Semana da Infraestrutura da Internet no Brasil
De 29 de novembro a 3 de dezembro de 2011 São Paulo
5º PTT Fórum - IPv6 Brasil - GTER 32 / GTS 18

Cerzindo
o
Gerenciamento de Patches
com
matraQa

Marcos Euzebio
marcos.euzebio@bcb.gov.br
Divisão de Segurança em TI - Diseg
Departamento de Tecnologia da Informação - Deinf
BANCO CENTRAL DO BRASIL

The Security Patch Treadmill

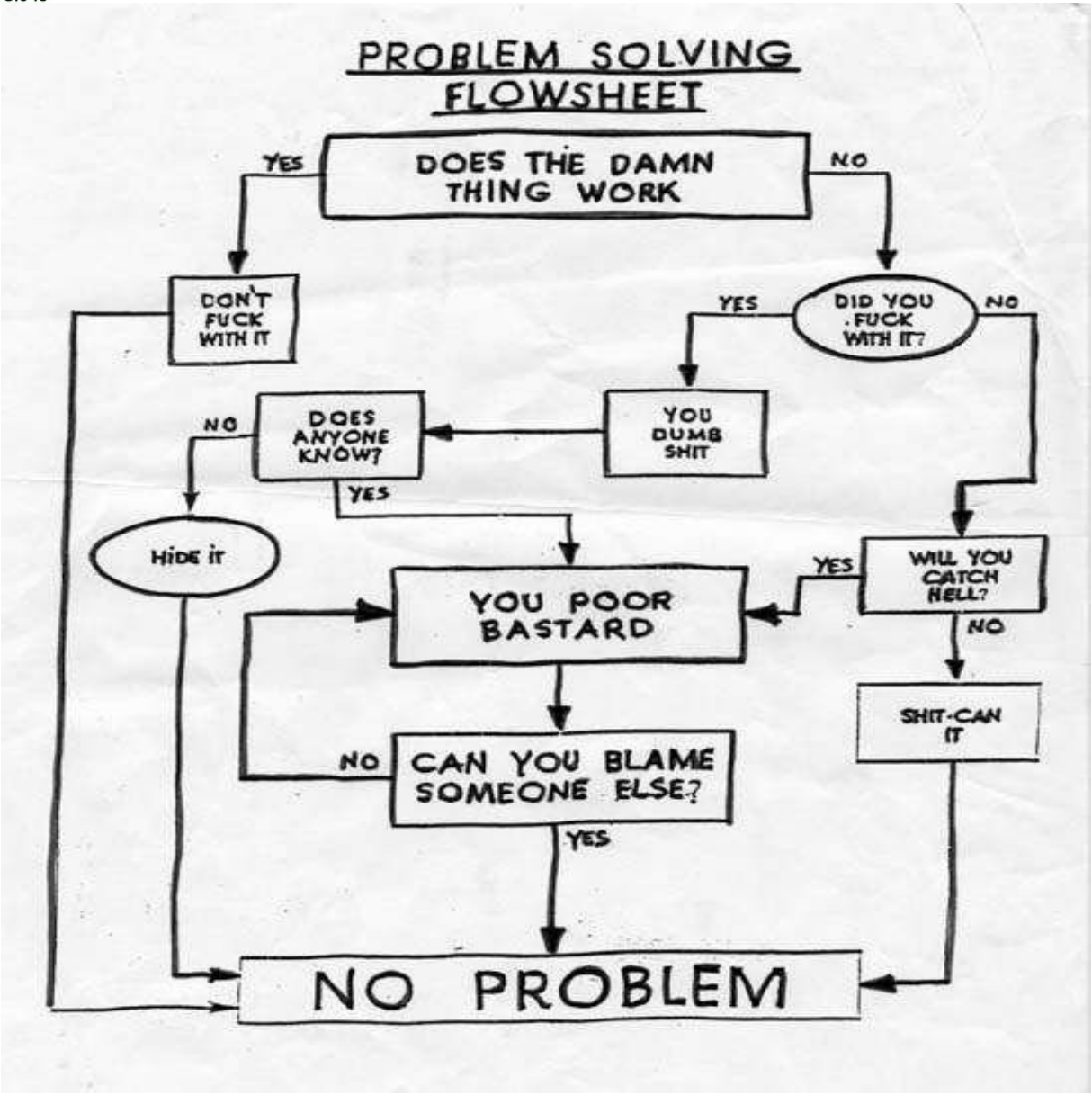
"Well, in our country," said Alice, panting a little, "you'd generally get somewhere else -- if you ran very fast for a long time, as we've been doing."

"A slow sort of country!" said the Queen. "Now here, you see, it takes all the running you can do, to keep in the same place."

--Through the Looking Glass, by *Lewis Carroll.*

www.schneier.com/crypto-gram-0103.html#1

If ain't broke, don't fix it



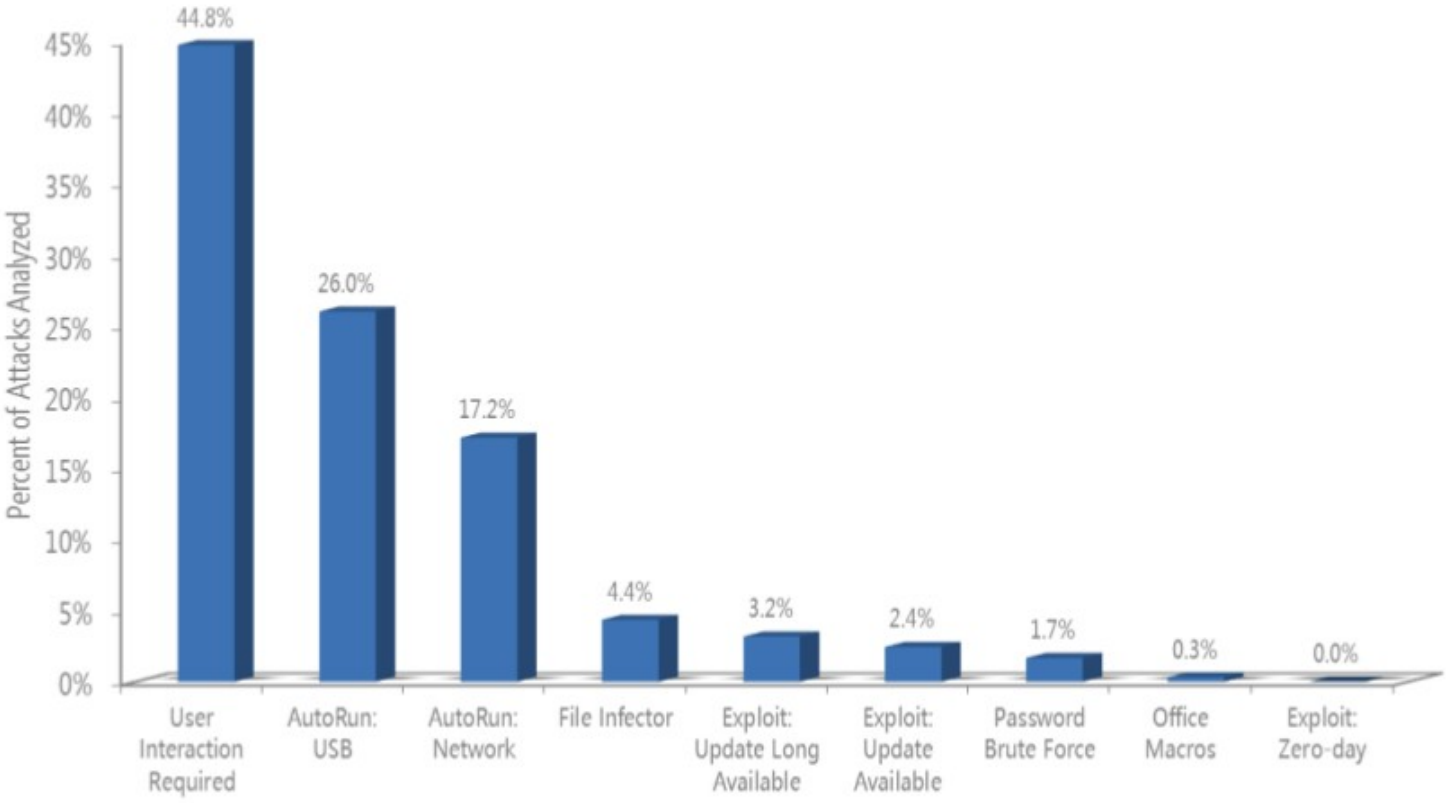
Critical Control 10: Continuous Vulnerability Assessment and Remediation

- important mechanism to detect known vulnerabilities
- if possible patch them or use additional host or network controls to prevent exploitation until a patch or update is released
- ...

isc.sans.edu/diary.html?storyid=11809

Microsoft Security Intelligence Report 2011

Figura 1. Malware detectado pelo MSRT no 1S11, por médias de métodos de propagação documentados

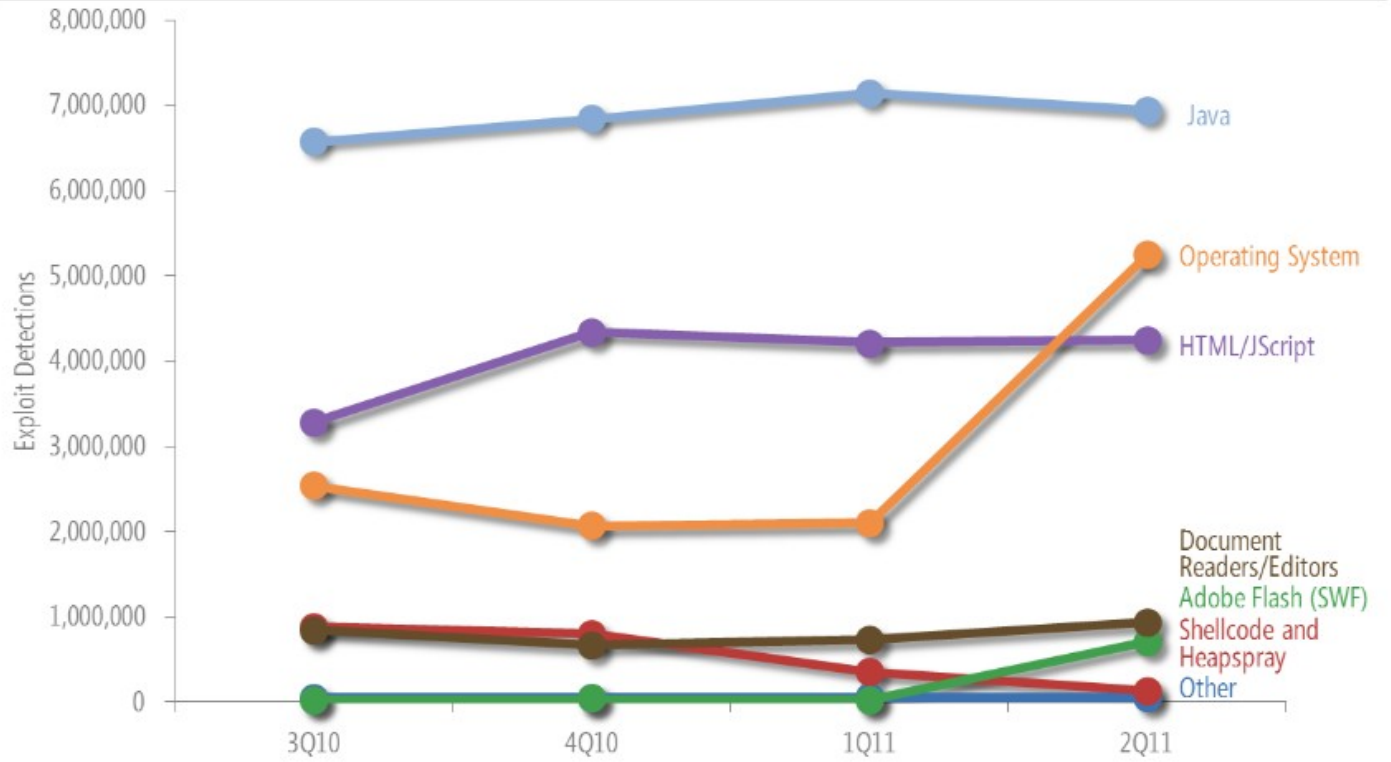


www.microsoft.com/sir

BANCO CENTRAL DO BRASIL

Microsoft Security Intelligence Report 2011

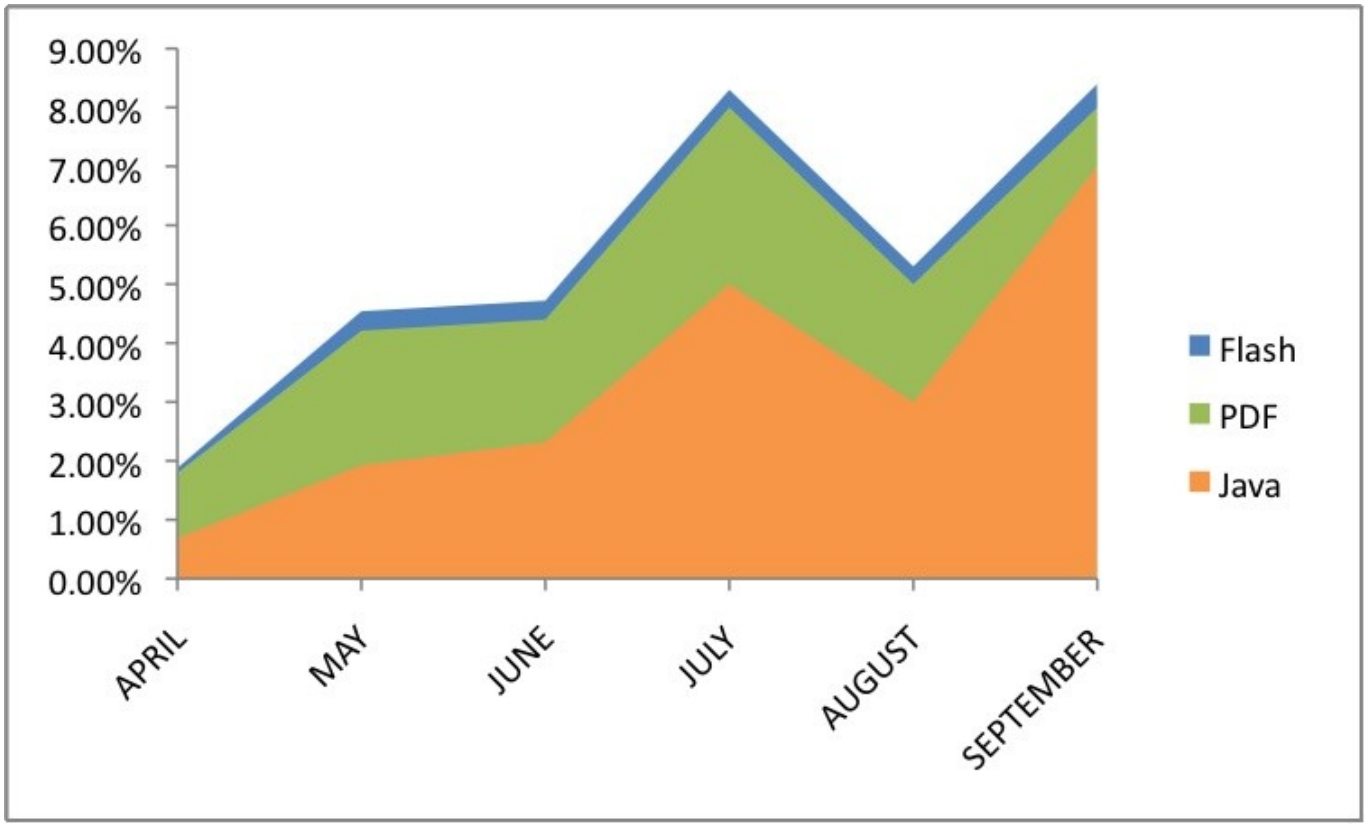
Figura 3. Exploits detectados e bloqueados por produtos anti-malware da Microsoft, 3T10–2T11, por plataforma ou tecnologia-alvo



www.microsoft.com/sir

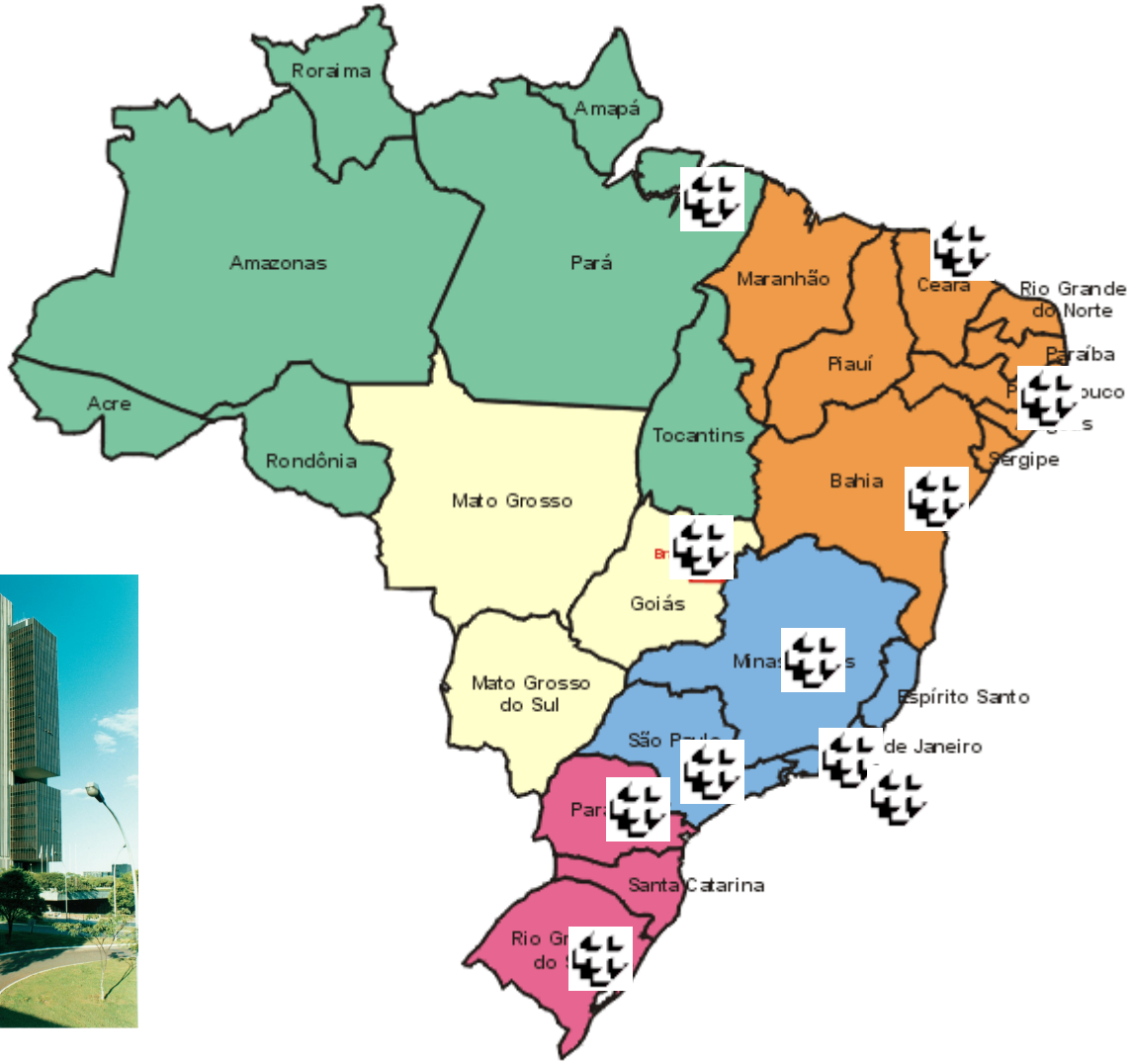
BANCO CENTRAL DO BRASIL

Cisco ScanSafe



blogs.cisco.com/security/java-exploits-another-example-of-tomorrows-threat-landscape-today-2

Banco Central do Brasil



BANCO CENTRAL DO BRASIL

Logística

Push by)robocopy(

Total: 7000+

BANCO CENTRAL DO BRASIL

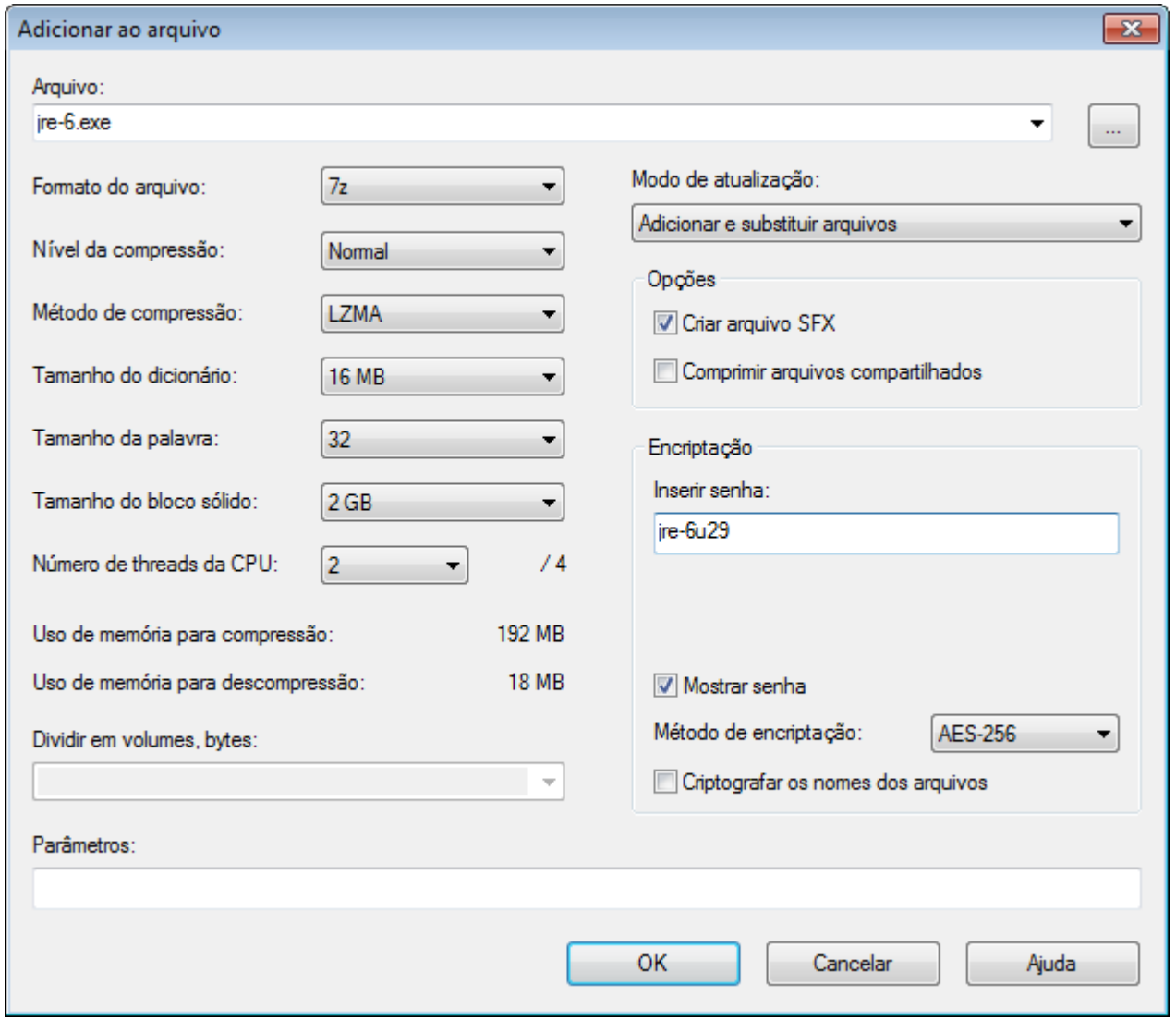
Estações – Download local

Flash 08 MB
Java 15 MB
Reader 40 MB

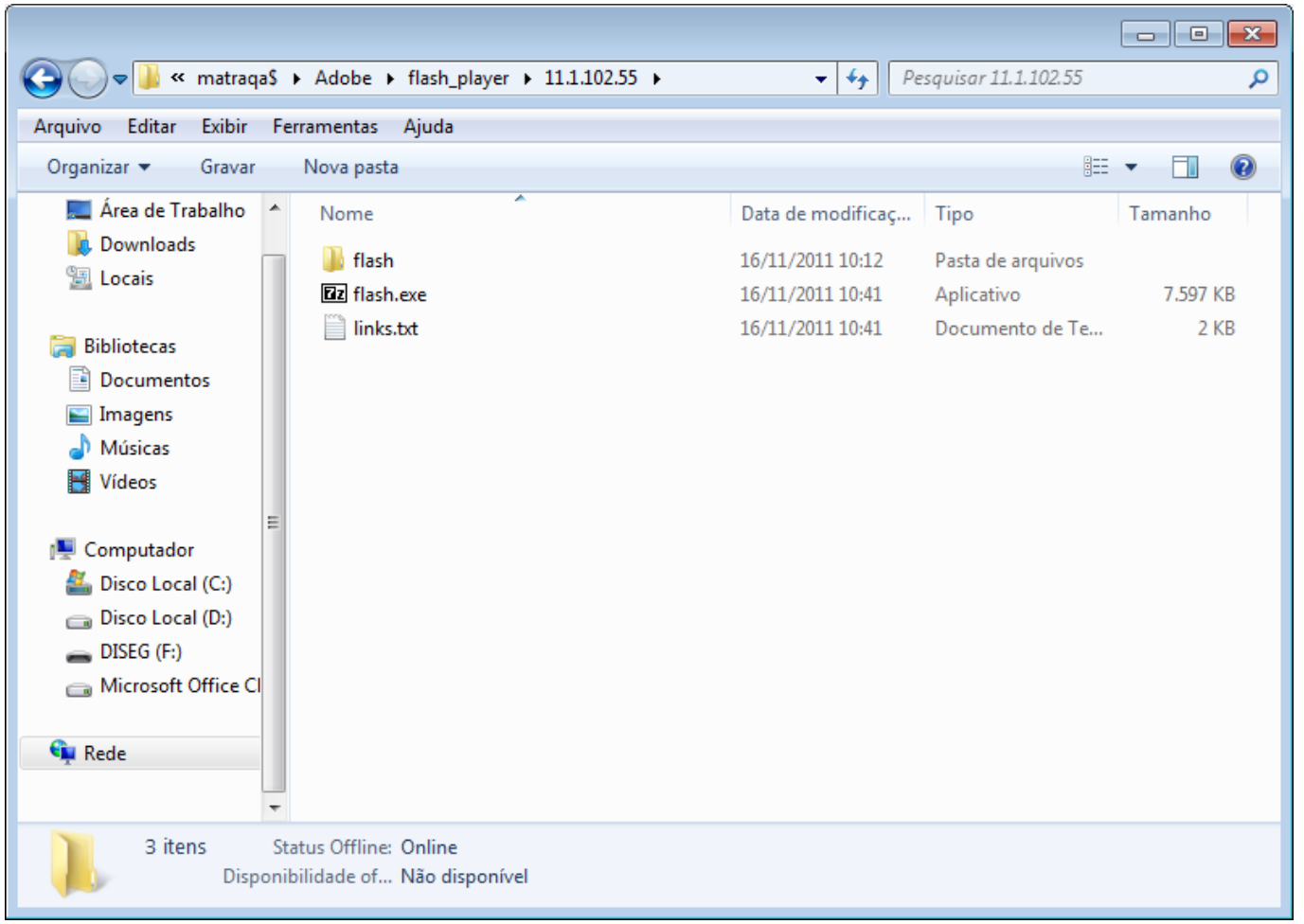
100 M

Pull by >wget<

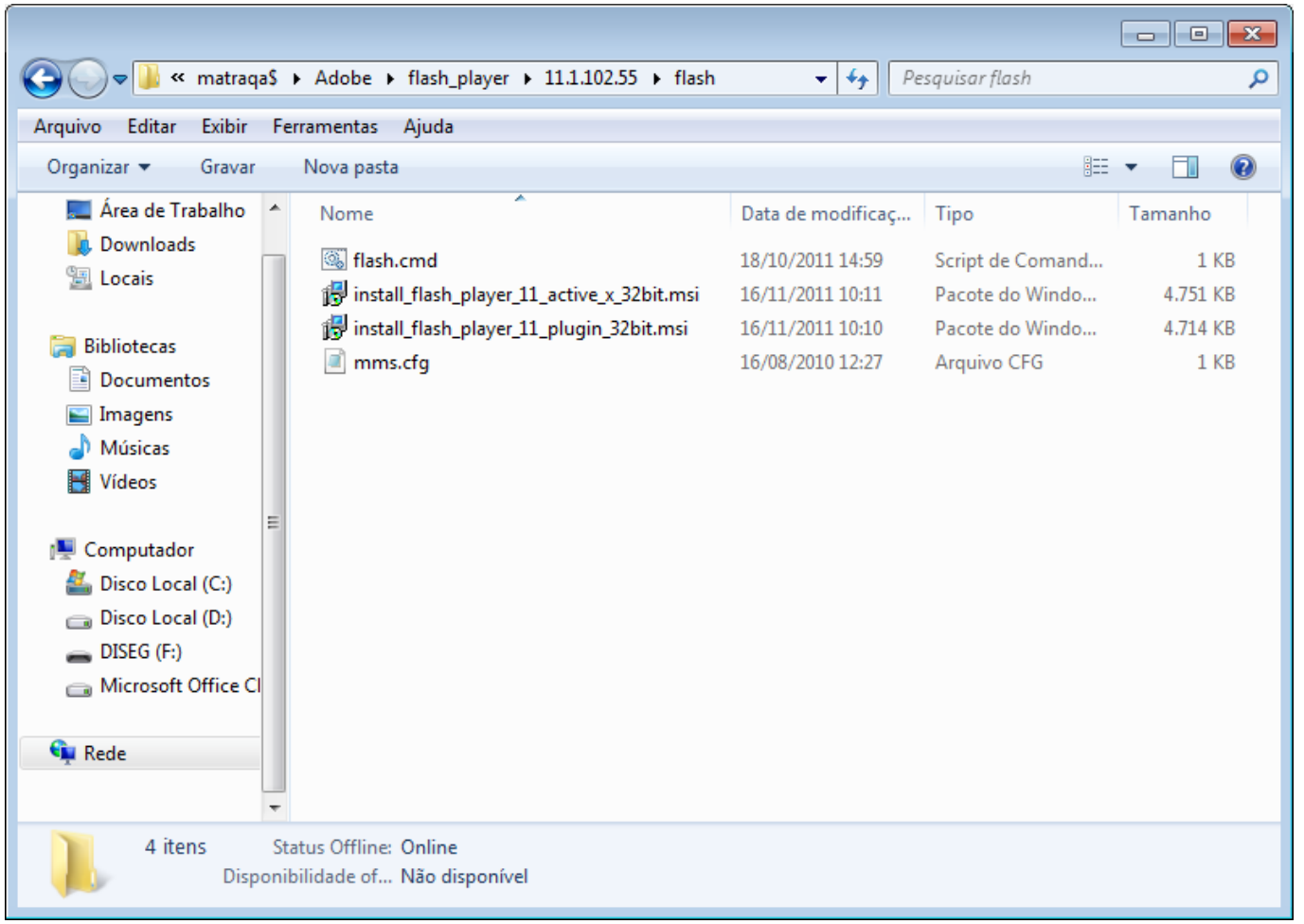
Empacotamento dos Componentes



Empacotamento dos Componentes



Empacotamento dos Componentes



Empacotamento dos Componentes

flash.cmd + (\\antivirusdf\matr...h_player\11.1.102.55\flash) - GVIM

Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
::@echo off
::::::::::::::::::::::::::::::::::::::::
:: script para instalacao do flash
::
if not "%1" == "" goto func_%1
   goto func_install

goto :eof

::::::::::::::::::::::::::::::::::::::::
:: install flash
::
:func_install
   pushd %~dp0

   msiexec /quiet /i install_flash_player_11_active_x_32bit.msi
   msiexec /quiet /i install_flash_player_11_plugin_32bit.msi

   if exist %windir%\system32\Macromed\Flash\mms.cfg goto :eof

      copy mms.cfg %windir%\system32\Macromed\Flash\mms.cfg

   popd
goto :eof
                                                    17,4          All
```

Laundry List

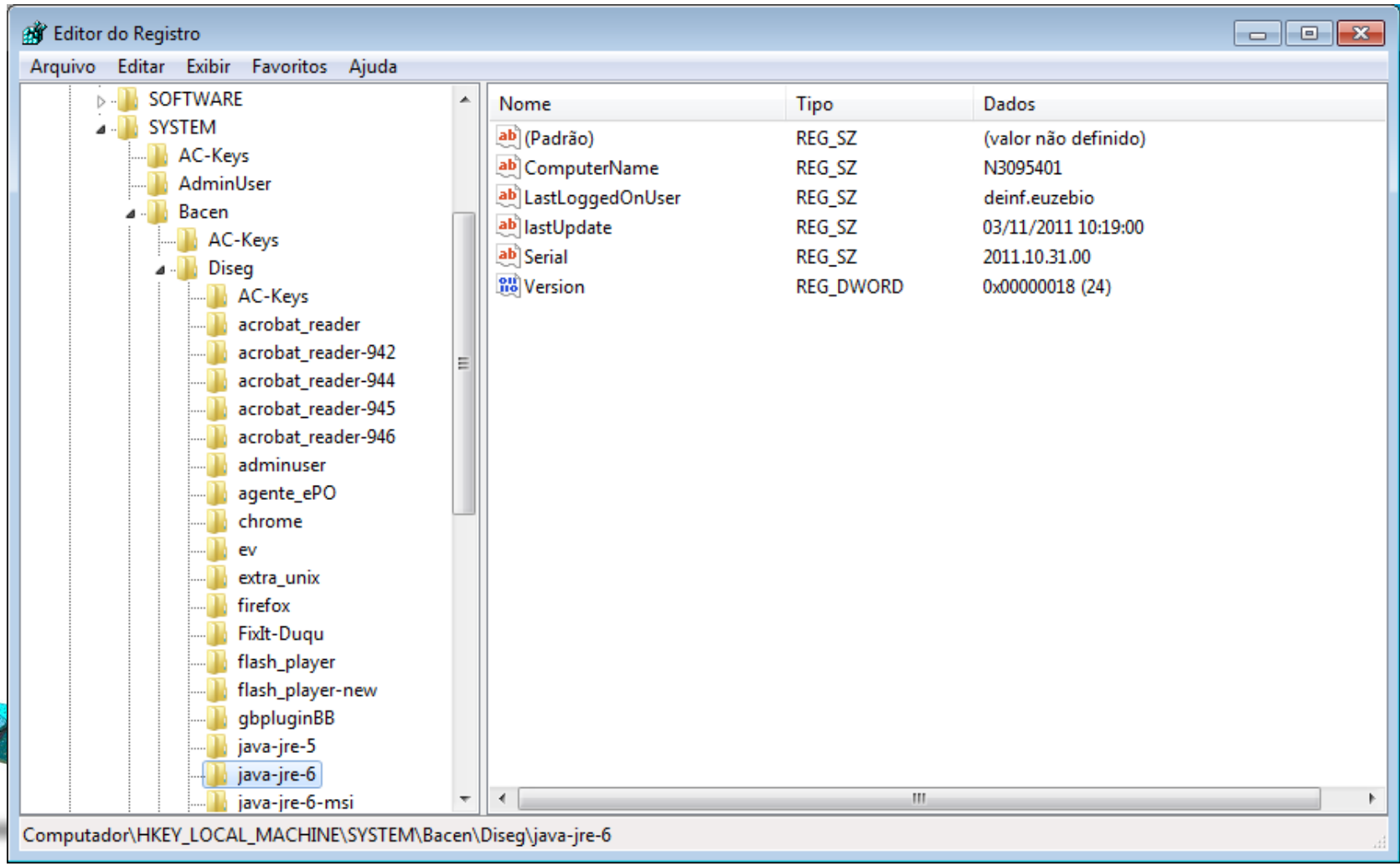
matraQa-startup-x86.tsk (F:\matraQa\matraQa) - GVIM

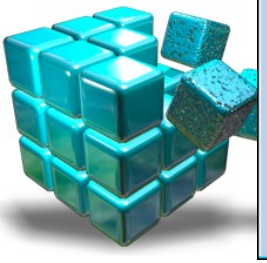
Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
#
# matraQa: arquivo de parametros para deployment das correcoes
#
# campos separados por | (barra vertical)
#           id(1): identificacao da correcao
#    restricao(2): grupos para os quais a operacao e permitida (unidos por ;)
#     operacao(3): install|update
#      matraca(4): versao da insercao da correcao na matraca
#       versao(5): versao da correcao mais atual
#    mecanismo(6): reg|filever|filereg|filedat, para determinar versao atual instalada
#      caminho(7): onde olhar na register ou file system a versao instalada
#        fonte(8): local de onde trazer a correcao (um ou mais unidos por ;)
#      comando(9): programa de instalacao (um ou mais unidos por ;)
#
# A T E N C A O :  nao coloque aspas nos parametros, senao peteca tudo
#
######## d) Flash Player da Macromedia/Adobe ######################
##
flash_player|OK|update|2011.11.18-00|11.1.102.55|reg,CurrentVersion,3|HKLM\SOFTWARE\Macromedia\FlashPlayer|/repo_av/extr
as/Adobe/flash_player/11.1.102.55/flash.exe|flash.exe x -y -pflash-11.1.102.55 -bd;del /q flash.exe;flash\flash.cmd inst
all;rd /s /Q flash
######## Mozilla Firefox ######################
#
firefox|OK|install|2011.11.18-00|8.0|reg,CurrentVersion,3|HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox|/repo_av/e
xtras/Mozilla/Firefox/8.0/firefox.exe|firefox.exe x -y -pfirefox-8.0 -bd;del /q firefox.exe;firefox\firefox.cmd install;
rd /s /Q firefox
######## a) agente ePO ###############
#
agente_ePO|OK|update|2011.04.18-00|4.5.0.1810|reg,Version,3|HKLM\SOFTWARE\Network Associates\ePolicy Orchestrator\Applic
ation Plugins\EPOAGENT3000|/repo_av/extras/McAfee/agente_ePO/4.5.0.1810/agente_ePO.exe|agente_ePO.exe x -y -pagente_ePO-
4.5.0.1810 -bd;agente_ePO\agente_ePO.cmd install;rd /s /Q agente_ePO;del /q agente_ePO.exe
                                                                                23,38         2%
```

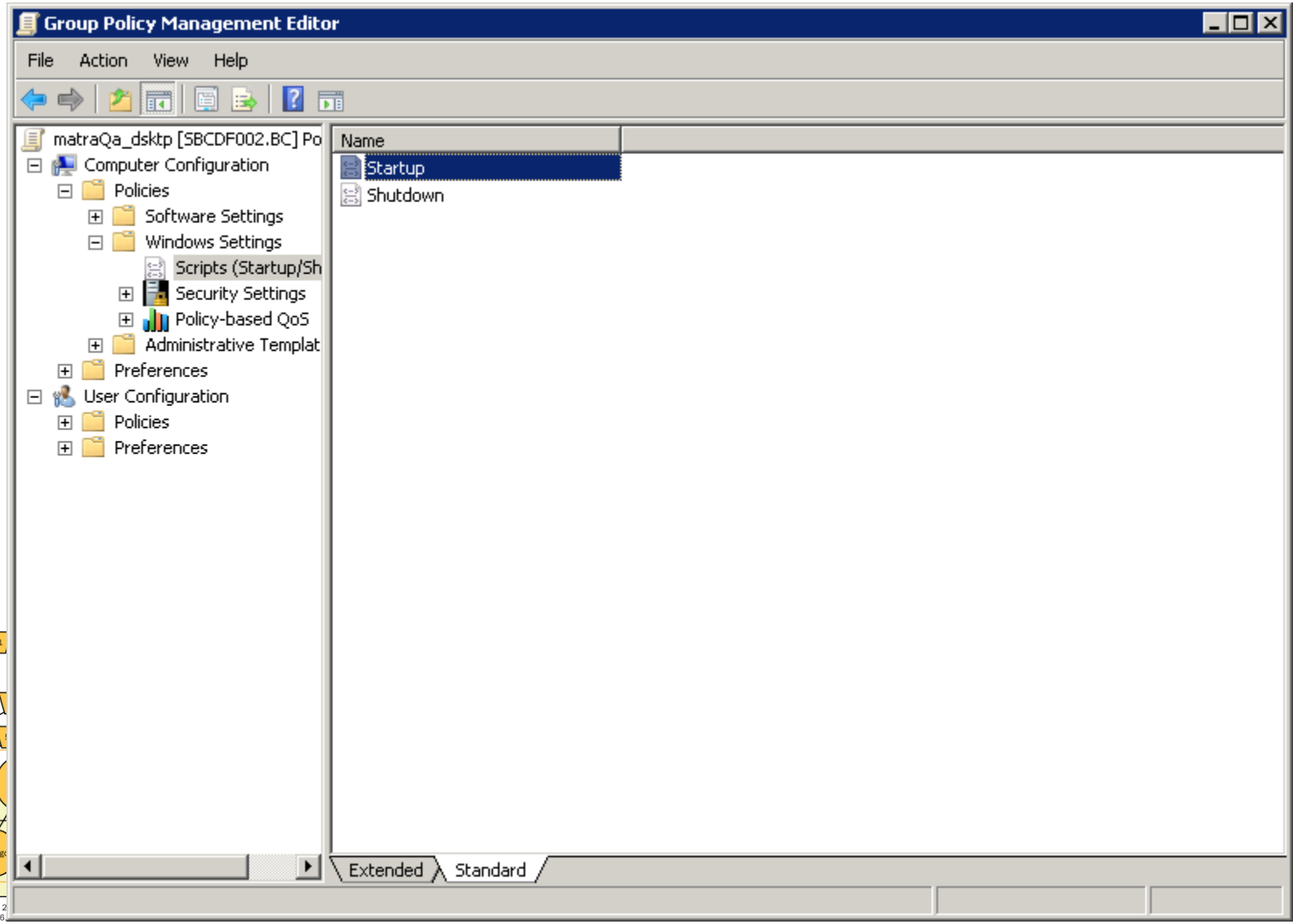
BANCO CENTRAL DO BRASIL

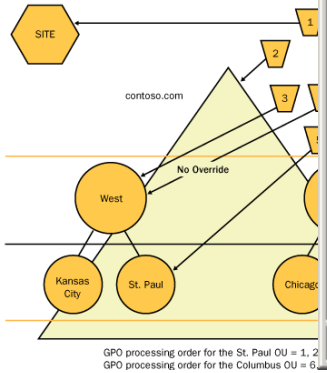
Distribuição dos Componentes



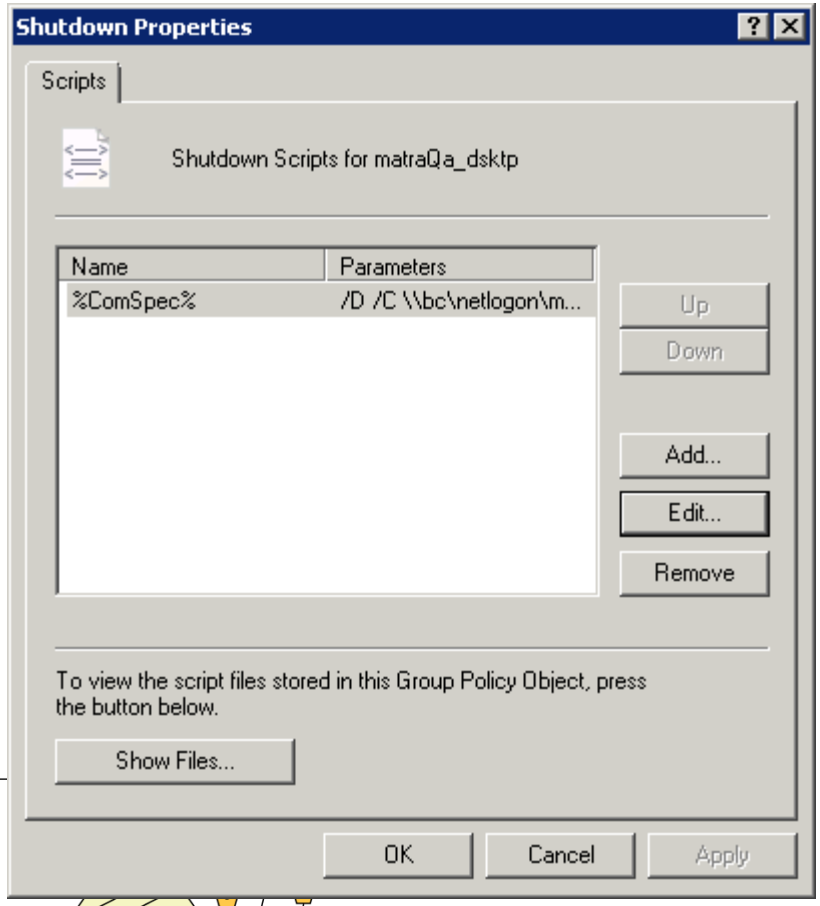


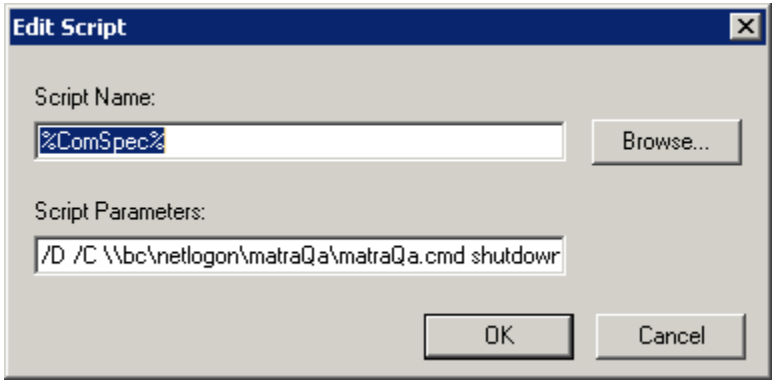
"Agente"

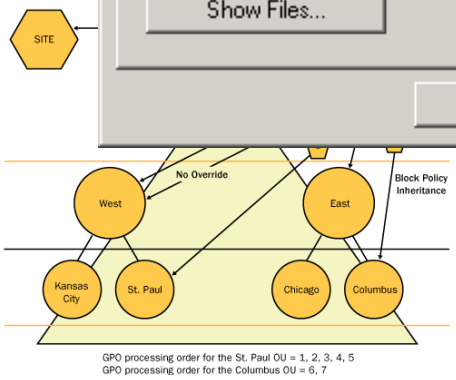

Group Policy Management Editor
File Action View Help
matraQa_dsktp [SBCDF002.BC] Po
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Sh
Security Settings
Policy-based QoS
Administrative Templat
Preferences
User Configuration
Policies
Preferences
Name
Startup
Shutdown
Extended
Standard


SITE
1
2
3
contoso.com
No Override
West
Kansas City
St. Paul
Chicago
GPO processing order for the St. Paul OU = 1, 2
GPO processing order for the Columbus OU = 6

Bootstrap





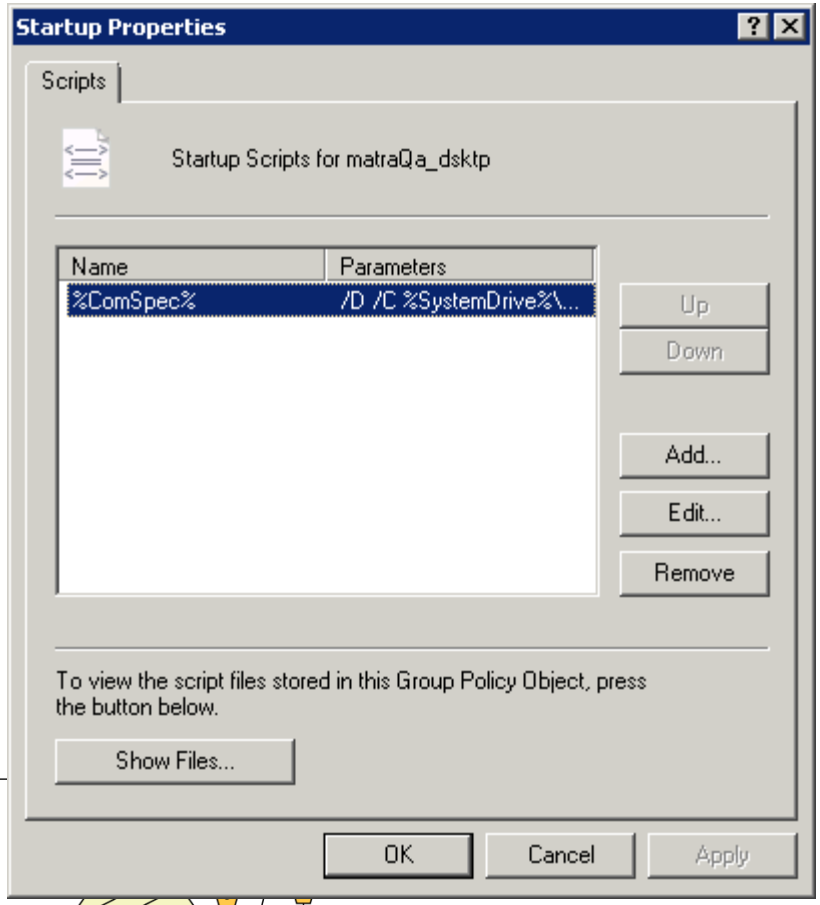


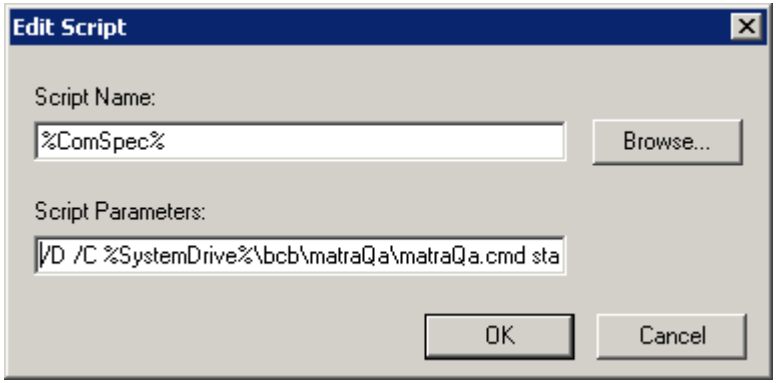
- Auto Install
- Auto Update

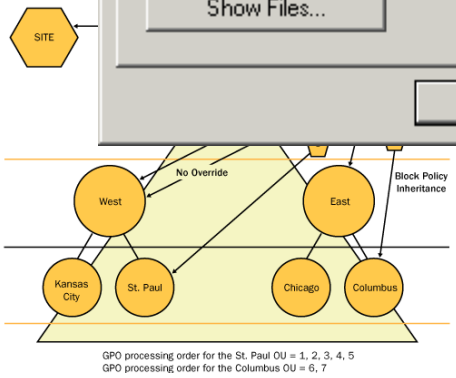
%ComSpec%
/D /C \\bc\netlogon\matraQa\matraQa.cmd shutdown >>%temp%\matraQa-%computername%.shutdown 2>&1

BANCO CENTRAL DO BRASIL

Execução



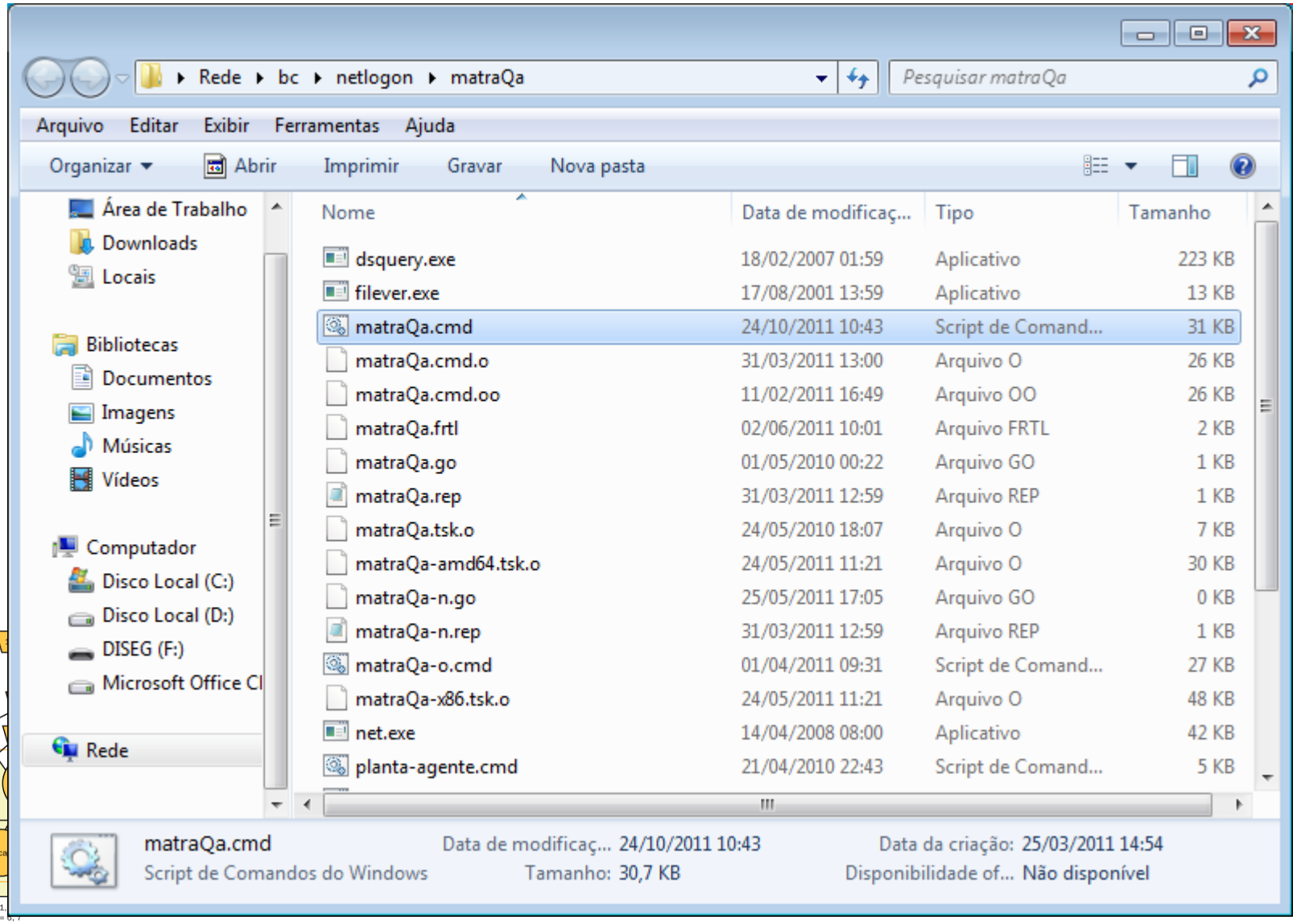


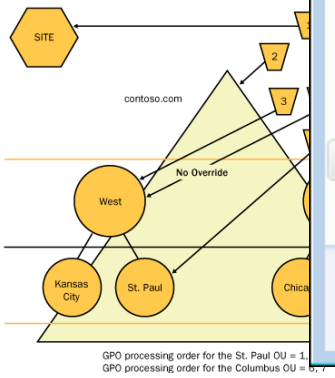


%ComSpec% /D /C %SystemDrive%\bcb\matraQa\matraQa.cmd startup >>%temp%\matraQa-%computername%.startup 2>&1

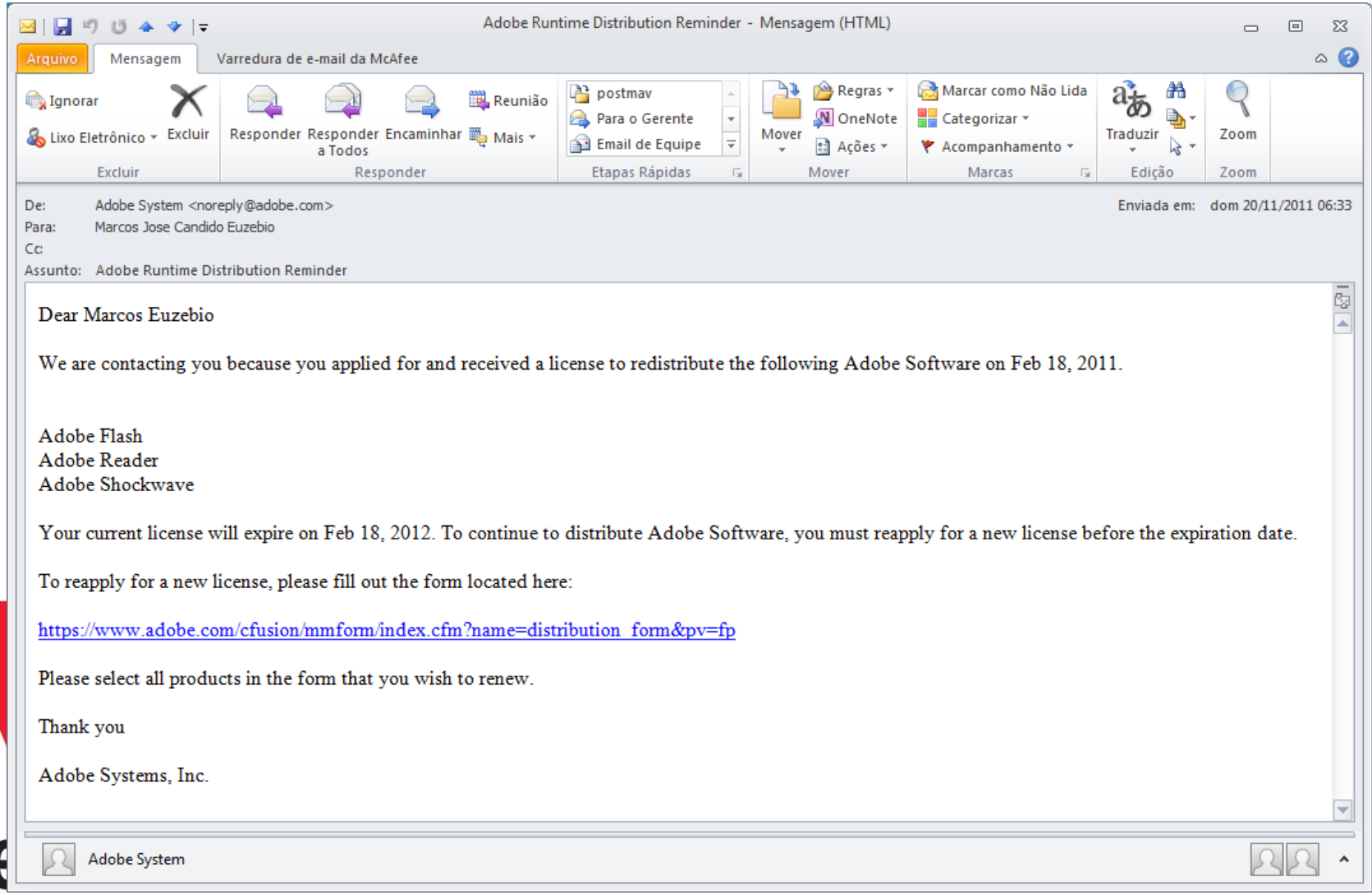
BANCO CENTRAL DO BRASIL

Bootstrap


Rede ▸ bc ▸ netlogon ▸ matraQa
Pesquisar matraQa
Arquivo Editar Exibir Ferramentas Ajuda
Organizar Abrir Imprimir Gravar Nova pasta
Área de Trabalho
Downloads
Locais
Bibliotecas
Documentos
Imagens
Músicas
Vídeos
Computador
Disco Local (C:)
Disco Local (D:)
DISEG (F:)
Microsoft Office Cl
Rede
Nome
Data de modificaç...
Tipo
Tamanho
dsquery.exe 18/02/2007 01:59 Aplicativo 223 KB
filever.exe 17/08/2001 13:59 Aplicativo 13 KB
matraQa.cmd 24/10/2011 10:43 Script de Comand... 31 KB
matraQa.cmd.o 31/03/2011 13:00 Arquivo O 26 KB
matraQa.cmd.oo 11/02/2011 16:49 Arquivo OO 26 KB
matraQa.frtl 02/06/2011 10:01 Arquivo FRTL 2 KB
matraQa.go 01/05/2010 00:22 Arquivo GO 1 KB
matraQa.rep 31/03/2011 12:59 Arquivo REP 1 KB
matraQa.tsk.o 24/05/2010 18:07 Arquivo O 7 KB
matraQa-amd64.tsk.o 24/05/2011 11:21 Arquivo O 30 KB
matraQa-n.go 25/05/2011 17:05 Arquivo GO 0 KB
matraQa-n.rep 31/03/2011 12:59 Arquivo REP 1 KB
matraQa-o.cmd 01/04/2011 09:31 Script de Comand... 27 KB
matraQa-x86.tsk.o 24/05/2011 11:21 Arquivo O 48 KB
net.exe 14/04/2008 08:00 Aplicativo 42 KB
planta-agente.cmd 21/04/2010 22:43 Script de Comand... 5 KB
matraQa.cmd
Script de Comandos do Windows
Data de modificaç... 24/10/2011 10:43
Tamanho: 30,7 KB
Data da criação: 25/03/2011 14:54
Disponibilidade of... Não disponível


SITE
contoso.com
No Override
West
Kansas City
St. Paul
GPO processing order for the St. Paul OU = 1,
GPO processing order for the Columbus OU = 8, 7

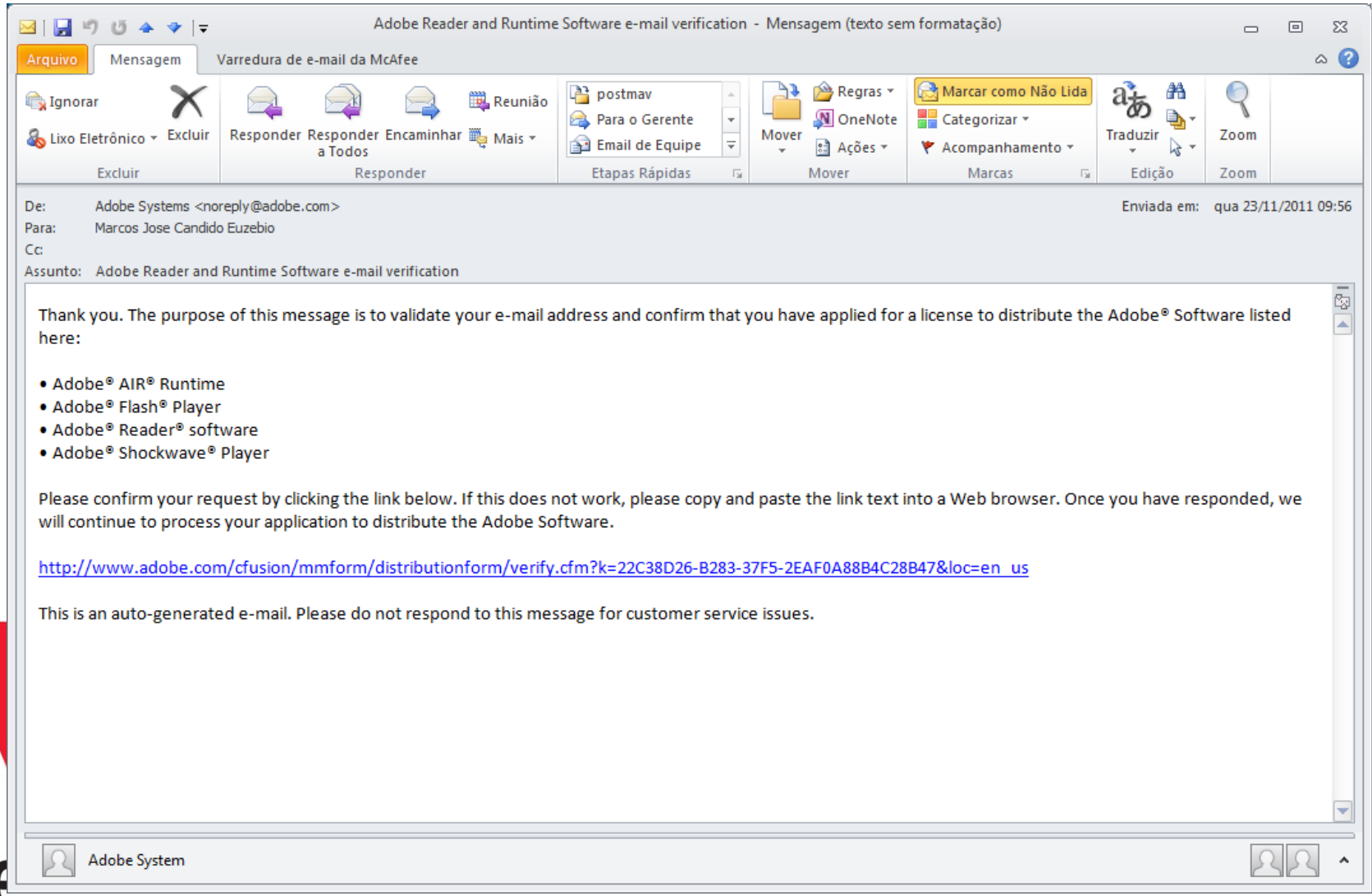
Partners



Adobe

BANCO CENTRAL DO BRASIL

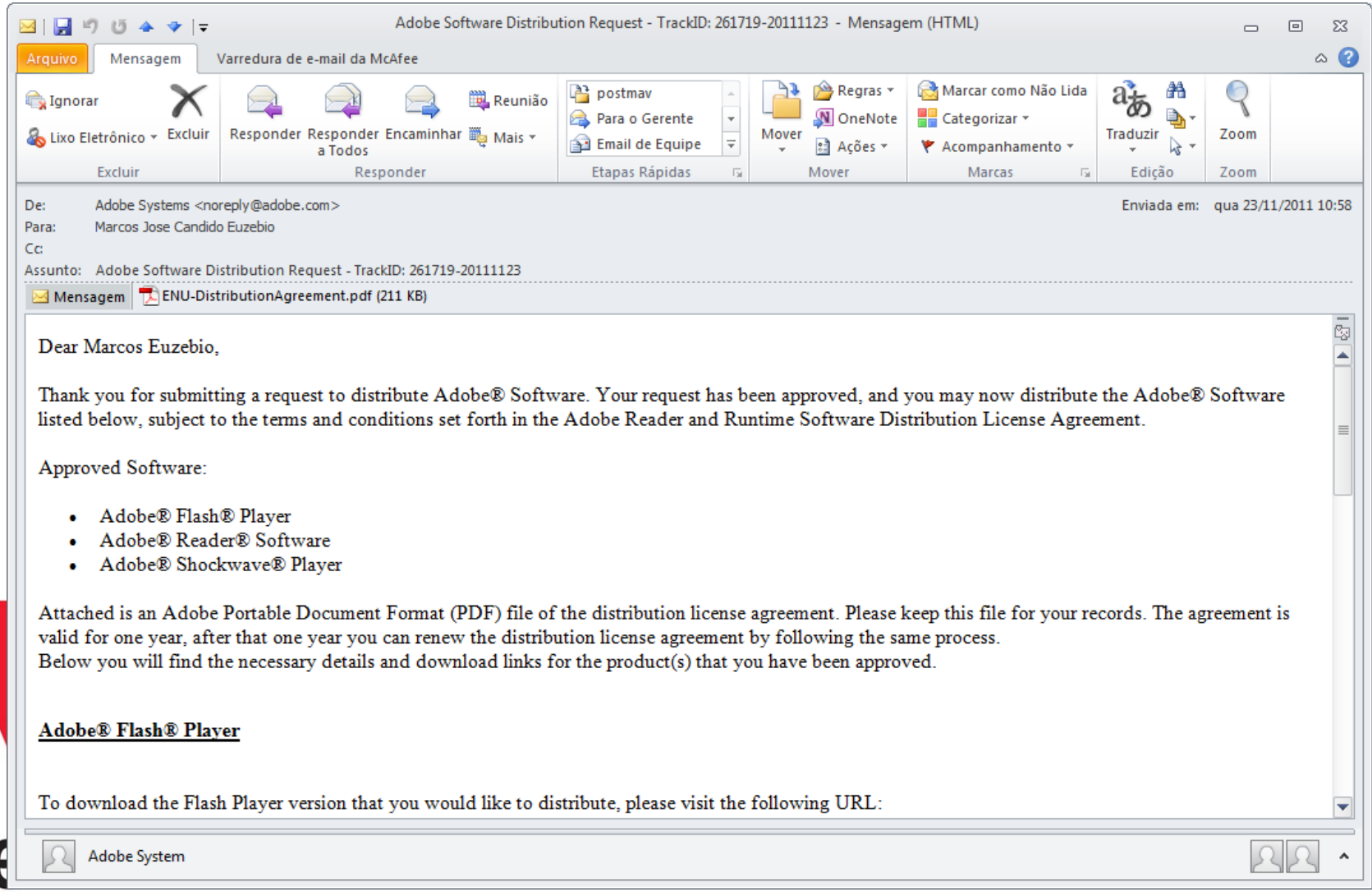
Partners



Adobe

BANCO CENTRAL DO BRASIL

Partners



Adobe

BANCO CENTRAL DO BRASIL

AM/PM

Antes

- Pilha MS OK
- Aplicações Indie
  - Sem patches
  - Vulneráveis
  - Longa janela de exposição
- Mitigações
  - Kill Bit
- Ampla superfície de ataque

Depois

- Pilha MS OK
- Aplicações Indie
  - Com patches
  - Cobertas
  - Curta janela de exposição
- Mitigações
  - Scriptáveis
- Superfície de ataque reduzida

Conclusão

matraQa:

- bom veículo para a atualização de aplicações perigosas no nosso ambiente;
- oferece mecanismos para configurar estas aplicações conforme nossas necessidades;
- blinda nosso ambiente através da instalação de workarounds;
- alternativa para distribuição de softwares com viés de segurança.

_M_étodo _a_utomatizado para o _tra_tamento _Q_ualificado de _a_tualizações

?

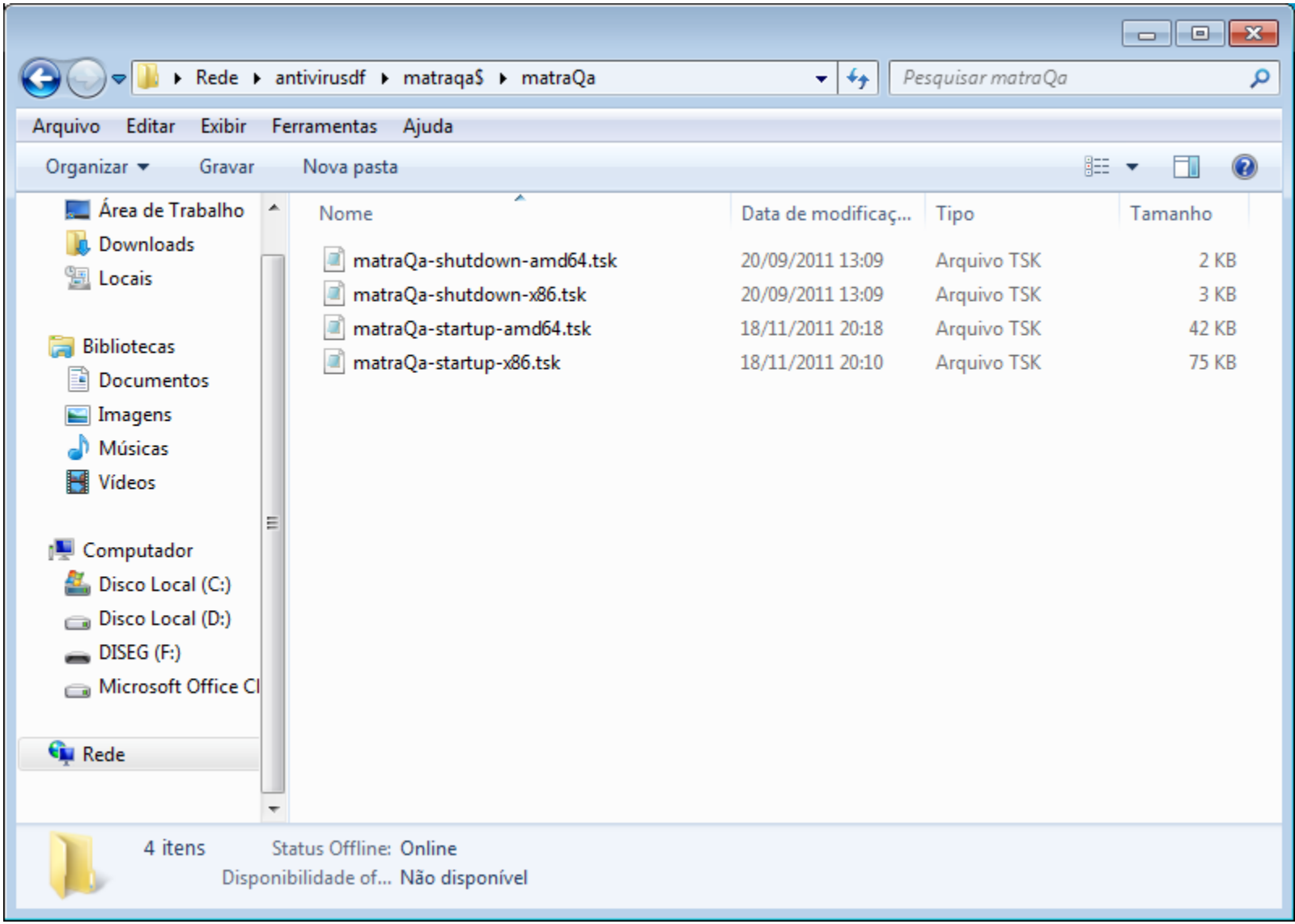
Show me the code

matraQa.cmd = (\\bc\netlogon\matraQa) - GVIM1

Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
::::::::::::::::::::::::::::::::::::::::
::
:: define repositorios
::
:sub_get_repo
   call :sub_log "get_repo: repositorio: %_REPO%"

   :: ta' no "cache"?
   if NOT "%_REPO%" == "" goto :eof

   :: consulta catalogo de repositorios
   set _REPO_LIST=%_MATRAQA_HOME%\%_MATRAQA_BASE%.rep

   :: get the gateway
   :: debug
   ipconfig

   set _GTW=default
   for /F "tokens=2 delims=:" %%i in ('ipconfig ^| find "Gateway"') do set _GTW=%%i

   :: gtw esta na tabela?
   for /F "tokens=2 delims=:" %%r in ('type "%_REPO_LIST%" ^| find "%_GTW%"') do set _REPO=%%r

   if NOT "%_REPO%" == "" goto :eof

   :: tem que descascar mais..., pega os tres primeiros octetos
   for /F "tokens=1-3 delims=." %%o in ("%_GTW%") do (
      set _O1=%%o
      set _O2=%%p
      set _O3=%%q
   )

   :: classe c
                                                          1029,1        97%
```

BANCO CENTRAL DO BRASIL


Rede ▸ antivirusdf ▸ matraqa$ ▸ matraQa
Pesquisar matraQa
Arquivo Editar Exibir Ferramentas Ajuda
Organizar Gravar Nova pasta
Área de Trabalho
Downloads
Locais
Bibliotecas
Documentos
Imagens
Músicas
Vídeos
Computador
Disco Local (C:)
Disco Local (D:)
DISEG (F:)
Microsoft Office Cl
Rede
Nome
Data de modificaç...
Tipo
Tamanho
matraQa-shutdown-amd64.tsk 20/09/2011 13:09 Arquivo TSK 2 KB
matraQa-shutdown-x86.tsk 20/09/2011 13:09 Arquivo TSK 3 KB
matraQa-startup-amd64.tsk 18/11/2011 20:18 Arquivo TSK 42 KB
matraQa-startup-x86.tsk 18/11/2011 20:10 Arquivo TSK 75 KB
4 itens
Status Offline: Online
Disponibilidade of... Não disponível

Show me the code

matraQa.cmd = (\\bc\netlogon\matraQa) - GVIM1

Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
::::::::::::::::::::::::::::::::::::::::
::
:: tenta obter versao em lista
::
:sub_get_version_list
    call :sub_log "get_version_list: componente:%~1 mecanismo:%~2 caminho:%~3"

   if %3 == "" goto :eof

   for /f "tokens=1,* delims=;" %%c in ("%~3") do (
       call :sub_get_version %1 %2 "%%c"
   if not "" == "%_CURRENT_VERSION%" goto :eof
       call :sub_get_version_list %1 %2 "%%d"
   )

   goto :eof

::::::::::::::::::::::::::::::::::::::::
::
:: obtem versao instalada do componente a ser corrigido
::
:sub_get_version
    call :sub_log "get_version: componente:%~1 mecanismo:%~2 caminho:%~3"

   set _CURRENT_VERSION=
   :: determina mecanismo
   for /f "tokens=1-3 delims=," %%m in (%2) do (
      set _mecanismo=%%m
      set _variable=%%n
      set _token=%%o
   )

   if "%_mecanismo%" == "reg" goto use_reg
```

937,1 88%

BANCO CENTRAL DO BRASIL

Show me the code

matraQa.cmd = (\\bc\netlogon\matraQa) - GVIM1

Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
::::::::::::::::::::::::::::::::::::::::
::
:: compara versoes
::
:sub_compare_versions
    call :sub_log "compare_versions versao_atual:%1 nova_versao: %2"

   :: a priori, versao esta ok, atualizada
   set _CURRENT_VERSION_OK=OK
   if "%~2" == "" goto :eof
   if "%~1" == "" goto current_version_nok

   for /f "tokens=1,* delims=._-" %%i in ("%~1") do (
      set _cv1=%%i
      set _cv2=%%j
   )

   for /f "tokens=1,* delims=._-" %%k in ("%~2") do (
      set _nv1=%%k
      set _nv2=%%l
   )

   if /i %_cv1% LSS %_nv1% goto current_version_nok
   if /i %_cv1% GTR %_nv1% goto :eof
   :: _cv1 == _nv1

    call :sub_compare_versions "%_cv2%" "%_nv2%"

   goto :eof

   :current_version_nok
      set _CURRENT_VERSION_OK=
```

854,0-1 80%

BANCO CENTRAL DO BRASIL

Show me the code

matraQa.cmd = (\\bc\netlogon\matraQa) - GVIM1

Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
::::::::::::::::::::::::::::::::::::::::
::
:: verifica se computador esta autorizado em uma lista de grupos
::
:sub_get_authorization_list
   call :sub_log "get_authorization_list: componente:%~1 restricao:%~2"

   if "" == %2 goto :eof

   set _delims=;
   set _parsefunc=sub_get_authorization_list_or
   :: echo %2 | find ":"
   :: if errorlevel 1 goto auth_process
   set _EL=
   for /f %%e in ('echo %2 ^| find ":"') do set _EL=%%e
   if "" == "%_EL%" goto auth_process
      set _delims=:
      set _parsefunc=sub_get_authorization_list_and

   :auth_process
   for /f "tokens=1,* delims=%_delims%" %%g in ("%~2") do call :%_parsefunc% %1 "%%g" "%%h"

   goto :eof

::::::::::::::::::::::::::::::::::::::::
::
:: verifica se computador esta autorizado em uma lista de grupos - and (:)
::
:sub_get_authorization_list_and
   call :sub_log "get_authorization_list_and: componente:%~1 restricao_prim:%~2 restricao_resto:%~3"

   :: echo %2 | find ";"
   :: if errorlevel 1 goto simple_term
```

500,0-1 45%

BANCO CENTRAL DO BRASIL

Show me the code

matraQa.cmd = (\\bc\netlogon\matraQa) - GVIM1

Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
::::::::::::::::::::::::::::::::::::::::
::
:: baixa lista de arquivos
::
:sub_download_list
    call :sub_log "download_list: componente:%~1 fonte:%~2"

   if %2 == "" goto :eof

   for /f "tokens=1,* delims=;" %%f in ("%~2") do (
       call :sub_download %1 "%%f"
       call :sub_download_list %1 "%%g"
   )

   goto :eof

::::::::::::::::::::::::::::::::::::::::
::
:: baixa arquivo
::
:sub_download
    call :sub_log "download: componente:%~1 fonte:%~2"

    call :sub_get_repo

   :: goto download_%~2
   :::::::::::::::::
   :download_startup
      call :sub_create_dir

      %_WGET% -N "http://%_REPO%/%~2" -P "%_MATRAQA_AREA%" 1>>"%_MATRAQA_LOG%" 2>&1
      if ERRORLEVEL 1 set _DOWNLOAD_OK=
```

784,1 76%

BANCO CENTRAL DO BRASIL

Show me the code

matraQa.cmd = (\\bc\netlogon\matraQa) - GVIM1

Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
::::::::::::::::::::::::::::::::::::::::
::
:: executa lista de instalacao
::
:sub_install_list
    call :sub_log "install_list: componente:%~1 comandos:%~2"

   if "" == %2 goto :eof

   for /f "tokens=1,* delims=;" %%c in ("%~2") do (
       call :sub_install %1 "%%c"
       call :sub_install_list %1 "%%d"
   )

   goto :eof

::::::::::::::::::::::::::::::::::::::::
::
:: instala ou agrega 'a lista de instalacao
::
:sub_install
    call :sub_log "install: componente:%~1 comando:%~2"

   :: goto install_%~2
      :::::::::::::::
      :install_startup
         if not exist "%_MATRAQA_AREA%" goto :eof

         pushd "%_MATRAQA_AREA%"

         :: start /low /b /wait %~3 1>>%_MATRAQA_LOG% 2>&1
         :: start locks for buildin commands like del, rd, etc...
```

644,0-1 61%

BANCO CENTRAL DO BRASIL

Show me the code

matraQa.cmd = (\\bc\netlogon\matraQa) - GVIM1

Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda

```
::::::::::::::::::::::::::::::::::::::::
::
:: logs diversos
::
:sub_log
     echo %DATE% %TIME% %1 %2 >> %_MATRAQA_LOG%
  goto :eof
```

1060,1 Bot