

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

The Security Patch Treadmill



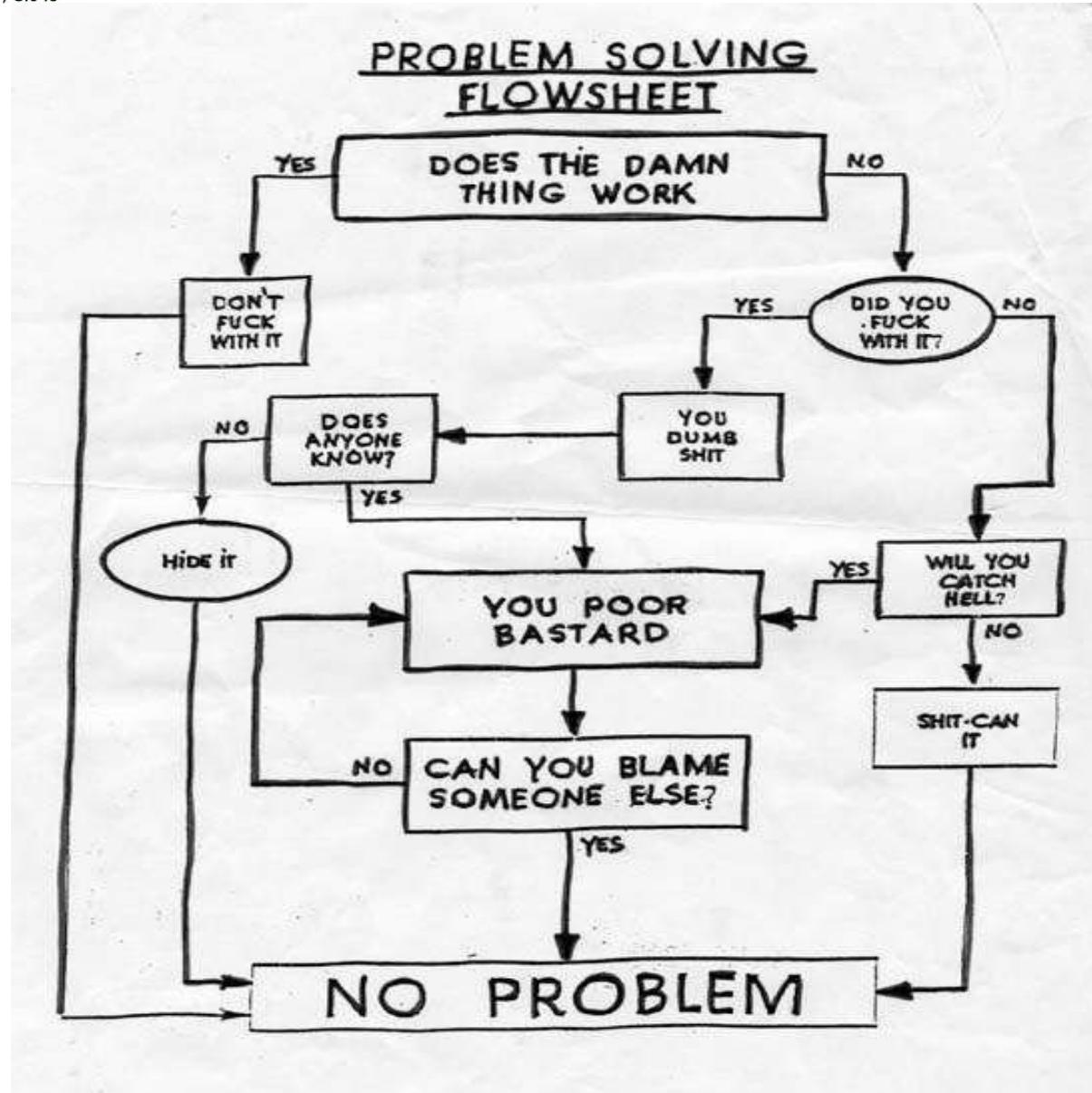
"Well, in our country," said Alice, panting a little, "you'd generally get somewhere else -- if you ran very fast for a long time, as we've been doing."

"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



Sans Top 20 Security Controls

Critical Control 10: Continuous Vulnerability Assessment and Remediation

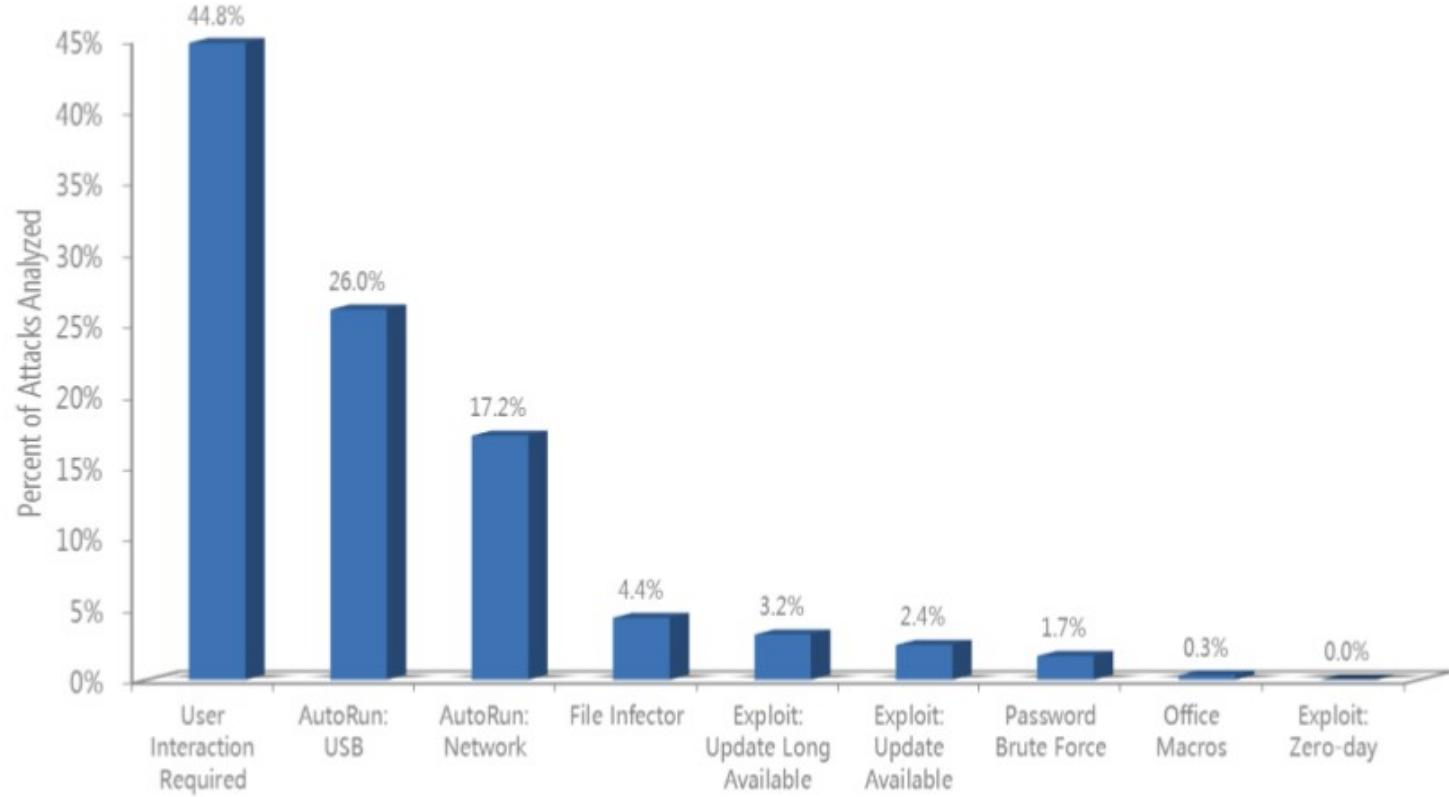


- important mechanism to detect known vulnerabilities
- if possible patch them or use additional host or network controls to prevent exploitation until a patch or update is released
- ...

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

Microsoft Security Intelligence Report 2011

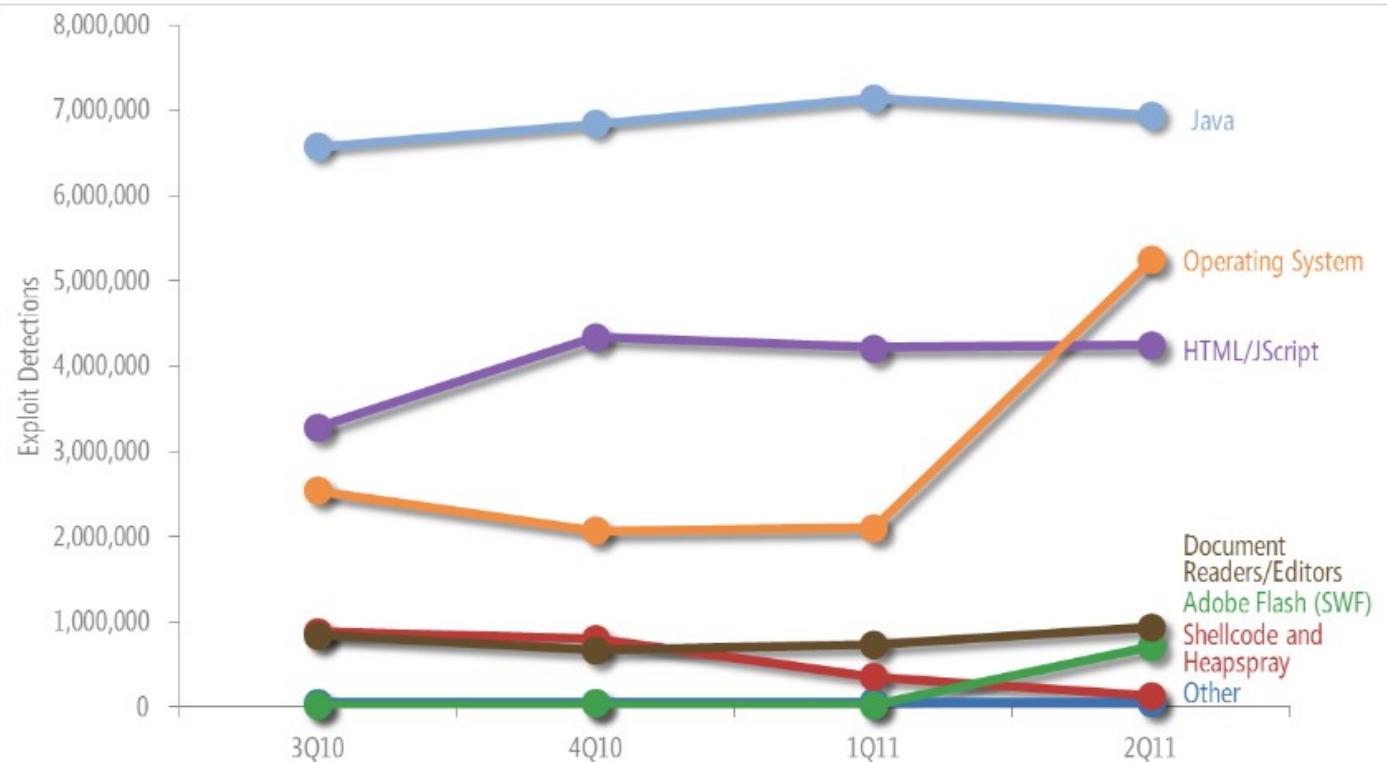
Figura 1. Malware detectado pelo MSRT no 1S11, por médias de métodos de propagação documentados



www.microsoft.com/sir

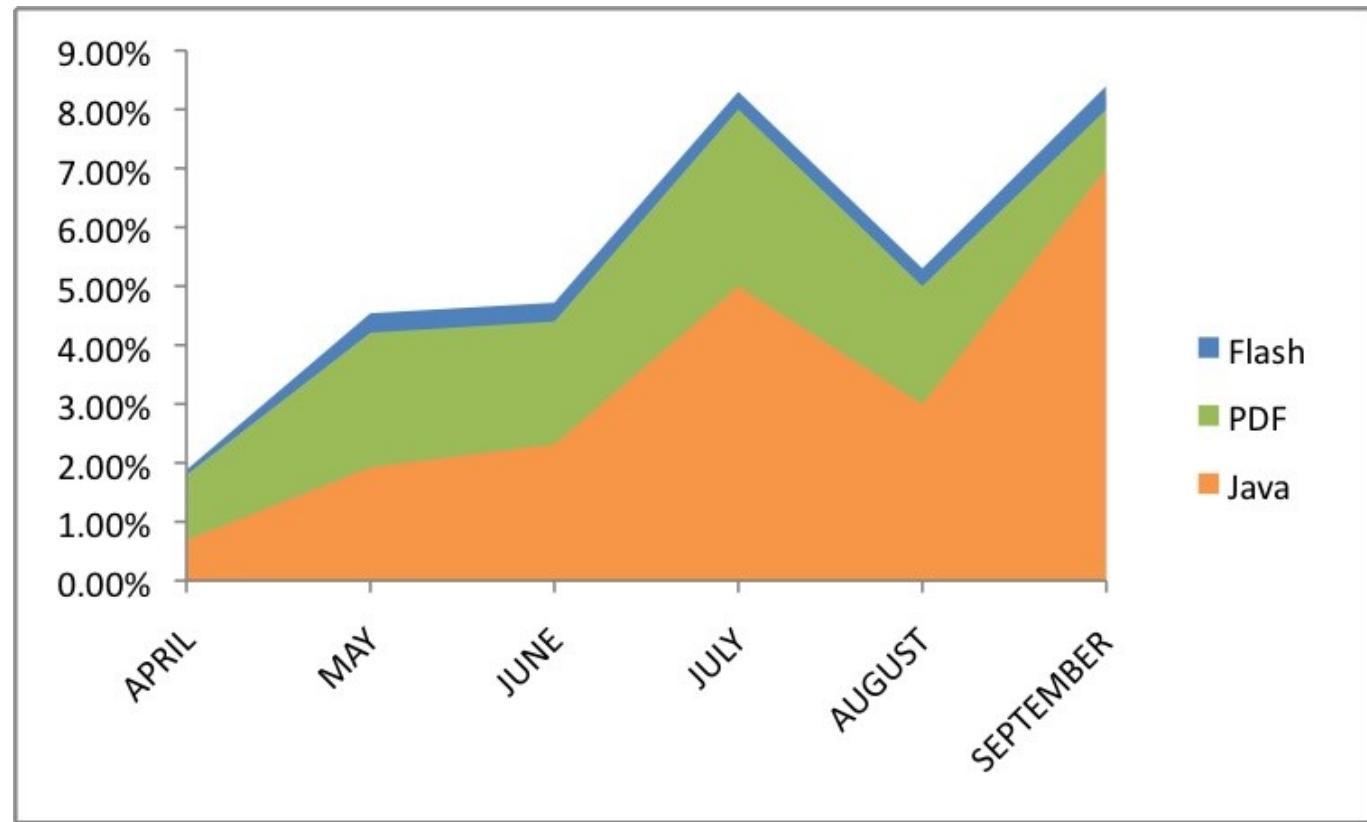
Microsoft Security Intelligence Report 2011

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



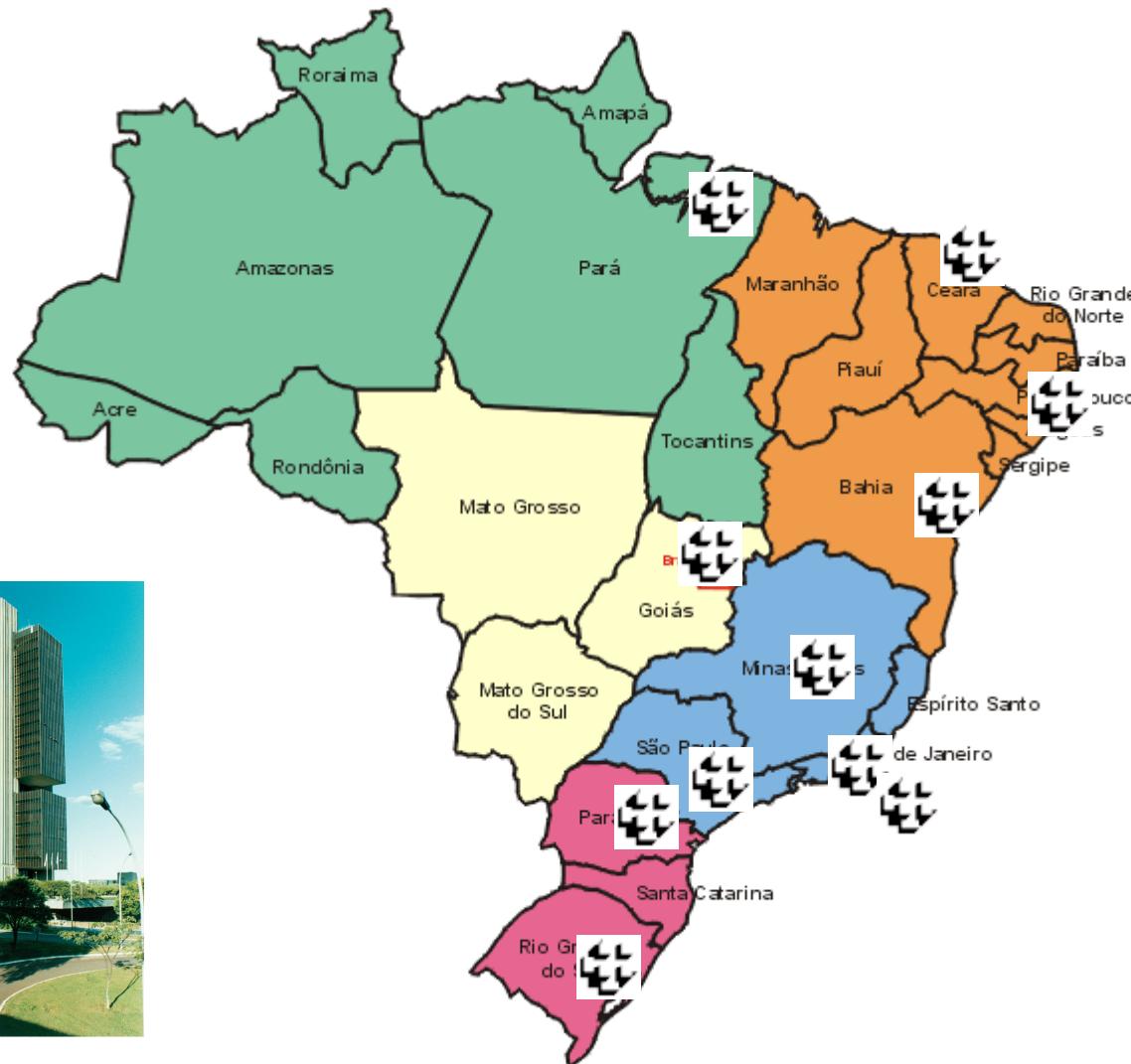
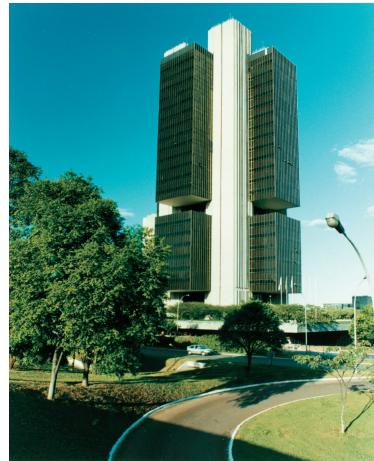
www.microsoft.com/sir

Cisco ScanSafe



[blogs.cisco.com/security/
java-exploits-another-example-of-tomorrows-threat-landscape-today-2](http://blogs.cisco.com/security/java-exploits-another-example-of-tomorrows-threat-landscape-today-2)

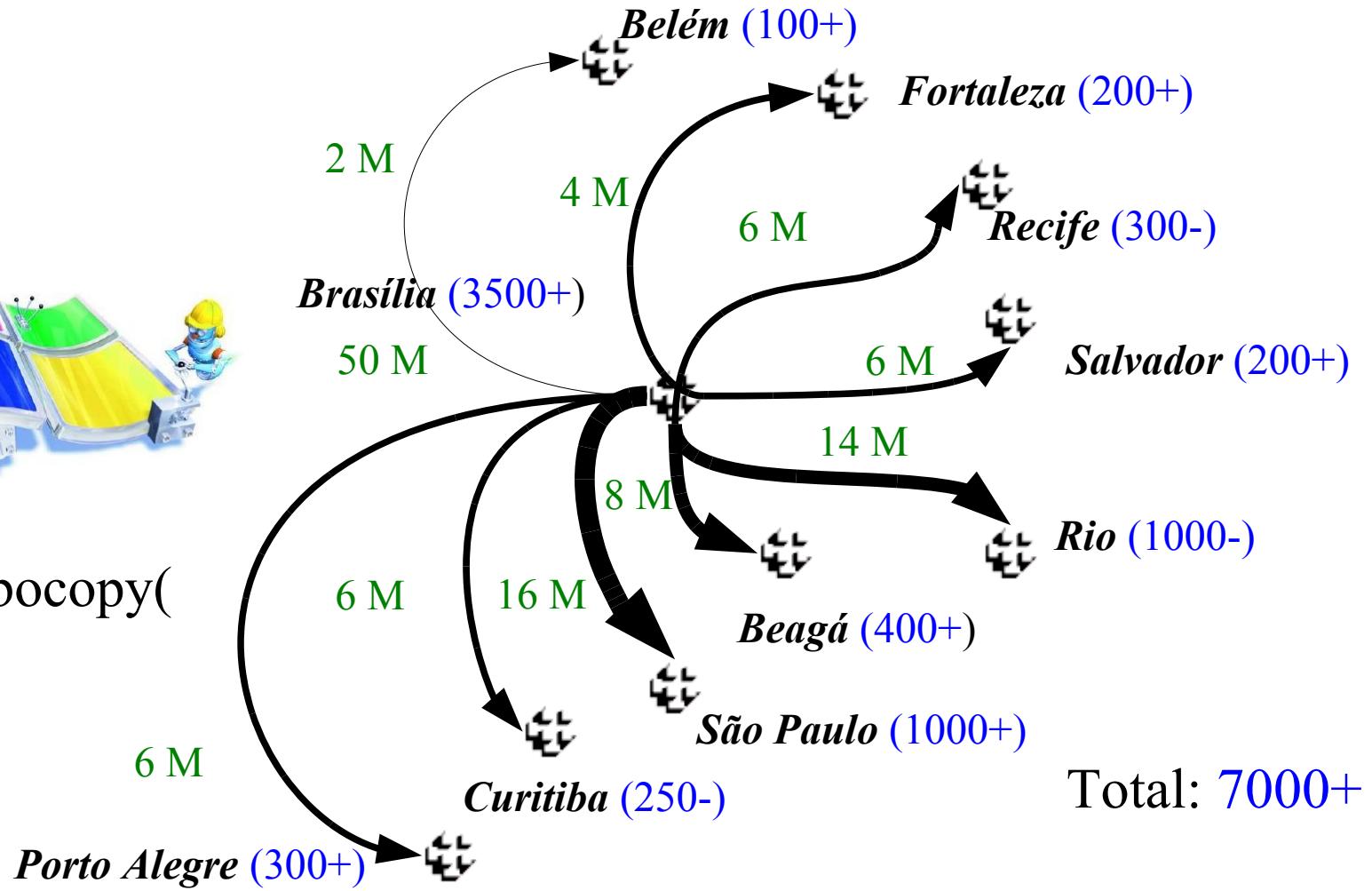
Banco Central do Brasil



Logística



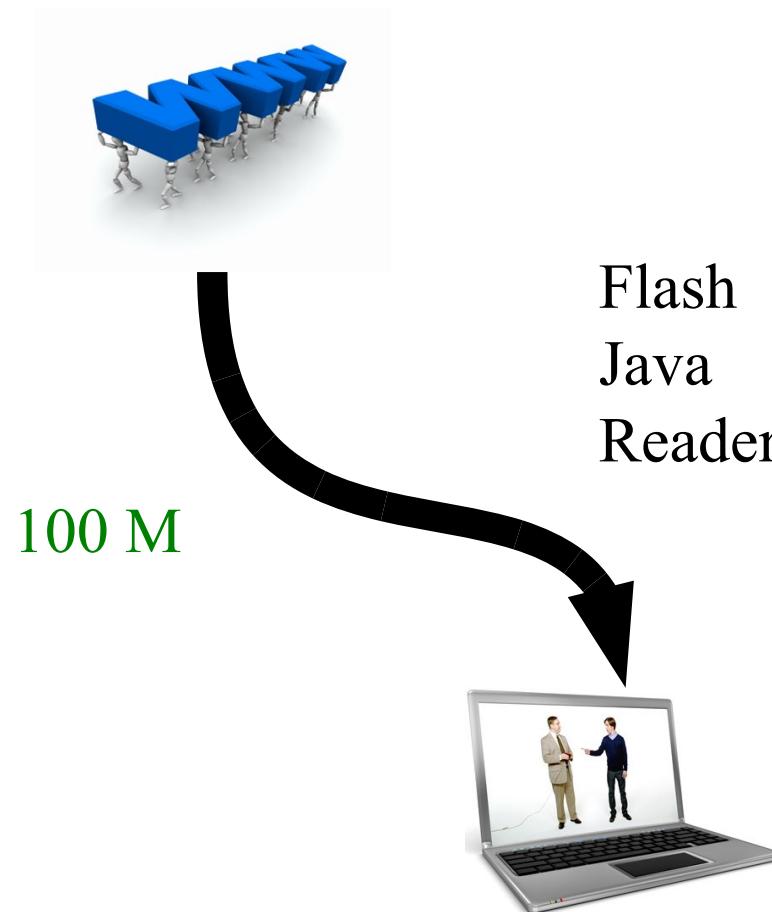
Push by)robocopy(



Estações – Download local



Pull by >wget<



Empacotamento dos Componentes



Adicionar ao arquivo

Arquivo: ire-6.exe

Formato do arquivo: 7z

Nível da compressão: Normal

Método de compressão: LZMA

Tamanho do dicionário: 16 MB

Tamanho da palavra: 32

Tamanho do bloco sólido: 2 GB

Número de threads da CPU: 2 / 4

Uso de memória para compressão: 192 MB

Uso de memória para descompressão: 18 MB

Dividir em volumes, bytes:

Parâmetros:

Modo de atualização: Adicionar e substituir arquivos

Opções

Criar arquivo SFX

Comprimir arquivos compartilhados

Encriptação

Inserir senha: ire-6u29

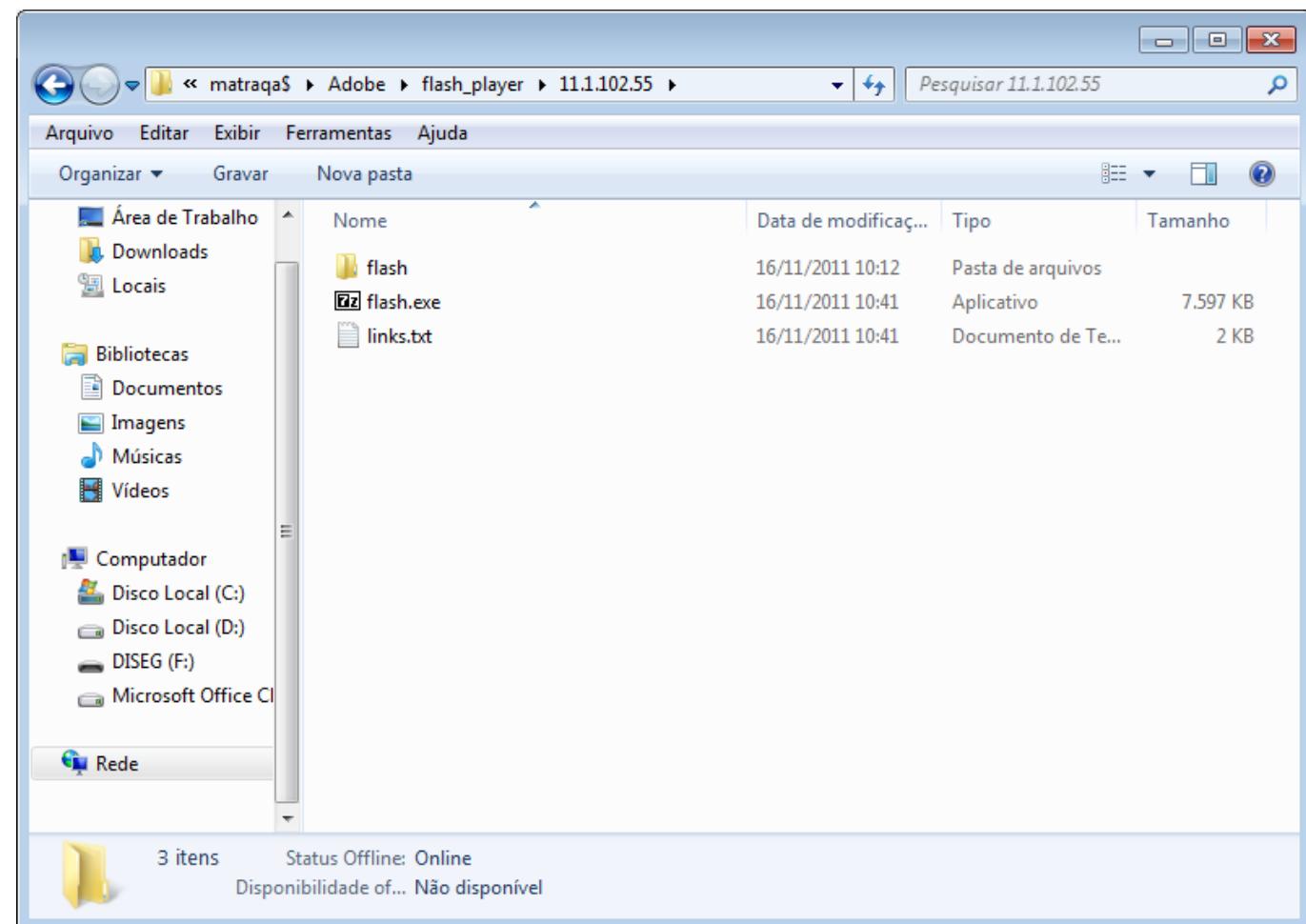
Mostrar senha

Método de encriptação: AES-256

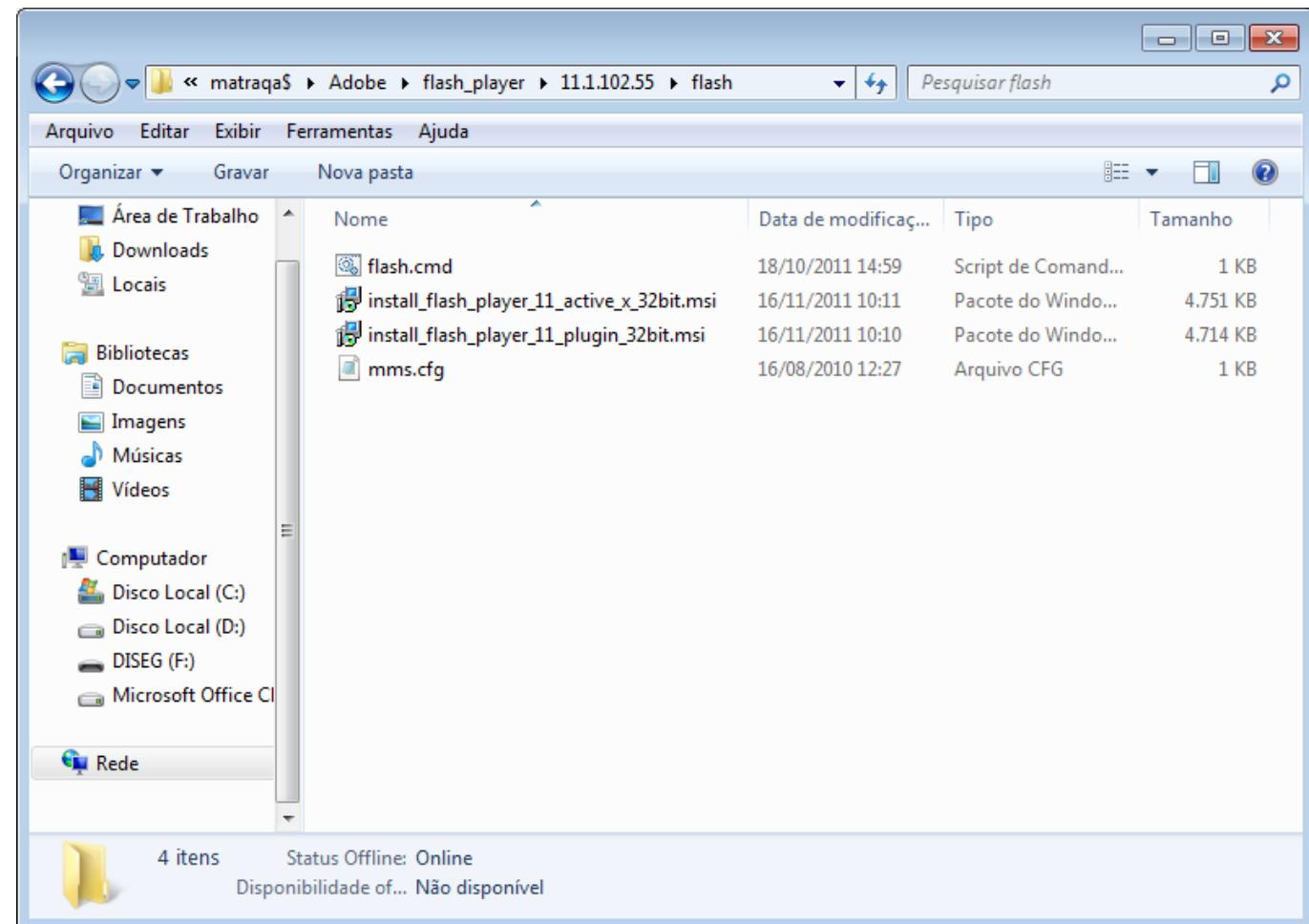
Criptografar os nomes dos arquivos

OK Cancelar Ajuda

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  
# matrac(a(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/extras/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 install;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/extras/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\Application 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%

Distribuição dos Componentes

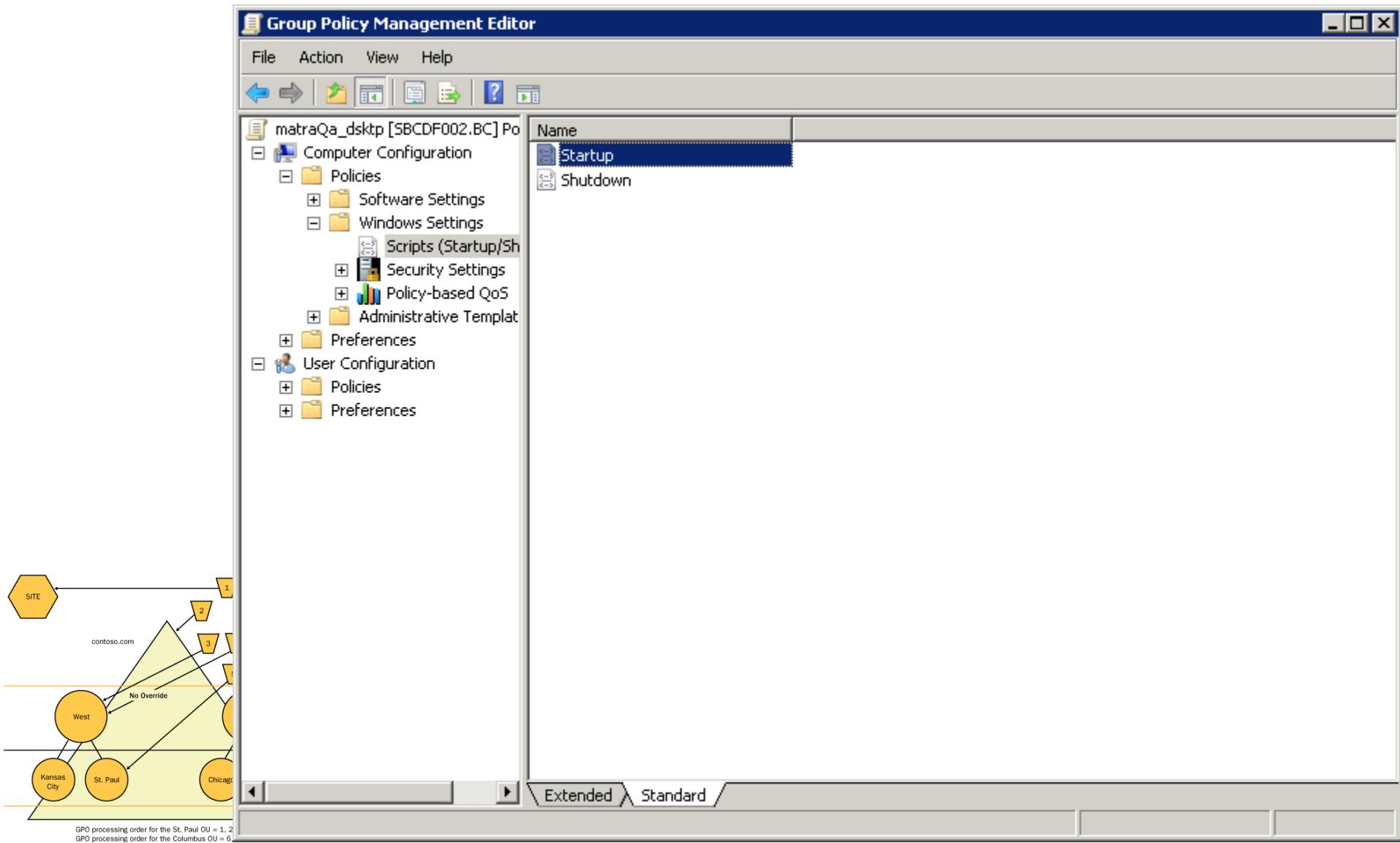
The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of registry keys under 'SYSTEM\Bacen\Diseg'. The right pane is a table showing registry entries with columns for Name, Type, and Data.

Nome	Tipo	Dados
ab (Padrão)	REG_SZ	(valor não definido)
ab ComputerName	REG_SZ	N3095401
ab LastLoggedOnUser	REG_SZ	deinf.euzebio
ab lastUpdate	REG_SZ	03/11/2011 10:19:00
ab Serial	REG_SZ	2011.10.31.00
Version	REG_DWORD	0x00000018 (24)

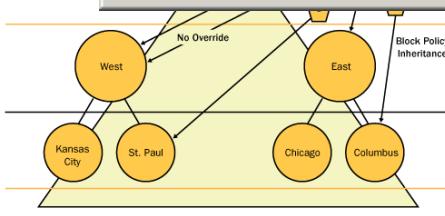
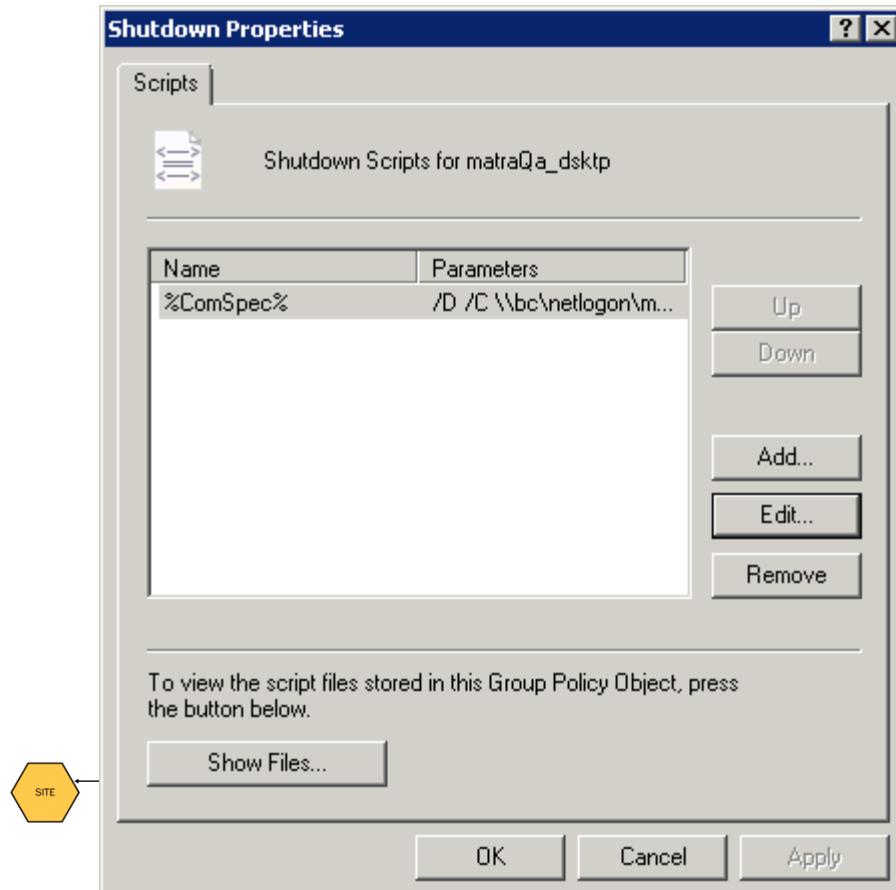
The status bar at the bottom shows the full path: Computador\HKEY_LOCAL_MACHINE\SYSTEM\Bacen\Diseg\java-jre-6



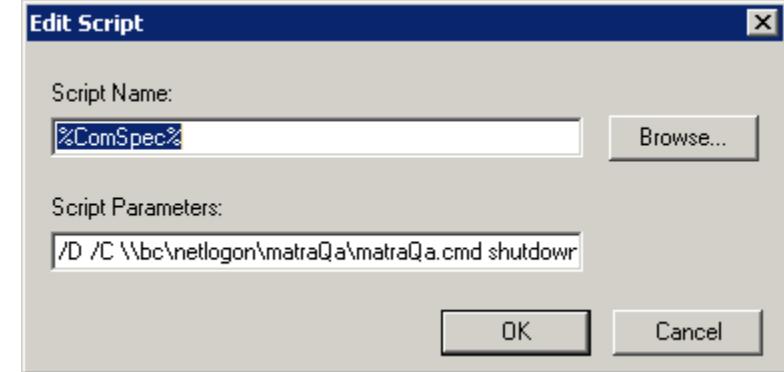
“Agente”



Bootstrap

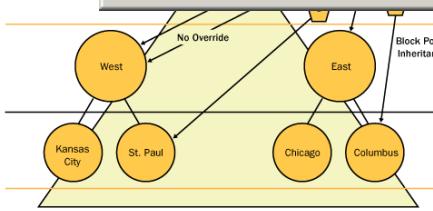
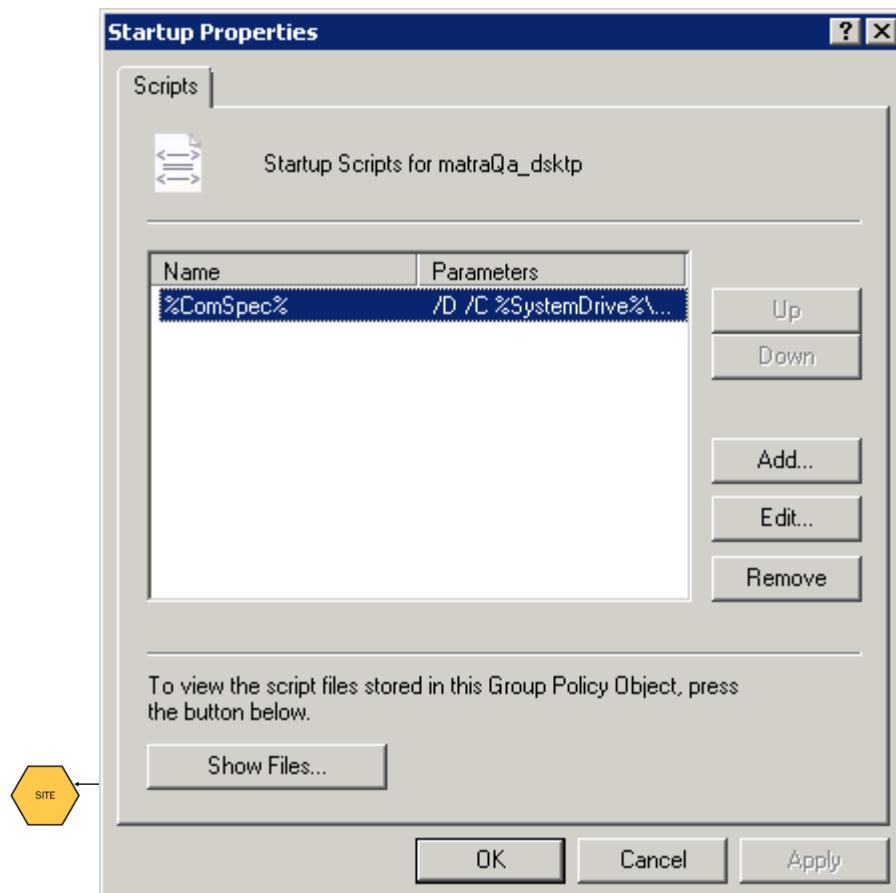


%ComSpec%
/D /C \\bc\\netlogon\\matraQa\\matraQa.cmd shutdown
>>%temp%\\matraQa-%computername%.shutdown 2>&1



- Auto Install
- Auto Update

Execução

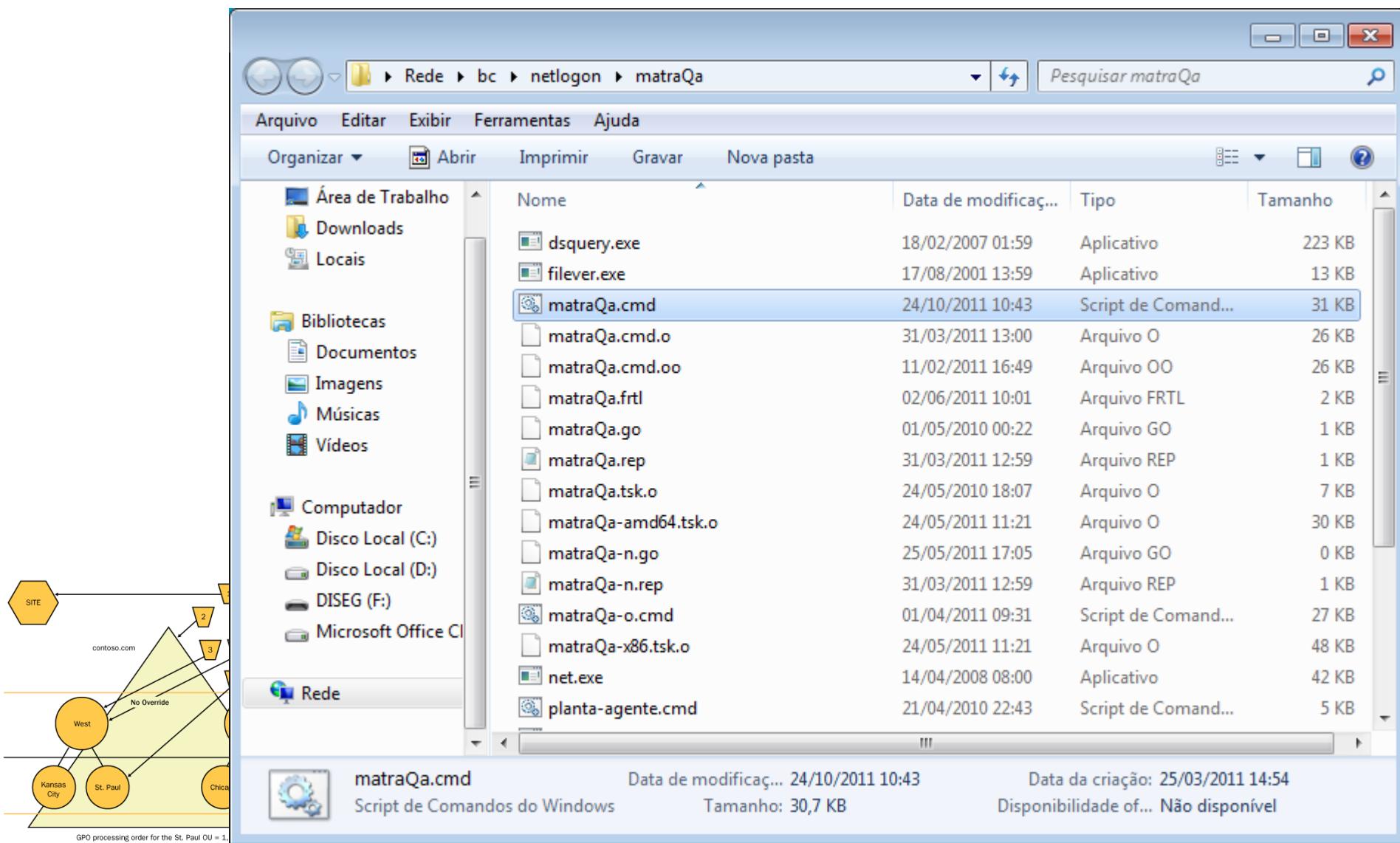


```
%ComSpec% /D /C %SystemDrive%\bcb\matraQa\matraQa.cmd startup  
>>%temp%\matraQa-%computername%.startup 2>&1
```

GPO processing order for the St. Paul OU = 1, 2, 3, 4, 5
GPO processing order for the Columbus OU = 6, 7



Bootstrap



Varredura de e-mail da McAfee

Adobe Runtime Distribution Reminder - Mensagem (HTML)

Arquivo Mensagem

Ignorar Lixo Eletrônico Excluir Excluir Responder Responder Encaminhar a Todos Reunião postmav Para o Gerente Email de Equipe Mover Regras OneNote Marcar como Não Lida Categorizar Ações Acompanhamento Marcas Traduzir Edição Zoom Zoom

De: Adobe System <noreply@adobe.com>
Para: Marcos Jose Candido Euzebio
Cc:
Assunto: Adobe Runtime Distribution Reminder

Enviada em: dom 20/11/2011 06:33

Dear Marcos Euzebio

We are contacting you because you applied for and received a license to redistribute the following Adobe Software on Feb 18, 2011.

Adobe Flash
Adobe Reader
Adobe Shockwave

Your current license will expire on Feb 18, 2012. To continue to distribute Adobe Software, you must reapply for a new license before the expiration date.

To reapply for a new license, please fill out the form located here:

https://www.adobe.com/cfusion/mmform/index.cfm?name=distribution_form&pv=fp

Please select all products in the form that you wish to renew.

Thank you

Adobe Systems, Inc.

Adobe System



Adobe Reader and Runtime Software e-mail verification - Mensagem (texto sem formatação)

Arquivo Mensagem Varredura de e-mail da McAfee

Ignorar X Lixo Eletrônico Excluir Responder Responder Encaminhar Reunião postmav Para o Gerente Email de Equipe Mover Regras OneNote Marcar como Não Lida Categorizar Ações Acompanhamento Traduzir Edição Zoom

Excluir Mais a Todos Etapas Rápidas Mover Marcas Zoom

De: Adobe Systems <noreply@adobe.com>
Para: Marcos Jose Candido Euzebio
Cc:
Assunto: Adobe Reader and Runtime Software e-mail verification

Enviada em: qua 23/11/2011 09:56

Thank you. The purpose of this message is to validate your e-mail address and confirm that you have applied for a license to distribute the Adobe® Software listed here:

- Adobe® AIR® Runtime
- Adobe® Flash® Player
- Adobe® Reader® software
- Adobe® Shockwave® Player

Please confirm your request by clicking the link below. If this does not work, please copy and paste the link text into a Web browser. Once you have responded, we will continue to process your application to distribute the Adobe Software.

http://www.adobe.com/cfusion/mmform/distributionform/verify.cfm?k=22C38D26-B283-37F5-2EAF0A88B4C28B47&loc=en_us

This is an auto-generated e-mail. Please do not respond to this message for customer service issues.

Adobe System

Adobe Software Distribution Request - TrackID: 261719-20111123 - Mensagem (HTML)

Arquivo Mensagem Varredura de e-mail da McAfee

Ignorar Lixo Eletrônico Excluir Excluir Responder Encaminhar a Todos Reunião postmav Para o Gerente Email de Equipe Mover Regras OneNote Marcar como Não Lida Categorizar Ações Acompanhamento Marcas Traduzir Edição Zoom Zoom

De: Adobe Systems <noreply@adobe.com>
Para: Marcos Jose Candido Euzebio
Cc:
Assunto: Adobe Software Distribution Request - TrackID: 261719-20111123

Enviada em: qua 23/11/2011 10:58

Mensagem ENU-DistributionAgreement.pdf (211 KB)

Dear Marcos Euzebio,

Thank you for submitting a request to distribute Adobe® Software. Your request has been approved, and you may now distribute the Adobe® Software listed below, subject to the terms and conditions set forth in the Adobe Reader and Runtime Software Distribution License Agreement.

Approved Software:

- Adobe® Flash® Player
- Adobe® Reader® Software
- Adobe® Shockwave® Player

Attached is an Adobe Portable Document Format (PDF) file of the distribution license agreement. Please keep this file for your records. The agreement is valid for one year, after that one year you can renew the distribution license agreement by following the same process.
Below you will find the necessary details and download links for the product(s) that you have been approved.

Adobe® Flash® Player

To download the Flash Player version that you would like to distribute, please visit the following URL:

Adobe System



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

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 _01=%%o
    set _02=%%p
    set _03=%%q
)

:: classe c
```

1829,1

97%

Arquivo Editar Exibir Ferramentas Ajuda

Organizar Gravar Nova pasta

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

Área de Trabalho

Downloads

Locais

Bibliotecas

Documentos

Imagens

Músicas

Vídeos

Computador

Disco Local (C:)

Disco Local (D:)

DISEG (F:)

Microsoft Office Cl

Rede

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  
  
:::::::::::::::::::  
::  
:: obtém versão 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%

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%

Show me the code



```
matraQa.cmd = (\bc\netlogon\matraQa) - GVIM1
Arquivo Editar Ferramentas Sintaxe Buffers Janela Ajuda
File Edit View Insert Tools Syntax Buffers Windows Help
::::::::::
::
:: 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%

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%

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%
```

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