



## VÍRUS OPASERV

"A sua capacidade de distribuição através de redes converte-o num código nocivo especialmente perigoso para entornos corporativos".

### 1. O QUE É?

#### Família de vermes W32/OPASERV, W32/OPASOFT, I.worm.Opaserv

Desde o mês de Setembro de 2002 até a data, uma família de vermes está a ameaçar na Internet e causar confusão entre alguns criadores de antivírus, que obviamente lhe atribuíram o mesmo nome, mas com diferentes extensões. Ao parecer, até essa data, já teria chegado à sua versão M ou N.

É importante destacar que um vírus tem uma estrutura de programação definida e se o seu autor criar variantes, estas têm ligeiras modificações no seu payload ou simplesmente o nome ou a extensão do ficheiro infectador é alterada.

Caso contrário, tratar-se-ia de um novo vírus ou verme em particular.

Esta família está totalmente controlada, pois é suficiente desenvolver uma rotina heurística, específica, para a sua estrutura viral amplamente conhecida. Devido a isso mencionamos as suas variantes mais notáveis, sem nos estender em tecnicismos que à maioria dos usuários lhes resulta irrelevantes.

### 2. QUE CLASSES HÁ?

**OPASERV.E** é uma variante que ao se executar descripta o seu código e se auto-copia a **%Windows%** com os nomes de **BRASIL.PIF** ou **BRASIL.EXE**.

Para se executar, a próxima vez que se iniciar o sistema, cria as seguintes chaves de registo:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
```

```
Brasil=%Windows%\BRASIL.PIF
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
```

```
Brasil=%Windows%\BRASIL.EXE
```

O verme propaga os ficheiros infectados BRASIL.PIF ou BRASIL.EXE e os executa como um processo que não se mostra na Barra de Tarefas do Windows.

Infecta através das unidades que compartilhem C:\ buscando os equipamentos que tenham completo acesso à rede, para tanto acessa a vulnerabilidade do Share Level Password do Windows (Nível compartilhado de Senhas), o qual permite que um intruso, em forma remota, possa ter acesso aos sistemas sem a necessidade de conhecer as senhas de acesso.

A solução de segurança para esta vulnerabilidade pode ser descarregada de:

<http://www.microsoft.com/technet/security/bulletin/ms00-072.asp>

O **OPASERV.G** é um verme identificado no dia 30 de Outubro de 2002, membro da mesma família e variante do verme **Opasoft**, descoberto em Setembro de 2002, criado pelo mesmo autor, e que a partir da sua primeira versão começou a propagar sub-seguintes variantes, com diferentes nomes de ficheiros de extensões **.EXE**, **PIF**, **SCR**, etc., mas todos com a mesma estrutura viral.

Esta última tem 28KB de extensão e possui uma rotina de ingresso furtivo, conhecida como **backdoor**, a qual se propaga através de redes locais e compartilhadas usando os serviços do **NETBIOS** do MS Windows.

É um **PE (Portable Executable)** e infecta todos os sistemas operativos.

**Windows95/98/NT/Me/2000/XP**, incluindo os servidores **NT/2000**.

O verme se auto-instala no directório do Windows com o nome **scrsvr.exe** e o agrega à chave de registo para se executar na próxima vez que se iniciar o sistema:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
```

```
ScrSvr="%nombre_del_gusano%"
```

Este verme rastreia as sub-nets pela **porta 137** de Serviço do NETBIOS e busca determinados endereços IP dentro de unidades de redes e se encontra que ele ou os equipamentos têm o serviço aberto "**File and Print Sharing**", começa o seu processo de infecção, tomando controlo dos mesmos em forma remota.



O **OPASERV.F** propaga-se nos equipamentos que compartilham a unidade **C:\** com completo acesso na rede onde se produz a infecção, para o qual emprega o comando **SMB (Server Message Block Protocol)** para acessar as unidades compartilhadas.

Este verme envia informação a um site na Web, actualmente desabilitado, do qual descarga os ficheiros infectados **mane!!.dat** e **FDP!!!!.dat** e os instala no directório raiz **C:\** os mesmos que são usados para o intercâmbio de informação com o portal localizado no Brasil.

Nos equipamentos remotos, o verme cria o arquivo **GAY.INI** em **C:\** e o regrava em **%Windows%\win.ini** e para se executar da próxima vez que se inicie o sistema cria a seguinte chave de registo:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
cronos = "%Windows%\MARCO!.SCR"
```

**%Windows%** é uma variável que por definição é **C:\Windows** para o Windows 95/98/Me/XP e **C:\Winnt** para o NT/2000.

O **OPASERV.H** propaga-se nas unidades que compartilham a unidade **C:\** e se auto-copia no directório **%Windows%** com o nome de **MSTASK.EXE**, e igualmente o regrava em: **%Windows%\win.ini** e para se executar da próxima vez que se iniciar o sistema cria a seguinte chave de registo:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mstask = "%Windows%\MSTASK.EXE"
```

O **OPASERV.I** propaga-se nas unidades que compartilham a unidade **C:\** e se auto-copia no directório **%Windows%** com o nome de **MQBKUP.EXE**, e igualmente o regrava em **%Windows%\win.ini** e para se executar da próxima vez que se iniciar o sistema cria a seguinte chave de registo:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mqbkup = "%Windows%\MQBKUP.EXE"
```

O verme activa-se em datas igual ou posteriores a 24 de Dezembro de 2002 e mostra uma mensagem dentro de uma janela do MS-DOS e, a seguir, apaga o conteúdo da CMOS e do disco rígido:

```
NOTICE:
Illegal Microsoft Windows license detected!
You are in violation of the Digital Millennium Copyright Act
Your unauthorized license has been revoked
For more information, please call us at:
NOPIRACY
If you are outside the USA, please look up the correct contact information on our
website, at:
www.bsa.org
Business Software Alliance
Promoting a safe & legal online world
```

O **OPASERV.J** (alguns antivírus o nomeiam como **Opaserv L/M/N**), reportado a partir de 27 de Dezembro de 2002, propaga-se nas unidades que compartilham a unidade **C:\** e se auto-copia no directório **%Windows%** com o nome de **MSTASK.EXE**, e igualmente o regrava em **%Windows%\win.ini** e para se executar da próxima vez que se iniciar o sistema cria a seguinte chave de registo:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
Mstask = "%Windows%\MSTASK.EXE"
```

Também infecta através das unidades compartilhadas de **C:\** buscando os equipamentos que tenham completo acesso à rede, para o qual aproveita a vulnerabilidade do **Share Level Password** do Windows.

O dispositivo de segurança para esta vulnerabilidade pode ser descarregado de:

<http://www.microsoft.com/technet/security/bulletin/ms00-072.asp>

Do mesmo modo, mostra a mesma mensagem do **Opaserv.I** e reinicia o sistema.



NOTICE:  
Illegal Microsoft Windows license detected!  
You are in violation of the Digital Millennium Copyright Act  
Your unauthorized license has been revoked  
For more information, please call us at:  
1-888-NOPIRACY  
If you are outside the USA, please look up the correct contact information on our website, at:  
www.bsa.org  
Business Software Alliance  
Promoting a safe & legal online world

A única modificação da mensagem é o número telefónico.

### 3. COMO ACTUA?

O Opaserv e as suas variantes introduzem-se nos equipamentos através da Internet, empregando para isso as portas de comunicações 137 e 139 que normalmente, por definição, se encontram abertas. Se o equipamento afectado compartilha arquivos ou recursos com outros computadores, o código malicioso transmitir-se-á a estes últimos aproveitando uma vulnerabilidade do Windows 9x e Me denominada "Share Level Password". Por tal motivo, pode infectar rapidamente a totalidade dos equipamentos conectados a uma rede.

Com relação ao Opaserv e a suas variantes, Luis Corrons, director do Laboratório de Investigação do Vírus da Panda Software, também destaca o facto de que "estes vermes estão propiciando o ressurgimento de outros códigos maliciosos mais veteranos, como o W95/CIH ou o W32/Funlove. Isso se deve", explica, "a que o Opaserv se copia nos equipamentos aos que afecta. Se esses computadores se encontram poluídos por um vírus, o ficheiro que contém o Opaserv ficará também poluído e levará a infecção onde se propague".

A F-Secure Corporation anuncia a aparição in the wild do código malicioso Opaserv, aliás Opasoft, que combina características de verme de rede com capacidades troianas desenvolvidas para obter acesso remoto não autorizado dos equipamentos infectados.

O Opaserv estende-se através de unidades compartilhadas de rede e se copia como ScrSvr.exe na pasta de sistemas Windows 9x, residindo no equipamento que afecta. Além disso, com o objectivo de se executar cada vez que se reinicia o computador, gera uma entrada no registo do Windows.

O componente troiano do Opaserv foi criado para obter o controlo remoto não autorizado das máquinas que infecta. O verme tenta conectar-se a um endereço de Internet (agora inactivo),

<http://www.opasoft.com>, para descarregar versões do código nocivo actualizadas se existirem e lançar sobre os sistemas cadeias script maliciosas.

Com relação à sua acção directa sobre os discos rígidos, assinalamos que o vírus realiza uma gravação nos dois primeiros terços do disco, por isso resulta irrecuperável. Das versões as quais acessamos até o momento, constatamos que os dois primeiros terços se gravavam com códigos de maneira geométrica, o que faz que este tipo de escritura seja muito rápida.



#### **4. COMO ELIMINÁ-LO?**

O BitDefender oferece-lhe uma imprescindível ferramenta de desinfecção do vírus Win32.Worm.Opaserv.A, desenvolvida para detectar e eliminar vírus que infectaram o seu sistema. Este aplicativo é também de um valor adicional graças ao seu tamanho, já que se descarrega facilmente inclusive com uma frágil conexão de Internet. Deste modo pode ser transferido por e-mail a clientes, amigos ou sócios.

Se suspeita que o seu sistema pode estar infectado com o Win32.Worm.Opaserv.A descarregue-o e execute-o no seu computador. **AntiOpaserv.exe**

Os serviços de Suporte Técnico da Panda Software puseram gratuitamente à disposição de todos os usuários que o desejem, o aplicativo PQREMOVE que detecta e elimina eficazmente este novo verme dos computadores afectados.

**PER ANTIVÍRUS®** versão 7.8 com registo de vírus em 30 de Dezembro de 2002 detecta e elimina eficientemente este verme e todas as suas variantes existentes e por criar-se.