# Spam vindo de servidores Web, a nova ameaça

***Danton Nunes, Internexo Ltda.***
***danton.nunes@inexo.com.br***

## Agenda

- Técnicas anti–spam modernas: SPF e Greylisting
- Spam via servidores web: o crime perfeito?
- Pesquisa de formulários vulneráveis
- Identificando uma mensagem via web
- Contramedidas: prevenção e canja de galinha só fazem mal a esta última
- Conclusões


## Agradecimento

Este trabalho não teria acontecido se eu não tivesse que estudar para preparar um documento de recomendações anti–spam para administradores de sistemas para o CERT.br.

## Técnicas anti–spam modernas: SPF e Greylisting

### SPF

O dono de um domínio publica uma política autorizando certos endereços IP a enviar e–mail em nome do domínio.

O servidor de destino valida uma mensagem em função da política do domínio do remetente.

alvo: e–mail de open–relays, zombies, vírus.

### Greylisting

A primeira mensagem de (IP,mail_from,rcpt_to) é rejeitada com erro temporário. Depois de certo tempo passa a ser aceita sem restrição.

alvo: mensagens que não vem de MTAs verdadeiros.

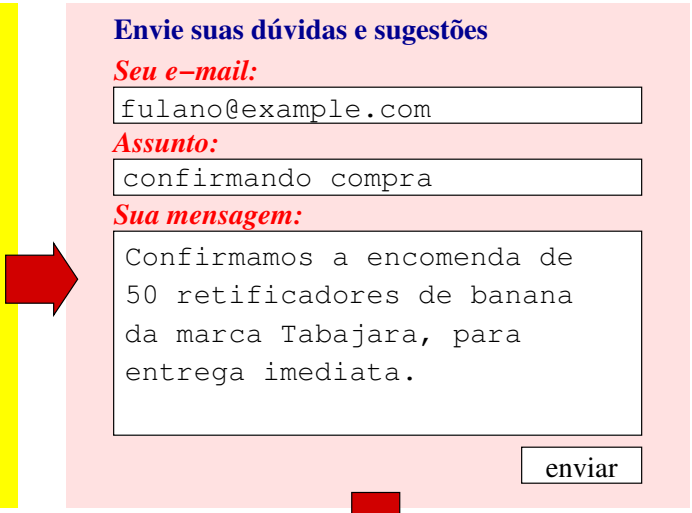
**A combinação SPF+GI é fatal para a maioria do spam "clássico".**

## Spam via servidores web: o crime perfeito?

## Funciona pelo abuso de formulários na web.

## Exemplo

```
<form action="envia.php" method="post">
<p>Envie suas dúvidas e sugestões.</p>
<p><label for="email">Seu e-mail:</label>
<input type="text" name="email" size="40" /></p>
<p><label for="assunto">Assunto:</label>
<input type="text" name="assunto" size="40" /></p>
<p><label for="mensagem">Sua mensagem:</label>
<textarea cols="40" rows="5" name="mensagem">
Escreva aqui sua mensagem.
</textarea></p>
<p><input type="submit" value="enviar" /></p>
</form>
```




```
<script language="php">
    mail($_POST['email'],$_POST['assunto'],
        $_POST['mensagem'],
        "To: faleconosco@aquimesmo.com.br\r\n".
        "Bcc: acompanhamento@aquimesmo.com.br\r\n");
</script>
```

```
From: fulano@example.com
To: faleconosco
Subject: confirmando compra

Confirmamos a encomenda de
50 retificadores de banana
da marca Tabajara, para
entrega imediata.
```

## Este é o uso normal do formulário. Porém....

## Spam via servidores web: o crime perfeito?

## ... o esquema pode ser facilmente abusado assim:

```
POST /envia.php HTTP/1.0
host: www.aquimesmo.com.br
Content-length: 4567

email%3dspammer%40metralha%2eltda%2ecom%0d%0aTo%3a%20huguinho%40
disney%2ecom%0d%0aTo%3a%20zezinho%40disney%2ecom%0d%0aTo%3a%20lu
izinho%40disney%2ecom%0d%0aTo%3a%20margarida%2epata%40hotmail%2e
com%0d%0aSubject%3a%20voc%ea%20ganhou%20na%20loteria%0d%0aConten
t%2dtype%3a%20text%2fplain%0d%0aX%2dvirus%2dscanned%3a%20amavisd
%2dnew%0d%0a%0d%0aCaro%20Pato%21%0d%0a%0d%0aVoc%ea%20ganhou%20um
%20quaquilh%e3o%20de%20d%f3lares%20da%20loteria%20de%20Pat%f3pol
is%2e%2e%2e%0d%0a%0d%0a...
```

```
email=spammer@metralha.ltda.com
To: huguinho@disney.com
To: zezinho@disney.com
To: luizinho@disney.com
To: margarida.pata@hotmail.com
Subject: você ganhou na loteria
Content-type: text/plain
X-virus-scanned: amavisd-new

Caro Pato!

Você ganhou um quaquilhão de dólares da loteria de Patópolis...
```

## adivinha para onde vai a mensagem...

**Spam via servidores web: o crime perfeito?**

**A mensagem sai como se fosse do usuário sob o qual roda o servidor web (normalmente nobody, apache, www, wwwrun).**

**A mensagem é encaminhada por um MTA legítimo, portanto resiste ao esquema de Greylisting.**

**A mensagem é enviada de um servidor normalmente autorizado a fazê–lo, portanto passa batido pelo SPF.**

**Resumo da história, não temos como nos defender desse tipo de spam com o esquema SPF+Greylisting, que até então era matador!**

**Solução: ações preventivas do lado do webserver.**

## Pesquisa de formulários vulneráveis

**Assim como antigamente os spammers procuravam por open relays atualmente há ferramentas de busca por formulários vulneráveis.**

**Sintoma: mensagens muito estranhas, como esta:**

```
nome="have415@inexo.com.br"
cidade="miller
Content-Type: multipart/mixed; boundary=\"2b598ec4d5259637104d3854b3418853\"
MIME-Version: 1.0
Subject: myself. e looks at his watch. t s
bcc: beacon5919@aol.com

This is a multi-part message in MIME format.

--2b598ec4d5259637104d3854b3418853
Content-Type: text/html; charset=\"us-ascii\"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

down to the girl who tended
--2b598ec4d5259637104d3854b3418853--

.
"
cep="have415@inexo.com.br"
```

**nota–se a tentativa de explorar o campo ’cidade’. Se o formulário for vulnerável, beacon5919@aol.com receberá uma mensagem.**

## Identificando uma mensagem via web

```
Return-Path: <apache@ds80-237-200-81.dedicated.hosteurope.de>
Delivered-To: inexo-inexo-danton.nunes@inexo.com.br
Received: (qmail 21092 invoked by uid 1000); 11 Mar 2005 02:49:22 -0000
Delivered-To: inexo-inexo-danton@inexo.com.br
Received: (qmail 21089 invoked from network); 11 Mar 2005 02:49:21 -0000
Received: from jam.seppenra.de (HELO
    ds80-237-200-81.dedicated.hosteurope.de) (80.237.200.81)
    by newquantum.inexo.com.br with SMTP; 11 Mar 2005 02:49:21 -0000
Received-SPF: none (newquantum.inexo.com.br: domain at
    ds80-237-200-81.dedicated.hosteurope.de does not designate permitted
    sender hosts)
Received: by ds80-237-200-81.dedicated.hosteurope.de (Postfix,
    from userid 1004)
    id 08AC3336DBA; Fri, 11 Mar 2005 01:24:20 +0100 (CET)
To: danton@inexo.com.br
Subject: Symantec Informa
From: symantec@symantec.com
content-type: text/html
X-priority: 1
```

típico usuário do Apache

um Received local ou na mesma rede

**Contramedidas: prevenção e canja de galinha só fazem mal a esta última**

**A prevenção a este tipo de spam é mais efetiva do lado do servidor web**

**Ações:**

- **Programação defensiva: não confiar em qualquer dado de fora.**
  - **depende da boa vontade dos programadores de scripts.**
  - **deveria ser prática comum de programação, mas não é.**

- **Uso de agentes de submissão especiais.**
  - **"wrappers" para o MSA regular, p.ex. simulador de qmail–inject, que só passam adiante mensagens em que destinatários se encontrem em uma lista administrada.**

- **Auditoria de código executável pelo servidor web (complicado)**

- **Log, log, log...**

## Conclusões

**Spam enviado por servidores web está na moda e representa um novo desafio para administradores de e–mail e de web.**

**Consegue passar ileso por SPF e Greylisting, até então as técnicas mais efetivas contra o spam convencional.**

**Baseia–se em scripts CGI (php, asp, perl, etc.) que não fazem crítica dos dados enviados pelo usuário.**

**Métodos de prevenção são mais efetivos do lado do servidor web: programação defensiva, MSAs especiais, etc.**

**Probes para identificar formulários vulneráveis estão à solta!**

**É uma reação adaptativa dos spammers!**