

Rootkits em CDs de áudio: o caso Sony / DRM - Digital Rights Management”

“Sony got caught with it's pants down!”

Ronan Pedroso Nogueira Gaeti
ronan at acmesecurity dot org
0x165130A6

"The **casual piracy**, the schoolyard piracy, **is a huge issue for us...**"

"**Two-thirds** of **all piracy comes from ripping and burning CDs**, which is why **making** the **CD** a **secure format** is of the **utmost importance...**"

"**Most people**, I think, **don't even know what a rootkit is**, so **why should they care about it?**"

Thomas Hesse, *president* of global digital business for **Sony BMG**.

- **Introdução**
- **A Descoberta**
- **A Remoção**
- **O Desinstalador**
- ***“ET Phones Home”***
- **A Réplica**
- **A Tréplica**
- **Status**

“**XCP** ficou popularizado no dia **31 de outubro** quando o analista **Mark Russinovich** (Sysinternals) descobriu o software **escondido** em seu próprio computador.”

<http://www.sysinternals.com>

A Descoberta

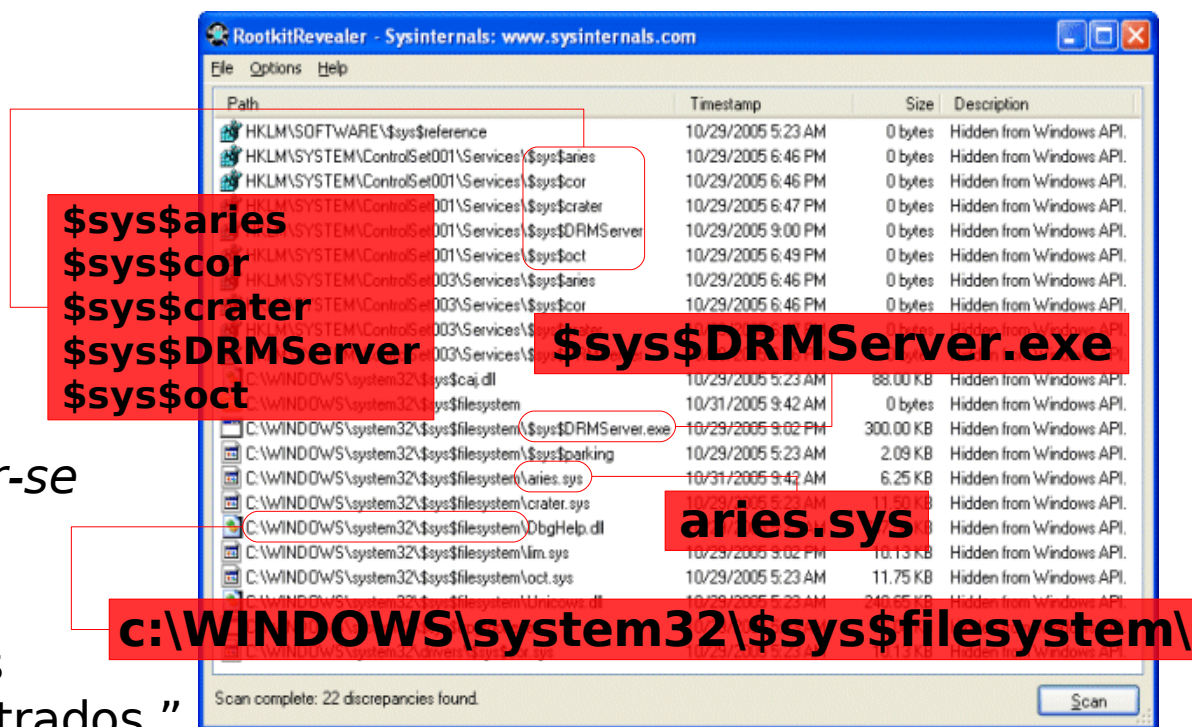
A Descoberta (1)

- Mark Russinovich descobre a presença de um *rootkit* em sua máquina enquanto testava uma nova versão do **RootkitRevealer**.

- Foram identificados:
 - ✓ entradas no **registro**
 - ✓ **diretório**
 - ✓ **driver**
 - ✓ **aplicação**

“A primeira vista parecia tratar-se de um bug no software...”

“ ... se não fossem pelos nomes **suspeitos** dos arquivos encontrados.”

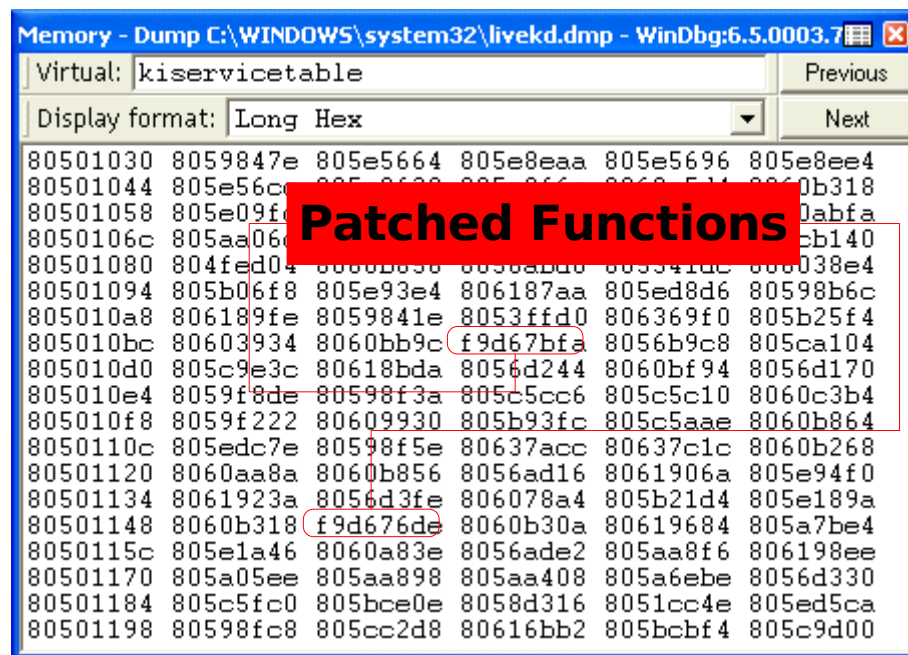


Dá-se início a uma investigação minuciosa...

Imediatamente após a identificação dos arquivos, Russinovich tentou utilizar:

- x ~~Autoruns~~
- x ~~Process Explorer~~
- ✓ LikeKd

LikeKd: é uma ferramenta escrita por M. Russinovich que permite explorar internamente o sistema usando o Microsoft Kernel Debugger.



Memory - Dump C:\WINDOWS\system32\livekd.dmp - WinDbg:6.5.0003.7

Virtual: kiservicetable

Display format: Long Hex

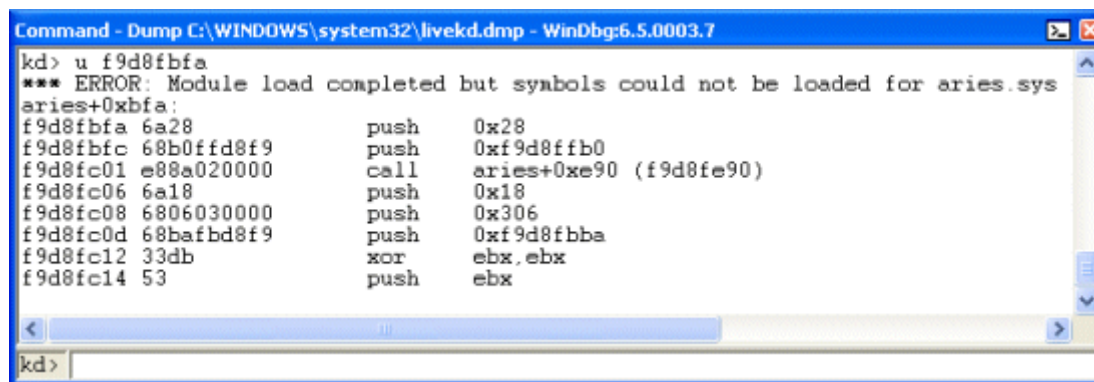
Patched Functions

80501030	8059847e	805e5664	805e8eaa	805e5696	805e8ee4
80501044	805e56c0	805e56c0	805e56c0	805e56c0	805e56c0
80501058	805e09f0	805e09f0	805e09f0	805e09f0	805e09f0
8050106c	805aa060	805aa060	805aa060	805aa060	805aa060
80501080	804fed04	804fed04	804fed04	804fed04	804fed04
80501094	805b06f8	805e93e4	806187aa	805ed8d6	80598b6c
805010a8	806189fe	8059841e	8053ffd0	806369f0	805b25f4
805010bc	80603934	8060bb9c	f9d67bfa	8056b9c8	805ca104
805010d0	805c9e3c	80618bda	8056d244	8060bf94	8056d170
805010e4	8059f8de	80598f3a	805c5cc6	805c5c10	8060c3b4
805010f8	8059f222	80609930	805b93fc	805c5aae	8060b864
8050110c	805edc7e	80598f5e	80637acc	80637c1c	8060b268
80501120	8060aa8a	8060b856	8056ad16	8061906a	805e94f0
80501134	8061923a	8056d3fe	806078a4	805b21d4	805e189a
80501148	8060b318	f9d676de	8060b30a	80619684	805a7be4
8050115c	805e1a46	8060a83e	8056ade2	805aa8f6	806198ee
80501170	805a05ee	805aa898	805aa408	805a6ebe	8056d330
80501184	805c5fc0	805bce0e	8058d316	8051cc4e	805ed5ca
80501198	80598fc8	805cc2d8	80616bb2	805bcbf4	805c9d00

Endereços **não** pertencentes ao **espaço do kernel** são chamados de:
"Patched Functions"

Checando um das chamadas foi possível identificar que pertencia ao driver:

aries.sys

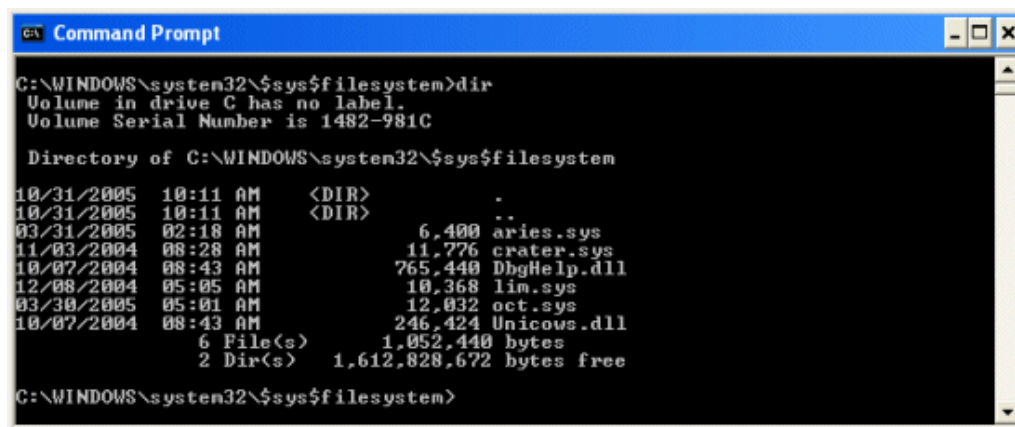


```
Command - Dump C:\WINDOWS\system32\livekd.dmp - WinDbg:6.5.0003.7
kd> u f9d8fbfa
*** ERROR: Module load completed but symbols could not be loaded for aries.sys
aries+0xbfa:
f9d8fbfa 6a28          push     0x28
f9d8fbfc 68b0ffd8f9    push     0xf9d8ffb0
f9d8fc01 e88a020000    call     aries+0xe90 (f9d8fe90)
f9d8fc06 6a18          push     0x18
f9d8fc08 6806030000    push     0x306
f9d8fc0d 68bafbd8f9    push     0xf9d8fbba
f9d8fc12 33db          xor      ebx,ebx
f9d8fc14 53            push     ebx
kd>
```

Identificado o driver responsável por esconder arquivos, diretórios, programas e chaves do registro!

- Seria suficiente remover o arquivo **aries.sys**?
- Talvez renomear ou remover o arquivo pudesse resolver o problema!
- Russinovich queria mais...

É comum os *rootkits* esconderem arquivos e diretórios da API do Windows **sem necessariamente** bloquear o **acesso** direto a eles.



```

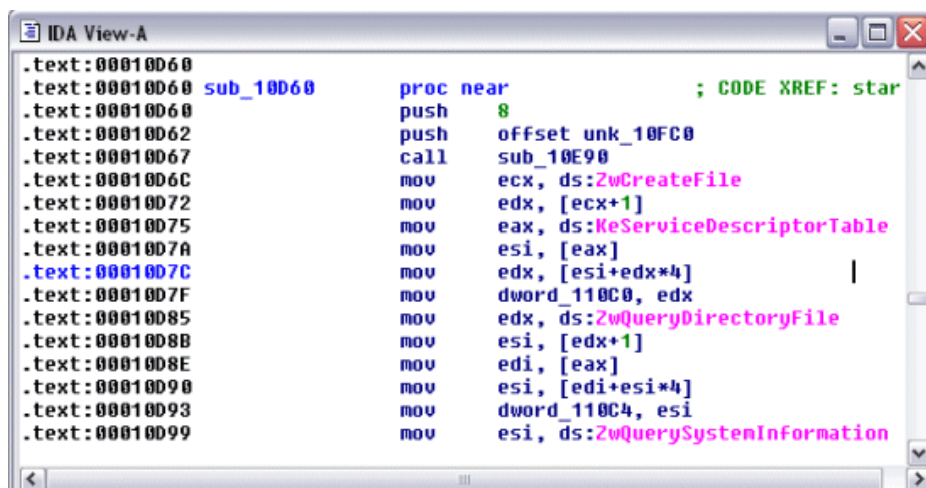
C:\WINDOWS\system32\$\sys$\filesystem>dir
Volume in drive C has no label.
Volume Serial Number is 1482-981C

Directory of C:\WINDOWS\system32\$\sys$\filesystem

10/31/2005  10:11 AM    <DIR>          ..
10/31/2005  10:11 AM    <DIR>          .
03/31/2005  02:18 AM             6,400 aries.sys
11/03/2004  08:28 AM             11,776 crater.sys
10/07/2004  08:43 AM           765,440 DbgHelp.dll
12/08/2004  05:05 AM             10,368 lim.sys
03/30/2005  05:01 AM             12,032 oct.sys
10/07/2004  08:43 AM          246,424 Unicows.dll
        6 File(s)              1,052,440 bytes
        2 Dir(s)              1,612,828,672 bytes free

C:\WINDOWS\system32\$\sys$\filesystem>
  
```

O que mais o driver **aries.sys** pode estar fazendo?



```

.text:00010D60
.text:00010D60 sub_10D60 proc near ; CODE XREF: star
.text:00010D60 push 8
.text:00010D62 push offset unk_10FC0
.text:00010D67 call sub_10E90
.text:00010D6C mov ecx, ds:2wCreateFile
.text:00010D72 mov edx, [ecx+1]
.text:00010D75 mov eax, ds:KeServiceDescriptorTable
.text:00010D7A mov esi, [eax]
.text:00010D7C mov edx, [esi+edx*4]
.text:00010D7F mov dword_110C0, edx
.text:00010D85 mov edx, ds:2wQueryDirectoryFile
.text:00010D8B mov esi, [edx+1]
.text:00010D8E mov edi, [eax]
.text:00010D90 mov esi, [edi+esi*4]
.text:00010D93 mov dword_110C4, esi
.text:00010D99 mov esi, ds:2wQuerySystemInformation
  
```

Utilizando o **IDA Pro**, Russinovich pode estudar as funções de inicialização do driver e constatar:

- Patched Functions
- O driver esconde **TODO E QUALQUER:**
 - arquivo
 - diretório
 - chave de registro

Iniciado por:
\$sys\$

Para provar sua teoria, Russinovich fez uma copia do arquivo **Notepad.exe** renomeando-o para:

\$sys\$Notepad.exe

O ARQUIVO DESAPARECEU!

Problemas na programação do driver:

- O driver aries utiliza um **descarregamento de driver inseguro**.
(condição de corrida dos threads)
- O rootkit não é suportado em todas as versões **x64 64-bit do Windows**.
(system call hooking)
 - Em breve o driver precisaria de updates.

O arquivo: **c:\Windows\System32\\$sys\$filesystem\aris.sys** é **renomeado!**

- ✓ O Sistema é reiniciado.
- ✓ Mascaramento foi **removido!**

→ Sigcheck©

Verifica e extrai informações de arquivos assinados digitalmente.

First 4 Internet

Essential System Tools

```
C:\WINDOWS\system32\$_sys$filesystem>sigcheck *

Sigcheck v1.2
Copyright (C) 2004-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\WINDOWS\system32\$_sys$filesystem\$_sys$DRMServer.exe:
    Verified:      Unsigned
    File date:     3:49 AM 12/14/2004
    Publisher:     First 4 Internet Ltd
    Description:   n/a
    Product:       n/a
    Version:       17.0.0.2
    File version:  17.0.0.2
C:\WINDOWS\system32\$_sys$filesystem\$_sys$parking:
    Verified:      Unsigned
    File date:     5:23 AM 10/29/2005
    Publisher:     n/a
    Description:   n/a
    Product:       n/a
    Version:       n/a
    File version:  n/a
C:\WINDOWS\system32\$_sys$filesystem\aries.sys.bak:
    Verified:      Unsigned
    File date:     2:18 AM 3/31/2005
    Publisher:     First 4 Internet
    Description:   F4IHook
    Product:       F4IHook
    Version:       1, 3, 7, 1
    File version:  1, 3, 7, 1
C:\WINDOWS\system32\$_sys$filesystem\crater.sys:
    Verified:      Unsigned
    File date:     8:28 AM 11/3/2004
    Publisher:     First 4 Internet
    Description:   Crater Device Driver
    Product:       Essential System Tools
    Version:       1.0.0.4
    File version:  1.0.0.4
C:\WINDOWS\system32\$_sys$filesystem\DbgHelp.dll:
    Verified:      Unsigned
    File date:     8:43 AM 10/7/2004
    Publisher:     Microsoft Corporation
    Description:   Windows Image Helper
    Product:       Debugging Tools for Windows(R)
    Version:       6.1.0017.1
    File version:  6.1.0017.1 <DbgBuild.020901-2218>
C:\WINDOWS\system32\$_sys$filesystem\lim.sys:
    Verified:      Unsigned
    File date:     5:05 AM 12/8/2004
```



“**XCP (Extended Copy Protection)** technology aims to provide **effective levels of protection** against the **unauthorized copying** of digital audio and data files without compromising sound quality and playability. **XCP helps to protect the rights of Artists and Record Labels** while accommodating consumer needs for **'fair use'** copying.”

“As with other copy-protected discs, albums featuring **XCP** (extended copy protection) **will allow for three copies to be made.**”

“**Sony BMG** is the **first** to **commercially deploy XCP.**”

<http://www.first4internet.com>

Russinovich lembrou que havia comprado um CD recentemente...

→ **Van Zant** - *“Get Right With The Man”*

[CONTENT/COPY-PROTECTED CD]



Media Player próprio

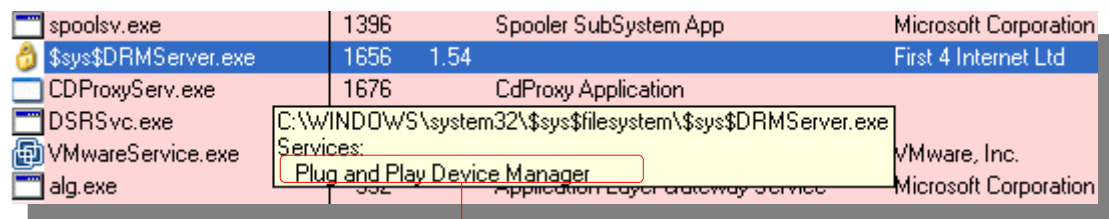
Até 3 cópias

É preciso relacionar o **rootkit** com o sistema de proteção do CD...

- O Process Explorer identificou o *player* como pertencente a *Macromedia*.

Enquanto isso...

Um aumento do uso de CPU pelo processo: **\$sys\$DRMServer.exe**



spoolsv.exe	1396	Spooler SubSystem App	Microsoft Corporation
\$sys\$DRMServer.exe	1656	1.54	First 4 Internet Ltd
CDProxyServ.exe	1676	CdProxy Application	
DSRSvc.exe			
VMwareService.exe			VMware, Inc.
alg.exe			Microsoft Corporation

C:\WINDOWS\system32\sys\$filesystem\sys\$DRMServer.exe
Services:
Plug and Play Device Manager

Plug and Play Device Manager

Esperava-se que ao fechar o *player* o processo **\$sys\$DRMServer.exe** parasse de consumir os ciclos da CPU.

Mas as coisas ainda **poderiam piorar...**

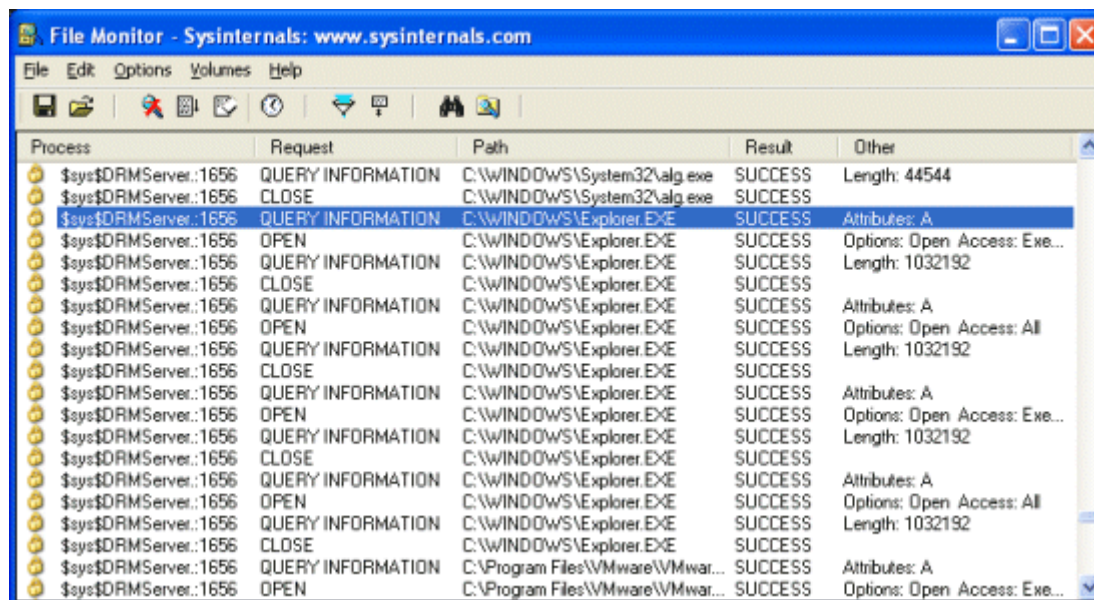
O processo continuava **consumir ciclos de CPU.**

→ File Monitor:

Scans:

Informações sobre os arquivos incluindo o tamanho.

→ 8 x a cada **2 segundos!**



Process	Request	Path	Result	Other
\$sys\$DRMServer.:1656	QUERY INFORMATION	C:\WINDOWS\System32\alg.exe	SUCCESS	Length: 44544
\$sys\$DRMServer.:1656	CLOSE	C:\WINDOWS\System32\alg.exe	SUCCESS	
\$sys\$DRMServer.:1656	QUERY INFORMATION	C:\WINDOWS\Explorer.EXE	SUCCESS	Attributes: A
\$sys\$DRMServer.:1656	OPEN	C:\WINDOWS\Explorer.EXE	SUCCESS	Options: Open Access: Exe...
\$sys\$DRMServer.:1656	QUERY INFORMATION	C:\WINDOWS\Explorer.EXE	SUCCESS	Length: 1032192
\$sys\$DRMServer.:1656	CLOSE	C:\WINDOWS\Explorer.EXE	SUCCESS	
\$sys\$DRMServer.:1656	QUERY INFORMATION	C:\WINDOWS\Explorer.EXE	SUCCESS	Attributes: A
\$sys\$DRMServer.:1656	OPEN	C:\WINDOWS\Explorer.EXE	SUCCESS	Options: Open Access: All
\$sys\$DRMServer.:1656	QUERY INFORMATION	C:\WINDOWS\Explorer.EXE	SUCCESS	Length: 1032192
\$sys\$DRMServer.:1656	CLOSE	C:\WINDOWS\Explorer.EXE	SUCCESS	
\$sys\$DRMServer.:1656	QUERY INFORMATION	C:\WINDOWS\Explorer.EXE	SUCCESS	Attributes: A
\$sys\$DRMServer.:1656	OPEN	C:\WINDOWS\Explorer.EXE	SUCCESS	Options: Open Access: Exe...
\$sys\$DRMServer.:1656	QUERY INFORMATION	C:\WINDOWS\Explorer.EXE	SUCCESS	Length: 1032192
\$sys\$DRMServer.:1656	CLOSE	C:\WINDOWS\Explorer.EXE	SUCCESS	
\$sys\$DRMServer.:1656	QUERY INFORMATION	C:\Program Files\VMware\VMwar...	SUCCESS	Attributes: A
\$sys\$DRMServer.:1656	OPEN	C:\Program Files\VMware\VMwar...	SUCCESS	Options: Open Access: Exe...

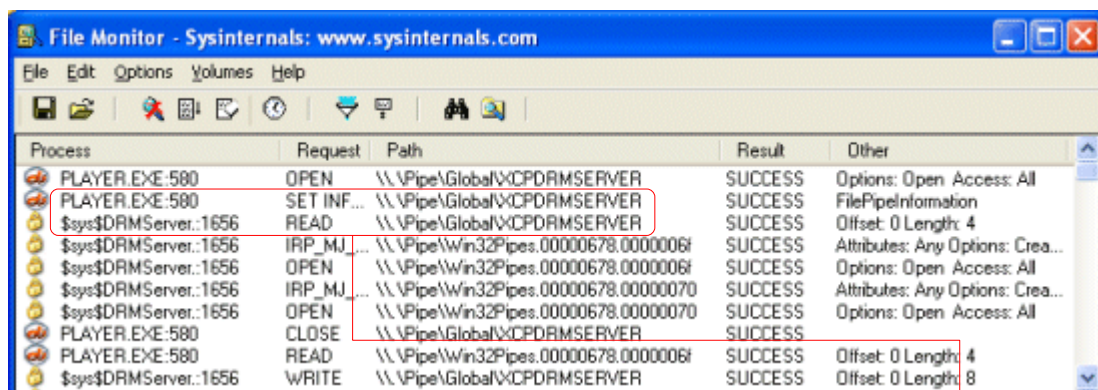
*"I was quickly **losing respect** for the developers of the software."*

Mark Russinovich

Mas ainda **não estava provada** a relação entre o *player* e o *rootkit*!

→ File Monitor:

Foi marcado a opção “**Named Pipes**” no menu “**Volumes**”.



Process	Request	Path	Result	Other
PLAYER.EXE:580	OPEN	\\Pipe\Global\XCPDRMSERVER	SUCCESS	Options: Open Access: All
PLAYER.EXE:580	SET INF...	\\Pipe\Global\XCPDRMSERVER	SUCCESS	FilePipeInformation
\$sys\$DRMServer:1656	READ	\\Pipe\Global\XCPDRMSERVER	SUCCESS	Offset: 0 Length: 4
\$sys\$DRMServer:1656	IRP_MJ...	\\Pipe\Win32Pipes.00000678.0000006f	SUCCESS	Attributes: Any Options: Crea...
\$sys\$DRMServer:1656	OPEN	\\Pipe\Win32Pipes.00000678.0000006f	SUCCESS	Options: Open Access: All
\$sys\$DRMServer:1656	IRP_MJ...	\\Pipe\Win32Pipes.00000678.00000070	SUCCESS	Attributes: Any Options: Crea...
\$sys\$DRMServer:1656	OPEN	\\Pipe\Win32Pipes.00000678.00000070	SUCCESS	Options: Open Access: All
PLAYER.EXE:580	CLOSE	\\Pipe\Global\XCPDRMSERVER	SUCCESS	
PLAYER.EXE:580	READ	\\Pipe\Win32Pipes.00000678.0000006f	SUCCESS	Offset: 0 Length: 4
\$sys\$DRMServer:1656	WRITE	\\Pipe\Global\XCPDRMSERVER	SUCCESS	Offset: 0 Length: 8

Pipes: são espaços de memória destinados a comunicação interprocesso.

Todos as instâncias de um “**Named Pipe**” compartilham o mesmo “**Pipe Name**”

PLAYER.EXE:580 ▶ \\Pipe\Global\XCPDRMSERVER
\$sys\$DRMServer:1656 ▶ \\Pipe\Global\XCPDRMSERVER

Conclusão:

O *rootkit* e seus arquivos associados **estavam relacionados ao DRM Software da First 4 Internet** que a Sony distribui em seus CDs.

A Remoção

Como **desinstalar** o Software/RootKit?

Não há uma entrada em “Adicionar ou Remover Programas”.

A EULA - (END-USER LICENSE AGREEMENT)

...
“As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD **will automatically install a small proprietary software program (the “SOFTWARE”) onto YOUR COMPUTER.** The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. **Once installed**, the SOFTWARE **will reside on YOUR COMPUTER until removed or deleted.** However, the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise. “
...

<http://www.sysinternals.com/blog/sony-eula.htm>

Opções:

- ✓ Remover o driver.
- ✓ Parar e remover o arquivo: **\$sys\$DRMServer.**
- ✓ Deletar as **Registry Keys:**

HKLM\System\CurrentControlSet\Services

Porém....

Safe Boot Registry Keys:

HKLM\System\CurrentControlSet\Control\SafeBoot

Chaves que são **carregadas** no **modo de segurança** (Safe Mode)
problema_segurança++;

Reiniciando o computador:

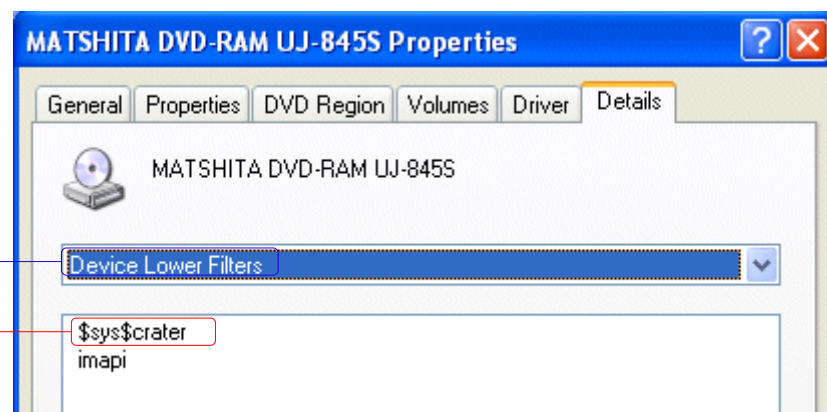
O driver de CD havia **desaparecido**.

Sistemas de filtros do Windows:

- ✓ **Ler e modificar** requisições de **I/O**

Device Lower Filters

\$sys\$crater



Não há uma interface administrativa.

As entradas dos filtros podem ser encontradas em:

HKLM\System\CurrentControlSet\Enum

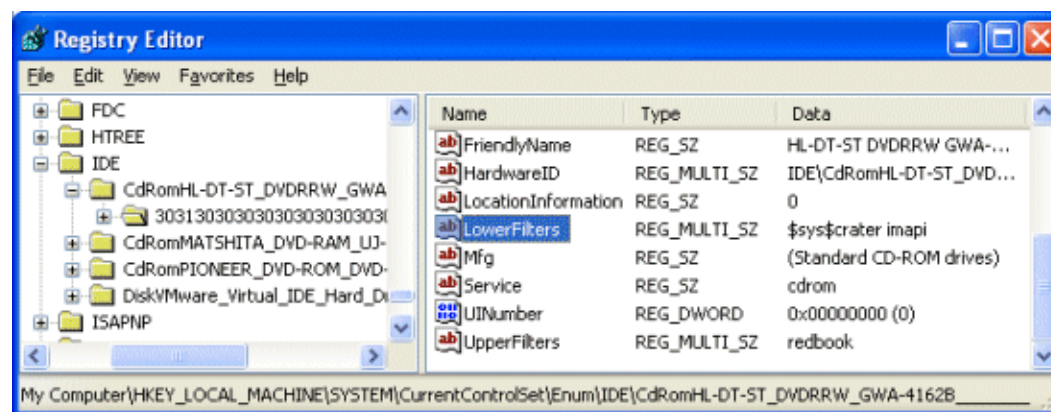
Essas chaves são **protegidas contra escrita**:

“Local System”

PsExec:

“light-weight telnet-replacement”

psexec -s -i -d regedit.exe



Entrada removida com sucesso!

Procurando por outras entradas **\$sys\$**:

✓ **\$sys\$Cor.sys (Corvus)**

upper filter for the **IDE channel device**

Reiniciando, mais uma vez.... o **Drive de CD** voltou!

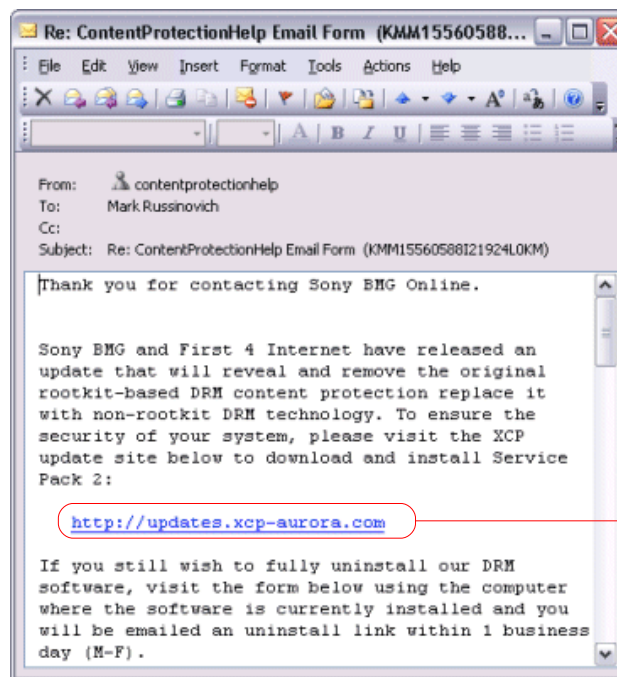
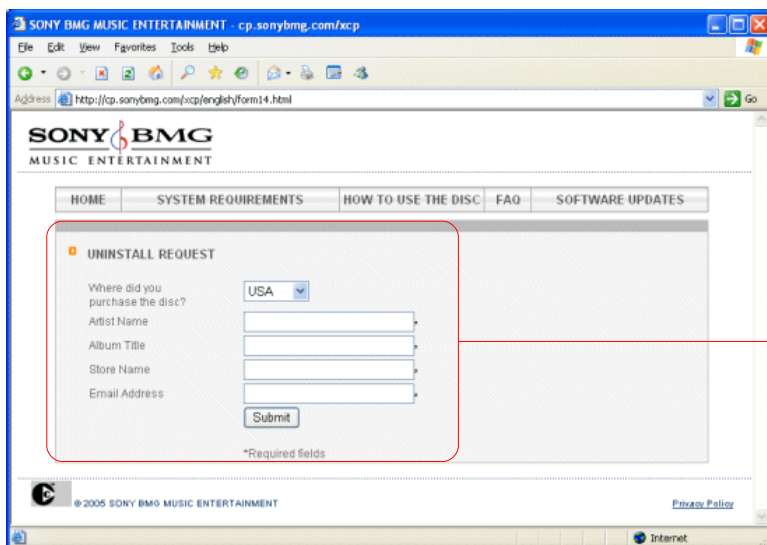
0 Service Pack

Cobertura do caso:

- ✓ Web Sites e Jornais
- ✓ USA Today
- ✓ BBC
- ✓ Washington Post

The RootKit **Service Pack**:

- ✓ No **FAQ** do site a Sony redireciona o usuário para o site:



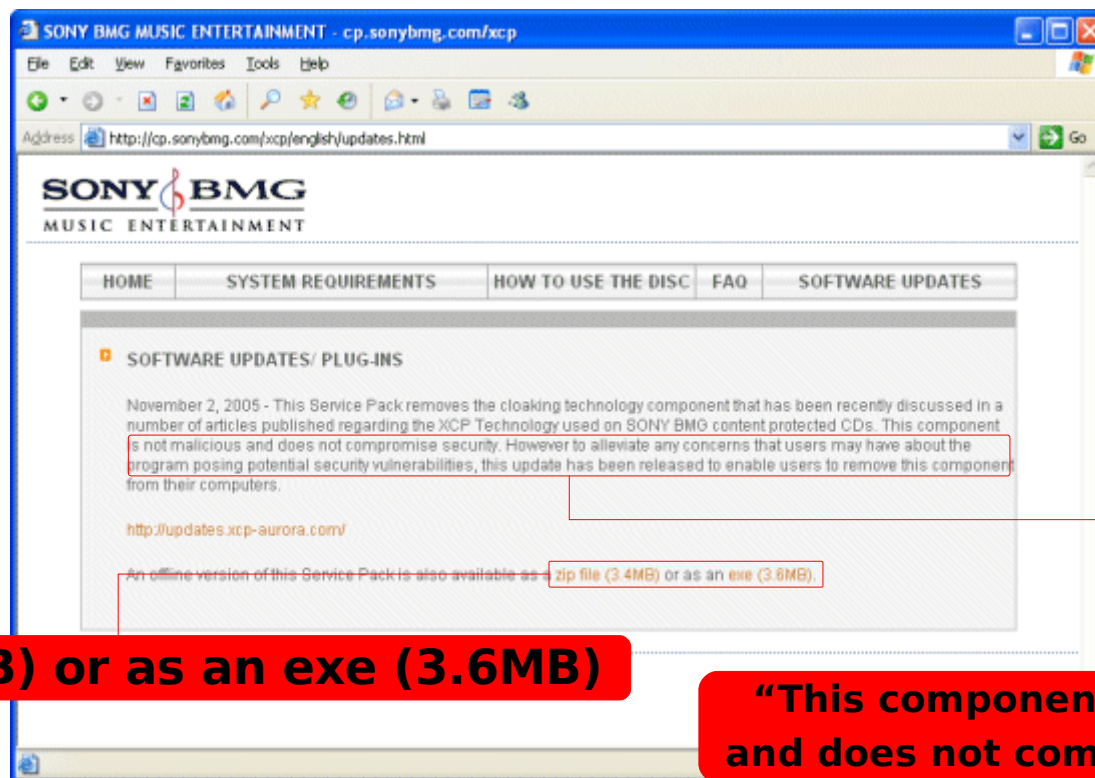
Atualização:

- Case ID
- Redirecionado para outro site.

<http://updates.xcp-aurora.com>

Informações Pessoais

Disponível no site da Sony em “**Software Updates**”:



zip file (3.4MB) or as an exe (3.6MB)

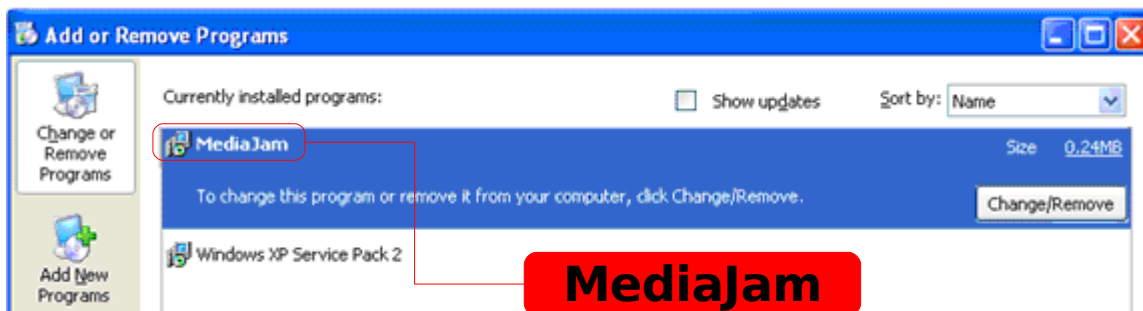
“This component is not malicious and does not compromise security”

Um software que esconde **qualquer arquivo** iniciado com **\$sys\$**:

✓ Obviamente é um **risco de segurança**!

Atualização dos drivers e executáveis para o DRM Software.

Sony Player ou DRM Software agora com o nome:



```
C:\Program Files\MediaJam>dir
Volume in drive C has no label.
Volume Serial Number is 1482-981C

Directory of C:\Program Files\MediaJam

11/04/2005  10:22 AM    <DIR>          .
11/04/2005  10:22 AM    <DIR>          ..
10/07/2004  08:43 AM             246,424 Unicows.dll
               1 File(s)          246,424 bytes
               2 Dir(s)    1,357,377,536 bytes free

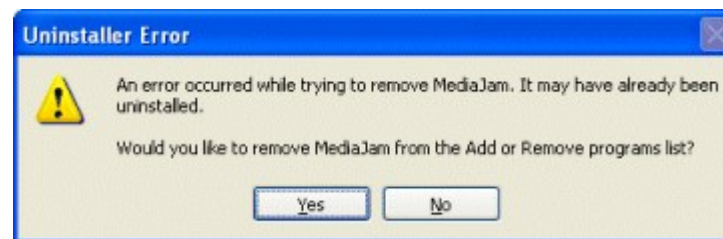
C:\Program Files\MediaJam>_
```

No diretório do MediaJam:

- ✓ Unicows.dll

Clicando em “**Change/Remove**”:

A **pressa** na criação do **patch** deve ter **impossibilitado** a realização de testes!



Patch equivalente a execução do comando:

net stop “network control manager”

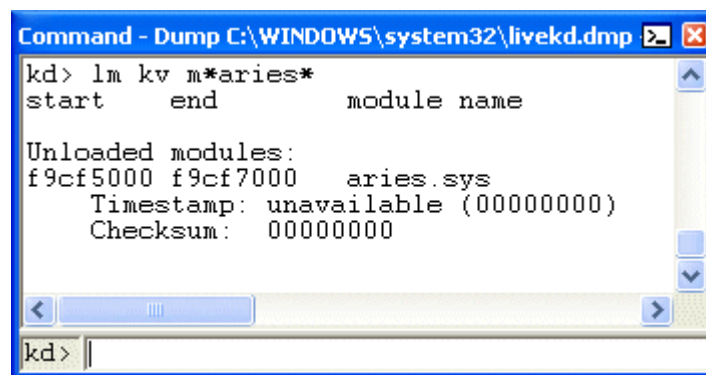
“Network Control Manager” = Aries Driver

- ✓ O comando diz ao Windows I/O System para **descarregar** o driver aries.sys da memória!

Dumping na System Call Table:

→ As entradas retornaram aos seus valores originais e o driver foi **descarregado da memória!**

- Descarregamento **inseguro** do driver;
- Risco de **Tela Azul**.



```
Command - Dump C:\WINDOWS\system32\livekd.dmp
kd> lm kv m*aries*
start      end      module name
Unloaded modules:
f9cf5000 f9cf7000 aries.sys
Timestamp: unavailable (00000000)
Checksum: 00000000
kd>
```

Uma forma **segura** para descarregar o driver seria: **reiniciando o sistema**, mantendo o driver **ativo** enquanto desliga o sistema!

O Desinstalador

Web based Uninstaller:

The screenshot shows a web browser window with the address bar displaying 'http://cp.sonybmg.com/xcp/english/form14.html'. The page header includes the Sony BMG Music Entertainment logo and navigation tabs: HOME, SYSTEM REQUIREMENTS, HOW TO USE THE DISC, FAQ, and SOFTWARE UPDATES. The main content area features a section titled 'UNINSTALL REQUEST' with a red border. Inside this section, there is a form with the following fields: 'Where did you purchase the disc?' (a dropdown menu set to 'USA'), 'Artist Name' (a text input field), 'Album Title' (a text input field), 'Store Name' (a text input field), and 'Email Address' (a text input field). A 'Submit' button is located below the email field. A note at the bottom of the form states '*Required fields'. The footer of the page includes the copyright notice '© 2005 SONY BMG MUSIC ENTERTAINMENT' and a link to the 'Privacy Policy'.

Informações Pessoais

Mesmo procedimento utilizado no
Service Pack!

If you **still wish** to **fully uninstall** our DRM software, visit the form below **using the computer where the software is currently installed** and you will be emailed an uninstall link within 1 business day...

The screenshot shows an email window with the title 'Re: ContentProtectionHelp Email Form (KMM15560588...)'. The email header includes the following information: 'From: contentprotectionhelp', 'To: Mark Russinovich', 'Cc:', and 'Subject: Re: ContentProtectionHelp Email Form (KMM15560588121924L0KM)'. The body of the email starts with 'Thank you for contacting Sony BMG Online.' followed by a paragraph: 'Sony BMG and First 4 Internet have released an update that will reveal and remove the original rootkit-based DRM content protection replace it with non-rootkit DRM technology. To ensure the security of your system, please visit the XCP update site below to download and install Service Pack 2:'. Below this paragraph is a blue hyperlink: '<http://updates.xcp-aurora.com>'. At the bottom of the email body, there is a red-bordered box containing the text: 'If you still wish to fully uninstall our DRM software, visit the form below using the computer where the software is currently installed and you will be emailed an uninstall link within 1 business day (M-F)'.

ActiveX Control:

- ✓ **CodeSupport.Ocx**

Informar o **CaseID** e o **motivo** da requisição.

O e-mail contendo o *link*:

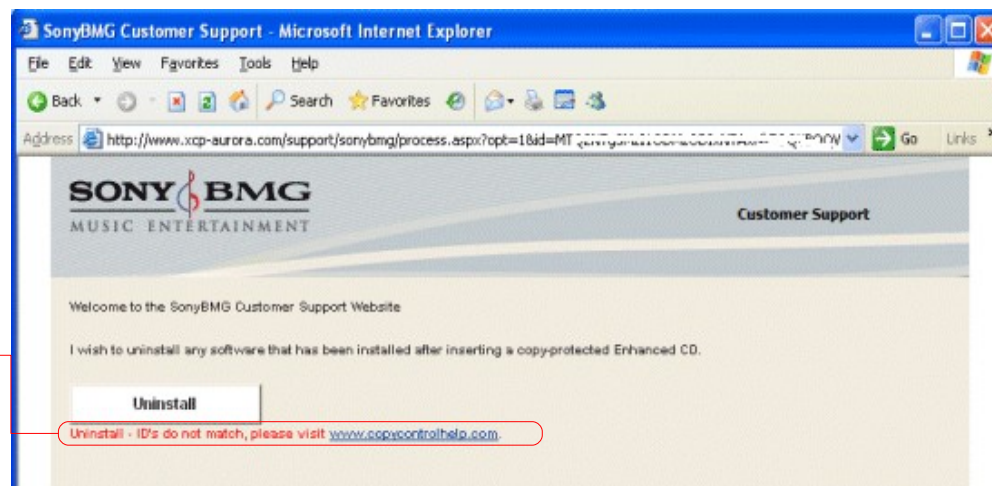
<http://www.xcp-aurora.com/support/sonybmj/process.aspx?opt=1&id=XYAUfasSFoSdasfDoFPPEWFEEoibnaZPQISfFgKGSGGIAAAAAAAAAAAAA>

Só funciona no computador em que foi feita a requisição!

Em **outro** computador:

- ✓ **CodeSupport.Ocx**

Uninstall: ID's do not match...



O Desinstalador (3)

Ed Felton (Freedom to Tinker) descobre **vulnerabilidades** no “*Web-based uninstaller*”:
(<http://www.freedom-to-tinker.com/?p=927>)

- **CodeSupport**: Safe for Scripting.

Qualquer site pode **solicitar “serviços”** ao CodeSupport

Permite que **qualquer** página:

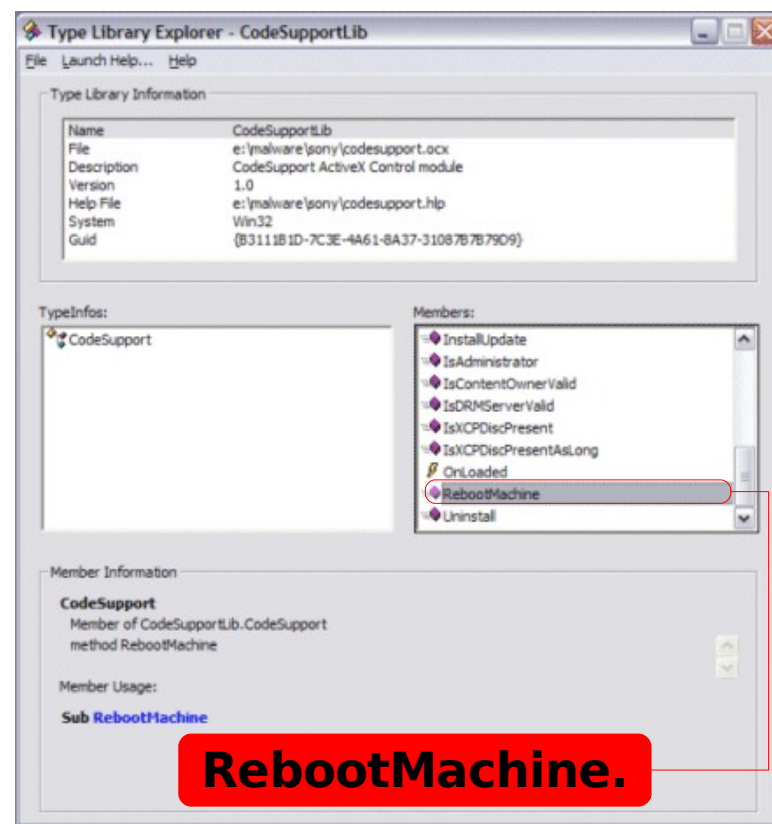
Instale e execute código.

- São exportadas 22 “*scriptable interfaces*”.

Remoção do componente:

Start, Run:

**cmd /k del
“%windir%\downloaded
program files\codesupport.*”**



“ET Phones Home”

Monitorando *Player* da Sony:

- ✓ Phone Home Behavior

→ **Ethereal:**

/toc/Connect?type=redirect&uid=668

```
⊟ Hypertext Transfer Protocol
+ GET /toc/Connect?type=redirect&uid=668 HTTP/1.1\r\n
  Accept: application/*, audio/*, image/*, message/*,\r\n
  User-Agent: SecureNet Xtra\r\n
  Host: connected.sonymusic.com\r\n
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  \r\n
```

```
⊟ Hypertext Transfer Protocol
+ HTTP/1.1 200 OK\r\n
  Date: Fri, 04 Nov 2005 15:50:38 GMT\r\n
  Server: Apache/1.3.27 (Unix)\r\n
  Last-Modified: Wed, 23 Feb 2005 17:17:04 GMT\r\n
  ETag: "6d58a-10-421cba90"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 16\r\n
  Keep-Alive: timeout=1, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/xml\r\n
  \r\n
```

First 4 Internet:

Nenhuma informação é utilizada para traçar o comportamento do usuário.

- Rotating banners updates:



- O comportamento seria **aceitável**:
 - Em outras circunstâncias
 - Estivesse previsto na EULA
 - Pudessem ser configurado/desabilitado

A Réplica

First 4 Internet e seu direito de resposta:

Phone Home Behavior:

"The player has a standard rotating banner that connects the user to additional content (e.g. provides a link to the artist web site). The player simply looks online to see if another banner is available for rotation. The communication is one-way in that a banner is simply retrieved from the server if available. No information is ever fed back or collected about the consumer or their activities."

Service Pack (3.6MB):

"In addition to removing the cloakig, Service Pack 2 includes all fixes from the earlier Service Pack 1 update. In order to ensure a secure installation, Service Pack 2 includes the newest version of all DRM components, hence the large file size for the patch. We have updated the language on our web site to be clearer on this point."

Risco de Tela Azul:

"This is pure conjecture. F4I is using standard Windows commands (net stop) to stop their driver. Nothing more."

A Tréplica

→ NTCrash2:

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: aries.sys

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFFFFFFFF8,0x00000000,0xF9CF5C88,0x00000000)

***      aries.sys - Address F9CF5C88 base at F9CF5000, DateStamp 424bb23f

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

Status

Sony/BMG disponibiliza o **Service Pack 2a**:



INFORMATION ON XCP CONTENT PROTECTION

XCP-AURORA SUPPORT

Please choose an update from the list below.

SOFTWARE UPDATES

Latest Update

Service Pack 2a

8|November|2005, 1.47Mb

This Service Pack removes the cloaking technology component that has been recently discussed in a number of articles published regarding the XCP Technology used on XCP content protected CDs. This component is not malicious and does not compromise security. However to alleviate any concerns that users may have about the program posing potential security vulnerabilities, this update has been released to enable users to remove this component from their computers.

Please note, Service Pack 2a is a maintenance release designed to reduce the file size of Service Pack 2. It includes all previous fixes found in Service Pack 1 and Service Pack 2.

[DOWNLOAD NOW](#)

1.47 MB

Copyright © 1999-2005 First 4 Internet Ltd. All rights reserved.

<http://updates.xcp-aurora.com/Update071105.exe>



HOME	HOW TO USE THE DISC	FAQ	XCP TITLES	SOFTWARE UPDATES	UNINSTALL REQUESTS	SONY BMG XCP EXCHANGE PROGRAM	CONTACT US
------	------------------------	-----	---------------	---------------------	-----------------------	----------------------------------	---------------

▶ UNINSTALL REQUESTS

November 15th, 2005 - We currently are working on a new tool to uninstall First4Internet XCP software. In the meantime, we have temporarily suspended distribution of the existing uninstall tool for this software. We encourage you to return to this site over the next few days. Thank you for your patience and understanding. In the meanwhile, if you have any security concerns about the XCP software, please [download the software update](#) to eliminate the vulnerability reported in the press.

“We currently are working on a new tool to uninstall First4Internet XCP software. In the meantime, we have temporarily suspended distribution of the existing uninstall tool for this software....”

- ✓ Estima-se que mais de **500.000** computadores possuam o *rootkit* instalado.
- ✓ **Malwares** se beneficiam da tecnologia.
- ✓ A Microsoft disponibilizará a detecção e remoção do rootkit no software:
Windows AntiSpyware
(também estará disponível no **Microsoft Windows Defender**)
- ✓ Ações foram movidas contra a Sony/BMG.
- ✓ Sony suspendeu a produção de Cds com a tecnologia XCP
- ✓ Sony realiza o **recall** dos Cds.
 - ✓ **4.7 milhões** de discos **produzidos**
 - ✓ **2.1 milhões** de discos **vendidos**
(<http://www.upsrow.com/sonybmgi/>)
- ✓ John Borland (Cnet) e revendedores afirmam que a **Sony NÃO teve perda nas vendas** dos **Cds infectados** com o notório **XCP** copy-restriction technology”

“It's very important to remember that **it's your intellectual property -- it's not your computer.** And in the pursuit of protection of intellectual property, it's important **not to defeat or undermine the security measures** that people need to adopt in these days.”

Stewart Baker, the assistant secretary for policy in the Department of Homeland Security.



<http://www.boycottsony.us/>

Welcome to Sony's DRM Planet:



Adriano Mauro Cansian

Carina Tebar Palhares

Jorge Luiz Corrêa

Mark's Sysinternals Blog

<http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html>
<http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html>
<http://www.sysinternals.com/blog/2005/11/sonys-rootkit-first-4-internet.html>
http://www.sysinternals.com/blog/2005/11/sony-you-dont-reeeeaaaally-want-to_09.html
<http://www.sysinternals.com/blog/2005/11/sony-no-more-rootkit-for-now.html>

The Register:

http://www.theregister.co.uk/2005/11/23/sony_drm_questions/
<http://www.theregister.co.uk/2005/11/22/analysis/>
http://www.theregister.co.uk/2005/11/21/gaffer_tape_trips_up_sony_drm/
http://www.theregister.co.uk/2005/11/15/outlaw_parliament_drm/
http://www.theregister.co.uk/2005/11/10/sony_drm_trojan/

Security Focus:

<http://www.securityfocus.com/brief/34>

Sony BMG:

<http://www.sonybm.com/>

Freedom to Tinker:

<http://www.freedom-to-tinker.com/?p=927>

EFF

<http://www.eff.org>



<http://www.securityradio.org>

? !