

Grupo de Resposta a Incidentes de Segurança

Malware em Mídias Removíveis

Malware em Mídias Removíveis

- Terminologia
- In the Wild
- Como o malware atua?
- Como identificar a presença do malware?
- Como se proteger do malware?
- Demonstração

Malware em Mídias Removíveis

- O que é um Malware

Malware é um termo geral para todo tipo de código malicioso.

- O vírus e o worm

São dois dos vários tipos de malware. O vírus tem por característica infectar outros executáveis e precisa ser explicitamente executado, enquanto o worm se copia para outras partes do computador, da rede, ou outras mídias e não precisa ser explicitamente executado.

- O rootkit

Basicamente, é um conjunto de técnicas para esconder do sistema e do usuário a presença de um invasor.



Malware em Mídias Removíveis

Malware agora explora drives USB

Quarta-feira, 02 de abril de 2008 - 16h29

SÃO PAULO – Especialistas em segurança dizem que a nova onda de malware explora a popularidade dos pen drives.

Segundo a empresa de segurança ESET, fabricante do antivírus NOD32, 10,3% dos vírus e afins detectados em março continham informações sobre programas que devem rodar automaticamente quando um dispositivo removível é conectado ao PC.

Para a empresa, as contaminações via e-mail se tornaram tão comuns que as pessoas esquecem outras formas de invasão, ligadas diretamente ao desktop. No entanto, desde meados do ano passado, começaram a surgir ameaças concebidas para rodar em dispositivos como pen drives e HDs removíveis, conectáveis pela porta USB.

Carlos Machado, da INFO

Fonte: <http://info.abril.com.br/aberto/infonews/042008/02042008-18.shl>

Malware em Mídias Removíveis

SEGUNDO A ESET (NOD32):

14-Jul-2008 :

O INF/Autorun continua na terceira posição com 4,6% do total de detecções e é um código malicioso utilizado para automaticamente executar e propor ações quando um meio externo como um CD, um DVD ou um dispositivo USB é lido por um computador.

“in the wild”

Malware em Mídias Removíveis

Mas meu PC tem anti-vírus atualizado...

“A enorme quantidade de novos Trojans colocados em circulação todos os meses indica que os cibercriminosos estão interessados em criar novas variantes com mais frequência, dificultando cada vez mais a detecção através das soluções de segurança, que não serão capazes de actualizar a tempo os ficheiros de assinaturas, deixando os utilizadores desprotegidos”

Afirma Luis Corrons. Panda Security.



Malware em Mídias Removíveis

HP distribui pendrive com malware

Quarta-feira, 09 de abril de 2008 - 16h28

SÃO PAULO - Um erro fez a HP distribuir pendrives que contêm códigos maliciosos. O malware, no entanto, só afeta servidores ProLiant.

O problema foi detectado pelo grupo australiano de segurança AusCERT.

Modelos de 256 MBe 1 GB da HP saíram de fábrica com códigos maliciosos capazes de abrir brechas de segurança nos servidores desta linha.

O malware abre brechas em servidores ProLiant rodando diversas versões do Windows, como 98, 95, XP, ME, NT e 2000, informou a AusCERT. Após ser avisada pelo grupo de segurança, a HP disponibilizou uma correção de segurança.

Segundo a fabricante dos memory keys, o problema tem caráter muito específico e a HP sequer chegou a receber queixas de clientes a respeito da falha. A empresa vai investigar como o código malicioso foi parar em alguns de seus modelos de memory key.

Felipe Zmoginski, do Plantão INFO

Fonte: <http://info.abril.com.br/aberto/infonews/042008/09042008-24.shl>



Malware em Mídias Removíveis

Funcionamento...

- Assim que a mídia é inserida, o malware é copiado para a mídia num arquivo do tipo .EXE e é criado um autorun.inf nessa mídia.
- O XP, na sua configuração padrão, não exibe esses arquivos.

Malware em Mídias Removíveis

- Autorun.inf

É um arquivo que diz para o Windows o que deve ser executado na mídia e como deve ser executado.

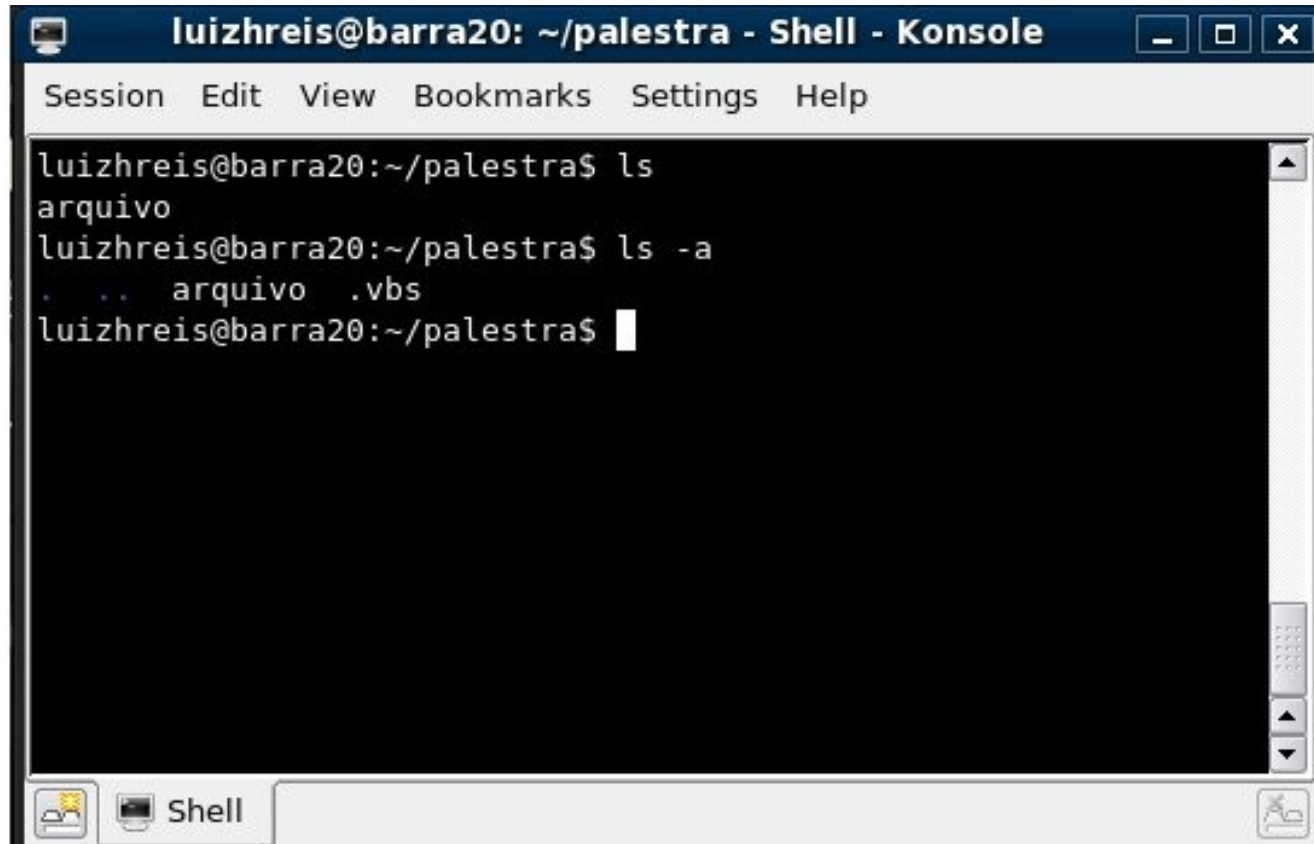


```
[Autorun]
shell\open='ò¿ª(&O)
shell\open\Command=boot.exe
shell\open\Default=1
shell\explore=xÊÔ' 'ÜAíÆ÷(&X)
shell\explore\Command=boot.exe
```

Malware em Mídias Removíveis

Funcionamento...

- Em algumas variações, o nome do arquivo do malware começa com “.”, o que leva ambientes Unix a crer que se trata de um arquivo oculto.

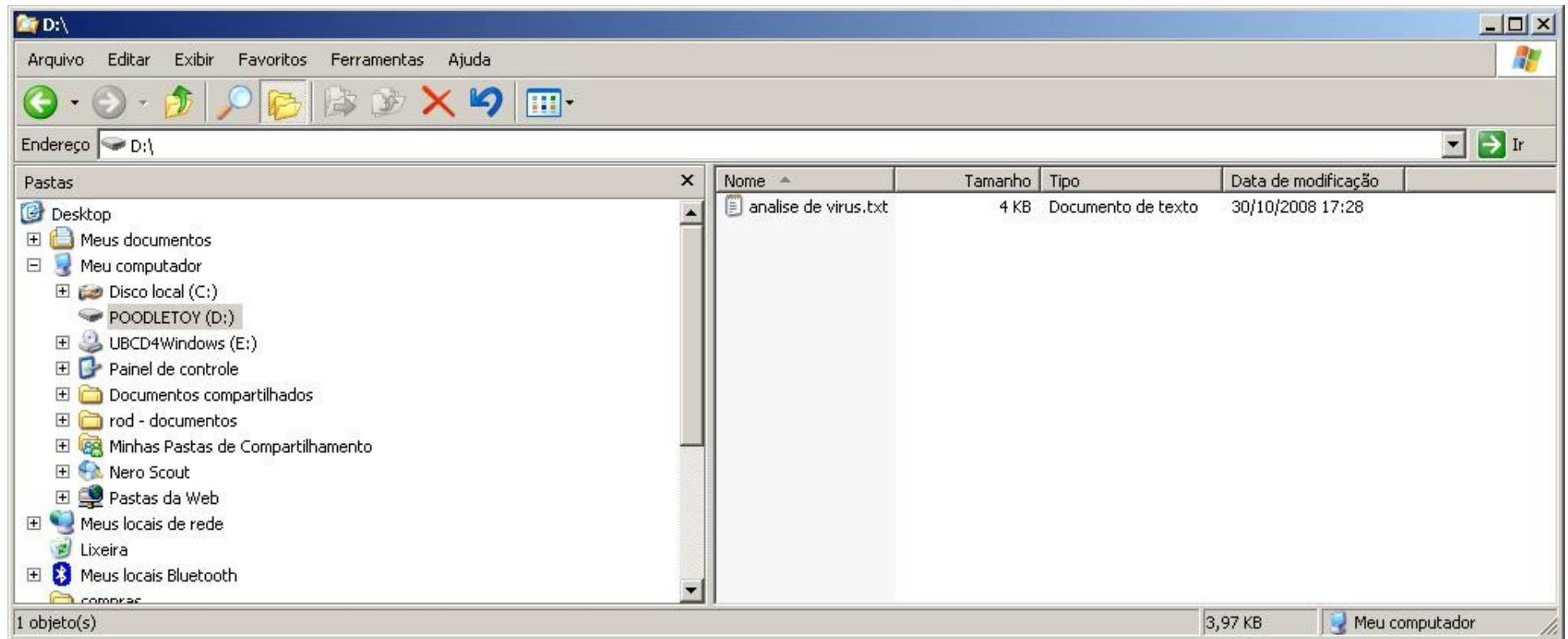


```
luizhreis@barra20: ~/palestra - Shell - Konsole
Session Edit View Bookmarks Settings Help

luizhreis@barra20:~/palestra$ ls
arquivo
luizhreis@barra20:~/palestra$ ls -a
. . arquivo .vbs
luizhreis@barra20:~/palestra$
```

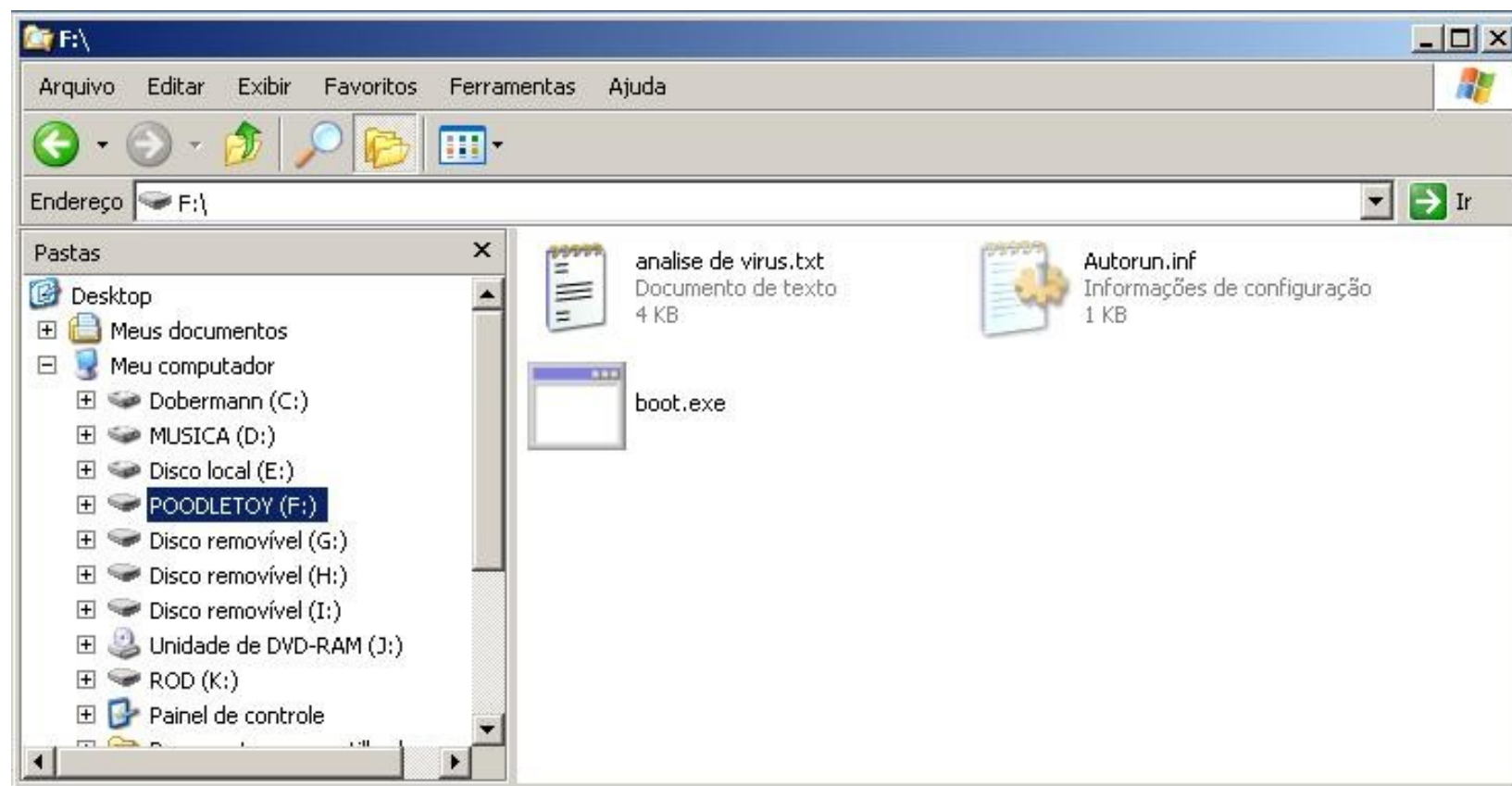
Malware em Mídias Removíveis

XP na configuração padrão



Malware em Mídias Removíveis

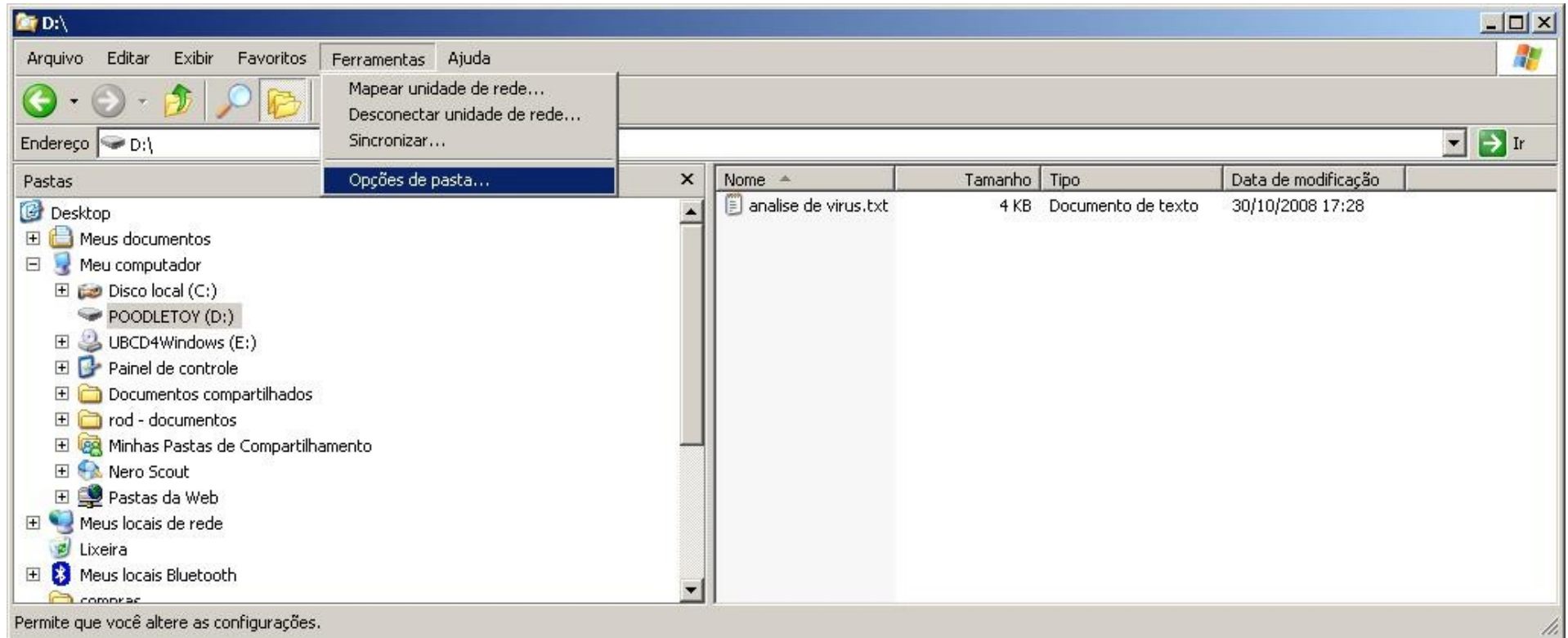
XP mostrando arquivos ocultos e de sistema



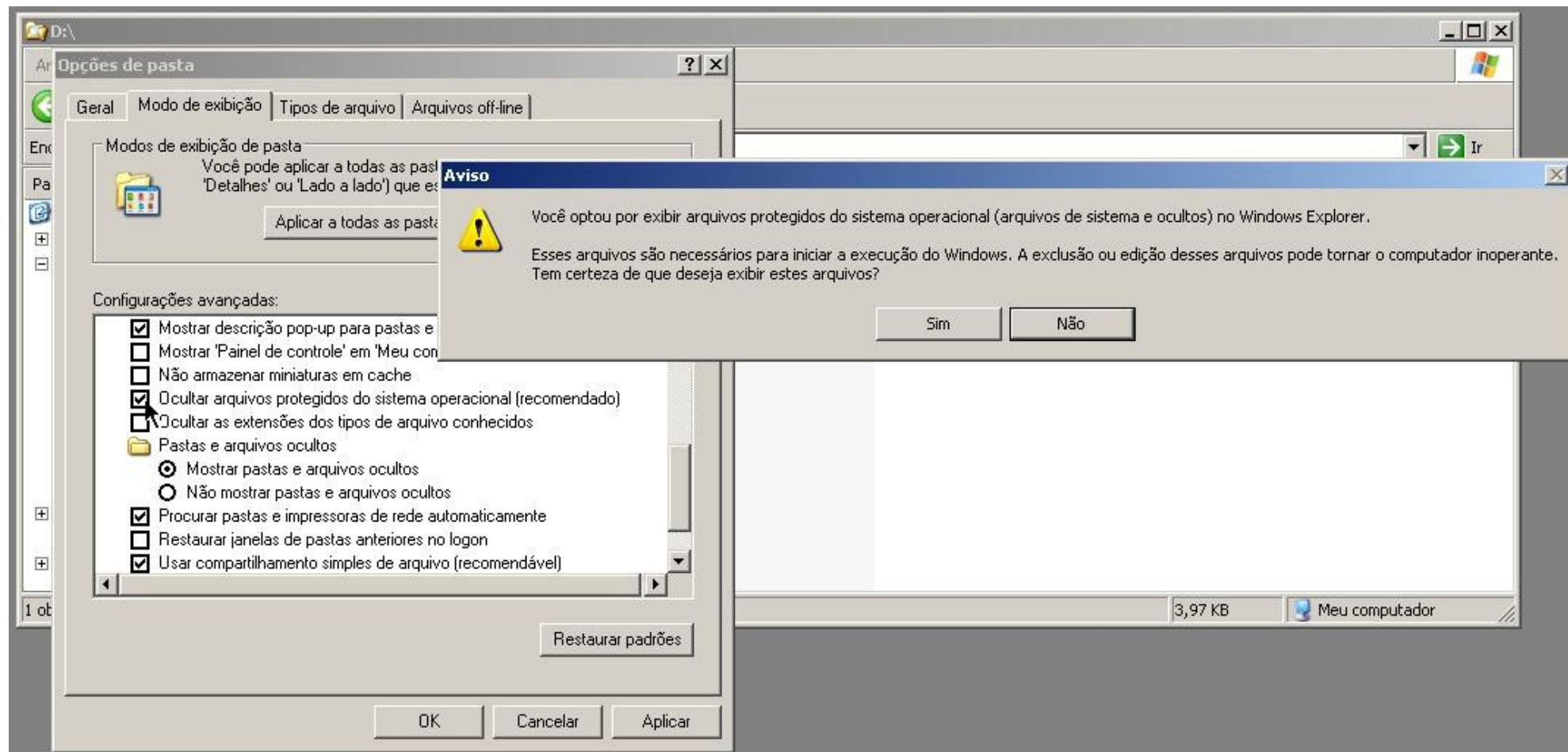
Malware em Mídias Removíveis

- Estes arquivos, normalmente, são criados em modo oculto e somente leitura e podem ser vistos se o Windows for configurado para exibir os arquivos ocultos e de sistema.
- Porém, em alguns casos, o registro do sistema é alterado e/ou monitorado para que qualquer arquivo em qualquer lugar do sistema que tenha o nome EXATO do executável do malware não seja visível nem acessível.

Malware em Mídias Removíveis



Malware em Mídias Removíveis



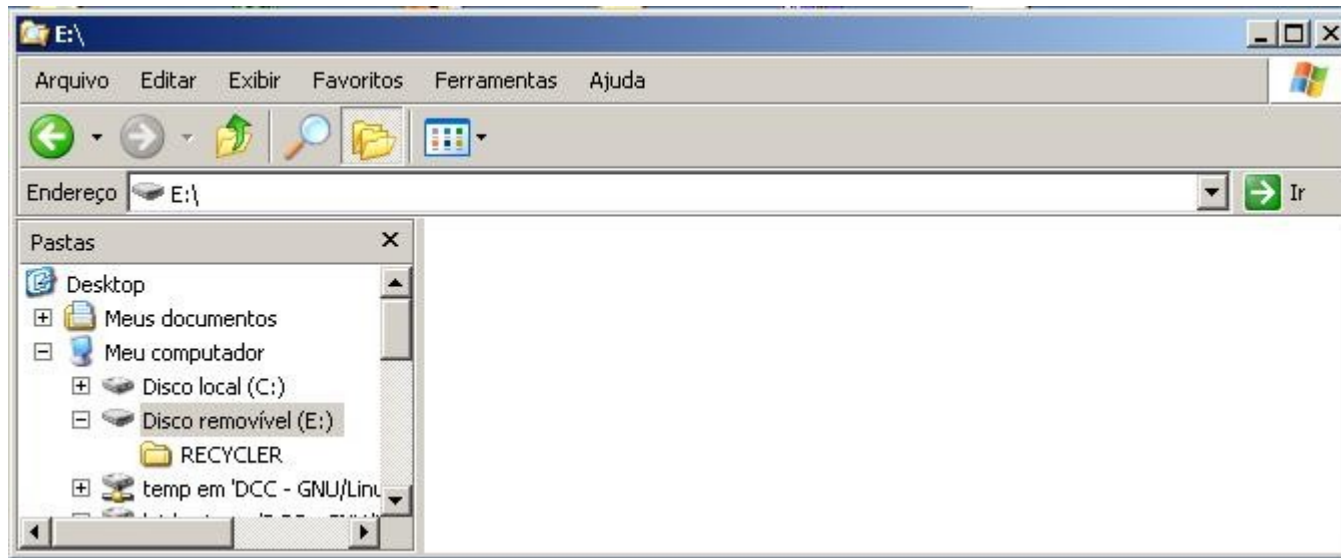
Malware em Mídias Removíveis

CURIOSIDADES...

- Se tiverem diversos malwares no mesmo ambiente, o que for executada por ultimo sobrescreve as outras.
- Entretanto, isso não significa que os anteriores foram excluídos. Os .EXE dos malwares continuam na mídia e podem ser explicitamente executados.

Obs: É possível que as variações do mesmo malware instalem variações dos mesmos arquivos.

Malware em Mídias Removíveis



Na configuração padrão do XP os malwares não ficam visíveis



Com o XP configurado para mostrar os arquivos ocultos é possível ver todos os malwares e só um autorun.inf



Malware em Mídias Removíveis

Características de uma destas pragas... BOOT.EXE

- Para o caso do BOOT.EXE, são instalados os seguintes arquivos:

%WINDIR%\linkinfo.dll – detectado como W32/Rectix

%SYSDIR%\drivers\lsDrv118.sys - detectado como Rkit/Agent

%SYSDIR%\drivers\nvmini.sys - detectado como Rkit/Agent

- Esse malware infecta outros .exe.
- Caso sejam removidos ou modificados os arquivos base do malware, citados acima, ele reinstala esses arquivos (por System Restore, por execução de outros binários infectados ou outros métodos) assim que o sistema é reiniciado.

Malware em Mídias Removíveis

- Também tenta infectar outros computadores da rede. Para isso, tenta o login como administrador e a senha segue a seguinte lista:

admin; aaa; !@# \$; asdf; asdfgh; !@# \$%; !@# \$%^; !@# \$%^&; !@# \$
%^&*; !@# \$%^&*(); !@# \$%^&*(); qwer; admin123; love; test123; owner;
mypass123; root; letmein; qwerty; abc123; password; monkey; password1;
1; 111; 123; 12345; 654321; 123456789

- Informações úteis sobre boot.exe:

MD5: 0x7DD21909643654212AF20B32741E7F88

Tamanho: 62.464 bytes

Alias: Win32.Alman.B[PCTools) / Downloader[Symantec] /

Virus.Win32.Alman.B[Kasperky Lab] / W32/Almanahe.C[McAfee] /

PE_CORELINK.C-1[Trend Micro] / W32/Alman-C[Sophos] /

Virus:Win32/Almanahe.B[Microsoft] / Virus.Win32.Delf.IRG[Ikarus]

Malware em Mídias Removíveis

- Informações úteis sobre boot.exe:

Registros criados:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_NVMINI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_NVMINI\0000
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_NVMINI\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_NVMINI
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_NVMINI\0000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_NVMINI\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\nvmini
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\nvmini\Security

Malware em Mídias Removíveis

- Informações úteis sobre boot.exe:

Hosts que requisita:

ys

beistri.net

URLs que requisita:

<http://beistri.net/files/1bk.exe>

<http://beistri.net/files/2xm.exe>

<http://beistri.net/files/3rkour.exe>

<http://info.958167.com/info.asp?action=post&HD=00CD1A40756E654749656E696C65746E&OT=3&IV=6.0&AV=0>

<http://info.958167.com/info.asp?action=update&version=0>

<http://dat.958167.com/dat.dat>

????\ll??

Malware em Mídias Removíveis

Soluções, remendos, gambiarras, etc...

Malware em Mídias Removíveis

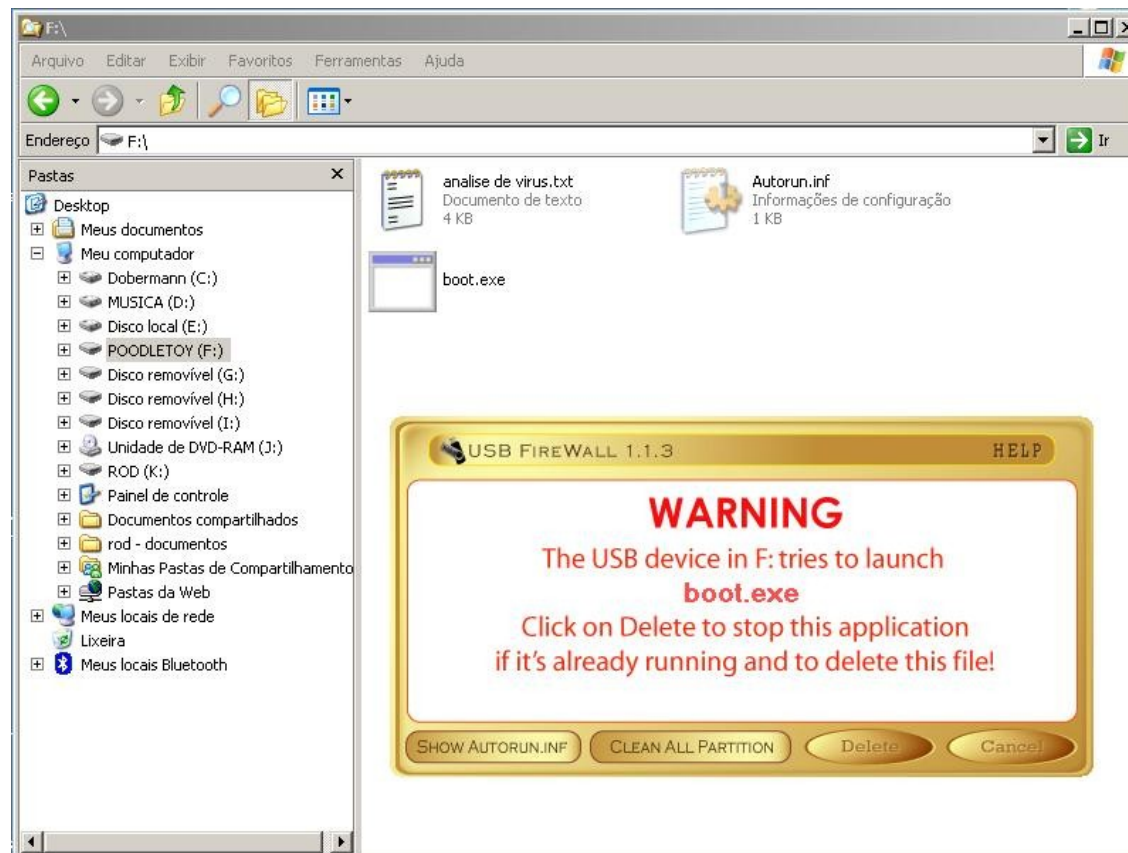
- Desativar o auto-executar não significa que o sistema está protegido. Mesmo com isso, o autorun.inf ainda pode ser executado.
- É importante ter um bom anti-vírus instalado, configurado e atualizado. Muitos são capazes de detectar outros tipos de malware.
- Criando um autorun.inf vazio na raiz da mídia em modo somente leitura pode fazer com que a substituição desse arquivo tenha que ser confirmada.



Malware em Mídias Removíveis

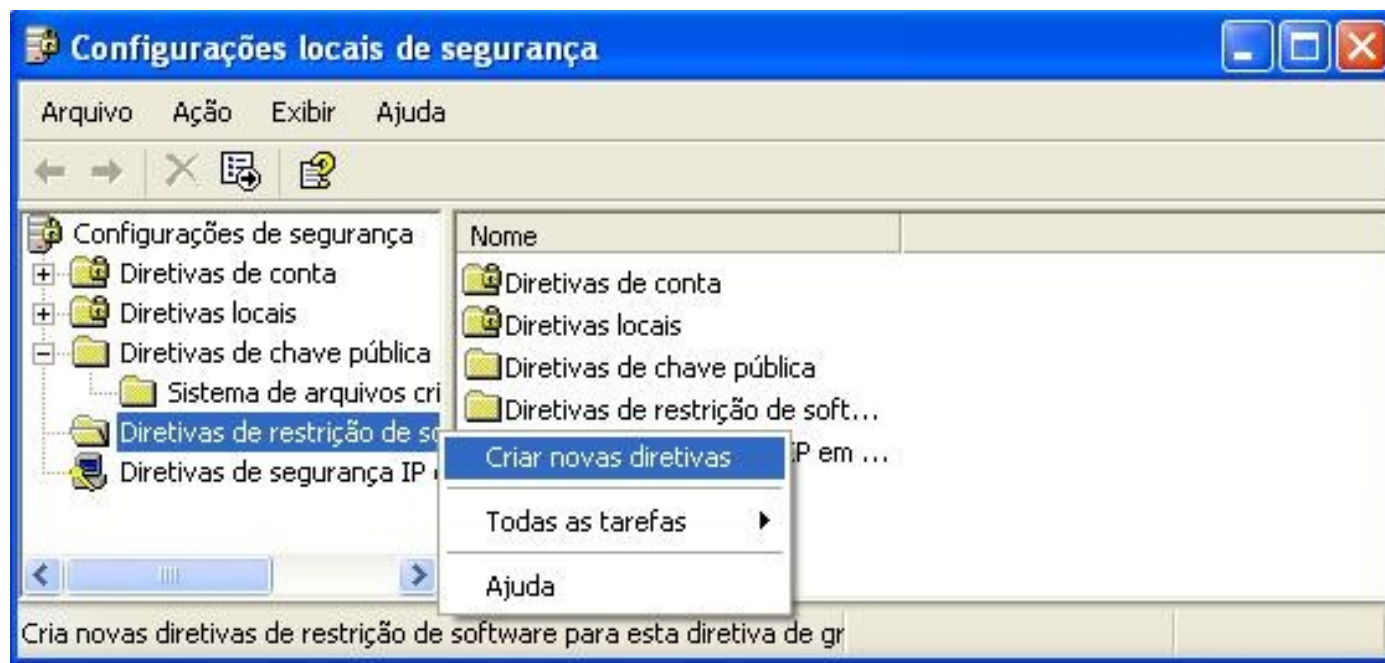
- USB Firewall:

Software que detecta e bloqueia todos os arquivos que estiverem se auto-executando da mídia. Também tem a opção de fazer a limpeza dessa mídia.



Malware em Mídias Removíveis

- Alterar as diretivas de acesso
Em Painel de Controle -> Ferramentas Administrativas ->
Diretiva de Segurança Local



Malware em Mídias Removíveis

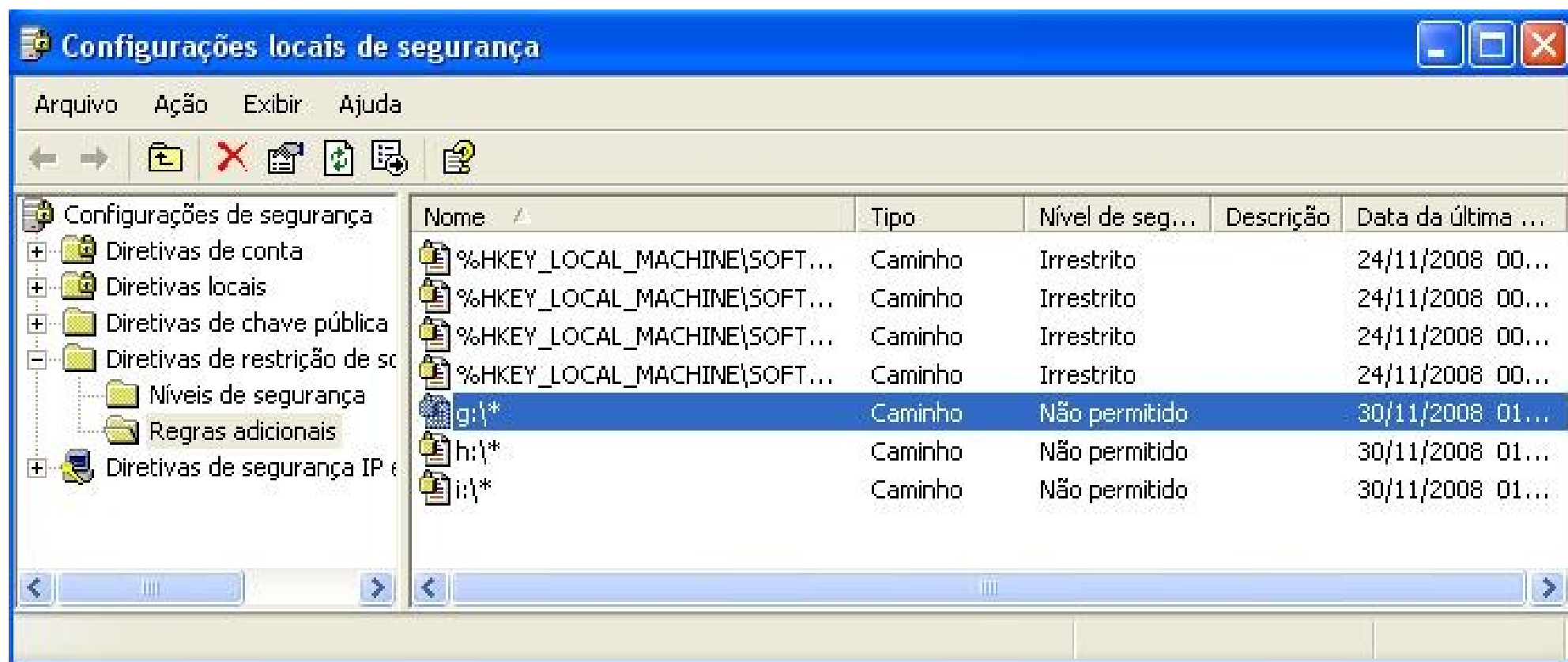
Clique com botão direito em Regras adicionais -> Nova regra de caminho

Defina uma regra para cada unidade em que uma mídia qualquer possa ser montada, da seguinte forma:

- [unidade]:* e nível de segurança “não permitido”
Isso garante que na raiz da unidade, ou em qualquer sub-diretório desta, a execução está bloqueada.
- [unidade]:*. * e nível de segurança “não permitido”
Apenas a execução na raiz da mídia está bloqueada, todas as subpastas tem execução permitida.
- [unidade]:\[caminho]* e nível de segurança “ilimitado”
Combinado com a 1ª regra, faz com que apenas o diretório especificado tenha livre execução.

Malware em Mídias Removíveis

Exemplo de regras:



Malware em Mídias Removíveis

Desta forma, os arquivos .exe .bat e .inf tem a sua execução bloqueada pelo sistema.



Malware em Mídias Removíveis

Informações extras:

- W32.Almanahe.C

http://www.symantec.com/norton/security_response/writeup.jsp?docid=2007-050416-0440-99

- WORM_SOHANAD.AG

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FSOHANAD%2EAG&VSect=P>

- <http://www.pctools.com/br/mrc/id/>
- http://www.pspl.com/virus_info/
- <http://www.f-secure.com/v-descs/>



Dúvidas?

Colaboração

Rodrigo Moscoso Teixeira Fernandez

Breno Guimarães de Oliveira

Guilherme Alves Cardoso Penha

Equipe GRIS