Jordan M. Bonagura

bonagura@staysafe.com.br

Hackers to Hackers Conference 2010, São Paulo

Quem sou eu

- Pesquisador Independente em SI
- Fundador do Projeto Stay Safe

StaySafe

Security as a Happy Hour!!

- Membro do Projeto GNSS - INPE
- Membro Diretor do Cloud Security Alliance - Brasil
- Membro da Comissão de Crimes de Alta Tecnologia da OAB

Agenda

- Motivações;
- Principais IMs;
- Protocolo MSNP 18;
- Problemas evidentes;
- Antiga vulnerabilidade;
- Ferramenta adotada;
- O efeito “King Kong”;
- Conseqüências e Resultados.

Motivações

Porque estudar um Instant Messaging?

- Aplicação muito utilizada;
- Fins Profissionais e Pessoais;
- Uma porta aberta na empresa;
- Espionar a namorada, vizinha, concorrência;
- ... Ou ser espionado por ela ...

Principais IMs

icq

skype™

AIM

pidgin

Windows Live Messenger

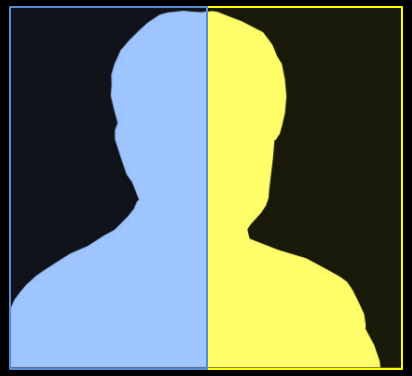
"...é um programa de comunicação instantânea pela Internet. É a nova geração do MSN Messenger, parte dos serviços online da Microsoft chamados de Windows Live".

Windows Live Messenger

"... é atualmente o IM mais usado no mundo com mais de 230 milhões de usuários".

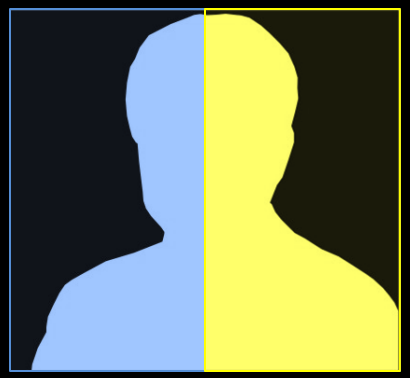
"... No Brasil, o serviço atinge mais de 75% dos usuários da Internet, o que significa mais de 34 milhões de usuários no país".

Protocolo MSNP18



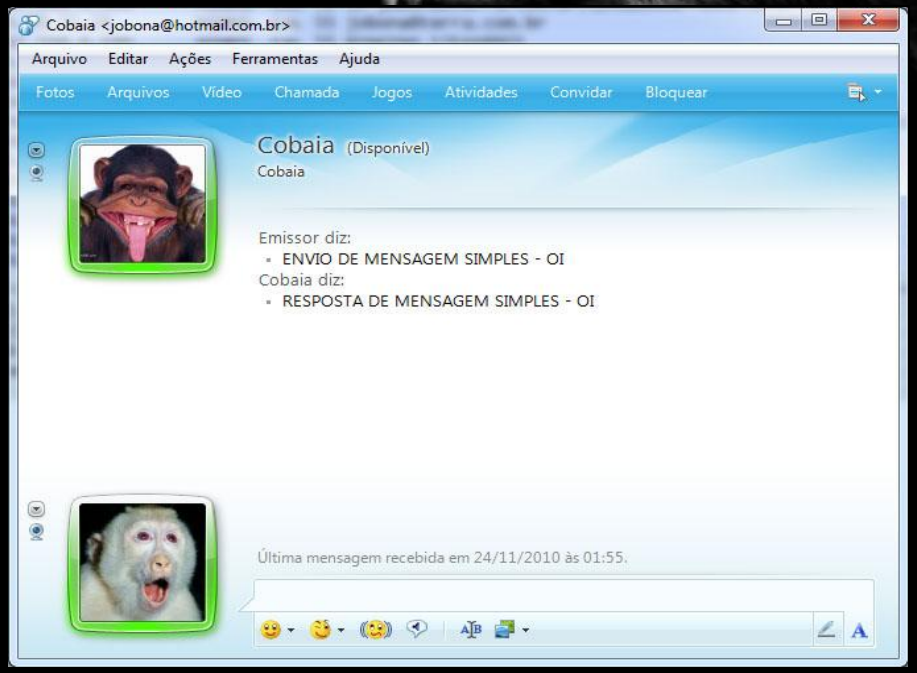
Emissor/Receptor

Microsoft

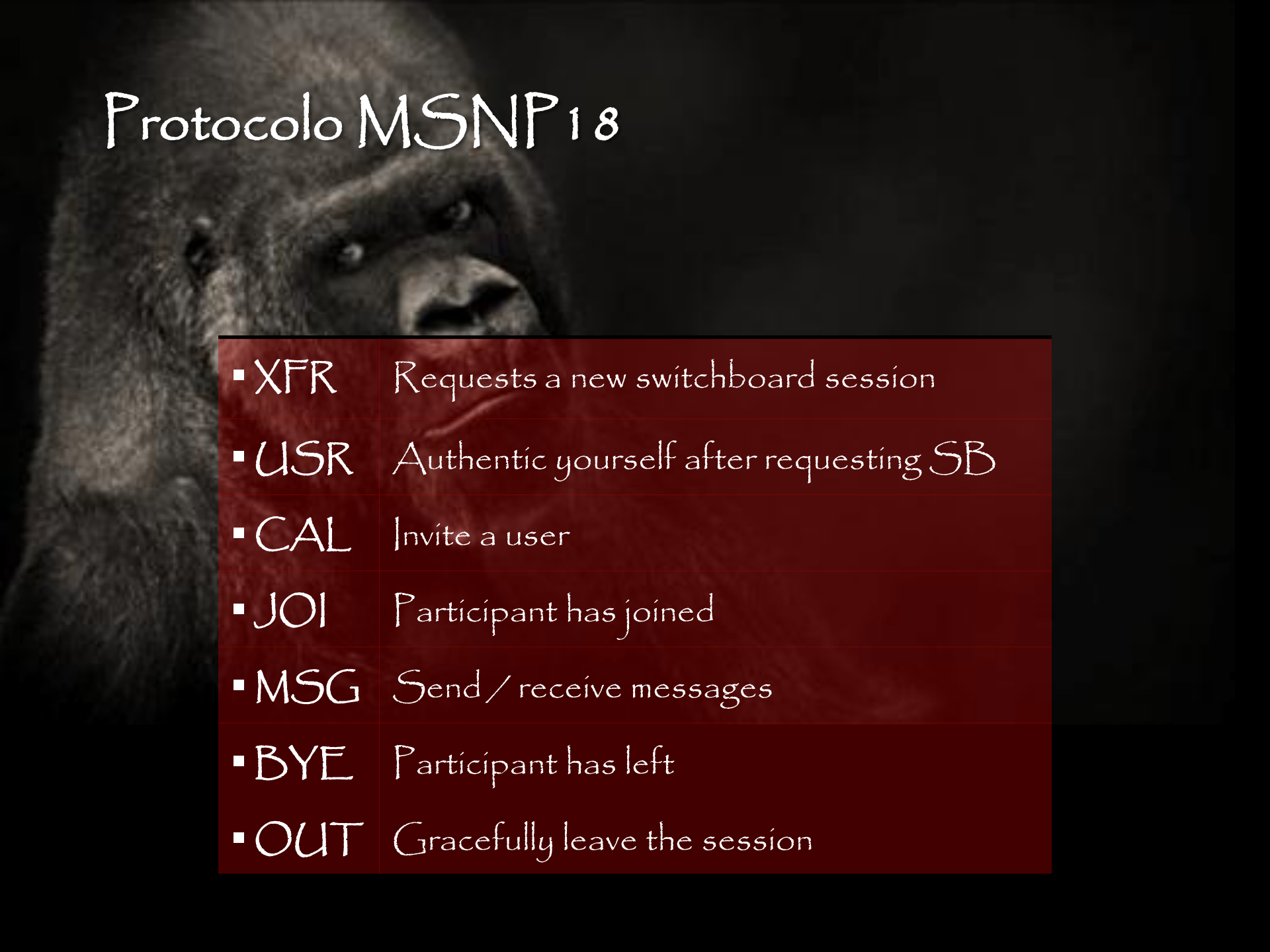


Emissor/Receptor

Protocolo MSNP18



Protocolo MSNP18



XFR	Requests a new switchboard session
USR	Authentic yourself after requesting SB
CAL	Invite a user
JOI	Participant has joined
MSG	Send / receive messages
BYE	Participant has left
OUT	Gracefully leave the session

Protocolo MSNP18

Microsoft - Wireshark

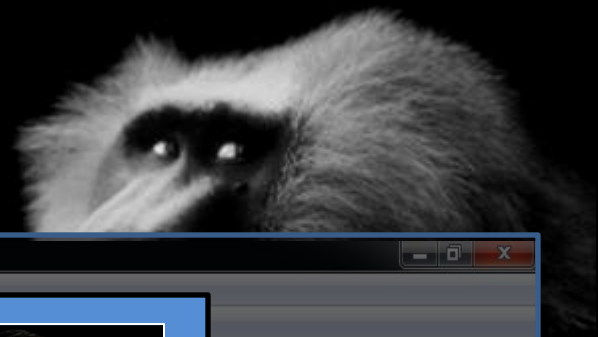
File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: msnms Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
72	22.601023	192.168.0.100	65.54.49.182	MSNMS	XFR 23 SB
73	22.833018	65.54.49.182	192.168.0.100	MSNMS	XFR 23 SB 65.55.71.28:1863 CKI 131448921.229241173.2365291 U messenger.msn.com 1
79	23.063436	192.168.0.100	65.55.71.28	MSNMS	USR 58 jobona@terra.com.br;{20AA699B-4B68-44D8-8EFB-94C8700B4B2B} 131448921.229241173.2365291
85	23.293535	65.55.71.28	192.168.0.100	MSNMS	USR 58 OK jobona@terra.com.br;{20aa699b-4b68-44d8-8efb-94c8700b4b2b} Emissor
86	23.294419	192.168.0.100	65.55.71.28	MSNMS	CAL 55 jobona@terra.com.br
88	23.559158	65.55.71.28	192.168.0.100	MSNMS	CAL 55 RINGING 131448921
89	23.559635	192.168.0.100	65.55.71.28	MSNMS	CAL 56 jobona@hotmail.com.br
90	23.559742	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@terra.com.br Emissor 2788999484:2550273072
93	23.808271	65.55.71.28	192.168.0.100	MSNMS	CAL 56 RINGING 131448921
96	24.276211	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br;{b575cef8-8c94-40f2-96cf-1e5e50c5117d} Cobaia 2788999484:2550273072
97	24.276700	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br Cobaia 2788999484:2550273072
99	24.278831	192.168.0.100	65.55.71.28	MSNMS	MSG 57 N 148
129	31.928297	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
142	36.905746	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
149	41.928082	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
156	46.937208	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
160	48.328489	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 150

⊞ Frame 99: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)
⊞ Ethernet II, Src: HonHaiPr_53:c8:0d (5c:ac:4c:53:c8:0d), Dst: D-Link_b7:db:2b (00:22:b0:b7:db:2b)
⊞ Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 65.55.71.28 (65.55.71.28)
⊞ Transmission Control Protocol, Src Port: 57031 (57031), Dst Port: msnp (1863), Seq: 154, Ack: 337, Len: 162
⊟ MSN Messenger Service
MSG 57 N 148\r\n
MIME-Version: 1.0\r\n
Content-Type: text/plain; charset=UTF-8\r\n
X-MMS-IM-Format: FN=Segoe%20UI; EF=; CO=0; CS=1; PF=0\r\n
\r\n
ENVIO DE MENSAGEM SIMPLES - OI

Protocolo MSNP18



Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: msnms

No.	Time	Source	Destination	Protocol	Info
72	22.601023	192.168.0			
73	22.833018	65.54.49.			
79	23.063436	192.168.0			
85	23.293535	65.55.71.			
86	23.294419	192.168.0			
88	23.559158	65.55.71.			
89	23.559635	192.168.0			
90	23.559742	65.55.71.			
93	23.808271	65.55.71.			
96	24.276211	65.55.71.			
97	24.276700	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br Cobaia 2788999484:2550273072
99	24.278831	192.168.0.100	65.55.71.28	MSNMS	MSG 57 N 148
129	31.928297	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
142	36.905746	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
149	41.928082	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
156	46.937208	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
160	48.328489	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 150


```
Frame 99: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)
Ethernet II, Src: HonHaiPr_53:c8:0d (5c:ac:4c:53:c8:0d), Dst: D-Link_b7:db:2b (00:22:b0:b7:db:2b)
Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 65.55.71.28 (65.55.71.28)
Transmission Control Protocol, Src Port: 57031 (57031), Dst Port: msnp (1863), Seq: 154, Ack: 337, Len: 162
MSN Messenger Service
    MSG 57 N 148\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    X-MMS-IM-Format: FN=Segoe%20UI; EF=; CO=0; CS=1; PF=0\r\n
    \r\n
    ENVIO DE MENSAGEM SIMPLES - OI
```

Protocolo MSNP18

Microsoft - Wireshark

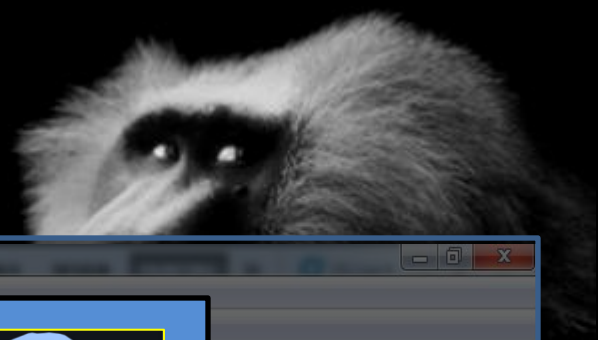
File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: msnms Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
72	22.601023	192.168.0.100	65.54.49.182	MSNMS	XFR 23 SB
73	22.833018	65.54.49.182	192.168.0.100	MSNMS	XFR 23 SB 65.55.71.28:1863 CKI 131448921.229241173.2365291 U messenger.msn.com 1
79	23.063436	192.168.0.100	65.55.71.28	MSNMS	USR 58 jobona@terra.com.br;{20AA699B-4B68-44D8-8EFB-94C8700B4B2B} 131448921.229241173.2365291
85	23.293535	65.55.71.28	192.168.0.100	MSNMS	USR 58 OK jobona@terra.com.br;{20aa699b-4b68-44d8-8efb-94c8700b4b2b} Emissor
86	23.294419	192.168.0.100	65.55.71.28	MSNMS	CAL 55 jobona@terra.com.br
88	23.559158	65.55.71.28	192.168.0.100	MSNMS	CAL 55 RINGING 131448921
89	23.559635	192.168.0.100	65.55.71.28	MSNMS	CAL 56 jobona@hotmail.com.br
90	23.559742	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@terra.com.br Emissor 2788999484:2550273072
93	23.808271	65.55.71.28	192.168.0.100	MSNMS	CAL 56 RINGING 131448921
96	24.276211	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br;{b575cef8-8c94-40f2-96cf-1e5e50c5117d} Cobaia 2788999484:2550273072
97	24.276700	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br Cobaia 2788999484:2550273072
99	24.278831	192.168.0.100	65.55.71.28	MSNMS	MSG 57 N 148
129	31.928297	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
142	36.905746	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
149	41.928082	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
156	46.937208	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
160	48.328489	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 150

⊞ Frame 160: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
⊞ Ethernet II, Src: D-Link_b7:db:2b (00:22:b0:b7:db:2b), Dst: HonHaiPr_53:c8:0d (5c:ac:4c:53:c8:0d)
⊞ Internet Protocol, Src: 65.55.71.28 (65.55.71.28), Dst: 192.168.0.100 (192.168.0.100)
⊞ Transmission Control Protocol, Src Port: msnp (1863), Dst Port: 57031 (57031), Seq: 861, Ack: 316, Len: 188
⊟ MSN Messenger Service
MSG jobona@hotmail.com.br Cobaia 150\r\n
MIME-Version: 1.0\r\n
Content-Type: text/plain; charset=UTF-8\r\n
X-MMS-IM-Format: FN=Segoe%20UI; EF=; CO=0; CS=1; PF=0\r\n
\r\n
RESPOSTA DE MENSAGEM SIMPLES - OI

Protocolo MSNP18



Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: msnms

No.	Time	Source			
72	22.601023	192.168.0			
73	22.833018	65.54.49.			
79	23.063436	192.168.0			
85	23.293535	65.55.71.			
86	23.294419	192.168.0			
88	23.559158	65.55.71.			
89	23.559635	192.168.0			
90	23.559742	65.55.71.			
93	23.808271	65.55.71.			
96	24.276211	65.55.71.			
97	24.276700	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br Cobaia 2788999484:2550273072
99	24.278831	192.168.0.100	65.55.71.28	MSNMS	MSG 57 N 148
129	31.928297	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
142	36.905746	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
149	41.928082	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
156	46.937208	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
160	48.328489	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 150


```
Frame 160: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
Ethernet II, Src: D-Link_b7:db:2b (00:22:b0:b7:db:2b), Dst: HonHaiPr_53:c8:0d (5c:ac:4c:53:c8:0d)
Internet Protocol, Src: 65.55.71.28 (65.55.71.28), Dst: 192.168.0.100 (192.168.0.100)
Transmission Control Protocol, Src Port: msnp (1863), Dst Port: 57031 (57031), Seq: 861, Ack: 316, Len: 188
MSN Messenger Service
    MSG jobona@hotmail.com.br Cobaia 150\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    X-MMS-IM-Format: FN=Segoe%20UI; EF=; CO=0; CS=1; PF=0\r\n
    \r\n
    RESPOSTA DE MENSAGEM SIMPLES - OI
```

Protocolo MSNP18

Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: msnms Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
72	22.601023	192.168.0.100	65.54.49.182	MSNMS	XFR 23 SB
73	22.833018	65.54.49.182	192.168.0.100	MSNMS	XFR 23 SB 65.55.71.28:1863 CKI 131448921.229241173.2365291 U messenger.msn.com 1
79	23.063436	192.168.0.100	65.55.71.28	MSNMS	USR 58 jobona@terra.com.br;{20AA699B-4B68-44D8-8EFB-94C8700B4B2B} 131448921.229241173.2365291
85	23.293535	65.55.71.28	192.168.0.100	MSNMS	USR 58 OK jobona@terra.com.br;{20aa699b-4b68-44d8-8efb-94c8700b4b2b} Emissor
86	23.294419	192.168.0.100	65.55.71.28	MSNMS	CAL 55 jobona@terra.com.br
88	23.559158	65.55.71.28	192.168.0.100	MSNMS	CAL 55 RINGING 131448921
89	23.559635	192.168.0.100	65.55.71.28	MSNMS	CAL 56 jobona@hotmail.com.br
90	23.559742	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@terra.com.br Emissor 2788 4:2550273072
93	23.808271	65.55.71.28	192.168.0.100	MSNMS	CAL 56 RINGING 131448921
96	24.276211	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br;{b575cef 4-40f2-96cf-1e5e50c5117d} Cobai 9009484:2550273072
97	24.276700	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br Cobaia 2 09484:2550273072
99	24.278831	192.168.0.100	65.55.71.28	MSNMS	MSG 57 N 148
129	31.928297	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
142	36.905746	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
149	41.928082	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
156	46.937208	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
160	48.328489	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 150

94

```
⊞ Frame 129: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits)
⊞ Ethernet II, Src: D-Link_b7:db:2b (00:22:b0:b7:db:2b), Dst: HonHaiPr_53:c8:0d (5c:ac:4c:53:c8:0d)
⊞ Internet Protocol, Src: 65.55.71.28 (65.55.71.28), Dst: 192.168.0.100 (192.168.0.100)
⊞ Transmission Control Protocol, Src Port: msnp (1863), Dst Port: 57031 (57031), Seq: 337, Ack: 316, Len: 131
⊟ MSN Messenger Service
    MSG jobona@hotmail.com.br Cobaia 94\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/x-msmsgscontrol\r\n
    TypingUser: jobona@hotmail.com.br\r\n
    \r\n
    \r\n
```

Typinguser:jobona@hotmail.com.br\r\n

Protocolo MSNP18

Microsoft - Wireshark

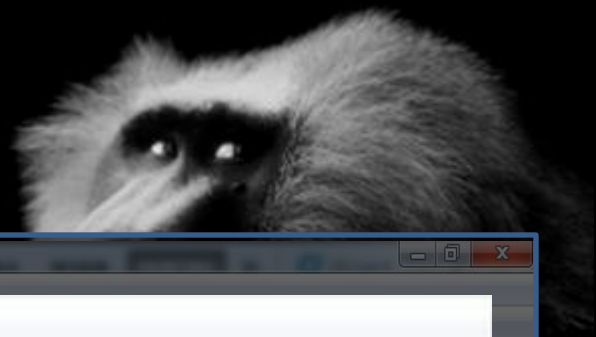
File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: msnms Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
72	22.601023	192.168.0.100	65.54.49.182	MSNMS	XFR 23 SB
73	22.833018	65.54.49.182	192.168.0.100	MSNMS	XFR 23 SB 65.55.71.28:1863 CKI 131448921.229241173.2365291 U messenger.msn.com 1
79	23.063436	192.168.0.100	65.55.71.28	MSNMS	USR 58 jobona@terra.com.br;{20AA699B-4B68-44D8-8EFB-94C8700B4B2B} 131448921.229241173.2365291
85	23.293535	65.55.71.28	192.168.0.100	MSNMS	USR 58 OK jobona@terra.com.br;{20aa699b-4b68-44d8-8efb-94c8700b4b2b} Emissor
86	23.294419	192.168.0.100	65.55.71.28	MSNMS	CAL 55 jobona@terra.com.br
88	23.559158	65.55.71.28	192.168.0.100	MSNMS	CAL 55 RINGING 131448921
89	23.559635	192.168.0.100	65.55.71.28	MSNMS	CAL 56 jobona@hotmail.com.br
90	23.559742	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@terra.com.br Emissor 2788999484:2550273072
93	23.808271	65.55.71.28	192.168.0.100	MSNMS	CAL 56 RINGING 131448921
96	24.276211	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br;{b575cef8-8c94-40f2-96cf-1e5e50c5117d} Cobaia 2788999484:2550273072
97	24.276700	65.55.71.28	192.168.0.100	MSNMS	JOI jobona@hotmail.com.br Cobaia 2788999484:2550273072
99	24.278831	192.168.0.100	65.55.71.28	MSNMS	MSG 57 N 148
129	31.928297	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
142	36.905746	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
149	41.928082	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
156	46.937208	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 94
160	48.328489	65.55.71.28	192.168.0.100	MSNMS	MSG jobona@hotmail.com.br Cobaia 150

⊞ Frame 72: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
⊞ Ethernet II, Src: HonHaiPr_53:c8:0d (5c:ac:4c:53:c8:0d), Dst: D-Link_b7:db:2b (00:22:b0:b7:db:2b)
⊞ Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 65.54.49.182 (65.54.49.182)
⊞ Transmission Control Protocol, Src Port: 56943 (56943), Dst Port: msnp (1863), Seq: 1, Ack: 1, Len: 11
⊟ MSN Messenger Service
    XFR 23 SB\r\n

Protocolo MSNP18



Microsoft - Wireshark

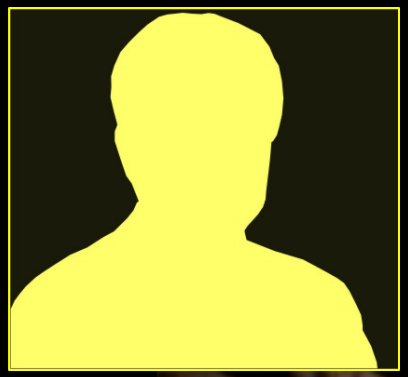
File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter:

No.	Info
72	XFR 23 SB
73	XFR 23 SB 65.55.71.28:1863 CKI 131448921.229241173.2365291 U messenger.msn.com 1
79	USR 58 jobona@terra.com.br;{20AA699B-4B68-44D8-8EFB-94C8700B4B2B} 131448921.229241173.2365291
85	USR 58 OK jobona@terra.com.br;{20aa699b-4b68-44d8-8efb-94c8700b4b2b} Emissor
86	CAL 55 jobona@terra.com.br
88	CAL 55 RINGING 131448921
89	CAL 56 jobona@hotmail.com.br
90	JOI jobona@terra.com.br Emissor 2788999484:2550273072
93	CAL 56 RINGING 131448921
96	JOI jobona@hotmail.com.br;{b575cef8-8c94-40f2-96cf-1e5e50c5117d} Cobaia 2788999484:2550273072
97	JOI jobona@hotmail.com.br Cobaia 2788999484:2550273072
99	MSG 57 N 148
129	MSG jobona@hotmail.com.br Cobaia 94
142	MSG jobona@hotmail.com.br Cobaia 94
149	MSG jobona@hotmail.com.br Cobaia 94
156	MSG jobona@hotmail.com.br Cobaia 94
160	MSG jobona@hotmail.com.br Cobaia 150

Frame
Ethe
Inte
Trans
MSN
XFR

Alguns problemas são evidentes...



Oi Manézinho... Quanto tempo?

Se você quer ganhar um milhão de reais clique aqui!

www.casadafortuna.com.br/virhus_do_capeta.exe

Alguns problemas são evidentes...

Vai, passa aí...

Eu prometo que serei bonzinho!!!

??????????????????

Beleza.

Só porque você é meu amigo!!!

A senha do banco é: *298887.*

Funcionário do mês

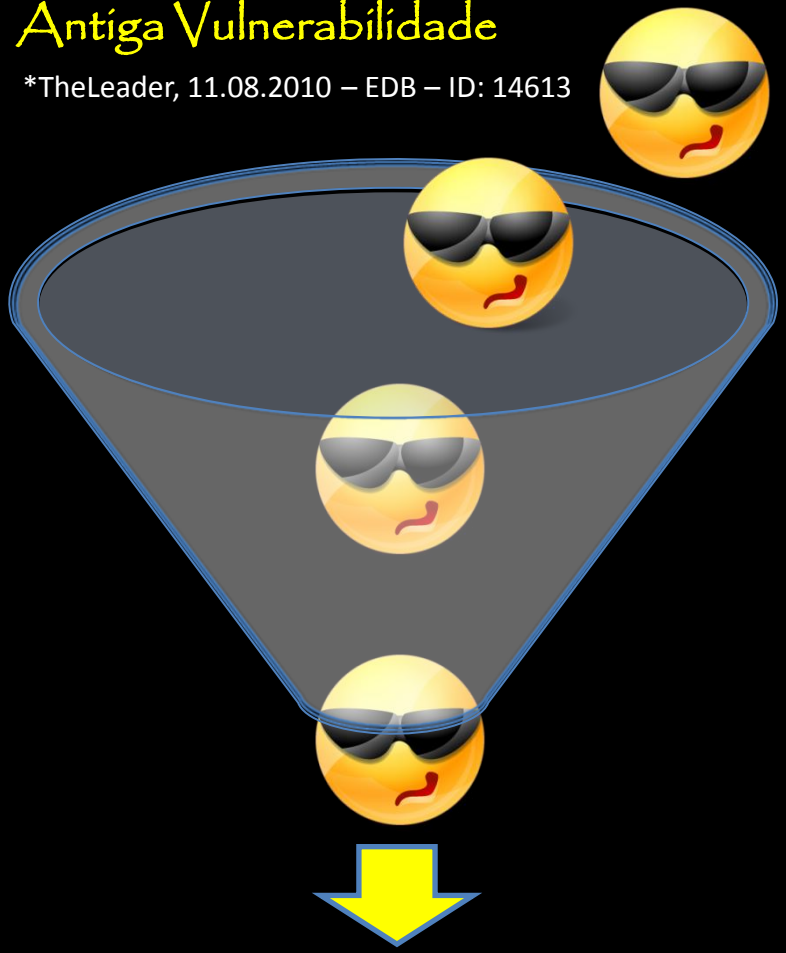
Alguns problemas são evidentes...

A mesma mão que acarícia... Da merda!

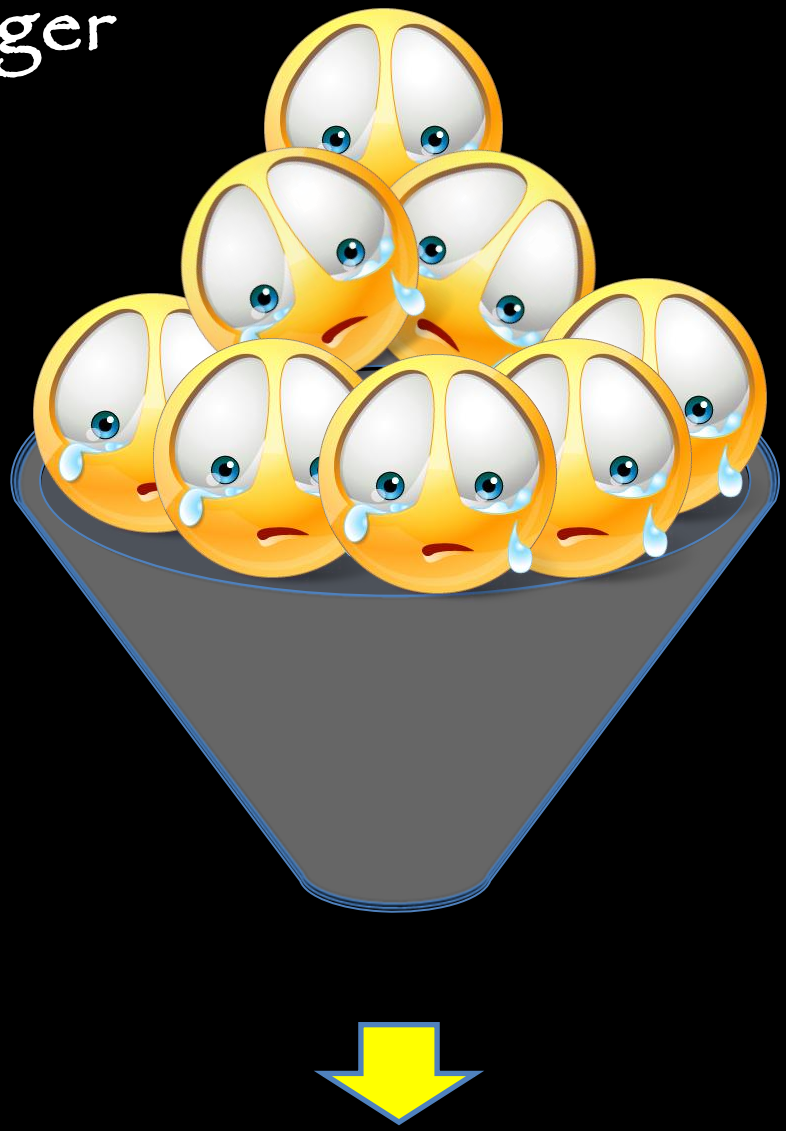
Aplicação Live Messenger

Antiga Vulnerabilidade

*TheLeader, 11.08.2010 – EDB – ID: 14613



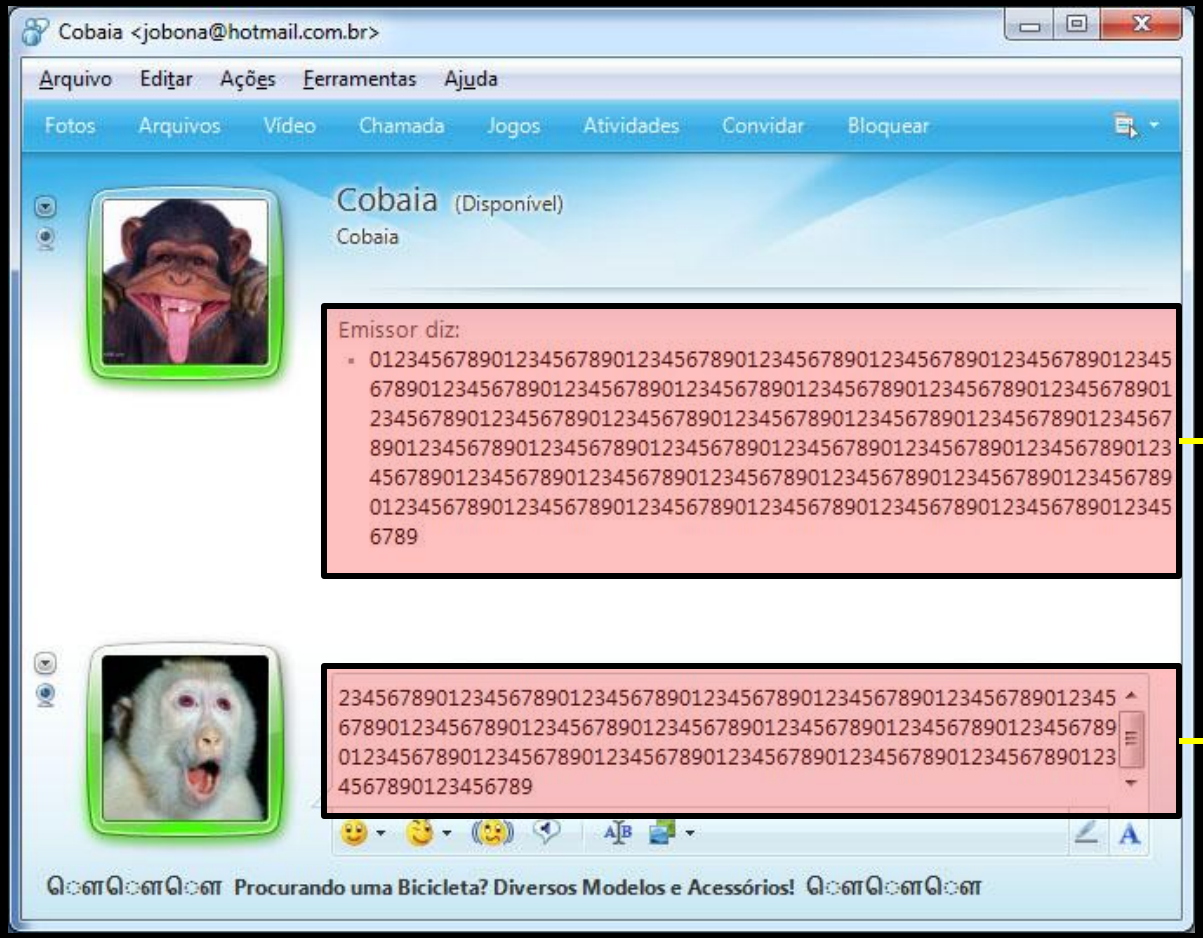
EXECUÇÃO



DENIAL OF SERVICE

Aplicação Live Messenger

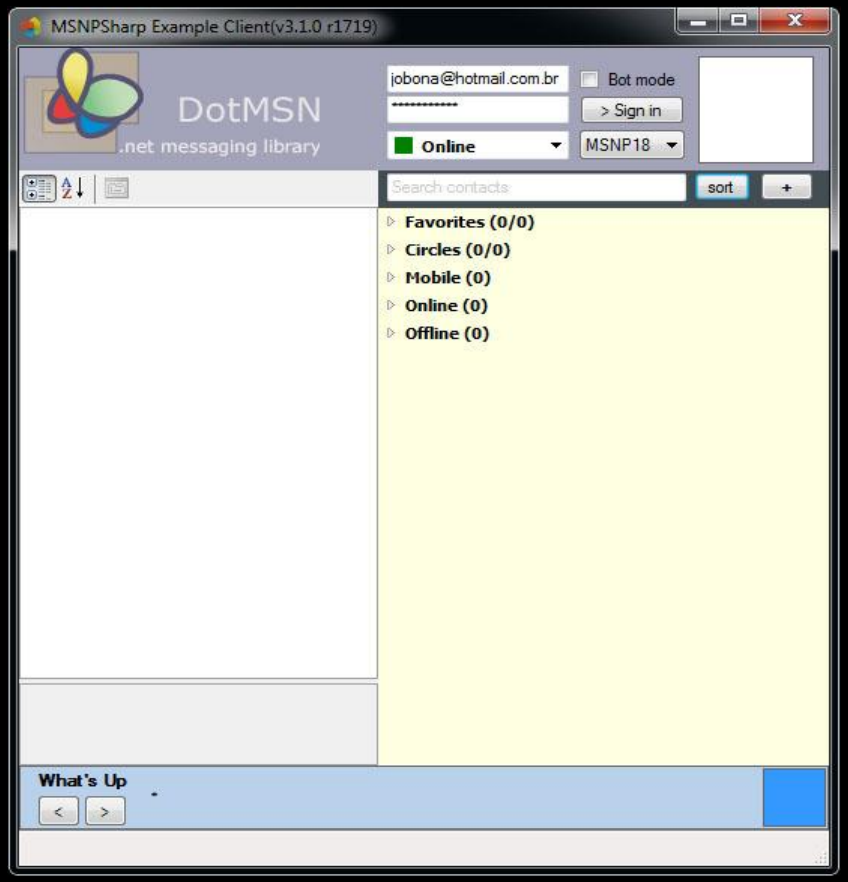
Corrigindo o funil????



Limitado para

400 caracteres

Ferramenta Adotada



DotMSNClient:

- Opensource;
- Alterações no protocolo MSNP;
- Independência das restrições existentes no Live Messenger.

MSNPSharp

Of the messenger By the messenger For the messenger


Live Messenger
X
King Kong

Deixe-me explicar...

Live Messenger X King Kong

- Ambos possuem imponente sucesso;
- O enredo é bastante simples;
- Quando fora de controle podem causar danos incalculáveis;
- Algumas falhas no roteiro acabam pondo tudo a perder.

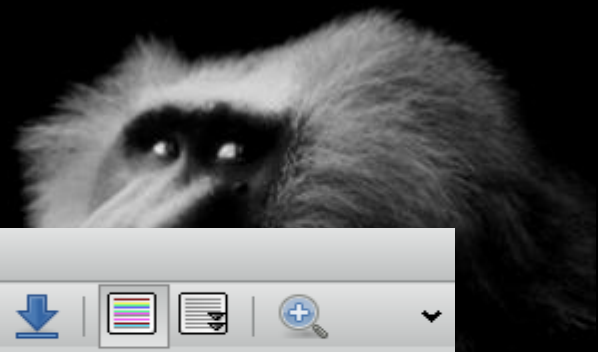

O Efeito
"King Kong"
DEMO 1
Algumas Solicitações

Algumas Solicitações

De acordo com a Microsoft:

- Solicitar no máximo 8 SB (XFR)
- Necessário um intervalo de 60 segundos;
- Obtenção de Resposta: XFR ok ou 800

Algumas Solicitações



File Edit View Go Capture Analyze Statistics Help

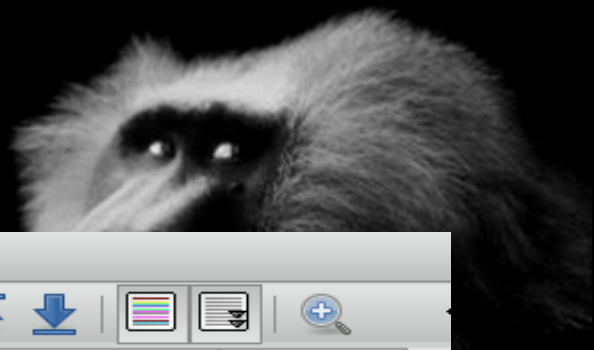
Filter: msnms | Expression... | Limpar

Source	Destination	Protocol	Info
10.0.2.15	65.55.71.36	MSNMS	XFR 20 SB
10.0.2.15	65.55.71.36	MSNMS	XFR 21 SB
10.0.2.15	65.55.71.36	MSNMS	XFR 22 SB
10.0.2.15	65.55.71.36	MSNMS	XFR 23 SB
10.0.2.15	65.55.71.36	MSNMS	XFR 24 SB
65.55.71.36	10.0.2.15	MSNMS	XFR 12 SB 65.54.48.31:1863 CKI 1795885784.19
65.55.71.36	10.0.2.15	MSNMS	XFR 13 SB 65.54.49.156:1863 CKI 1134973126.1
65.55.71.36	10.0.2.15	MSNMS	800 20
65.55.71.36	10.0.2.15	MSNMS	800 21
65.55.71.36	10.0.2.15	MSNMS	XFR 15 SB 65.55.71.195:1863 CKI 1357965540.1
65.55.71.36	10.0.2.15	MSNMS	800 24
65.55.71.36	10.0.2.15	MSNMS	XFR 19 SB 65.55.71.195:1863 CKI 123540847.85
65.55.71.36	10.0.2.15	MSNMS	XFR 16 SB 65.54.48.162:1863 CKI 403611979.22
10.0.2.15	65.54.48.31	MSNMS	USR 25 jobona@hotmail.com.br 1795885784.1932

▷ Frame 35 (217 bytes on wire, 217 bytes captured)
▷ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: CadmusCo_6b:57:c0 (08:00:27:6b:57:c0
▷ Internet Protocol, Src: 65.55.71.36 (65.55.71.36), Dst: 10.0.2.15 (10.0.2.15)
▷ Transmission Control Protocol, Src Port: msnp (1863), Dst Port: 40571 (40571), Seq: 461, Ack: 144,
▽ MSN Messenger Service

```
XFR 19 SB 65.55.71.195:1863 CKI 123540847.85248241.18142182 U messenger.msn.com 1\r\n
XFR 18 SB 65.54.48.157:1863 CKI 735142585.51086.11078177 U messenger.msn.com 1\r\n
```

Algumas Solicitações



File Edit View Go Capture Analyze Statistics Help

Filter: msnms | Expression... | Limpar

Source	Destination	Protocol	Info
10.0.2.15	65.55.71.36	MSNMS	XFR 32 SB
65.55.71.36	10.0.2.15	MSNMS	XFR 31 SB 65.54.48.76:1863 CKI 1212915329.44
65.55.71.36	10.0.2.15	MSNMS	XFR 32 SB 65.54.49.68:1863 CKI 1514128151.21
65.55.71.36	10.0.2.15	MSNMS	XFR 34 SB 65.55.71.30:1863 CKI 1970587581.16
65.55.71.36	10.0.2.15	MSNMS	800 40
65.55.71.36	10.0.2.15	MSNMS	800 41
10.0.2.15	65.54.48.76	MSNMS	USR 44 jobona@hotmail.com.br 1212915329.4412
65.54.48.76	10.0.2.15	MSNMS	USR 44 OK jobona@hotmail.com.br Jordan%5Ftes
10.0.2.15	65.54.48.76	MSNMS	CAL 45 jobona@terra.com.br
65.54.48.76	10.0.2.15	MSNMS	CAL 45 RINGING 1212915329
65.54.48.76	10.0.2.15	MSNMS	JOI jobona@terra.com.br Jordan 2788999484
10.0.2.15	65.54.48.76	MSNMS	MSG 46 U 97
10.0.2.15	65.55.71.36	MSNMS	PNG
65.55.71.36	10.0.2.15	MSNMS	QNG 48

▷ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: CadmusCo_6b:57:c0 (08:00:27:6b:57

▷ Internet Protocol, Src: 65.55.71.36 (65.55.71.36), Dst: 10.0.2.15 (10.0.2.15)

▷ Transmission Control Protocol, Src Port: msnp (1863), Dst Port: 40571 (40571), Seq: 428, Ack: 1

▽ MSN Messenger Service

```
800 41\r\n
800 42\r\n
800 43\r\n
XFR 36 SB 65.54.61.199:1863 CKI 1870357141.1322246.21148228 U messenger.msn.com 1\r\n
XFR 37 SB 65.55.71.195:1863 CKI 1295028701.8253143.147125253 U messenger.msn.com 1\r\n
XFR 38 SB 65.54.48.159:1863 CKI 1495441885.145217154.24044175 U messenger.msn.com 1\r\n
```

O Efeito "King Kong"

DEMO 2

Mensagens Ocultas

Mensagens Ocultas

- Algumas alterações no código e as mensagens se tornam ocultas ao receptor...

Vídeo 1

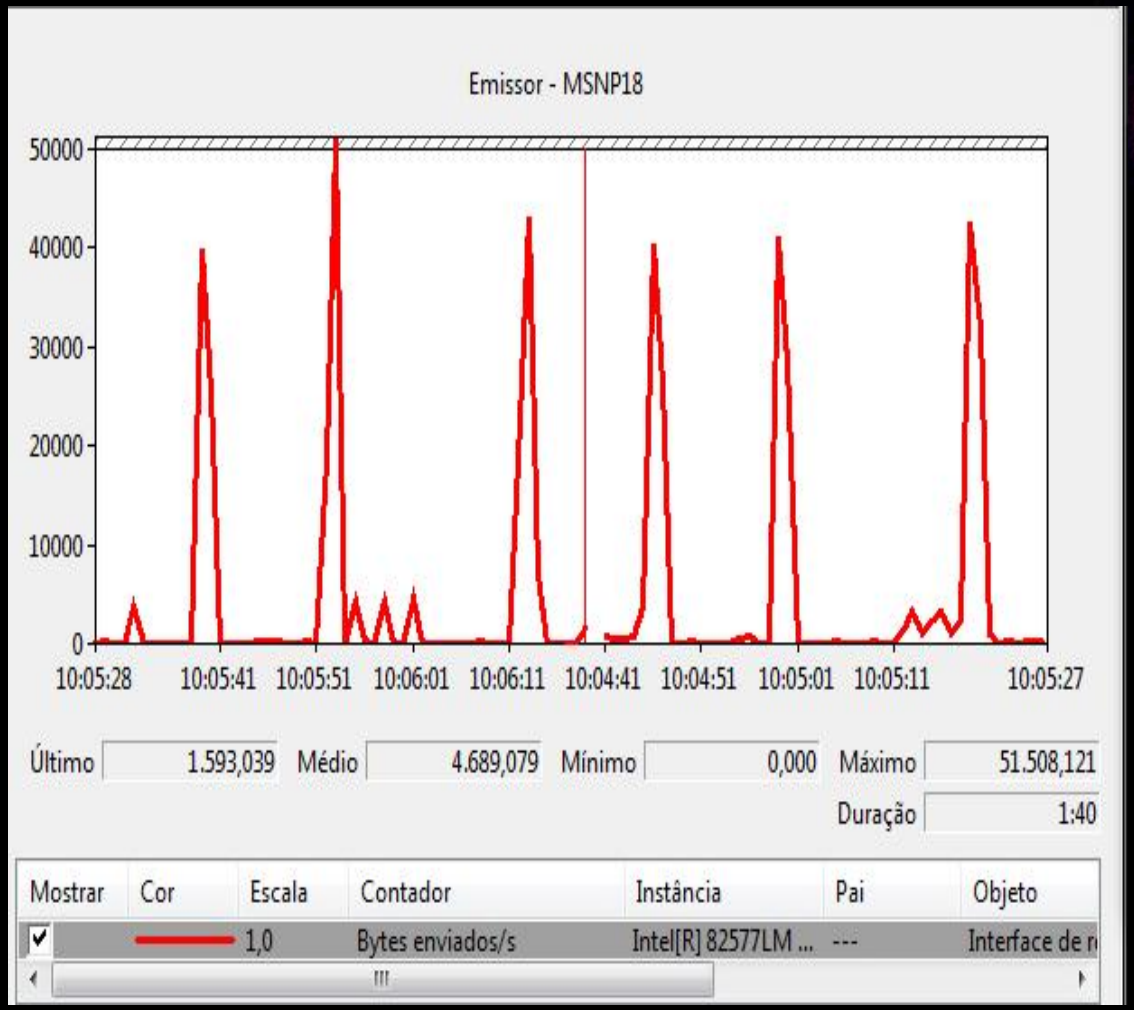

DEMO 3
Flood Oculto
O Efeito "King Kong"

"Flood" Oculto

- Algumas Solicitações (XFR's);
- MSG's Ocultas;

Vídeos 2

"Flood" Oculto



Vídeos 3


Possibilidades
O Efeito "King Kong"

Possibilidades

- Hijacking; → CAL/ JOI
- Envio de Mensagem Forjada - Cabeçalho; → CAL
- Denial of Service (Nudge); → XFR/ MSG

Um Shellzinho – Connection Back

- XFR + MSG "Mensagem "Personalizada"

Sim, é possível:

Tentem uma "Mensagem Personalizada" na solicitação de transferência de arquivo. ☺ ☺

Agradecimentos

Sandra De Marco Bonagura

Por todos os ensinamentos!!!

Luís Felipe Féres dos Santos

Apoio nos testes de execução.

Obrigado

Jordan M. Bonagura

bonagura@staysafe.com.br
www.staysafe.com.br
@jbonagura

jobona@hotmail.com.br