

Como tratar SPAM em servidores cPanel



Esse artigo tem como objetivo fornecer um melhor entendimento sobre os incidentes de e-mails causados por SPAM, ou comprometimentos de e-mails.

Nele iremos abordar de forma segmentada uma das metodologias de "troubleshooting" para o caso.

1

Inicialmente precisaremos verificar se há indícios de SPAM em nosso servidor, uma excelente forma de avaliar é através a fila de e-mails, quase sempre em caso de SPAMs poderemos ver vários e-mails de um mesmo remetente congelados na fila, além disso podemos checar o conteúdo da mensagem em questão.

Podemos listar as mensagens presas na fila e ordená-las com o seguinte comando através do acesso SSH ao servidor:

```
exim -bp | grep "<*>" | awk {'print $4'} | sort | uniq -c | sort -n
```

Podemos também acompanhar a fila através da interface do WHM indo em **"Mail Queue Manager"**, aqui podemos também implementar vários filtros na pesquisa.

Enter dates as: Month, day of month, year. For example, 1 April 2007 will be "4/1/2007".

Mail Queue Manager

Select Query

Search Type:

☒ Begins With

☐ Exact

☐ Partial

Start Date:

4/29/2021

End Date:

6/30/2021

Start Time:

03:05 AM

End Time:

03:05 AM

Run Re

The search matches 91 records.

Go

Deliver Selected Delete Selected Deliver All De

Podemos ver o conteúdo das mensagens utilizando o seu ID, assim poderemos procurar por indícios de conteúdos maliciosos, podemos realizar essa atividade através da linha de comando da seguinte forma:

Primeiro iremos filtrar com o grep a conta na qual queremos saber os IDs de suas mensagens, ou seja, a conta que suspeitamos que está enviando SPAM.

```
exim -bp | grep conta@dominioexemplo.com.br
```

A saída deve ser algo similar ao que podemos ver abaixo:

```
52h 1.7K 1lxVOI-0066Pc-89 <conta@dominioexemplo.com.br>
52h 5.0K 1lxVOY-0066Pc-90 <conta@dominioexemplo.com.br>
52h 1.2K 1lxVOq-0066Pc-PZ <conta@dominioexemplo.com.br>
52h 5.0K 1lxVP0-0066Pc-BB <conta@dominioexemplo.com.br>
52h 1.2K 1lxVP7-0066Pc-Dq <conta@dominioexemplo.com.br>
52h 1.6K 1lxVPD-0066Pc-BJ <conta@dominioexemplo.com.br>
52h 1.7K 1lxVPN-0066Pc-F4 <conta@dominioexemplo.com.br>
52h 1.4K 1lxVPT-0066Pc-Dv <conta@dominioexemplo.com.br>
45h 1.4K 1lxbjX-0085tn-EL <conta@dominioexemplo.com.br>
38h 1.3K 1lxiZb-0065kc-Cn <conta@dominioexemplo.com.br>
```

Agora que possuímos o ID da mensagem podemos verificar o seu conteúdo, utilizaremos novamente o comando `exim`, agora com os parâmetros `M`, `v` e `h`, com eles poderemos verificar o cabeçalho da mensagem:

```
exim -Mvh 1lxVOY-0066Pc-90
```

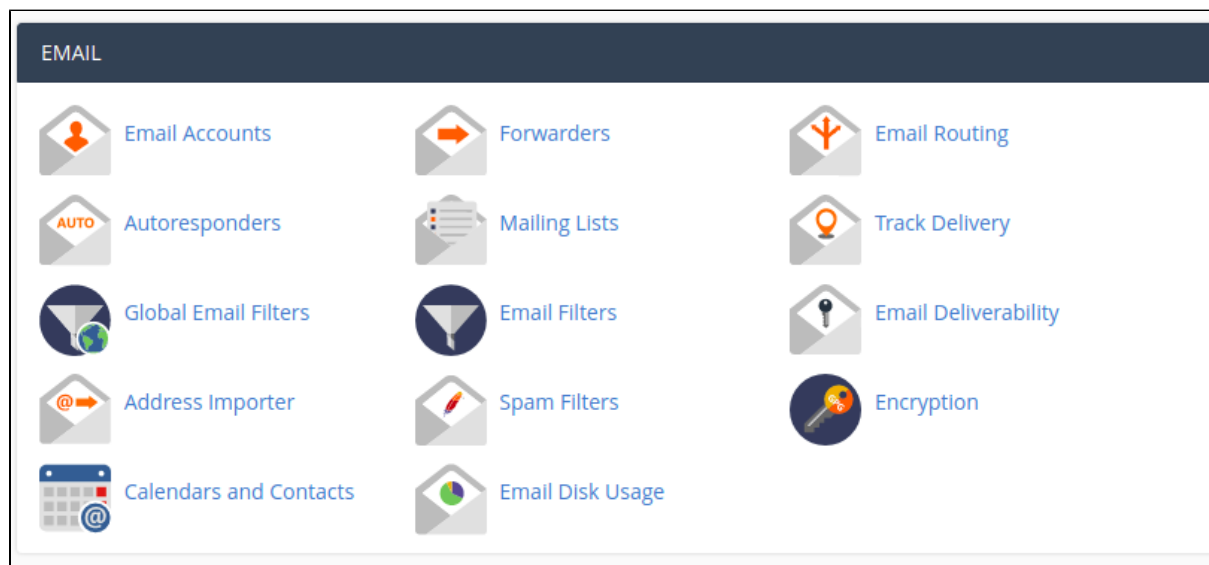
Vamos analisar a saída do comando que executamos acima:

```
291P Received: from 1.red-0-168-192.example.host-com.br ([192.168.0.1]:53234 helo=[127.0.0.1])
  by rbr46.dizinc.com with esmtpsa (TLS) tls TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  (Exim 4.94.2)
  (envelope-from <conta@dominioexemplo.com.br>)
  id 1lxVOY-0066Pc-90; Sun, 27 Jun 2021 11:04:22 -0300
038 Date: Sun, 27 Jun 2021 16:04:31 +0200
079 Subject: Most significant deal on prescription medicationsworking in your body
070I Message-ID: <th9fy8h232l5tle1t6srkylf.1439221883483@sofaprime.com.br>
053F From: "CANADIAN PHARNACY" <conta@dominioexemplo.com.br>
```

Acima podemos ver nos campos **"Subject"** e **"From"** evidências claras de que trata-se de um disparo de SPAM, podemos fazer as mesmas verificações também pela interface do WHM no **"Mail Queue Manager"**, para vermos mais detalhes da mensagem, basta que cliquemos na lupa localizada no canto direito.

2

O próximo passo é tratar o incidente, agora devemos redefinir a senha da conta afetada e então seguir com a limpeza da fila, podemos redefinir a senha através do cPanel relativo ao domínio da conta, iremos em **"E-mail >> E-mail Accounts >> Localizaremos a conta e iremos em Manage ou gerenciar no canto direito >> Vamos agora em Nova senha e por fim em Update Mail Settings"**



Após isso reiniciaremos o serviço de autenticação do cPanel através do WHM, iremos em **"Restart Services >> IMAP Server"** e então em **"Restart Services >> Mail Server (Exim)"**.

Por fim limparemos a nossa fila de e-mails, podemos realizar o procedimento utilizando a linha de comando da seguinte forma:

```
exim -bp | exiqgrep -i | xargs exim -Mrm
```

Podemos realizar a limpeza através da interface do WHM em **"Mail Queue Manager"**. Após finalizada iremos acompanhar novamente a fila, caso após alguns minutos não tenha novas incidências poderemos seguir para o próximo passo, caso ainda existam novas incidências é possível que o envio partindo da conta possa vir de um script, ou partir de um abuso relativo a uma aplicação, como por exemplo, enviar e-mails em massa através de um formulário de contato desprotegido de um site. Conseguiremos verificar o caso em mais detalhes investigando o arquivo de log **"/var/log/exim_mainlog"**, filtraremos pela conta que desejamos investigar, seguiremos como no exemplo:

```
grep conta@dominioexemplo.com.br /var/log/exim_mainlog
```

Em adição, podemos utilizar a interface para verificações dos logs no WHM, basta ir em "**ConfigServer Security & Firewall >> Search System Logs**"

Firewall Status: Enabled and Running

WARNING: RESTRICT_SYSLOG is disabled. See SECURITY WARNING in Firewall Configur

AllInfocsfIldOther

Server Information

Check Server Security	Perform a basic security, stability and settings check on the server
Firewall Information	View the csf+Ild readme.txt file
Watch System Logs	Watch (tail) various system log files (listed in csf.syslogs)
Search System Logs	Search (grep) various system log files (listed in csf.syslogs)

Agora basta escolhermos o log desejado e a conta que iremos filtrar:

 ConfigServer Security & Firewall - csf v14.10

Log: /var/log/exim_mainlog (196401 kb) ▼

Text: conta@dominioexemplo.com.br ☐ -I ☐ -E ☐ wildcard

Search

Procure pelo campo cwd, nele teremos uma ideia de onde está partindo o script ou o abuso, identificaríamos algo similar ao exemplo abaixo, leremos "exemplo", como o nome da conta cPanel:

```
cwd=/home/exmplo/public_html
```


No caso acima, é bem provável que a aplicação web da conta "exemplo", por exemplo o site hospedado na conta, está sendo utilizado para disparar SPAM, caso a conta possua um formulário desprotegido, provavelmente ele é a raiz do problema, nesse caso iremos adicionar um CAPTCHA ao formulário e problema deve ser sanado. Agora acompanharemos a fila de e-mails novamente e confirmaremos que o disparo de fato cessou.

Delist Sorbs

sorbs.net/cgi-bin/support

Seguiremos a mesma lógica para outras RBLs, infelizmente algumas não possuem formulários, nesse caso é necessário aguardar que a listagem se desfaça com o tempo.


Esses são os passos padrões para identificar problemas relacionados a listagens, caso possua quaisquer outras dúvidas, entre em contato com o nosso [Suporte Técnico](#).

 Este artigo te ajudou?

Your Rating:

Results:

3 rates

 Ainda precisa de ajuda?

ABRIR UM CHAMADO