

Estudo do protocolo msnms juntamente com a implantação do msn-proxy

Levi B. Muñoz¹, André Moraes²

¹Curso Superior de Tecnologia em Redes de Computadores
FACULDADE DE TECNOLOGIA SENAC PELOTAS (FATEC PELOTAS)
Rua Gonçalves Chaves, 602 – 96.015-000 – Pelotas – RS – Brasil

{levi.munoz, chameoandre}@gmail.com

Abstract. *This article describes the protocol used by the software owner msnms windows live messenger Microsoft® for instant communication between hosts, the article attempts study whether a software-msn proxy could capture and make the appropriate control of information among the hosts trafficked, such a tool much sought after by seeking private at all times monitor the progress of employee productivity.*

Resumo. *Este artigo descreve o protocolo proprietário msnms usado pelo software windows live messenger da Microsoft® para comunicação instantânea entre hosts, o artigo procura estudar se um software de proxy-msn conseguiria capturar e fazer o controle adequado das informações trafegadas dentre os hosts, tal ferramenta muito procurada por empresas privadas que procuram a todo momento monitorar o andamento da produtividade do funcionário.*

1. Introdução

Você pode achar que precisa analisar o tráfego de uma conversa de mensagem instantânea, por diversas razões. Um cenário possível, quando um funcionário suspeito de dar informações da instituição utiliza o software do messenger. Há vários aplicativos de mensagens instantâneas, e enquanto cada uma utiliza seu próprio protocolo, existem outros que possuem certas semelhanças em comum. A concentração do conteúdo deste artigo será no tráfego do MSN Messenger Service (MSNMS).

2. MSN Messenger Service(MSNMS)

O MSNMS [msnms:11 2011] é um protocolo proprietário da Microsoft® desenvolvido para o seu comunicador instantâneo mais conhecido como Windows Live Messenger, o MSNMS usa TCP como seu protocolo de transporte. A porta TCP padrão para o tráfego MSNMS é a 1863.

3. Msn-proxy

Msn-proxy [msn proxy:11 2011] um sniffer poderoso, que suporta apenas o protocolo msnms, capturando os pacotes na porta 1863, marca-os e interpreta seus significados gravando em banco de dados, possui uma interface gráfica via browser muitíssima amigável. É normalmente utilizado por administradores de redes, em situações que empresas ou instituições públicas necessitam monitorar as mensagens trocadas através de softwares

messengers que utilizam o protocolo msnms para se comunicarem. Este tipo de solução funciona apenas na porta 1863 sendo necessário outros métodos para monitorar a porta 80 do browser caso o usuário não use o software messenger. O proxy deve ser rodado como serviço no computador que controlará o fluxo MSN. Ele é quem fará a conexão final com os servidores da rede MSN. Dessa forma, sempre que um cliente MSN tentar se conectar será interceptado pelo msn-proxy que irá controlar o acesso conforme suas configurações. A interface web roda em um servidor HTTP e é de simples instalação, sendo desenvolvida em PHP. Nela irá configurar as opções gerais de acesso MSN (protocolos, bloqueios, etc...), as opções de cada usuário (protocolos, contatos permitidos e bloqueados, etc...), e ainda poderá controlar quem está online, além é claro da opção de monitoração das conversas. É importante também dizer que é necessário um DB MySQL onde as configurações serão armazenadas.

4. Windows Live Messenger

Wlm(Windows Live Messenger) [wlm:11 2011] é um programa de comunicação instantânea pela Internet. É a nova geração do MSN Messenger, parte dos novos serviços online da Microsoft chamados de Windows Live. O novo programa introduz novos recursos além de incluir os já existentes no MSN Messenger. O Windows Live Messenger surgiu depois da proposta da Microsoft em reunir os serviços do MSN ao sistema operacional Windows.

5. Amsn

Amsn [amsn:11 2011] é um programa de mensagens instantâneas via Internet que foi desenvolvido para possibilitar que usuários de sistemas operacionais baseados no GNU/Linux entrem em contato com usuários do Windows Live Messenger. Este último atualmente se encontra disponível apenas para o Windows Vista ou Windows Seven.

6. Ubuntu Server 10.04 Its

O Ubuntu server [ubuntu:11 2011] é uma versão do Ubuntu destinada a servidores, sem ambiente gráfico pré-instalado. O Ubuntu Server é recomendado para utilizadores com alguns conhecimentos de Linux. Os utilizadores menos experientes deverão optar pelo Ubuntu normal ou pelo Kubuntu.

7. Windows XP

O Windows XP [windows:11 2011] é uma família de sistemas operacionais de 32 e 64 - bits produzido pela Microsoft, para uso em computadores pessoais, incluindo computadores residenciais e de escritórios, notebooks e media centers. O nome "XP" deriva de eXPerience, o Windows XP é o sucessor de ambos os Windows 2000 e Windows Me e é o primeiro sistema operacional para consumidores produzido pela Microsoft construído em nova arquitetura e núcleo (Windows NT 5.1). O Windows XP foi lançado no dia 26 de Outubro de 2001, e mais de 400 milhões de cópias estavam em uso em Janeiro de 2006, de acordo com estimativas feitas naquele mês por uma empresa de estatísticas.

8. Instalação do Msn-proxy

Para seguir a avaliação da ferramenta msn-proxy e o comportamento do protocolo msnms serão demonstrados os passos e requisitos de instalação do serviço no servidor linux ubuntu.

8.1. Requisitos:

Servidor de Banco de Dados MySQL; Biblioteca Libevent; Biblioteca Libmysqlclient.

Faça o download dos fontes em:

<http://sourceforge.net/projects/msn-proxy/>

8.2. Instalação:

Descompactar:

```
$ tar zxvf msn-proxy-0.7
```

```
$ cd msn-proxy
```

Compilar:

```
$ make
```

```
$ su
```

```
# make install
```

Criar o database msn-proxy:

```
$ mysql -u root -p
```

```
mysql> create database msnproxy;
```

```
mysql> grant all privileges on msnproxy.* to msnproxy@localhost  
identified by 'digite sua senha aqui';
```

```
mysql> flush privileges;
```

Configurações do MySQL:

```
# vi /usr/local/etc/msn-proxy/mysql/conf
```

```
# "host or socket|port (zero for socket)|user|pass|database name"
```

```
#/tmp/mysql.sock|0|msn-proxy|secret|msn-proxy
```

```
/var/run/mysqld/mysqld.sock|0|msnproxy|digite sua senha aqui|msnproxy
```

Copiar pasta php para /var/www/msnproxy; Editar arquivo de configurações MySQL:

```
# vi /var/www/msnproxy/
```

```
$host = ":/var/run/mysqld/mysqld.sock";
```

```
$user = "msnproxy";
```

```
$pass = "digite sua senha aqui";
```

```
$db = "msnproxy";
```

```
$port = 3306;
```

Iniciar msn-proxy para criar as tabelas no banco:

```
# msn-proxy
```

Remover permissões do arquivo /usr/local/etc/msn-proxy/mysql/conf:

```
# chmod 600 /usr/local/etc/msn-proxy/mysql/conf
```

Inserir o ip do servidor:

```
$ mysql -u msnproxy -p msnproxy mysql> insert into defaults  
(internal_host) values ('192.168.100.250');
```

Redirecionar a porta 1863 no iptables:

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 1863 -j REDIRECT --to-port 1863
```

Iniciar o msn-proxy:

```
# msn-proxy &
```

Agora basta acessar via web para visualizar os usuários e as configurações. Abra seu navegador preferido e acesse:

http://ip_servidor/msn-proxy

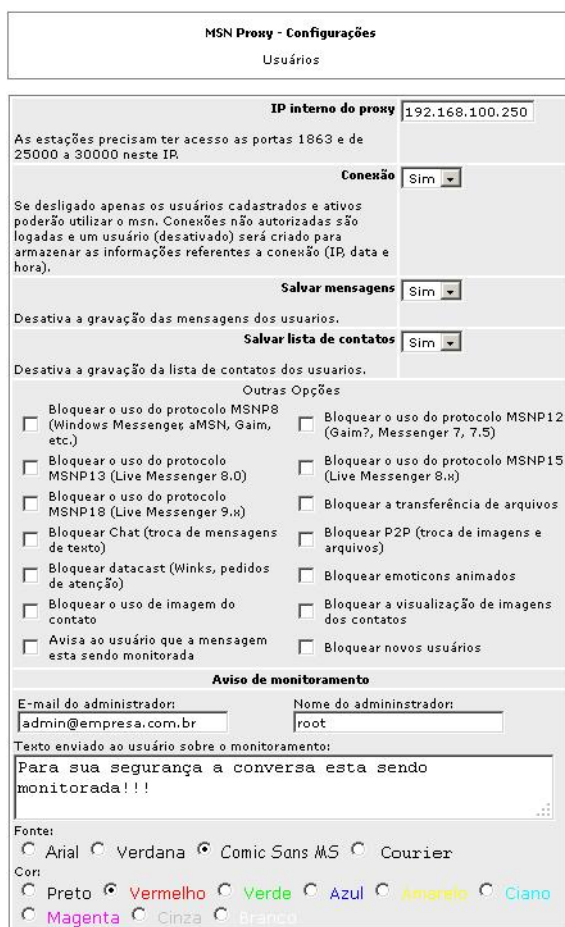


Figura 1. Tela de configurações do Msn-proxy

9. Configurações

Logo que abrir o msn-proxy no navegador aparece uma opção de configuração como visto na Figura 1 onde, será definido o modo de como o msn-proxy irá funcionar, pode-se configurar para salvar mensagens, salvar listas de contatos, outras opções referentes a outros messengers. E por ultimo e não menos importante o aviso de monitoramento, que sempre que implementado em alguma empresa, deve ser avisado ao funcionário que existe, a falta desse aviso pode gerar discussões judiciais por ser considerado invasão de privacidade.

10. Ambiente de Testes

Para fazer a avaliação da aplicação Msn-proxy foi criado um ambiente que retrata uma rede corporativa sendo um servidor gateway(Linux Ubuntu) e uma estação cliente(Windows Xp) todo o tráfego de rede passa pelo servidor que faz o gerenciamento dessas informações dando o devido tratamento a ela. Na estação windows foi instalado o amsn e windows live messenger, que são os comunicadores instantâneos mais populares do mercado.

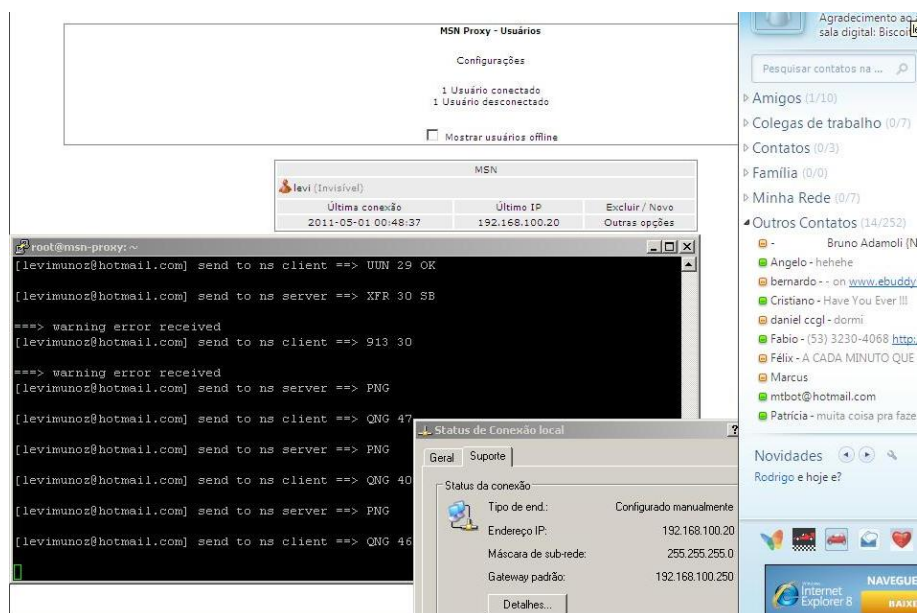


Figura 2. Tela de Depuração do Msn-proxy

11. Diferentes Messengers

Foi testado a capacidade de utilizar diferentes messenger na estação windows, tanto o messenger amsn e o windows live messenger, não tiveram problemas para se conectar, para acompanhar essa conexão foi aberta uma sessão no servidor linux e assim obter os detalhes da conexão. Para iniciar essa visualização o msn-proxy foi iniciado da seguinte forma: msn-proxy -v.

12. Messenger Web

Existe uma quantidade infinita de messengers web que são páginas de internet que possuem a possibilidade de se conectar a sua conta usada no messenger local(amsn, windows live messenger) essas outras formas de se conectar não são cobertas pelo msn-proxy na rede interna ou seja qualquer funcionário que use esse tipo de serviço não será monitorado, nesses casos é feito um bloqueio desse tipo de serviço de outras formas não abordadas neste artigo.

13. Messenger Externos

Como o servidor msn-proxy também é um gateway de rede, conexões externas vindas de qualquer ip com origem qualquer porta com destino a rede local, todo o tráfego entrante

na porta TCP 1863 é capturada pelo msn-proxy que recebe as conexões desviadas pelo firewall. Neste caso se o usuário que estiver usando qualquer tipo de messenger fora da rede, seja messenger via computador, celular ou qualquer outra forma será capturada pois o destino vai ser a porta TCP 1863 que esta sobre controle do msn-proxy.

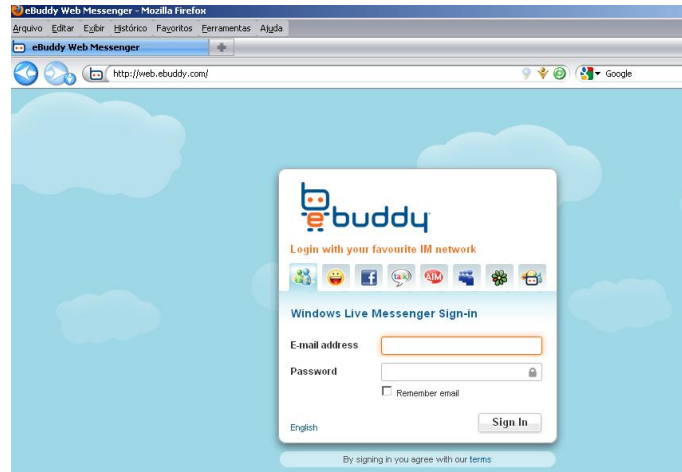


Figura 3. Ebuddy famoso messenger web

14. Opções de Bloqueios

O msn-proxy além do monitoramento faz uma série de bloqueios caso seja necessário, pode-se proibir certos contatos de se comunicarem, opção essa que conforme é selecionada já esta valendo, marcar a opção N, pode ser bloqueado emotions, adicionar novos usuários, imagem de contato e transferências de arquivos. Destas opções somente a de bloquear contato é instantâneo as outras opções é necessário que o usuário saia e entre novamente no messenger. Da mesma forma que possui os bloqueios a ferramenta possui a opção de classificação por grupos ou status, podendo fazer a listagem de todos os contatos, listar contatos liberados e listar contatos bloqueados, e se o usuário tiver uma webcam ela é identificada e marcada ao lado do usuário.



Figura 4. Listagem de contatos do usuário Levi

15. Armazenamento das Informações

O msn-proxy pode utilizar tanto o banco de dados MySQL ou PostgreSQL para guardar os registros dos eventos ocorridos nessas filtragens, o banco de dados utiliza 6 tabelas simples que a qualquer momento pode ser consultada direto via comando no banco

de dados ou com um utilitário gráfico para acesso a banco de dados. Na Figura 4 foi feita uma busca por todos os registros da tabela log, nos retornando o usuário buscapelotas@hotmail.com que teve a sua entrada negada ao serviço de messenger, já na mesma consulta o usuário levimunoz@hotmail.com teve seu acesso autorizado. Outras informações preciosas também se encontram nessa consulta como data e horário do acesso, informações que podem ser úteis em eventuais auditorias.

The screenshot shows the phpMyAdmin interface with a query executed on the 'log' table. The query is: `SELECT * FROM `log` LIMIT 0, 30`. The results are displayed in a table with the following columns: id, sb_id, date, email, display_name, to, and type. The data rows are as follows:

| id | sb_id | date | email | display_name | to | type |
|----|-------|---------------------|--------------------------|--------------|----|-----------------------|
| 1 | 0 | 2011-05-01 00:45:49 | buscapelotas@hotmail.com | | | client version denied |
| 2 | 0 | 2011-05-01 00:45:54 | buscapelotas@hotmail.com | | | client version denied |
| 21 | 1 | 2011-05-01 00:48:51 | levimunoz@hotmail.com | levi | | join |
| 23 | 2 | 2011-05-01 00:48:51 | levimunoz@hotmail.com | levi | | join |

Figura 5. Exemplo de consulta aos registros do msn-proxy

16. Conclusão

Solução de grande desempenho com software livre, essa foi a proposta de implantação a uma empresa fictícia que estaria sofrendo perdas financeiras devido a funcionários que passavam informações para a empresa concorrente através do serviço de messenger. A solução que passa por ter um servidor linux e outras ferramentas inclusas, a principal foi a utilização da aplicação msn-proxy que se mostrou bem útil para fazer o monitoramento, alguns erros ainda ocorrem por ser um software que não teve mais atualizações, mas mesmo assim cumprindo com sua função. Ao implantarmos esse tipo de monitoramento o administrador deve estar ciente que pode estar invadindo a privacidade do funcionário, por essa razão o monitoramento deve ser comunicado ao funcionário. A questão técnica de operação e manutenção da ferramenta é simples, então se você está procurando uma opção de baixo custo e com boas funcionalidades essa é a aplicação que você precisa.

Referências

amsn:11 (2011). Disponível em <http://www.amsn-project.net/> acesso em abr 2011.

msn proxy:11 (2011). Disponível em <http://sourceforge.net/search/?q=msn-proxy> acesso em fevereiro 2011.

msnms:11 (2011). Disponível em <http://wiki.wireshark.org/msnms> acesso em maio 2011.

ubuntu:11 (2011). Disponível em <http://www.ubuntu.com/> acesso em fevereiro 2011.

windows:11 (2011). Disponível em <http://www.microsoft.com> acesso em fevereiro 2011.

wlm:11 (2011). Disponível em <http://www.microsoft.com> acesso em março 2011.