Some alert windows changed to make graphic interface ligher. You no longer have you convert targeted server address into IP address format by yourself if you want to use one or several wingates. **Brutal Gift** is now able to perform this conversion by itself (only on Mac OS X !). The attack power display system has been corrected and improved. A major bug with the proxy testing system has been fixed : all the different proxy/sock abilities (FTP, POP3, SMTP) were all tested with the FTP server checking parameters... Moreover you're now able to check if your proxy/sock servers are compatible with Web (HTTP).

• **Version 3.6** : a bug with the "Resume Attack" system has been fixed. Indeed, the number of passwords sent that was read when you wanted to resume an attack was wrong. Some invisible cosmetic changes has been made too.

• **Version 3.5** : an IP spoofing system has been added. It adds proxy/sock server support and a proxy server tester. You can use only one wingate or a wingate list. Some bugs have been corrected. Please note you have to convert the targeted server address into IP address format (eg. 127.0.0.1) if you want to use one or several wingates. To easily perform this conversion, you could download *IP Reverse X* from Team Handicap at *http://www.teamhandicap.com/releases.html*.

• **Version 3.2** : "Password's Structure Advanced System" (I had to give it a name...) has been added in the Word List Lab. It may be used in the case that some characters of the targeted password are already known. This great idea comes from Jokke Du Vet. ISPs often use the same structure for their passwords. How stupid ;-) !

• **Version 3.0** : the original attack log system has been given up but a new socket status system has been added. The pros is that it does not slow down too much the attack process. A word counter has been added into the "Dictionary" tab of the main window. A simple word list editor has been added into the "Dictionary" tab of the main window. It makes you able to fastly create a custom word list without opening a text editor. Some minor bugs have been fixed.

• **Version 2.0** : initial release. Amazingly faster than version 1.0, 500 maximum connections, rtf text format supported, possibility to deactivate attack log and alerts to make process really much faster, possibility to resume an attack, faster time-out process, more informations (eg. average number of words sent per second) displayed during the attack progress, new birthday numbers mode in the word list lab and more...

• **Version 1.0** : non officialy released. 8 maximum connections, rtf text format non supported, attack log deactivation option non available.

SYSTEM REQUIREMENTS

This is a universal binary application optimized for Mac OS X.

CREDITS

• Coded by DCHKG.
• Interface by DCHKG.
• Design by DCHKG.
• Full credits to DCHKG.

THANKS

Many thanks and best regards to Nilkimas.
Many thanks to the Mac X BrotherZ team.

GENERAL

If you have ideas or if you find a bug in this program, please contact dchkg :

dchkg@free.fr
http://dchkg.perso.wanadoo.fr