动态免杀

插入Excel.SheetMacroEnabled对象

下载回来的10.doc实际上是一个RTF文档，里面内嵌了一个Excel.SheetMacroEnabled对象，Excel.SheetMacroEnabled是一个启用宏的Excel对象，相当于把一个带宏的Excel嵌入了Word文档中：

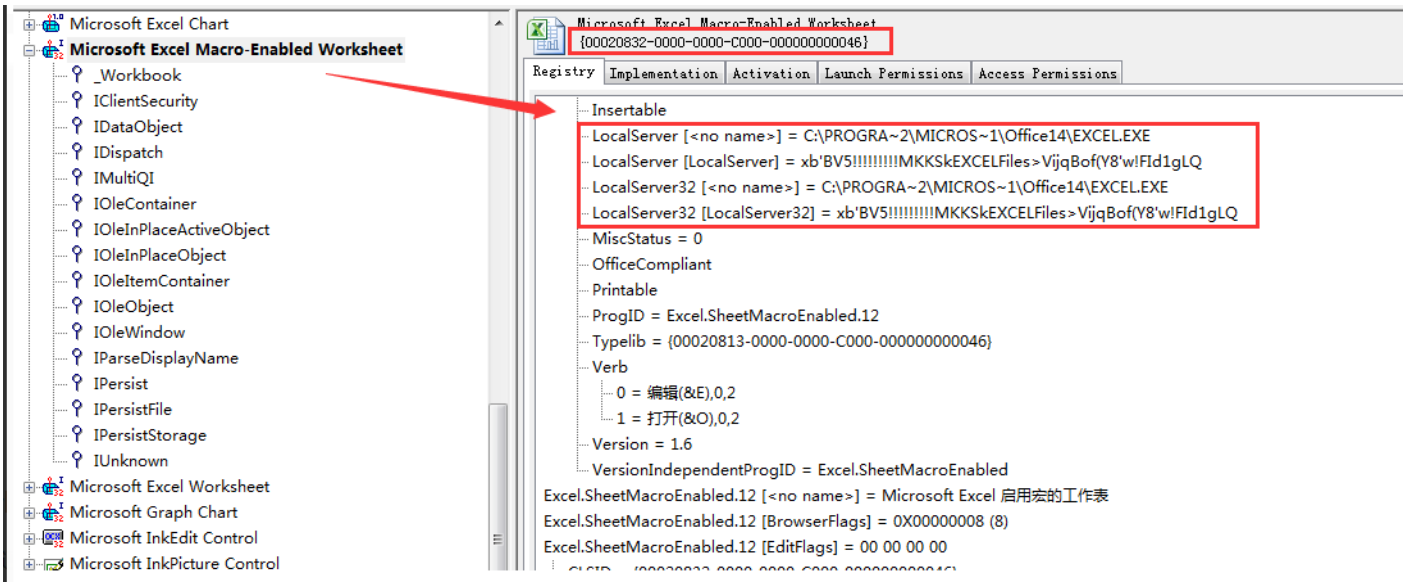
```
{\object\objemb\objw7238\objh2929\objscalex0\objscaley2{\*\objclass
Excel.SheetMacroEnabled.12}\objupdate{\*\objdata 010500000200000001b000000CRLF
457863656c2e53686565744d6163726f456e61626c65642e31320000000000000000000006a0000
CRLF
d0cf11e0a1b11ae1000000000000000000000000000000003e000300feff090006000000000000
0000000000010000000100000000000000010000032000000010000000feffffff000000000000
0000ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
```

下图分别是Excel.SheetMacroEnabled.12对象的对象名和CLSID：

```
 0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f Dump
01 05 00 00 02 00 00 00 1b 00 00 00 45 78 63 65 ............Exce
6c 2e 53 68 65 65 74 4d 61 63 72 6f 45 6e 61 62 l.SheetMacroEnab
6c 65 64 2e 31 32 00 00 00 00 00 00 00 00 00 00 led.12..........
70 00 00 d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 p..邢.唷??....□4[
00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ...........>...?
ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 01  ...............
00 00 00 01 00 00 00 00 00 00 00 00 10 00 00 02 ................
00 00 00 01 00 00 00 fe ff ff ff 00 00 00 00 00 .......?    .....
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --

ff ff ff 52 00 6f 00 6f 00 74 00 20 00 45 00 6e       R.o.o.t. .E
00 74 00 72 00 79 00 00 00 00 00 00 00 00 00 00 .t.r.y..........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 16 00 05 00 ff ff ff ff ff ff ff ff 02 ........
00 00 00 32 08 02 00 00 00 00 00 c0 00 00 00 00 ...2.......?...□
00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 80 ..F............€
52 8c 4b 25 ba d3 01 03 00 00 00 40 04 00 00 00 R孪%河.....@....[
00 00 00 01 00 4f 00 6c 00 65 00 00 00 00 00 00 .....O.l.e......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
```

在OleView中查看Excel.SheetMacroEnabled对象，CLSID正是{00020832-0000-0000-C000-000000000046}，并且LocalServer指向了EXCEL.EXE，这表示该对象对应的COM组件是一个单独的EXE组件，COM将通过其远程处理架构（通常涉及远程过程调用（RPC））来将这个exe加载起来，也就是说EXCEL.EXE将会和之前的Eqnedt32.exe一样，由COM直接创建而不是由WinWord.exe启动，这个特点可以有效对抗一些通过进程链来动态检测威胁的杀毒软件的查杀：


Microsoft Excel Chart
Microsoft Excel Macro-Enabled Worksheet
_Workbook
IClientSecurity
IDataObject
IDispatch
IMultiQI
IOleContainer
IOleInPlaceActiveObject
IOleInPlaceObject
IOleItemContainer
IOleObject
IOleWindow
IParseDisplayName
IPersist
IPersistFile
IPersistStorage
IUnknown
Microsoft Excel Worksheet
Microsoft Graph Chart
Microsoft InkEdit Control
Microsoft InkPicture Control
Microsoft Excel Macro-Enabled Worksheet
{00020832-0000-0000-C000-000000000046}
Registry
Implementation
Activation
Launch Permissions
Access Permissions
Insertable
LocalServer [<no name>] = C:\PROGRA~2\MICROS~1\Office14\EXCEL.EXE
LocalServer [LocalServer] = xb'BV5!!!!!!!!!MKKSkEXCELFiles>VijqBof(Y8'w!FId1gLQ
LocalServer32 [<no name>] = C:\PROGRA~2\MICROS~1\Office14\EXCEL.EXE
LocalServer32 [LocalServer32] = xb'BV5!!!!!!!!!MKKSkEXCELFiles>VijqBof(Y8'w!FId1gLQ
MiscStatus = 0
OfficeCompliant
Printable
ProgID = Excel.SheetMacroEnabled.12
Typelib = {00020813-0000-0000-C000-000000000046}
Verb
0 = 编辑(&E),0,2
1 = 打开(&O),0,2
Version = 1.6
VersionIndependentProgID = Excel.SheetMacroEnabled
Excel.SheetMacroEnabled.12 [<no name>] = Microsoft Excel 启用宏的工作表
Excel.SheetMacroEnabled.12 [BrowserFlags] = 0X00000008 (8)
Excel.SheetMacroEnabled.12 [EditFlags] = 00 00 00 00