

Charly Kühnast

Recentemente, um colega que estava planejando uma viagem tentou navegar num site mantido por uma grande cidade da Alemanha. Talvez tenha sido mera coincidência, mas ele acabou digitando errado o endereço da URL. A página onde ele foi parar imediatamente tentou atacar uma vulnerabilidade em seu navegador. Uma solução possível – além de atualizações regulares, mas com certeza você já ouviu muito isso – seria um proxy antivírus como o HAVP [1].

Proxy antivírus

A instalação do proxy HTTP antivírus é um simples `configure && make && make install`. É necessário especificar seu antivírus preferido, que precisa já estar instalado, na etapa `configure`.

A página onde ele foi parar imediatamente tentou atacar uma vulnerabilidade em seu navegador.

Eu escolhi o *ClamAV*, o que me oferece uma linha de comando semelhante a `configure --with-scanner=libclamav`. Recomenda-se criar também um usuário e um grupo para o HAVP:

```
useradd havp; groupadd havp
```

Sob o diretório do HAVP, existe um diretório `etc`; e sob este, os subdiretórios `havg` e `init.d`. O segundo contém um script para iniciar e parar, que eu movi para `/etc/init.d`. Depois, eu digitei `cp -r havp /etc/` para copiar o diretório `havg` para o local certo. Entre outras coisas, esse diretório contém o

arquivo de configuração central, `havg.conf`. O próximo passo foi apagar a seguinte linha:

```
REMOVETHISLINE
deleteme
```

O autor do programa colocou essa armadilha para se certificar de que os usuários realmente parem para examinar cuidadosamente o arquivo de configuração.

Terapia de grupo

O passo seguinte foi configurar o HAVP para rodar sob a conta do usuário `havg`, e para que ele integrasse o grupo `havg`. As configurações para diversos antivírus localizam-se mais adiante no arquivo de configuração.

Eu escolhi usar a `libclamav`, e mantive suas configurações padrão, que posso alterar depois. Obviamente, o HAVP tem um recurso de gerar um log, e por isso eu criei um diretório `/var/log/havg` e conferi a ele permissão de escrita para o usuário `havg`:

```
mkdir /var/log/havg
chown havp /var/log/havg
```

Agora eu só preciso de um diretório onde o HAVP armazenará seus arquivos temporários para verificação de vírus. Montarei uma partição vazia nesse diretório, pois o HAVP precisa de um sistema de arquivos com suporte a travas mandatárias, e não qualquer diretório velho.

Infelizmente, não tenho uma partição extra, então terei que resolver com um disco RAM por enquanto. Essa configuração serve para fins de teste, mas não é uma boa idéia em sistemas em produção, pois um disco RAM não oferece espaço suficiente a longo prazo. Prosseguindo:

```
mkdir /var/tmp/havg
chown havp /var/tmp/havg
mkfs.ext3 /dev/ram0
mount /dev/ram0 /var/tmp/havg -o mand
```

Isso deve iniciar o HAVP, mas parece que estou sem sorte. Ao iniciar, ele me informa que eu não editei o arquivo `havg.conf`, o que obviamente não é verdade.

A resposta a esse dilema é ocultar o script de inicialização, que ainda possui `/usr/local/etc` como caminho do arquivo de configuração. Depois de solucionar isso, o HAVP sobe limpíssimo. Por padrão, ele escutará na porta 8080. Depois de configurar o *Firefox* para usar o proxy, podemos fazer o teste.

Quando tentei baixar o vírus de teste *EICAR*, o HAVP me mostrou a página de impedimento da **figura 1**. Muito bem, HAVP! ■

Mais Informações

[1] HAVP: <http://www.server-side.de>

O autor

Charly Kühnast é administrador de sistemas Unix no datacenter Moers, perto do famoso rio Reno, na Alemanha. Lá ele cuida, principalmente, dos firewalls.

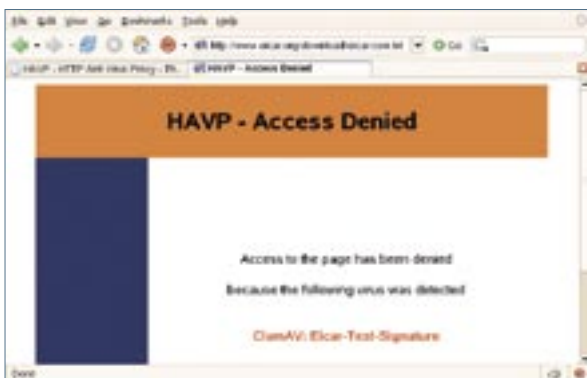


Figura 1 Se o seu navegador esbarrar num site perigoso, o HAVP vai entrar na linha de fogo bravamente e impedir a disseminação da praga.

LINUX NEW MEDIA
The Pulse of Linux

07/12/2006

LINUXPARK

Inscreva-se agora pelo site!!


Vagas limitadas!

www.linuxpark.com.br

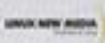


3º Seminário 2006:
**O mercado de Linux e
Software Livre no Brasil**

APROVEDOR  Itautec 

APÓIO   

PROMOÇÃO 

REALIZAÇÃO 

ORGANIZAÇÃO 