Последнее время активизировался спам с поддельным полем From. Если на вашем сервере не настроены различные ограничения по приему почты, то это может стать проблемой. Я обычно настраиваю ограничения с помощью стандартных restrictions в postfix. Но вот с подделкой поля from упустил момент, сейчас исправлю.

Сподвигло меня к разбору этой ситуации огромное количество спама примерно следующего содержания:

```
I greet you!

I have bad news for you.
06/28/2018 - on this day I hacked your operating system and got full access to your account eme@eme.ru
On that day your account (eme@eme.ru) password was: gyhbtj5pq6b

It is useless to change the password, my malware intercepts it every time.

How it was:
In the software of the router to which you were connected that day, there was a vulnerability.
I first hacked this router and placed my malicious code on it.
When you entered in the Internet, my trojan was installed on the operating system of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone
numbers and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a small amount of money to unlock.
```

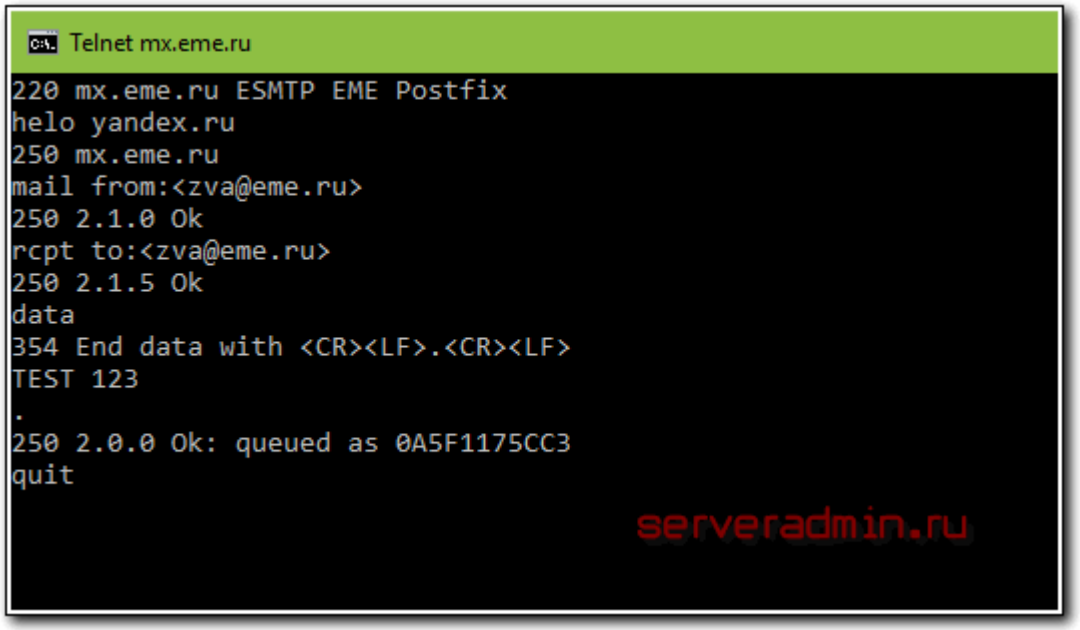
```
But I looked at the sites that you regularly visit, and came to the big delight of your favorite resources.
I'm talking about sites for adults.

I want to say - you are a big pervert. You have unbridled fantasy!

After that, an idea came to my mind.
I made a screenshot of the intimate website where you have fun (you know what it is about, right?).
After that, I took off your joys (using the camera of your device). It turned out beautifully, do not hesitate.

I am strongly belive that you would not like to show these pictures to your relatives, friends or colleagues.
I think $971 is a very small amount for my silence.
Besides, I spent a lot of time on you!

I accept money only in Bitcoins.
My BTC wallet: 15ZHnf1MPn6ybb8yUeAoCQ1AJtiKhg3NrP

You do not know how to replenish a Bitcoin wallet?
In any search engine write "how to send money to btc wallet".
It's easier than send money to a credit card!

For payment you have a little more than two days (exactly 50 hours).
Do not worry, the timer will start at the moment when you open this letter. Yes, yes .. it has already started!

After payment, my virus and dirty photos with you self-destruct automatically.
Narrative, if I do not receive the specified amount from you, then your device will be blocked, and all your contacts
will receive a photos with your "joys".

I want you to be prudent.
- Do not try to find and destroy my virus! (All your data is already uploaded to a remote server)
- Do not try to contact me (this is not feasible, I sent you an email from your account)
- Various security services will not help you; formatting a disk or destroying a device will not help either, since your
data is already on a remote server.
```

```
P.S. I guarantee you that I will not disturb you again after payment, as you are not my single victim.
 This is a hacker code of honor.

From now on, I advise you to use good antiviruses and update them regularly (several times a day)!

Don't be mad at me, everyone has their own work.
Farewell.
```

Смысл письма в том, что человек якобы взломал ваш компьютер и следил за вами. Наследил там чего-то важного по посещаемым сайтам и через веб камеру и теперь грозится это обнародовать. Расчет на то, как я понял, что человек по порнографическим сайтам лазил. Для убедительности, в письме приложен пароль, взятый из какой-то публичной базы данных слитых учеток. Сейчас таких баз полно. Пароли могут быть реальными!!! Один человек сказал, что знает этот свой пароль, но только он не от почты, а использовался на сайте booking.com.

В письме используется поддельный адрес From, для того, чтобы письмо выглядело якобы отправленное с вашей учетки, что должно подтверждать реальность угроз. В общем, подход системный получился. Конечно, все это подделка и развод. Я решил сберечь нервы пользователей и каким-то образом оградить людей от подобных писем. С помощью postfix это сделать очень просто. Базовые методы борьбы со спамом я уже подробно расписывал в отдельном разделе в статье по настройке postfix. Но текущая ситуация там не учитывается. Сейчас исправим это.

Для начала давайте проверим, реально ли на ваш почтовый сервер отправить письмо с поддельным полем From. Для этого подключимся к нему по Telnet и попробуем вручную выполнить отправку.



Список команд, которые я вводил:

```
telnet mx.eme.ru 25
helo yandex.ru
mail from:<zva@eme.ru>
rcpt to:<zva@eme.ru>
data
Test
.
quit
```

Я использовал поддельные данные в поле helo, представившись yandex.ru и дальше отправил тестовое письмо. Сервер его принял и успешно доставил в ящик. Вот исходный текст этого письма.

```
Return-Path: <zva@eme.ru>
Delivered-To: zva@eme.ru
Received: from yandex.ru (broadband-7[redacted]u [[redacted]])
    by mx.eme.ru (Postfix) with SMTP id 0A5F1175CC3
    for <zva@eme.ru>; Wed,  7 Nov 2018 17:56:38 +0300 (MSK)
Message-Id: <20181107145649.0A5F1175CC3@mx.eme.ru>
Date: Wed,  7 Nov 2018 17:56:38 +0300 (MSK)
From: zva@eme.ru
X-KLMS-Rule-ID: 3
X-KLMS-Message-Action: skipped
X-KLMS-AntiSpam-Status: not scanned, whitelist
X-KLMS-AntiPhishing: not scanned, whitelist
X-KLMS-AntiVirus: Kaspersky Security 8.0 for Linux Mail Server, version 8.0.1.721, not scanned, whitelist

TEST 123
```


Обратите внимание, что используется антиспам Kaspersky Security 8.0 for Linux Mail Server. Но у него настроен белый список на адреса исходного домена. Получается, что антивирус так же проверяет поле From, которое подделано, и не защищает пользователей от таких писем.

Для того, чтобы запретить отправку писем с левых почтовых серверов, которые ставят в поле From наш домен, необходимо добавить еще одну проверку в раздел **smtpd_sender_restrictions** следующим образом:

```
smtpd_sender_restrictions =     permit_mynetworks,
                                permit_sasl_authenticated,
                                reject_authenticated_sender_login_mismatch,
```

```
                                reject_unknown_sender_domain,
                                reject_non_fqdn_sender,
                                reject_unlisted_sender,
                                reject_unauth_destination,
                                check_sender_access hash:/etc/postfix/sender_access
```

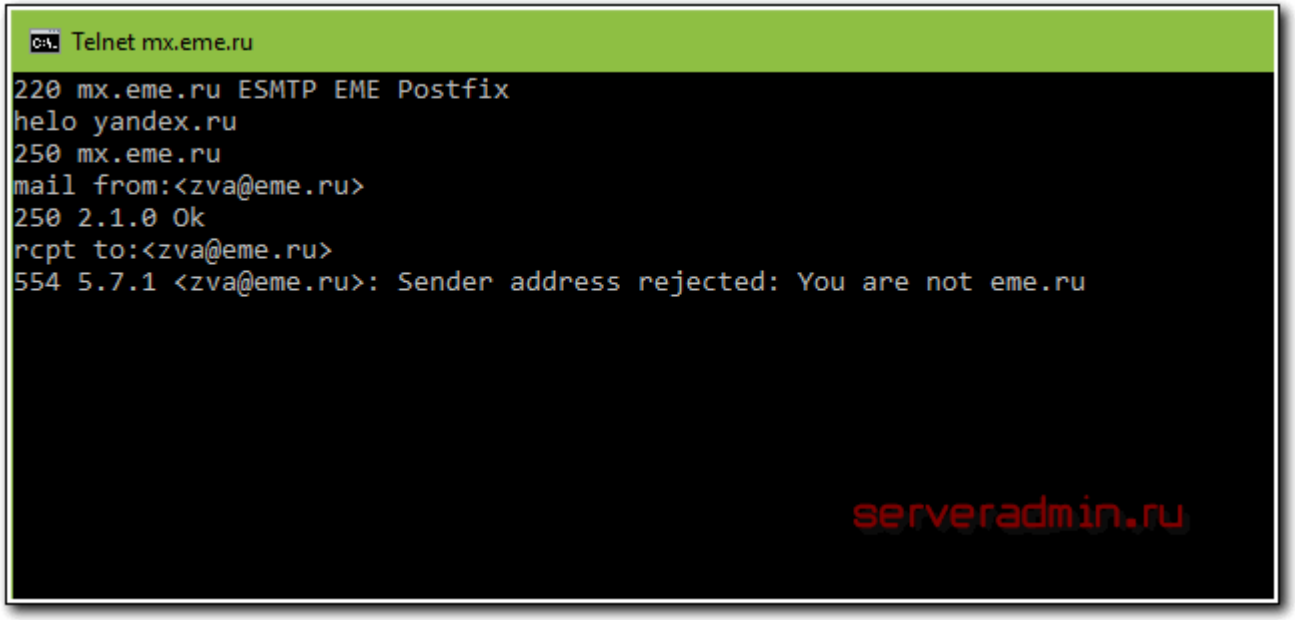
К существующим ограничениям я добавил еще одно в самый конец. Создадим указанный файл sender_access со следующим содержимым.

```
# mcedit /etc/postfix/sender_access
eme.ru REJECT You are not eme.ru
# postmap /etc/postfix/sender_access
```

Всем, кто захочет отправить нам письмо с доменом нашего сервера, мы будем выдавать ошибку и отвечать, что вы это не мы :) Перечитываем конфигурацию postfix:

```
# postfix reload
```

Теперь попробуем еще раз через telnet отправить письмо с полем From из нашего домена.



Сервер выдал ошибку 554. В логе почтового сервера будет следующая строка:

```
Nov  7 17:59:45 ememail postfix/smtpd[17430]: NOQUEUE: reject: RCPT from broadband: 554 5.7.1 <zva@eme.ru>: Sender
address rejected: You are not eme.ru; from=<zva@eme.ru> to=<zva@eme.ru> proto=SMTP helo=yandex.ru
```

Все, больше ни один отправитель не сможет использовать в поле From наш домен. Вообще странно, что изначально это возможно. Протокол smtp давно пора как-то изменить, чтобы раз и навсегда защитить его от спама. На него нагородили уже столько костылей, но ничего не помогает.

Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!