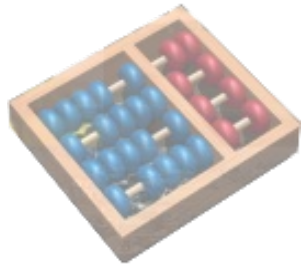
# Instituto de Computação - Unicamp

## Ataques contra o SMTP

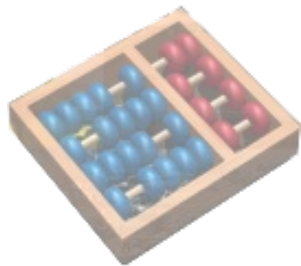
## Como as botnets enviam spam

Miguel Di Ciurcio Filho
Administração de Sistemas
miguel@ic.unicamp.br



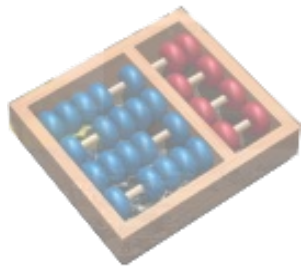
# E-mail no IC

- Recebe há muitos anos - usuários tinham acesso ao mbox via NFS.
- É importantíssimo para as atividades de professores e alunos (2400 usuários).
- Qualquer problema é notado rapidamente.



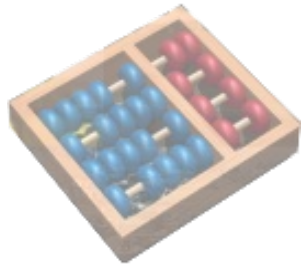
# E-mail no IC

- CentOS
- **Postfix**
- Dovecot
- Amavis
- Squirrelmail

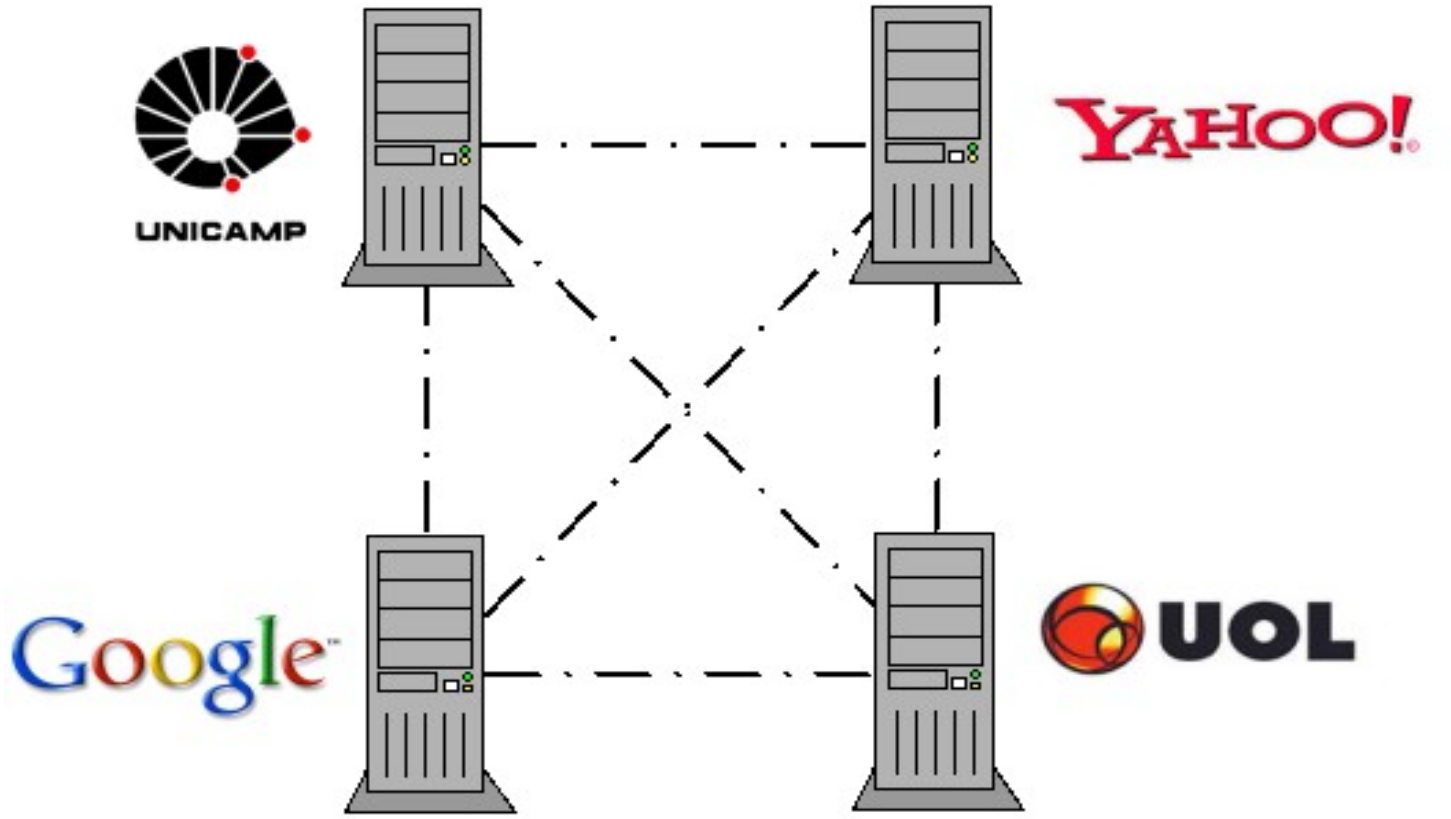


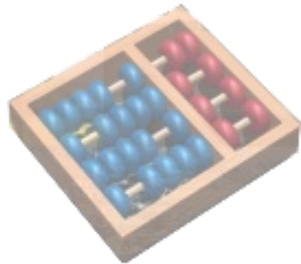
# SMTP

- É o protocolo, não temos outro. Paciência.
- Modelos “pull” não são escaláveis. Desista.
- Existe há 27 anos e continua em uso.
- Talvez seja tarde demais para mudar.



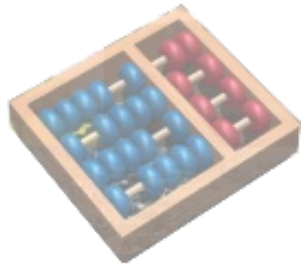
# Pseudo-federação



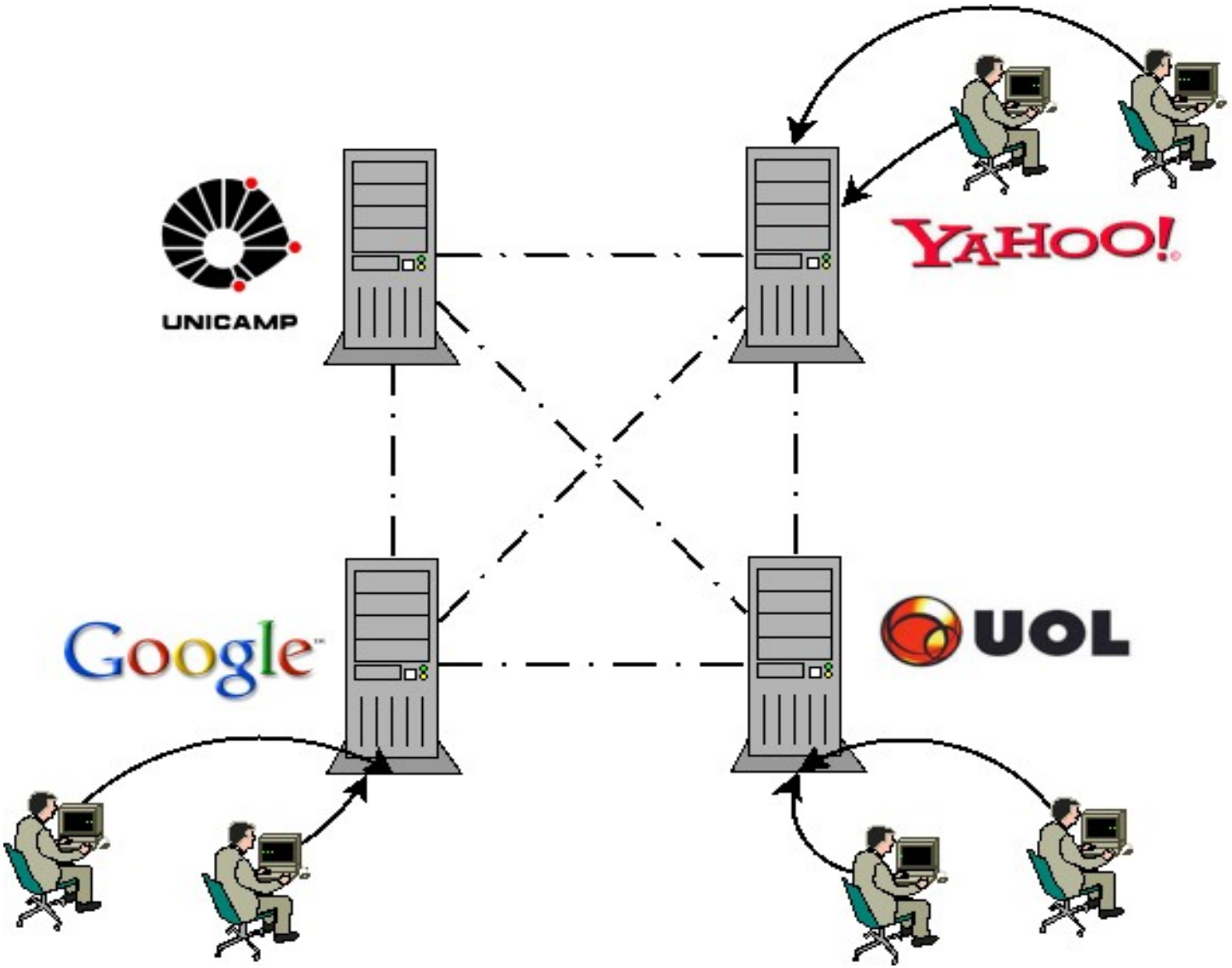



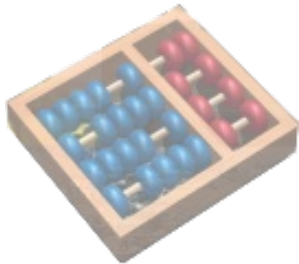
# Pseudo-federação

- Redes estáveis.
- Facilmente identificáveis.
- Alta concentração de usuários.



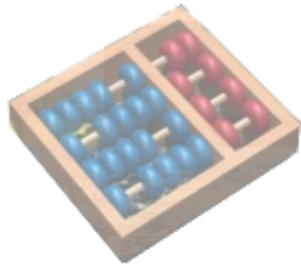
# Pseudo-federação



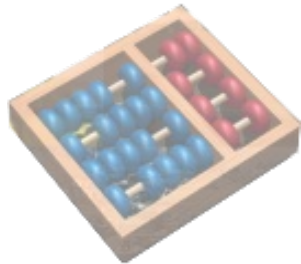



# Pseudo-federação

- Usuários submetem mensagens no provedor.
- Provedores podem identificar facilmente abuso.
- Usuários não acessam diretamente o MX dos destinatários.
- Gerência da porta 25 já!

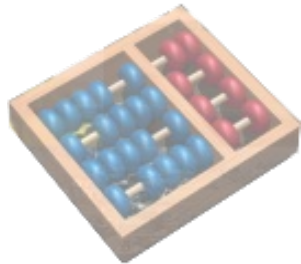


Porém...

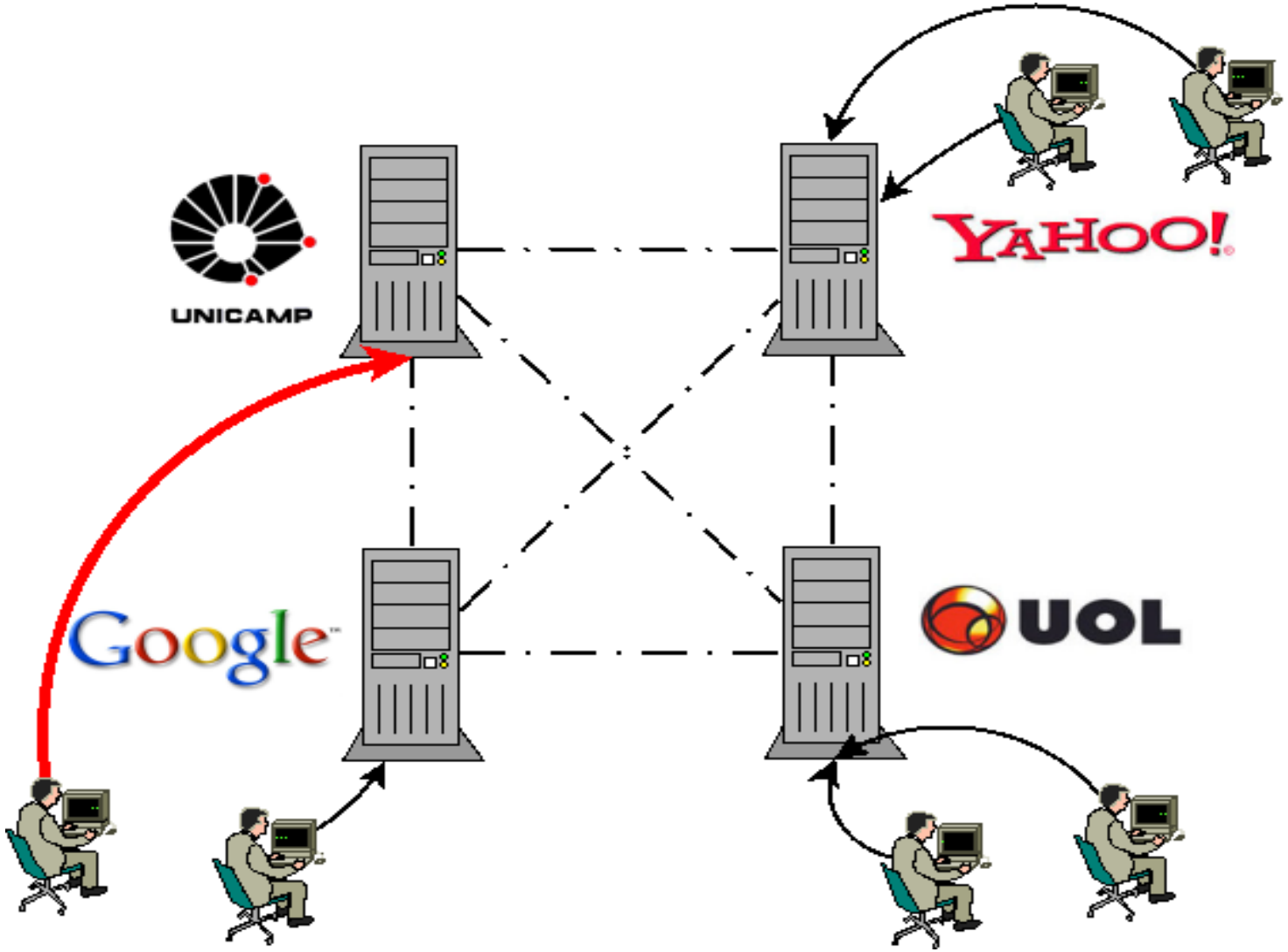


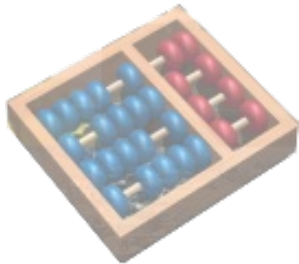
# Botnet

- Conjunto de computadores controlados por um terceiro remotamente.
- Cada computador é chamado de zumbi.
- O software malicioso faz de tudo para não ser detectado.
- Os zumbis são utilizados para vários propósitos, entre eles enviar spam.

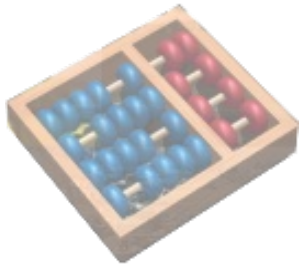


# Pseudo-federação



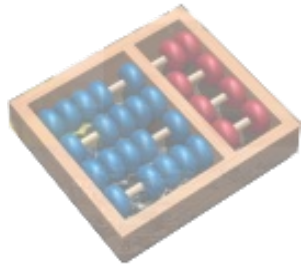



# Então, como evitar os zumbis?

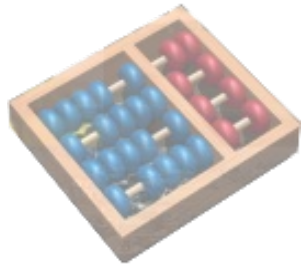


# Como evitar os zumbis?

- RFCs são fundamentais.
- Servidores da “federação” seguem as RFCs, zumbis não.
- Zumbis exploram alguns “equívocos” do protocolo.

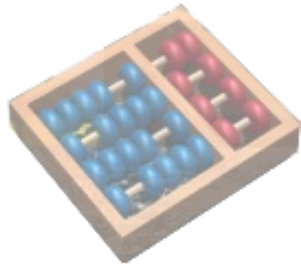


# O bom e velho SMTP...



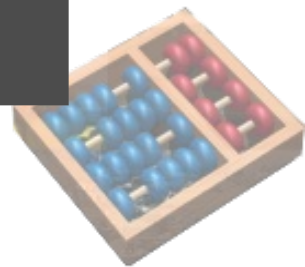
```
$ dig +short -t mx gmail.com
```

```
5 gmail-smtp-in.l.google.com.
10 alt1.gmail-smtp-in.l.google.com.
20 alt2.gmail-smtp-in.l.google.com.
30 alt3.gmail-smtp-in.l.google.com.
40 alt4.gmail-smtp-in.l.google.com.
```

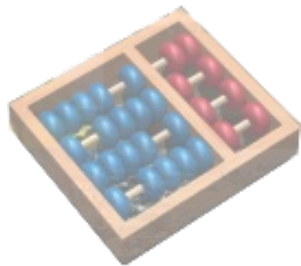


```
220 gmail-smtp-in.l.google.com ESMTP
EHLO taquaral.ic.unicamp.br
250-mx.google.com
250-SIZE 35651584
250 PIPELINING
MAIL FROM: <miguel@ic.unicamp.br>
250 2.1.0 Ok
RCPT TO: <miguel.filho@gmail.com>
250 2.1.0 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Teste
From: Miguel <miguel@ic.unicamp.br>

Esse é o corpo.
.
250 2.0.0 Ok: queued as D3F99100A4
```

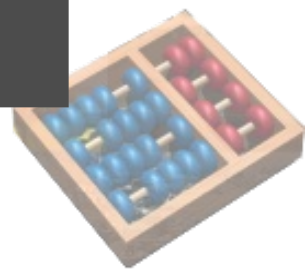


Zumbis não são educados.



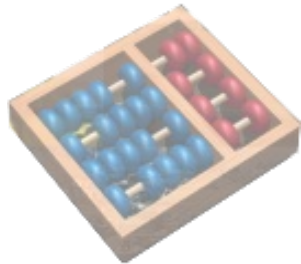
```
220 gmail-smtp-in.l.google.com ESMTP
EHLO taquaral.ic.unicamp.br
250-mx.google.com
250-SIZE 35651584
250 PIPELINING
MAIL FROM: <miguel@ic.unicamp.br>
250 2.1.0 Ok
RCPT TO: <miguel.filho@gmail.com>
250 2.1.0 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Teste
From: Miguel <miguel@ic.unicamp.br>

Esse é o corpo.
.
250 2.0.0 Ok: queued as D3F99100A4
```



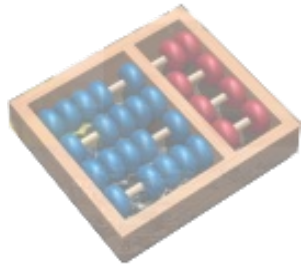
# HELO/EHLO

- “A client SMTP SHOULD start an SMTP session by issuing the EHLO  command.”
- “The argument clause contains the **fully-qualified domain name** of the SMTP client”



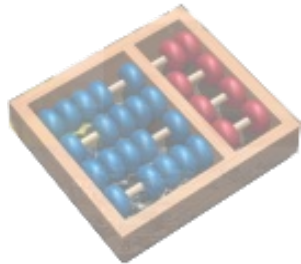
# HELO/EHLO

- “A client SMTP SHOULD start an SMTP session by issuing the EHLO  command.”
- “The argument clause contains the **fully-qualified domain name** of the SMTP client”

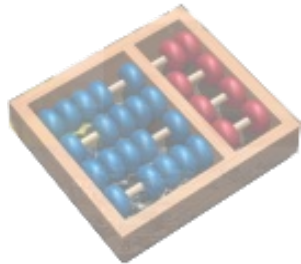


# HELO/EHLO

- Zumbis não fornecem um FQDN
  - pecezao
  - xyzjufhhjtyf
- Utilize **reject_non_fqdn_helo_hostname**

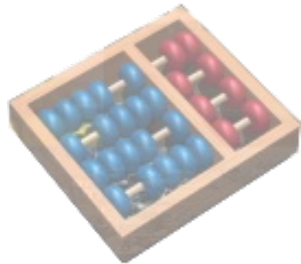


Zumbis não dizem olá de verdade.



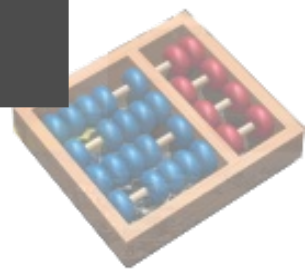
# HELO/EHLO

- FQDNs válidos e inválidos:
  - localhost
  - Seu próprio nome
- RFC não dá essa dica.



```
220 gmail-smtp-in.l.google.com ESMTP
EHLO localhost
250-mx.google.com
250-SIZE 35651584
250 PIPELINING
MAIL FROM: <miguel@ic.unicamp.br>
250 2.1.0 Ok
RCPT TO: <miguel.filho@gmail.com>
250 2.1.0 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Teste
From: Miguel <miguel@ic.unicamp.br>

Esse é o corpo.
.
250 2.0.0 Ok: queued as D3F99100A4
```

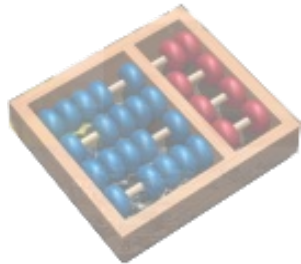


# HELO/EHLO

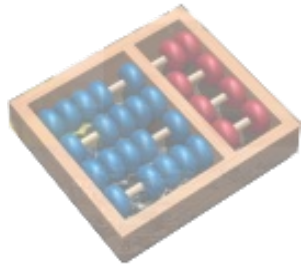
check_helo_access regexp:/etc/postfix/helo-checks.regexp

/^mx\.dominio\.br$/ REJECT You are not me

/localhost/ REJECT No, you are not localhost

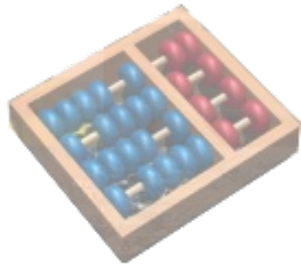


Zumbis dizem olá com um sorriso amarelo.



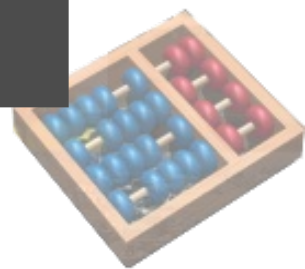
# HELO/EHLO

“In situations in which the SMTP client system does not have a meaningful domain name (e.g., when its address is dynamically allocated and no reverse mapping record is available), the client SHOULD send an address literal...”



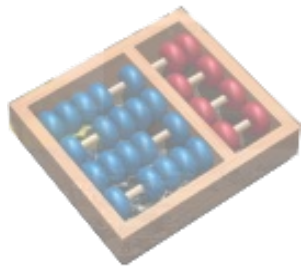
```
220 gmail-smtp-in.l.google.com ESMTP
EHLO [143.106.7.43]
250-mx.google.com
250-SIZE 35651584
250 PIPELINING
MAIL FROM: <miguel@ic.unicamp.br>
250 2.1.0 Ok
RCPT TO: <miguel.filho@gmail.com>
250 2.1.0 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Teste
From: Miguel <miguel@ic.unicamp.br>

Esse é o corpo.
.
250 2.0.0 Ok: queued as D3F99100A4
```



# HELO/EHLO

- IP literal não é utilizado na “federação”
- Zumbis é que usam IP literal
- É seguro negar esses casos

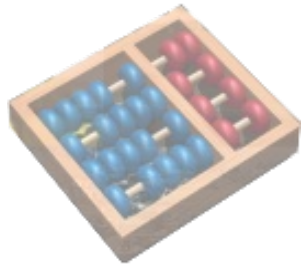


# HELO/EHLO

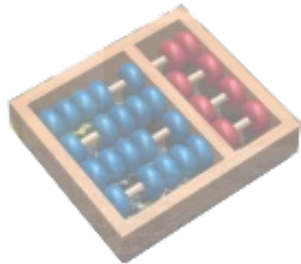
check_helo_access regexp:/etc/postfix/helo-checks.regexp

/^\[[[:digit:]\.]*\]$/ REJECT Local policy prohibits address literals in helo

/^[[:digit:]\.]*$/ REJECT Local policy prohibits IP address in helo

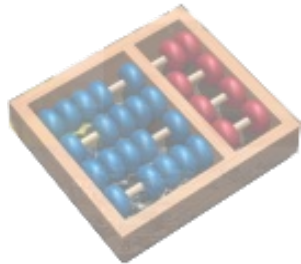


Zumbis não tem reverso.

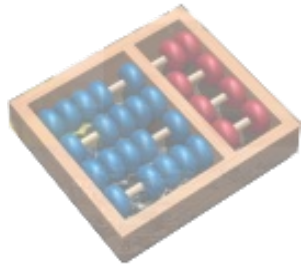


# Reverso

- RFC 1912: Common DNS Operational and Configuration Errors
- “**Make sure your PTR and A records match**. For every IP address, there should be a matching PTR record in the in-addr.arpa domain.”
- Utilize **reject_unknown_client_hostname**

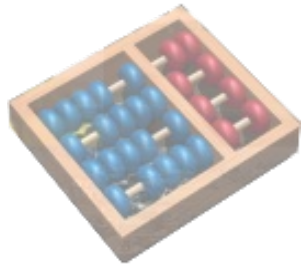


Zumbis tem muita pressa.



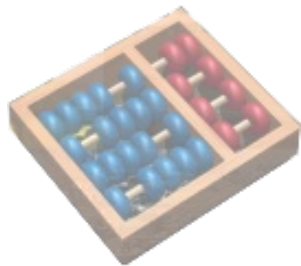
# Limitação de velocidade

- Zumbis abrem conexões loucamente
  - Mantêm muitas conexões simultâneas
  - Abrem novas conexões rapidamente
  - Tentam entregar para muitos remetentes
- Não deixe seu servidor sem limites

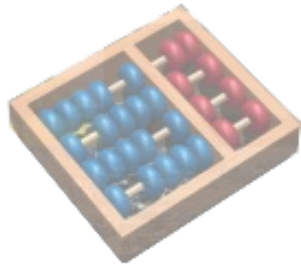


# Limitação de velocidade

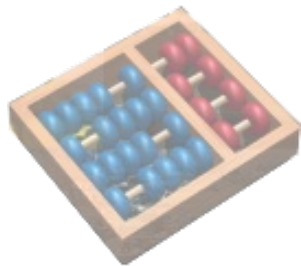
- smtpd_client_connection_rate_limit = 15
- smtpd_client_connection_count_limit = 10
- smtpd_client_message_rate_limit = 25



Zumbis não reconhecem quando erram.

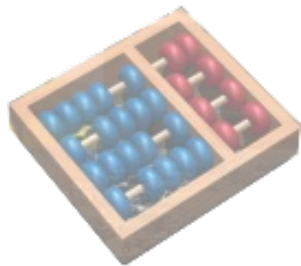


```
220 gmail-smtp-in.l.google.com ESMTP
EHLO taquaral.ic.unicamp.br
250-mx.google.com
250-SIZE 35651584
250 PIPELINING
MAIL FROM: <miguel@ic.unicamp.br>
250 2.1.0 Ok
RCPT TO: <miguel.filho@gmail.com>
450 4.7.1 Greylisting, come back latter
EHLO taquaral.ic.unicamp.br
250-mx.google.com
250-SIZE 35651584
250 PIPELINING
```



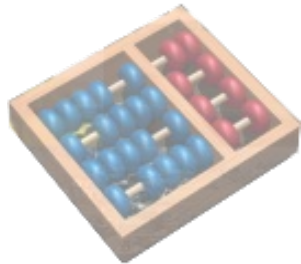
# Erros são ignorados

- Zumbis ignoram erros
  - Servidores aceitam comandos após erro (RFC autoriza)
  - Controles de velocidade podem ser irrelevantes

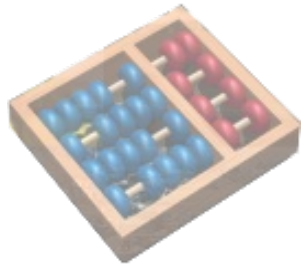


# Zumbis devem sofrer se errarem

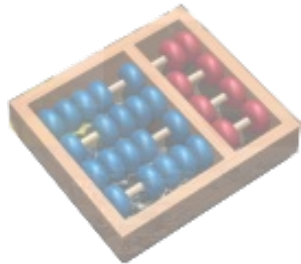
- smtpd_hard_error_limit = 3
- smtpd_soft_error_limit = 1
- smtpd_error_sleep_time = 20s



Zumbis são fracos. Eles dão reboot.

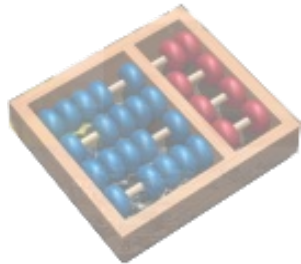


```
220 gmail-smtp-in.l.google.com ESMTP
EHLO taquaral.ic.unicamp.br
250-mx.google.com
250-SIZE 35651584
250 PIPELINING
MAIL FROM: <miguel@ic.unicamp.br>
250 2.1.0 Ok
RCPT TO: <miguel.filho@gmail.com>
450 4.7.1 Greylisting, come back latter
RSET
250 2.0.0 Ok
```



# RSET

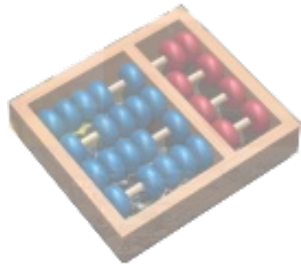
“This command specifies that the current mail transaction will be aborted.  Any stored sender, recipients, and mail data MUST be discarded, and all buffers and state tables cleared.”



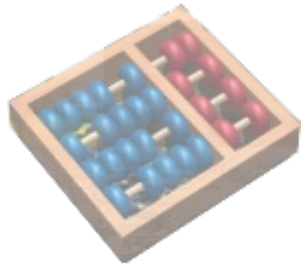
# RSET

- smtpd_junk_command_limit = 1
- smtpd_error_sleep_time = 20s

- **Colocar os zumbis para dormir é muito eficiente**

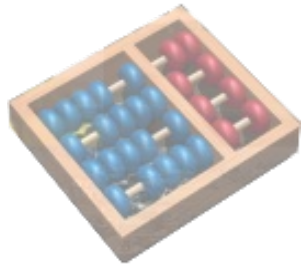


Zumbis estão na SpamHaus.

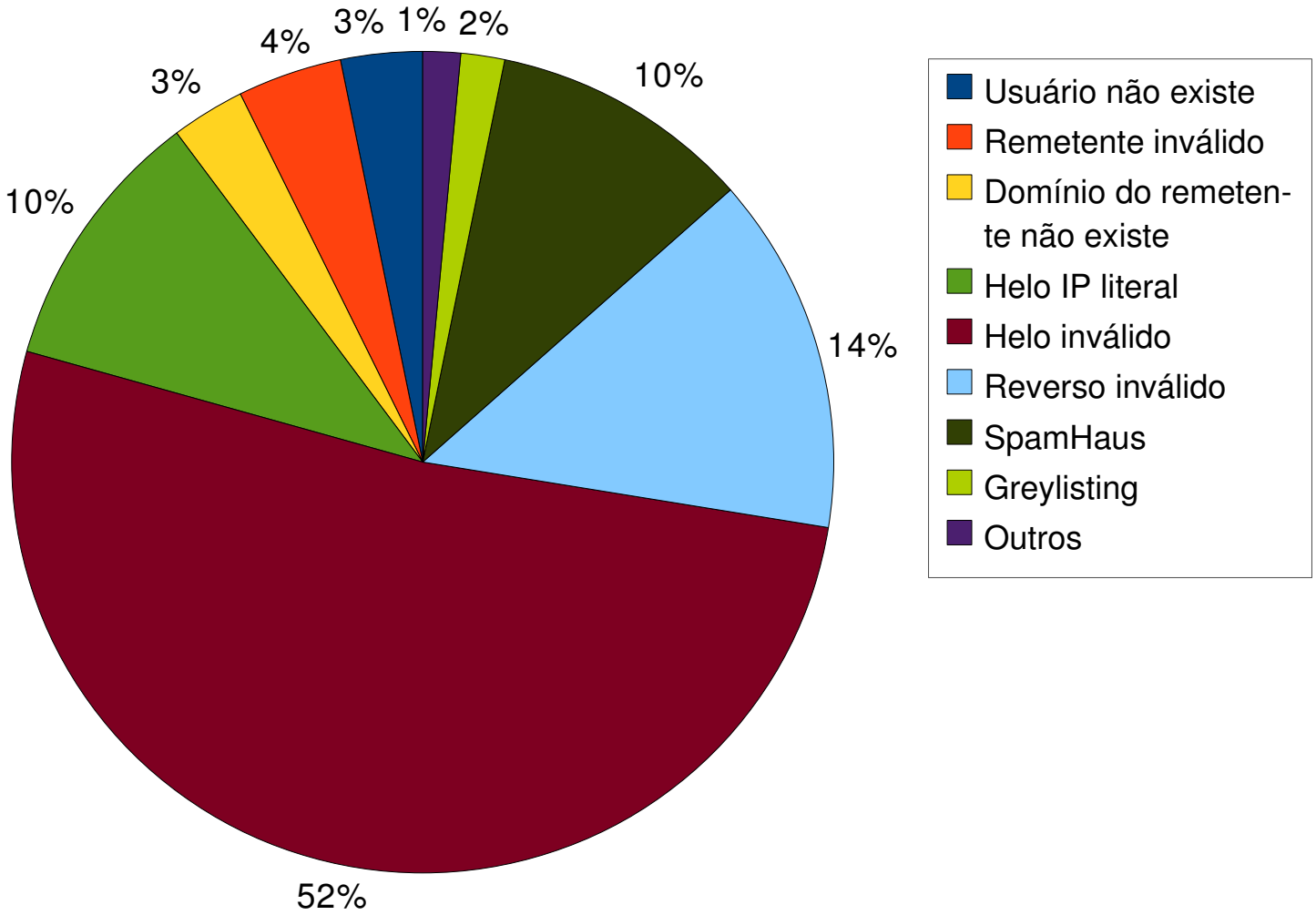


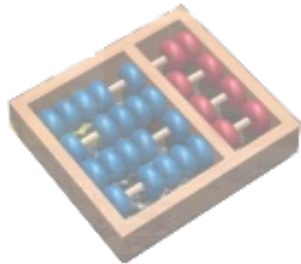
# Mais técnicas anti-spam

- Verificar se domínio remetente tem MX
  - IP público
- Potencial para falsos positivos:
  - Verificar se FQDN no EHLO/HELO existe
  - Verificar se FQDN do EHLO/HELO é o mesmo do cliente se conectando



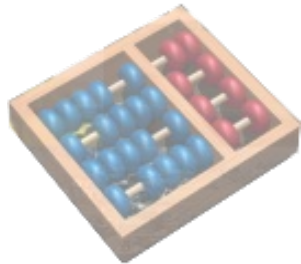
# Eficiência em números



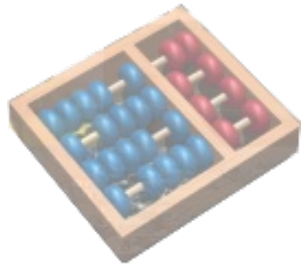



# Mais números

- ~220000 mensagens recusadas
- ~6300 desconexões depois de um RSET e outras ~6000 timeouts variados e conexões ignoradas por *rate limiting*
- ~23000 chegaram ao Amavis
  - 1425 eram spam

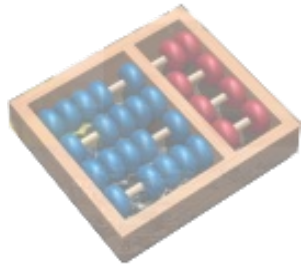


93% de lixo



# Seja um bom cidadão

- Faça seu servidor entregar mensagens com calma
  - smtp_destination_concurrency_limit = 5
  - smtp_destination_recipient_limit = 10



Obrigado!

http://www.ic.unicamp.br/~miguel