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

Motivação

"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.***

Agenda

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

Introdução

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

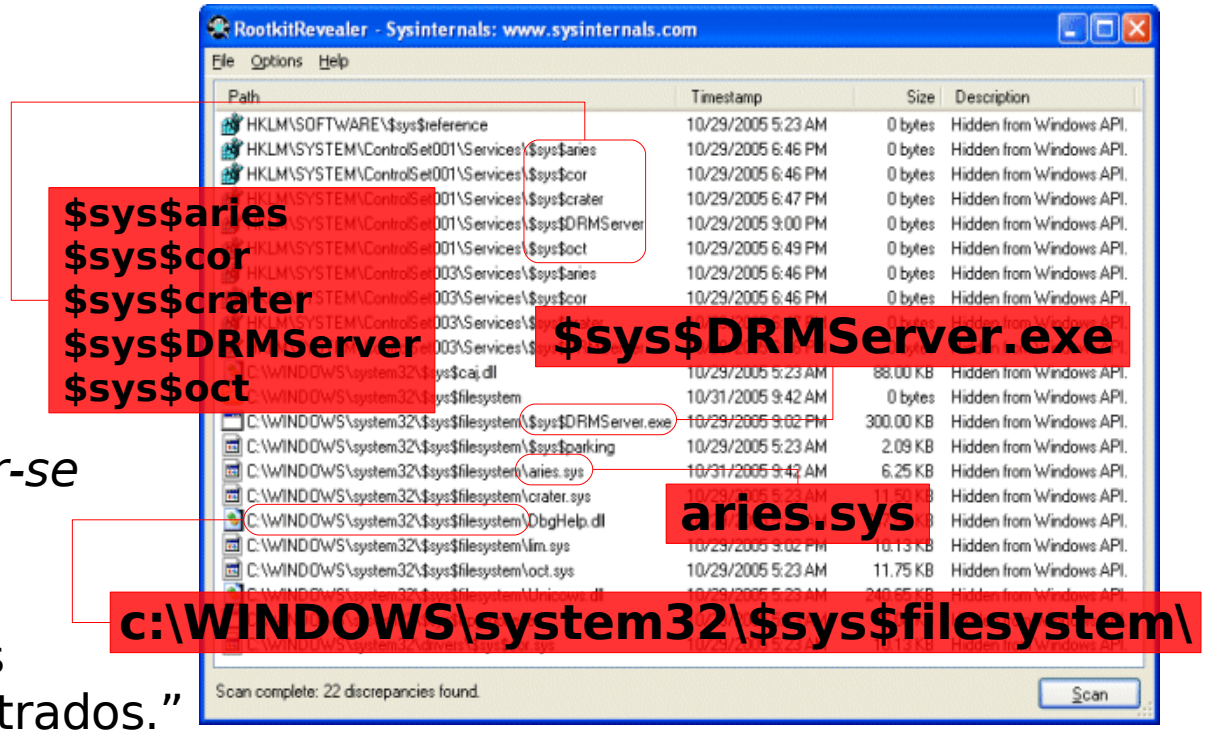
http://www.sysinternals.com

A Descoberta

A Descoberta (1)

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

- 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."

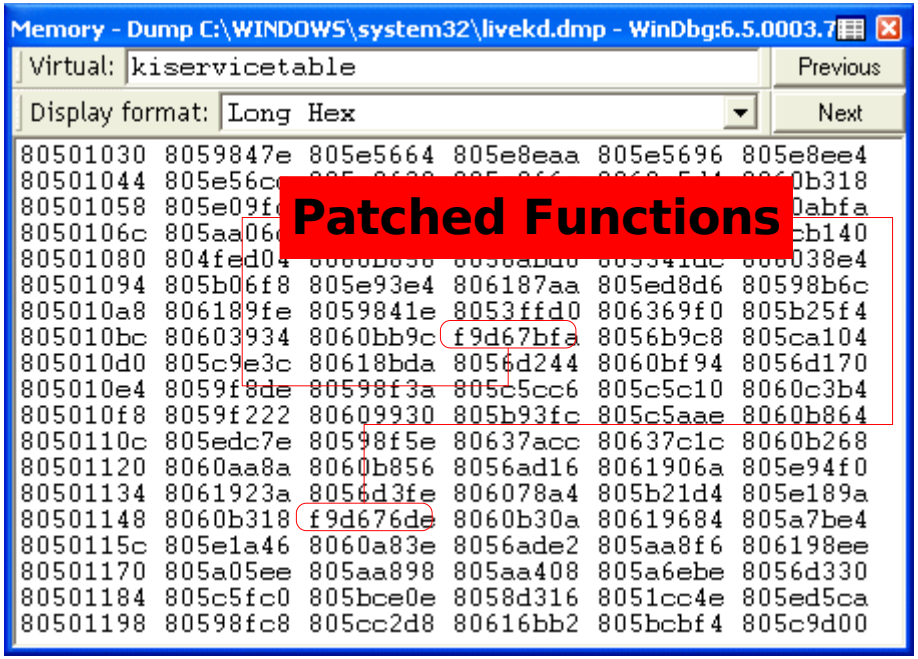
Dá-se iníncio a uma investigação minuciosa...

A Descoberta (2)

Imediatamente após a identificação dos arquivos, Russinovich tentou utilizar:

- ✗ ~~**Autoruns**~~
- ✗ ~~**Process Explorer**~~
- ✓ **LikeKd**

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

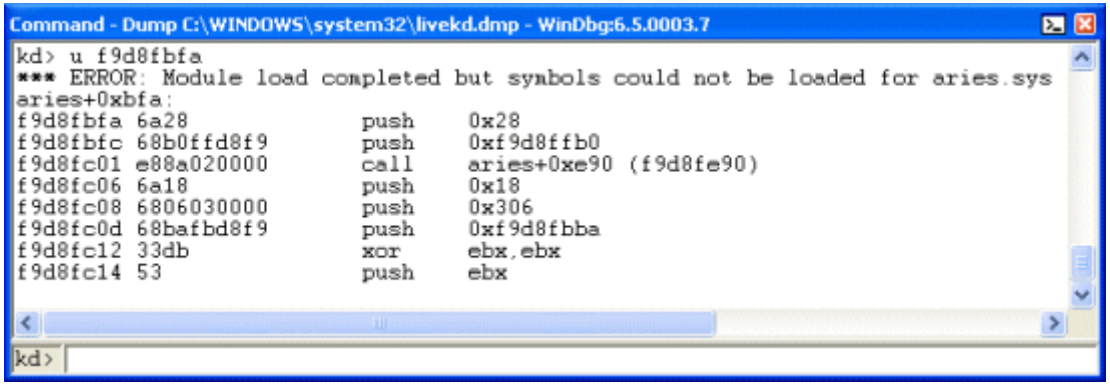


Endereços **não** pertencentes ao **espaço do kernel** são chamados de:
"***Patched Functions***"

A Descoberta (3)

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

aries.sys

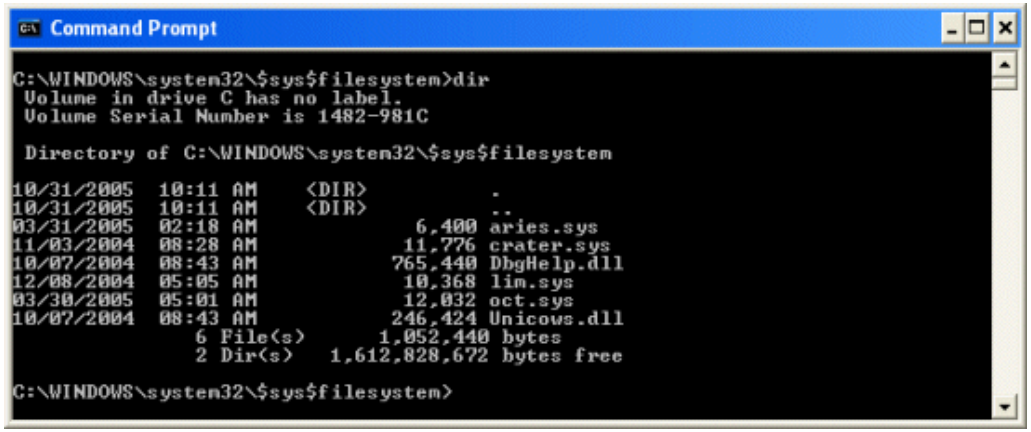


Identificado o driver responsável por esconder arquivos, diretórios, programas e chaves do registro!

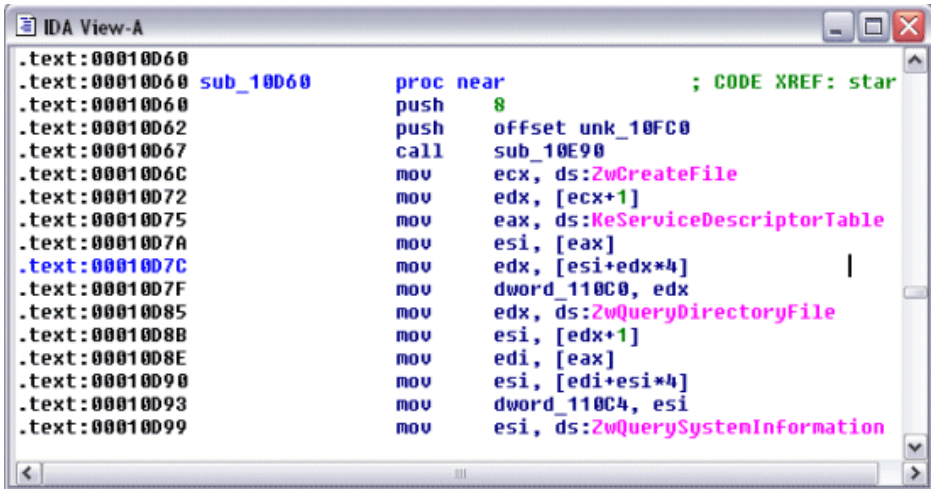
- Seria suficiente remover o arquivo **aries.sys**?
- Talvez renomear ou remover o arquivo pudesse resolver o problema!
- Russinovich queria mais...

A Descoberta (4)

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



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



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

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

Iniciado por:
sys

A Descoberta (5)

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

sysNotepad.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!**

A Descoberta (6)

- 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
```

A Descoberta (7)

“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*.”

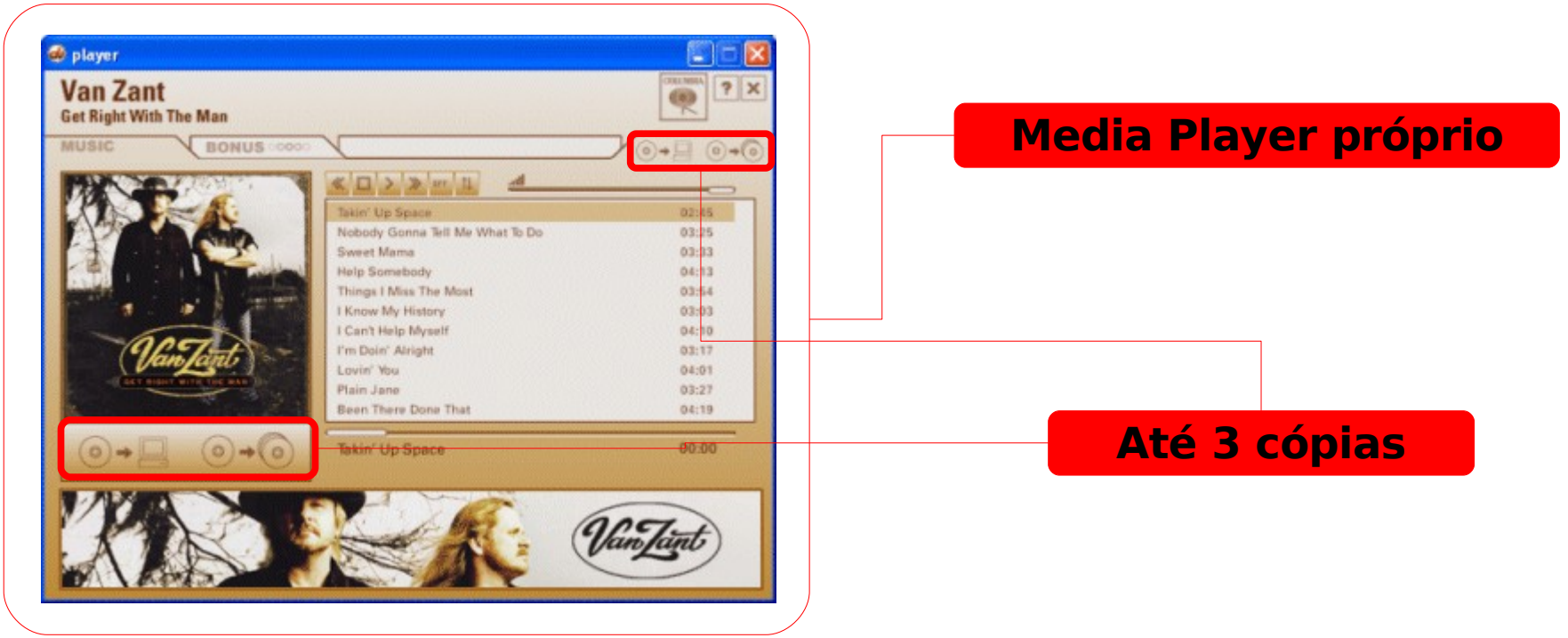
http://www.first4internet.com

A Descoberta (8)

Russinovich lembrou que havia comprado um CD recentemente...

- **Van Zant** - *"Get Right With The Man "*

[CONTENT/COPY-PROTECTED CD]



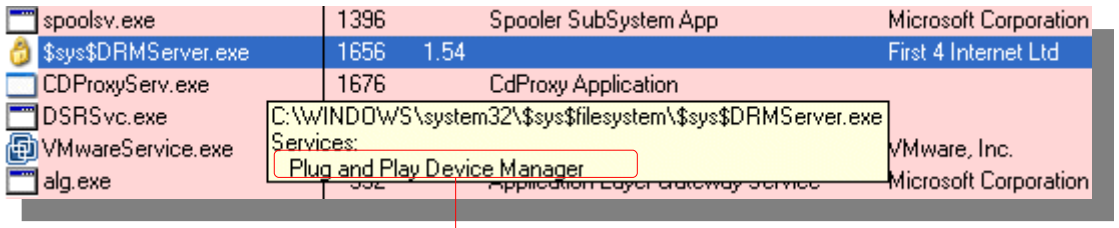
A Descoberta (9)

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: **sysDRMServer.exe**



Plug and Play Device Manager

A Descoberta (10)

Esperava-se que ao fechar o *player* o processo **sysDRMServer.exe** parasse de consumir os ciclos da CPU.

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

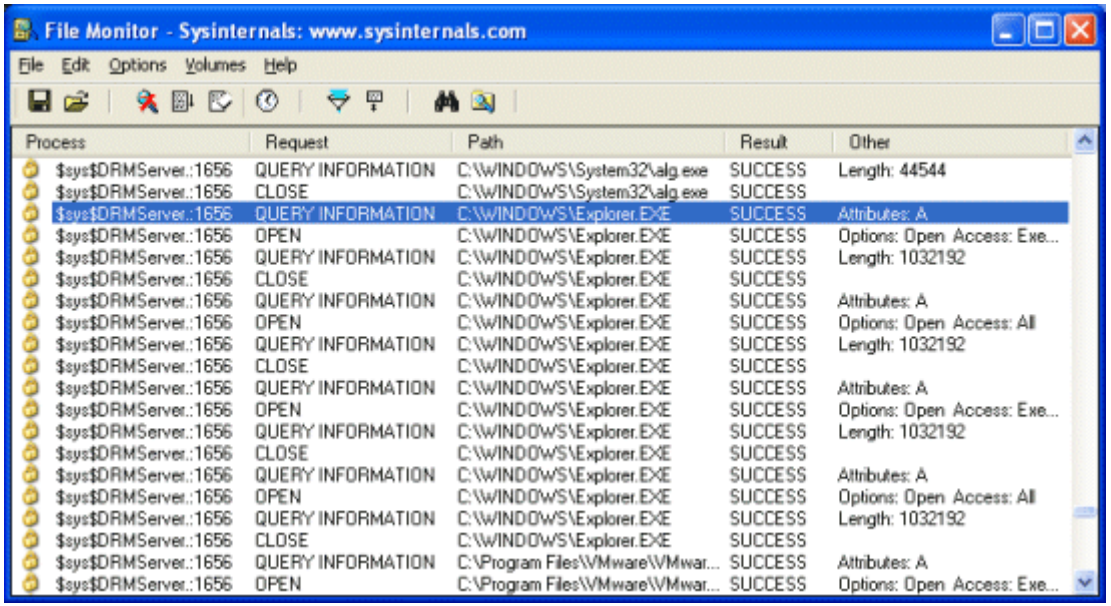
O processo continuava **consumir ciclos de CPU.**

- **File Monitor**:

  Scans:

  Informações sobre os arquivos incluindo o tamanho.

  - 8 x a cada **2 segundos**!



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

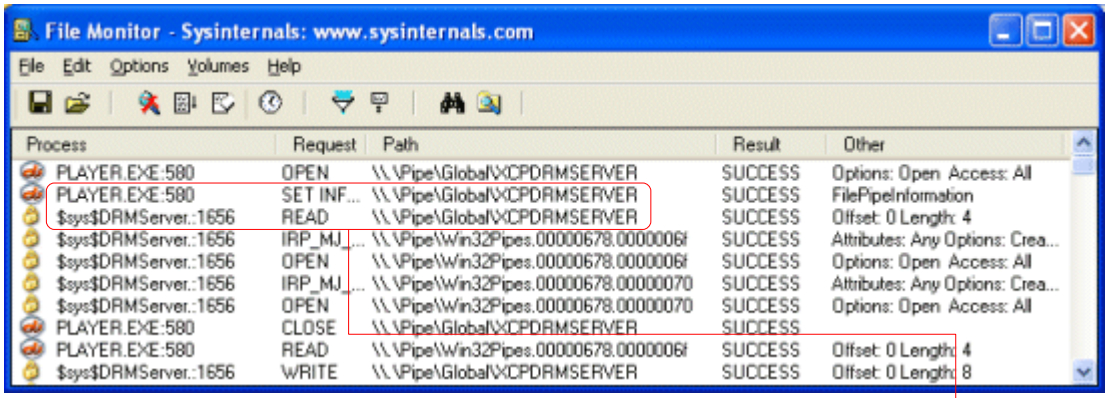
Mark Russinovich

A Descoberta (11)

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

- **File Monitor**:

  Foi marcado a opção "**Named Pipes**" no menu "**Volumes**".



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
sysDRMServer: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

A Remoção (1)

Como **desinstalar** o Software/RootKit?

Não há um 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: **sysDRMServer**.
- Deletar as **Registry Keys**:

  HKLM\System\CurrentControlSet\Services

Porém....

A Remoção (2)

Safe Boot Registry Keys:

HKLM\System\CurrentControlSet\Control\SafeBoot

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

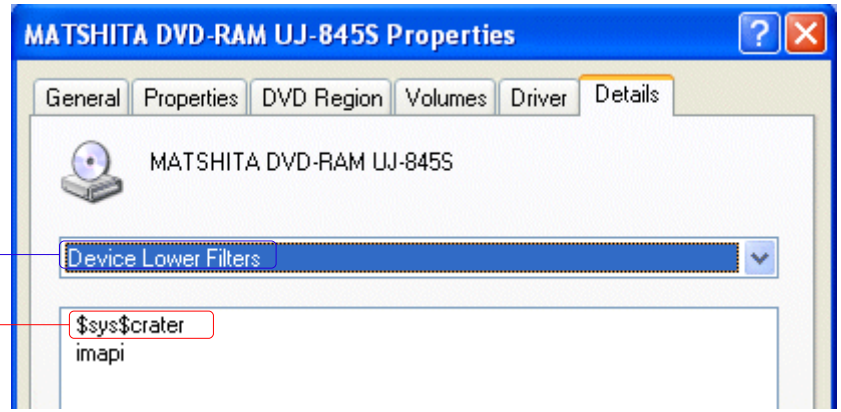
problema_segurança++;

Reiniciando o computador:

O driver de CD havia **desaparecido**.

Sistemas de filtros do Windows:

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



Device Lower Filters

syscrater

Não há uma interface administrativa.

A Remoção (3)

As entradas dos filtros podem ser encontradas em:

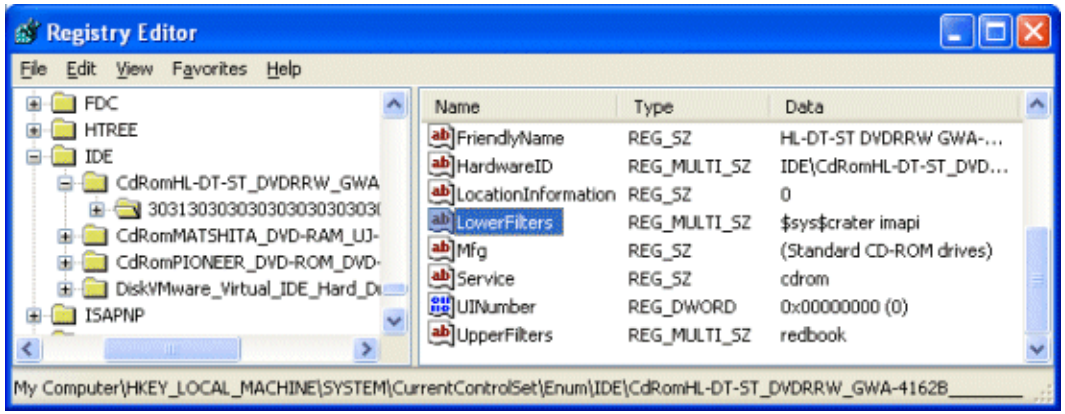
HKLM\System\CurrentControlSet\Enum

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**:

- **sysCor.sys (Corvus)**
  upper filter for the **IDE channel device**

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

0 Service Pack

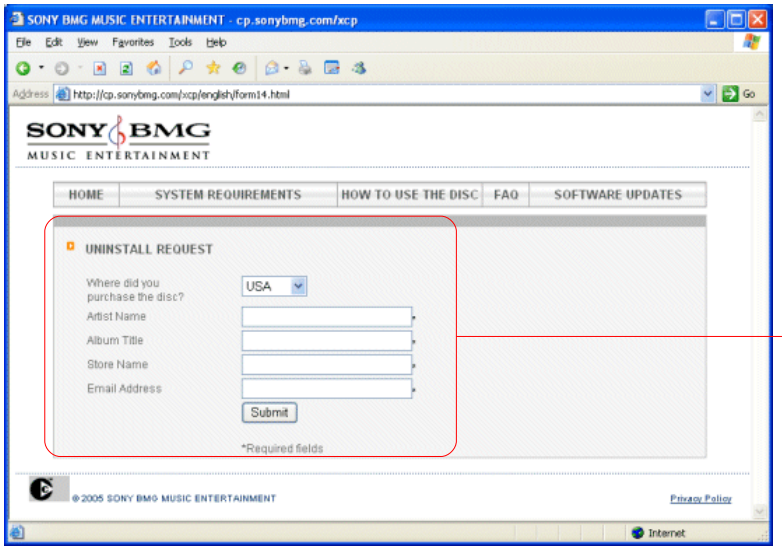
O Service Pack (1)

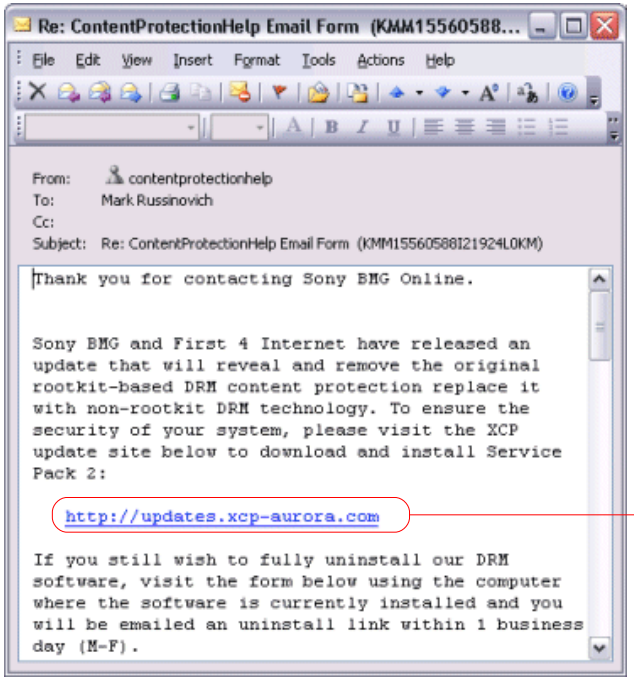
Cobertura do caso:

- 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:

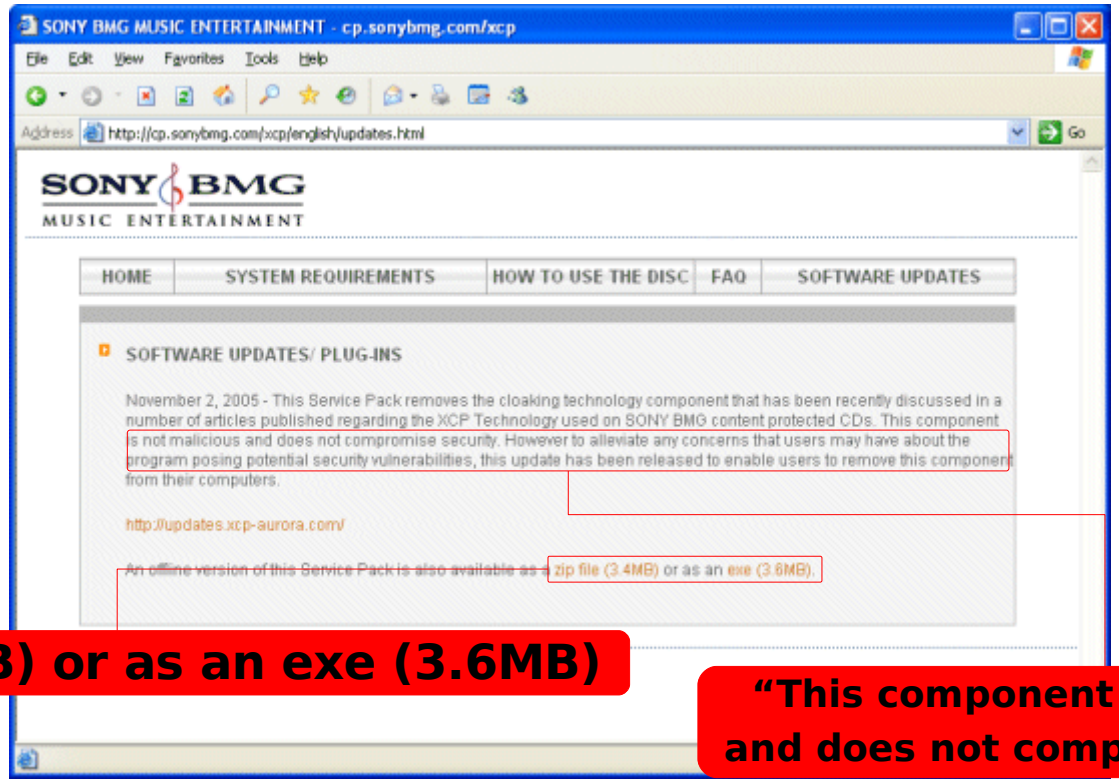
- Case ID
- Redirecionado para outro site.

http://updates.xcp-aurora.com

Informações Pessoais

O Service Pack (2)

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 Sofware.

O Service Pack (3)

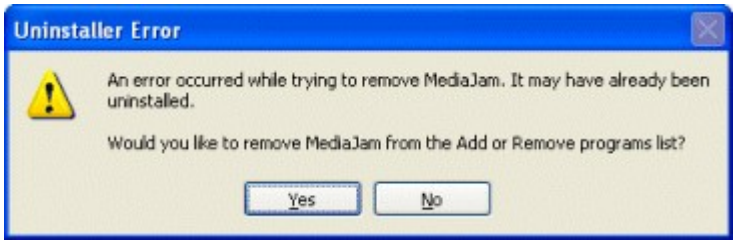
Sony Player ou DRM Software agora com o nome:


```
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!

O Service Pack (4)

Patch equivalente a execução do comando:

net stop “network control manager”

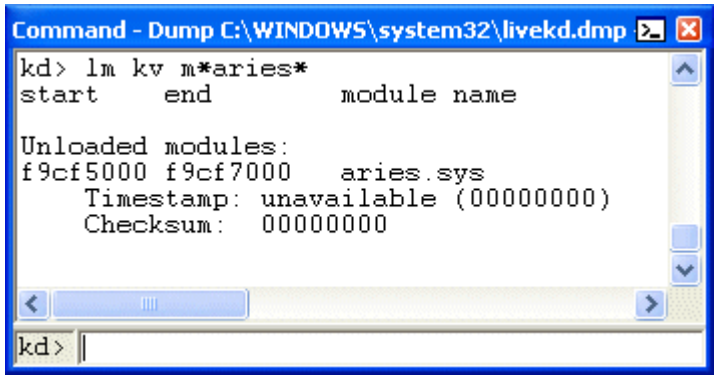
“Network Control Manager” = **Aries Driver**

- 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.**

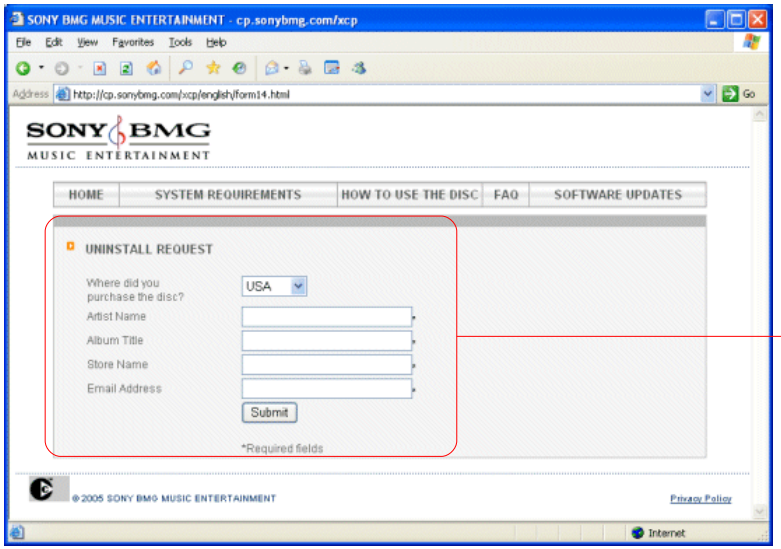


Uma forma **segura** para descarregar o driver seria: **reiniciando o sistema**, mantendo o driver **ativo** enquanto desliga o sistema!

O Desinstalador

O Desinstalador (1)

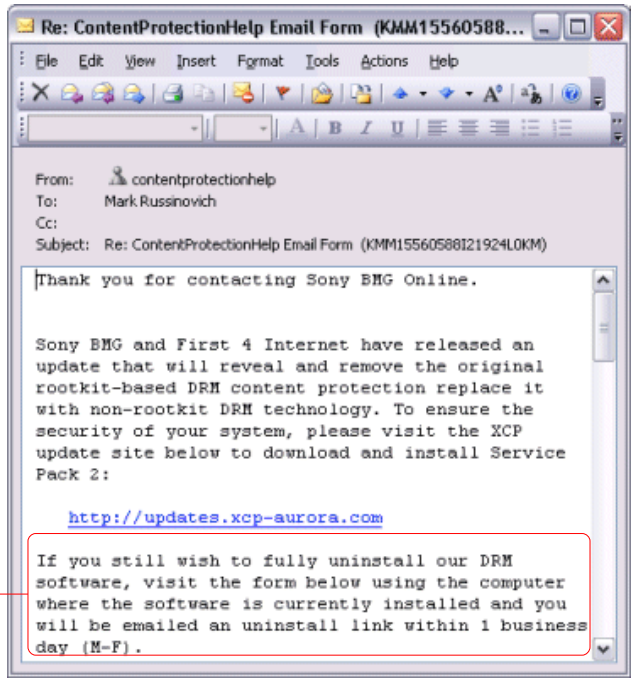
Web based Uninstaller:



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...



O Desinstalador (2)

ActiveX Control:

- **CodeSupport.Ocx**

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

O e-mail contendo o *link*:

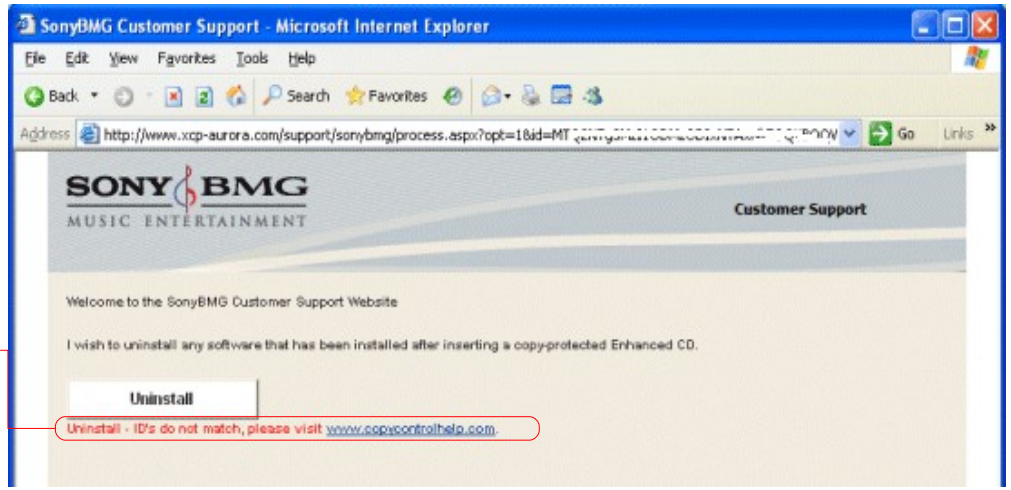
http://www.xcp-aurora.com/support/sonybmg/process.aspx?opt=1&id=XYAUfasSFoSdasfDoFPPEWFFEoibnaZPQISfFgKGSGGIAAAAAAAAAA

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)

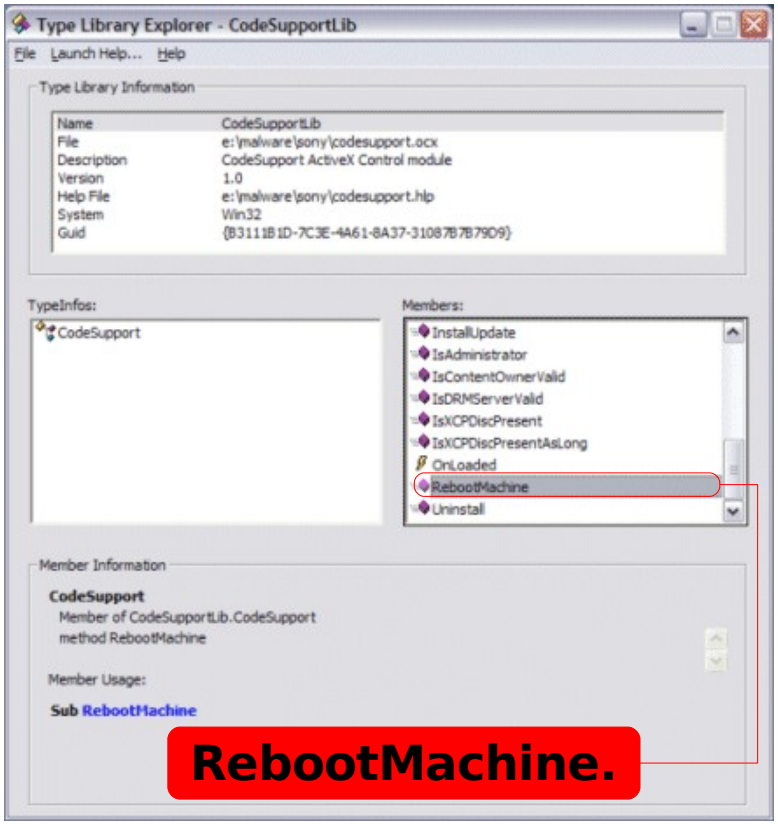
- **CodeSupport**: Safe for Scripting.

  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”

ET Phones Home

Monitorando *Player* da Sony:

- ✓ Phone Home Behavior

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

- → **Ethereal:**

```
Hypertext Transfer Protocol
  GET /toc/Connect?type=redirect&uId=668 HTTP/1.1\r\n
  Accept: application/*, audio/*, image/*, message/*,
  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
  - Pudesse ser configurado/desabilitado

A Réplica

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.”

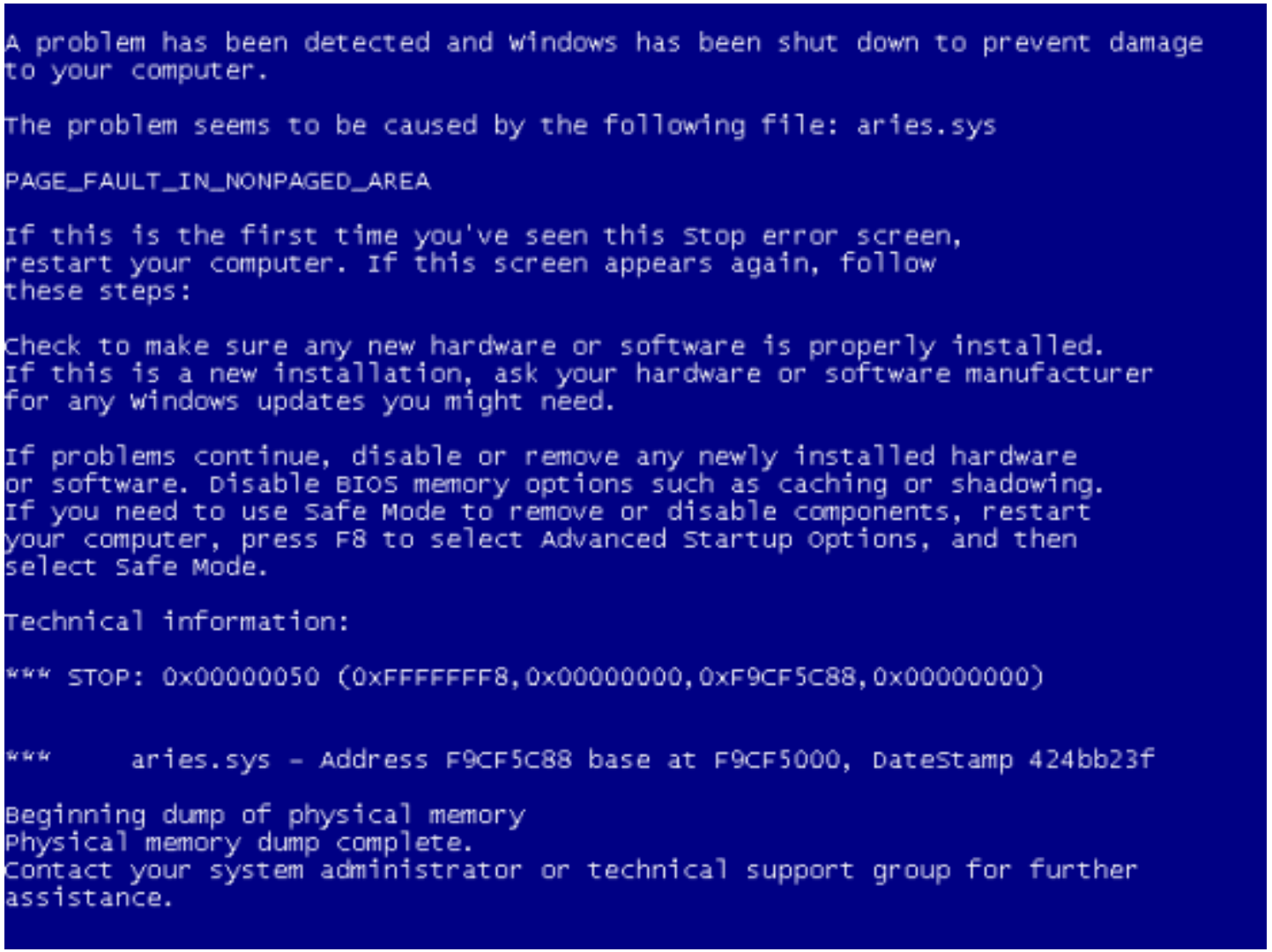
Risco de Tela Azul:

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

A Tréplica

A Tréplica

- **NTCrash2:**



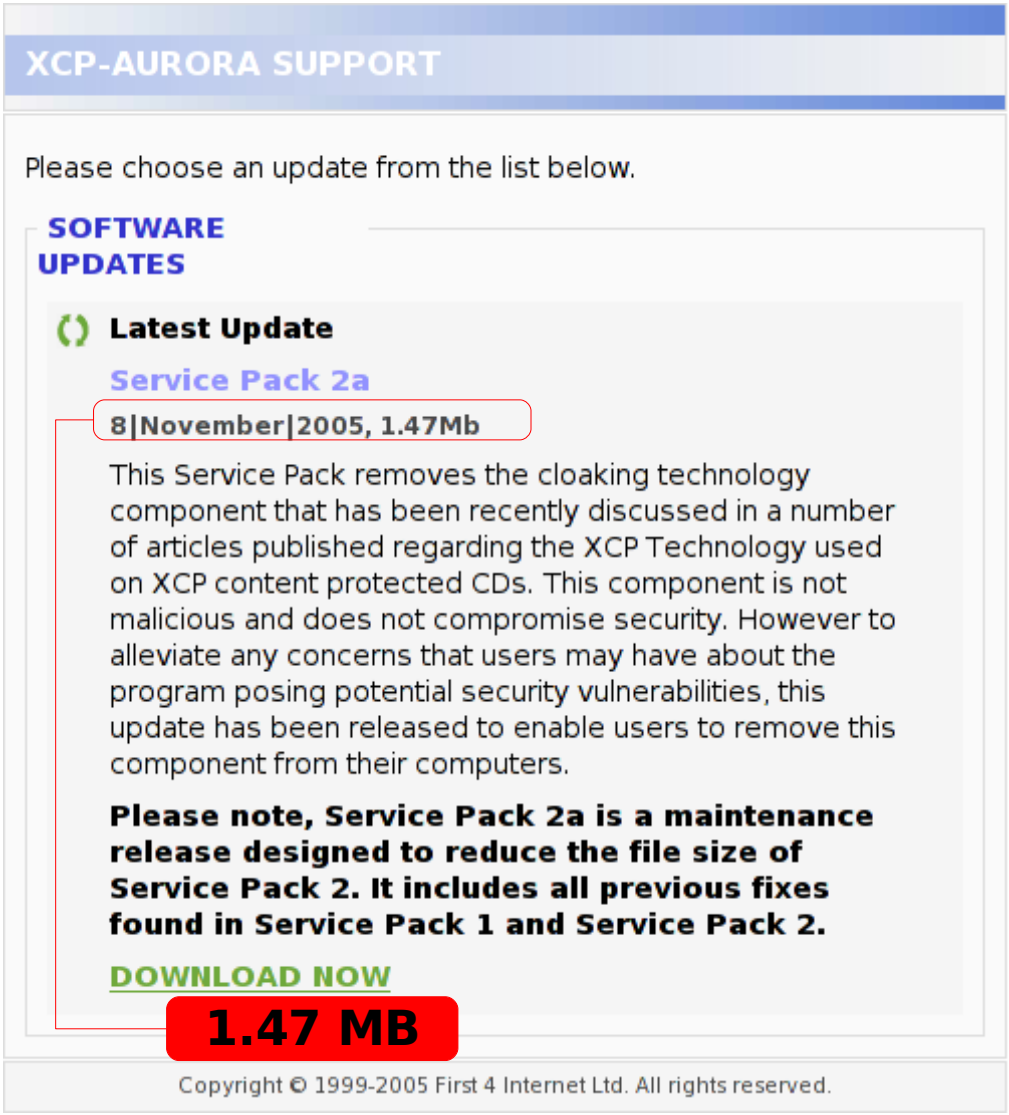
Status

Status (1)

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

INFORMATION ON XCP CONTENT PROTECTION

Status (2)



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

Status (3)

SONY BMG MUSIC ENTERTAINMENT

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...."

Status (3)

- 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/sonybmg/)

- John Borland (Cnet) e revendedores afirmam que a **Sony NÃO teve perda nas vendas** dos **Cds infectados** com o notório **XCP** copy-restriction technology”

Status (4)

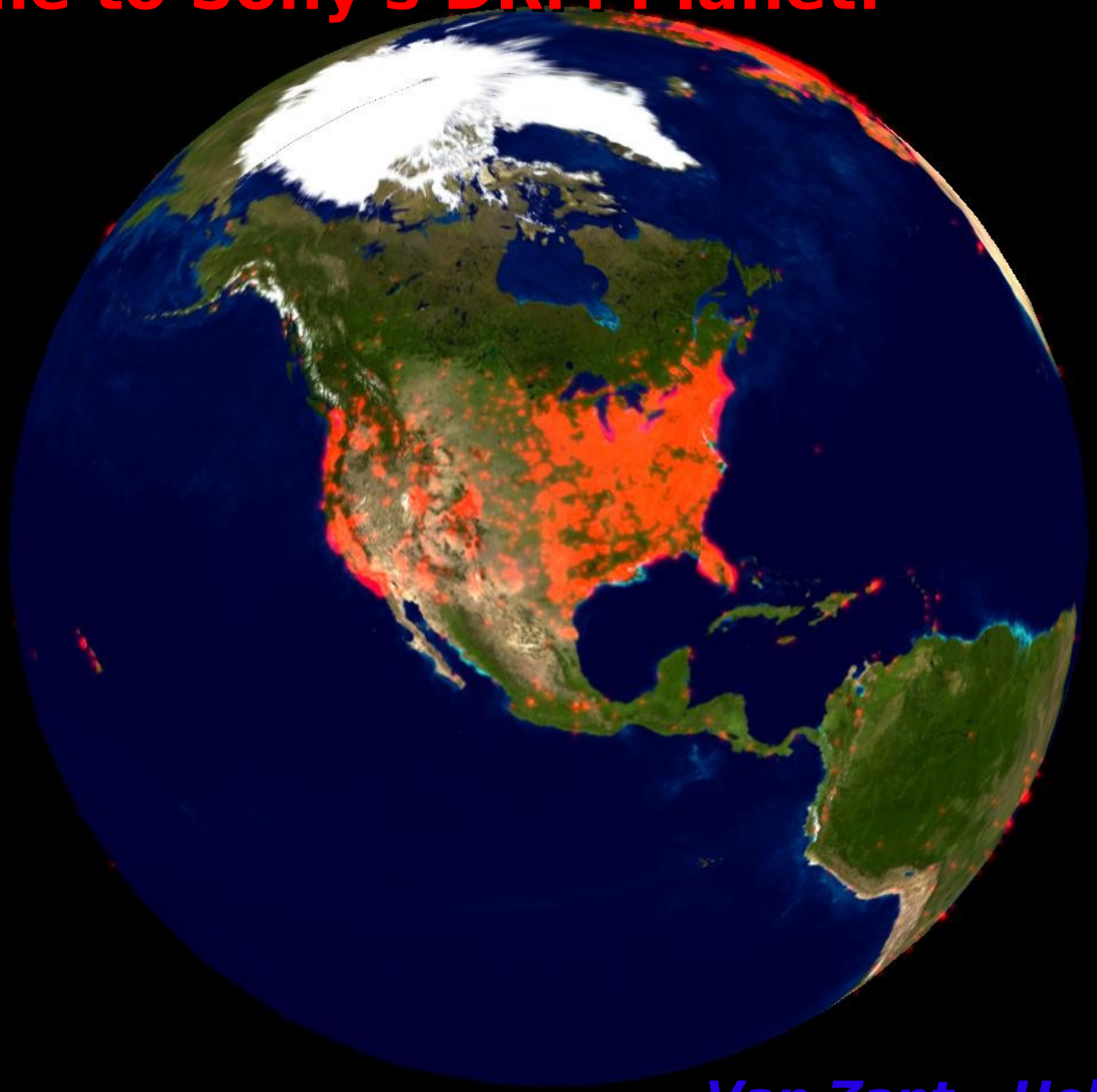
“It's very important to remember that **it's your intellectual property** -- **it's not your computer.** And in the pursuit of protection of intellectual property, it's important **not to defeat or undermine the security measures** that people need to adopt in these days.”

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

http://www.boycottsony.us/

Status (5)

Welcome to Sony's DRM Planet:



Van Zant – Help Somebody

Agradecimentos

Adriano Mauro Cansian

Carina Tebar Palhares

Jorge Luiz Corrêa

Referências

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.sonybmg.com/

Freedom to Tinker:

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

EFF

http://www.eff.org

...Google

Visite

http://www.securityradio.org

Dúvidas?

?!