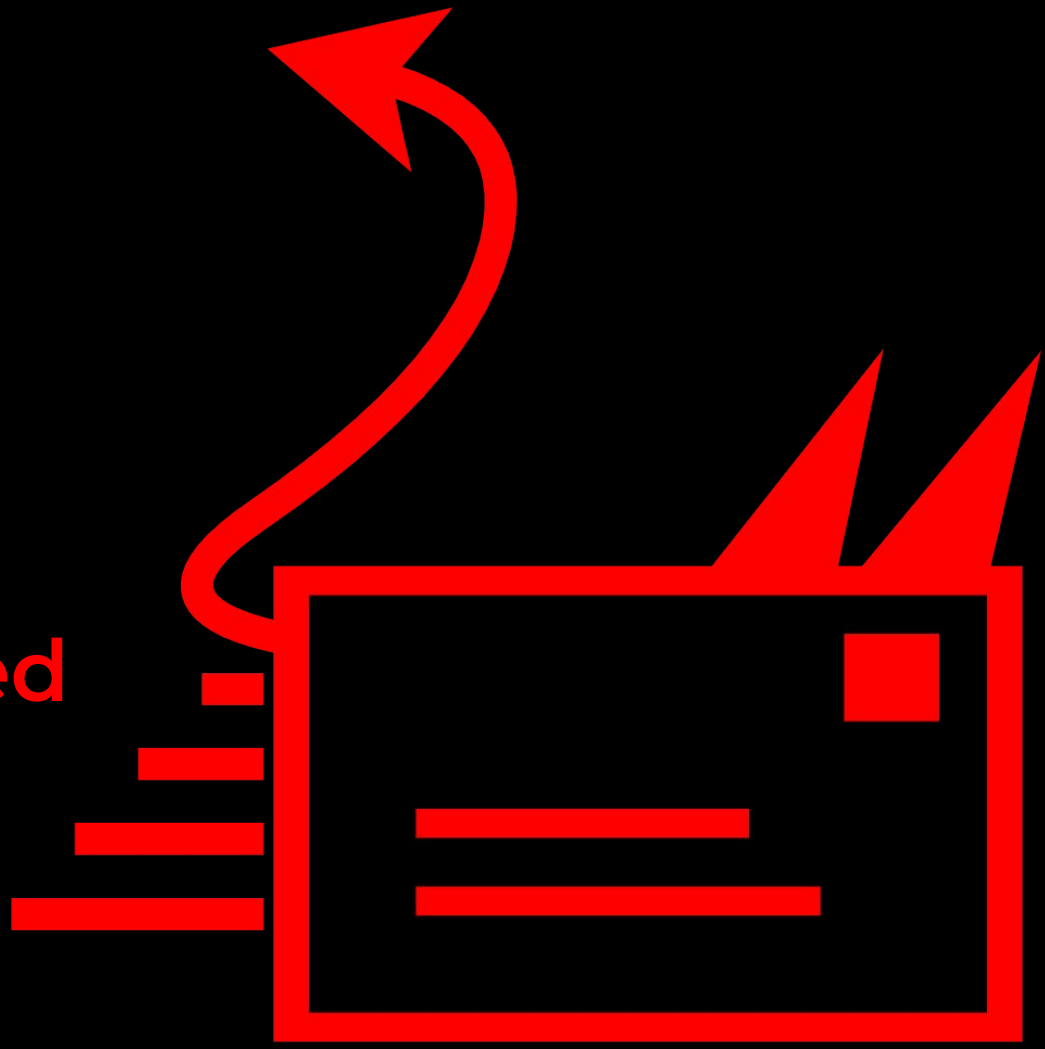
SEC Consult

an Eviden business

SMTP Smuggling Revisited

Still Smuggling Emails Worldwide?!



Timo Longin

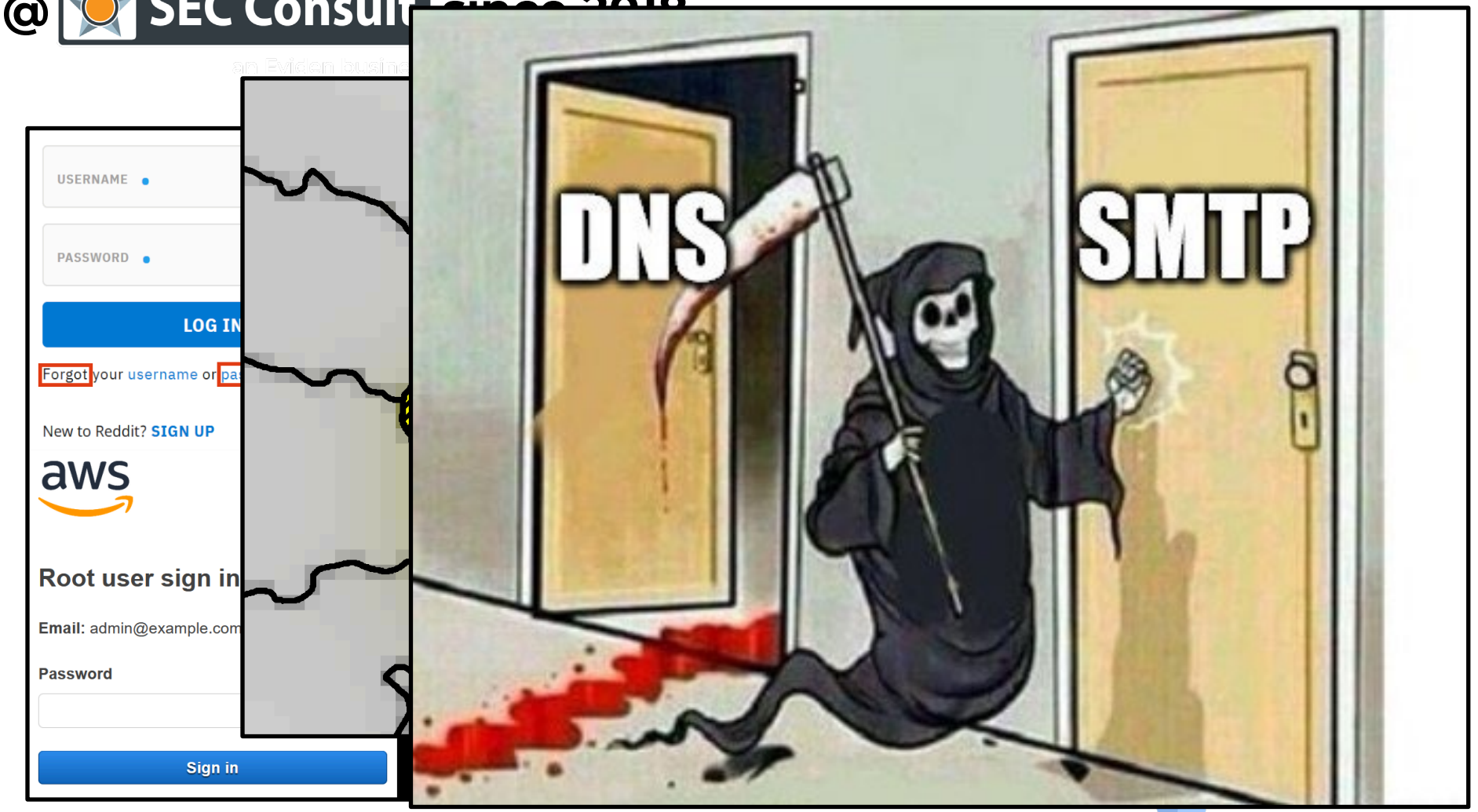
SMTP What?

SMTP Smuggling – A (once) novel technique for spoofing e-mails

PortSwigger Top 10 Web Hacking Techniques of 2023

$whoami

@ SEC Consult since 2018



Timo Longin

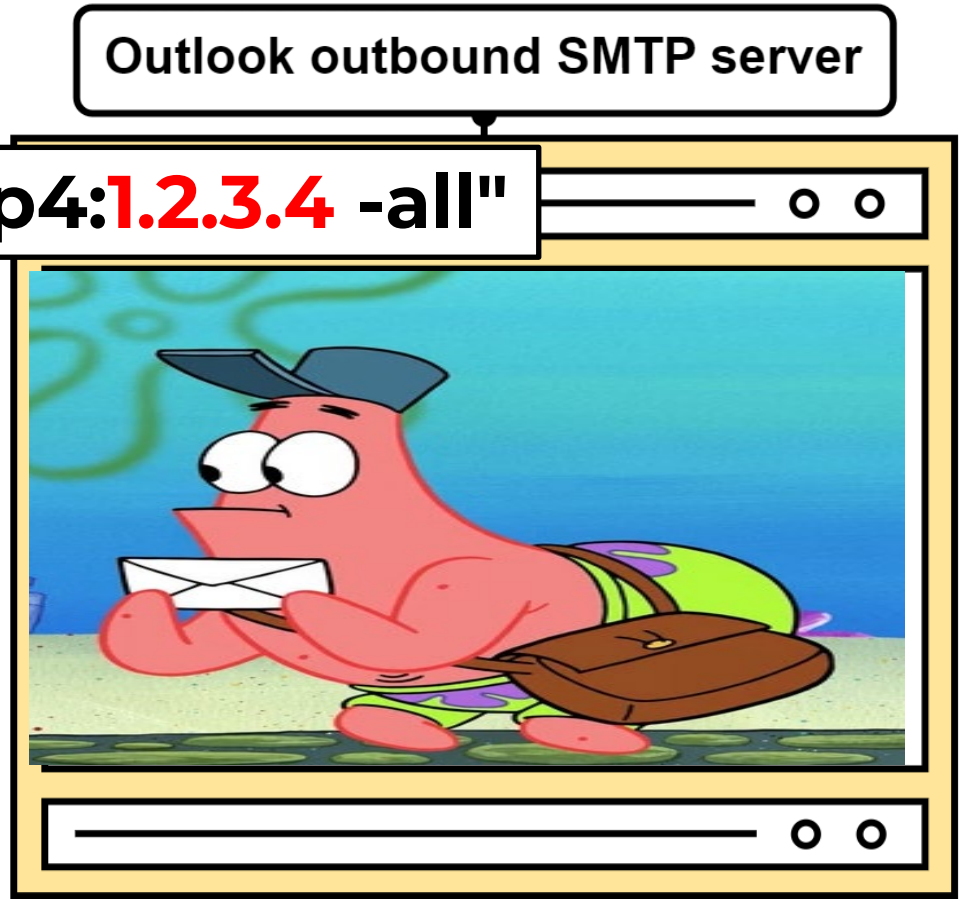
@login@infosec.exchange
@timolongin
Timo Longin @ LinkedIn

The Basics

SMTP Infrastructure

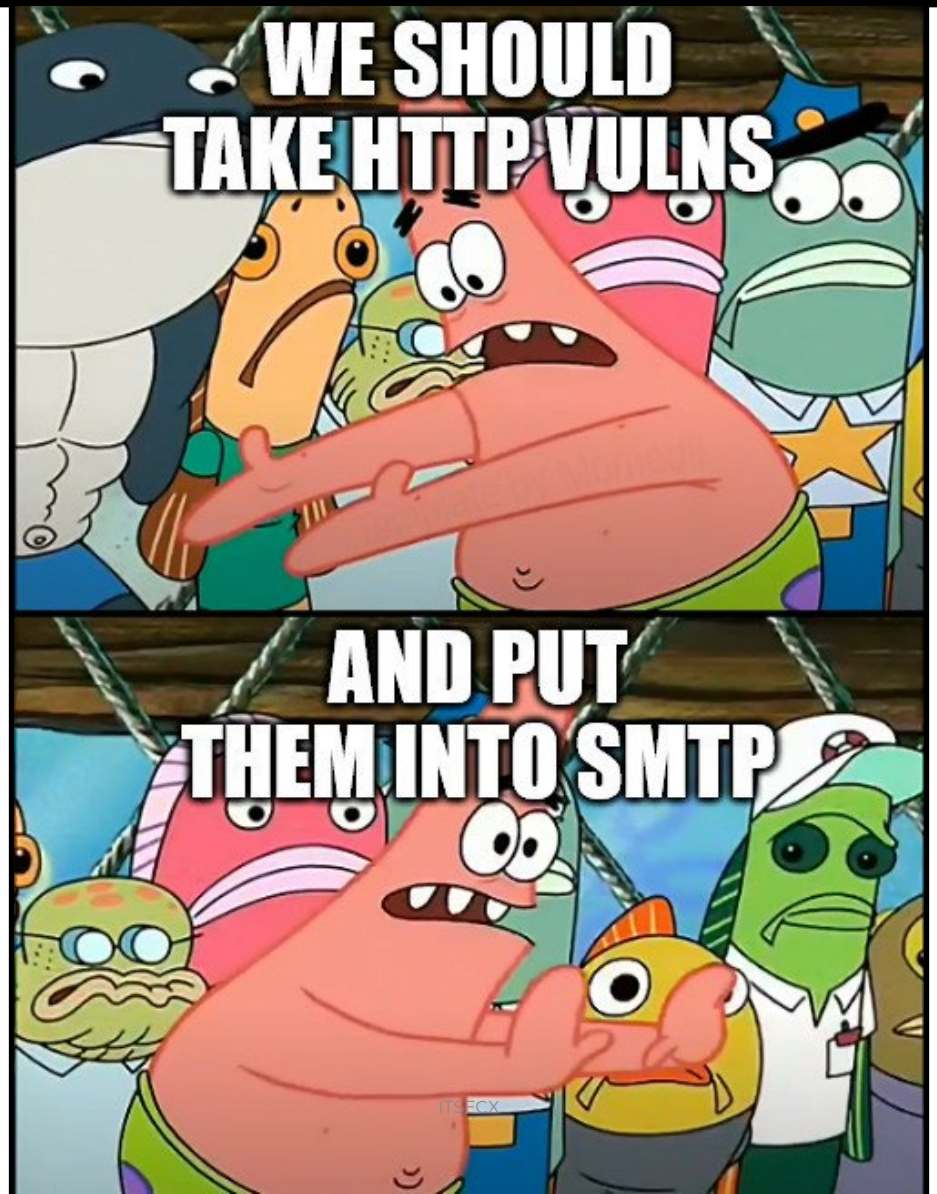
outlook.com IN TXT "v=spf1 ip4:1.2.3.4 -all"

smtp-mail.outlook.com
TCP/587



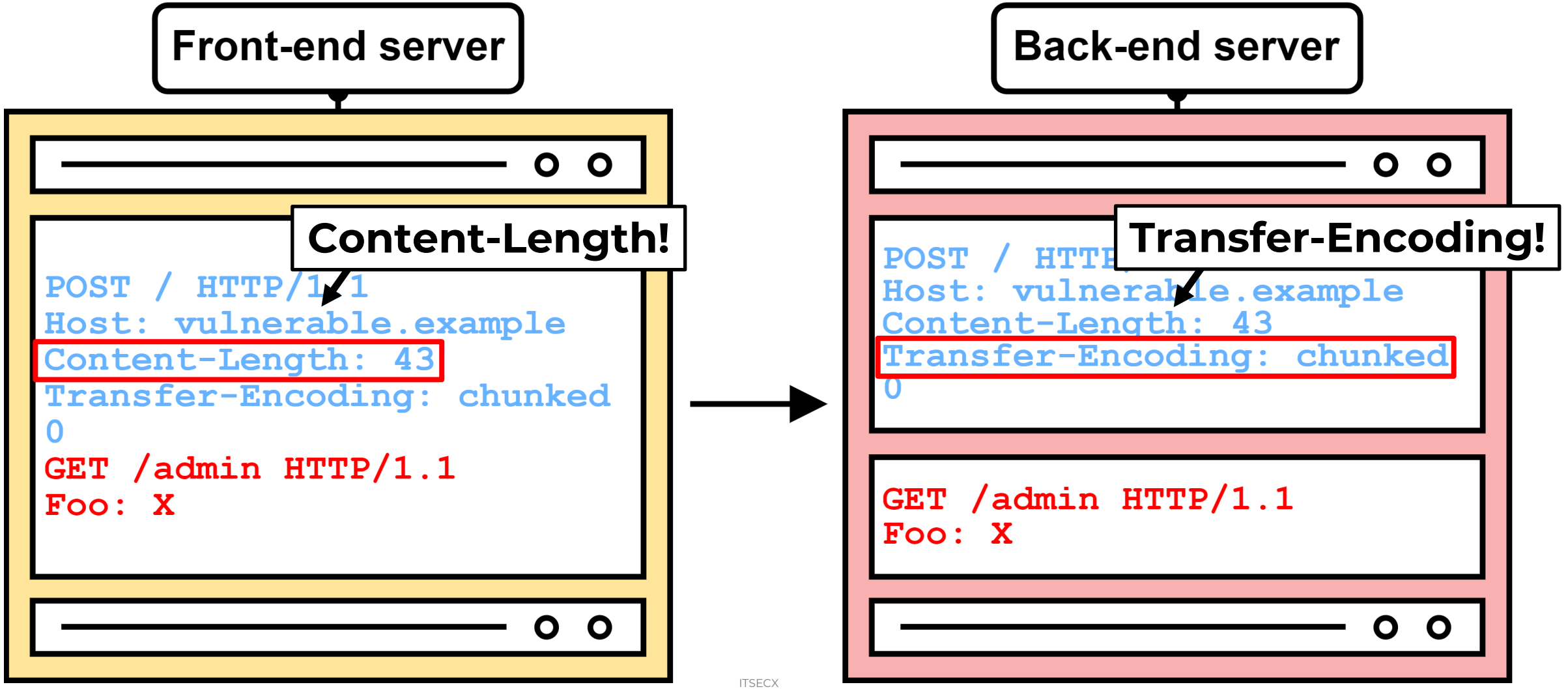
SMTP Smuggling Theory

From HTTP to SMTP



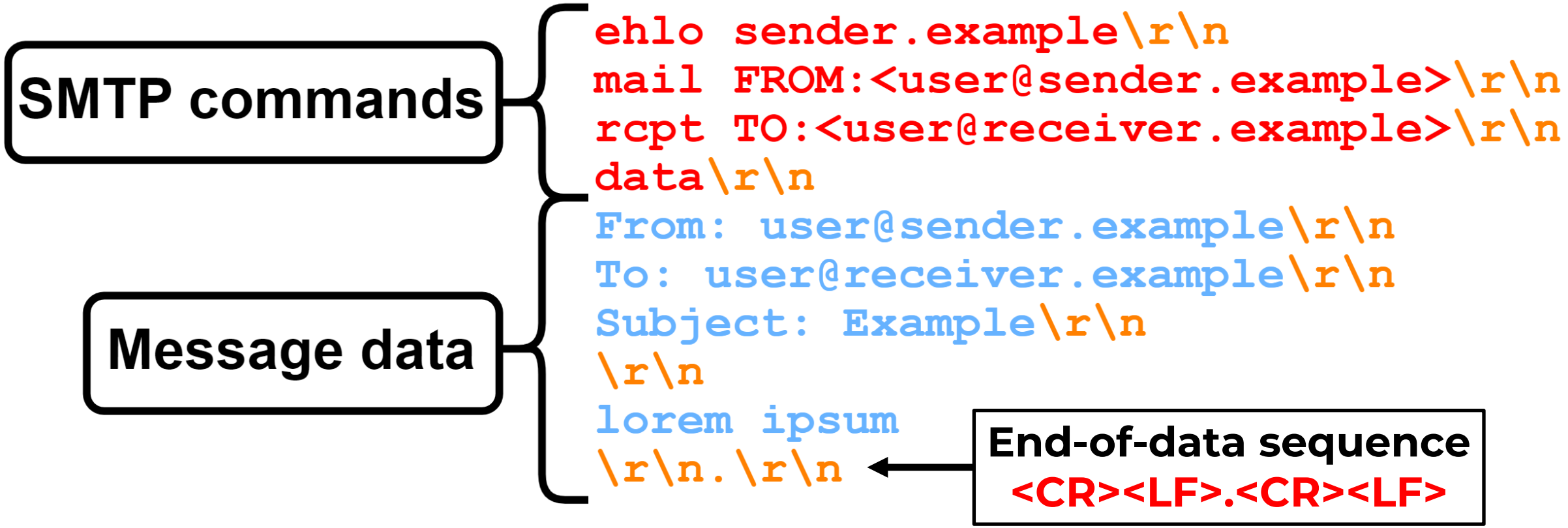
SMTP Smuggling Theory

HTTP Request Smuggling



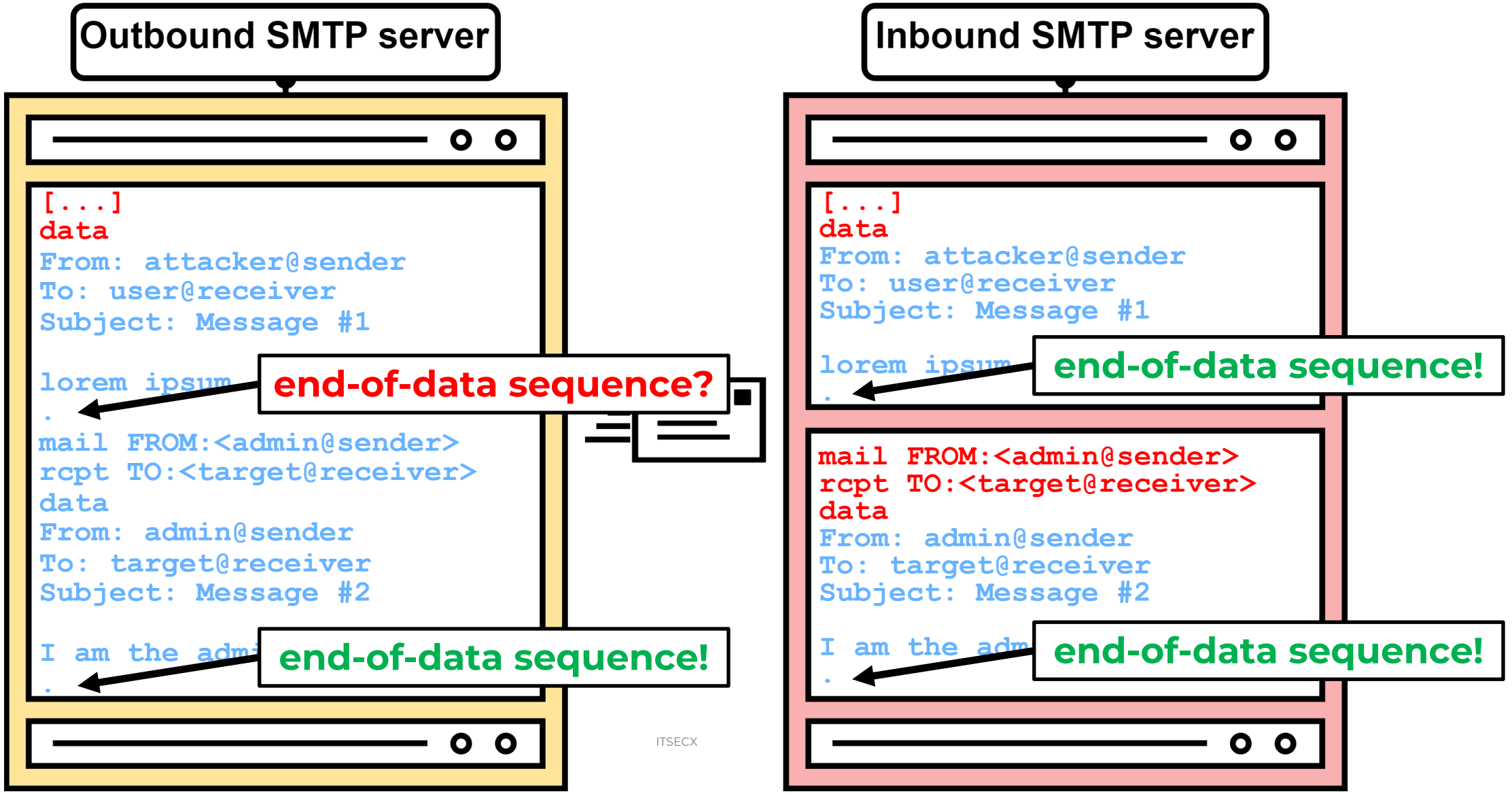
SMTP Smuggling Theory

SMTP Protocol



SMTP Smuggling Theory

SMTP Smuggling?



SMTP Smuggling

<CR><LF>.<CR><LF> is a lie?

Server responses:

250 End data with <CR><LF>.<CR><LF>

250 Start mail input; end with <CRLF>.<CRLF>

250 Send data ending with <CRLF>.<CRLF>

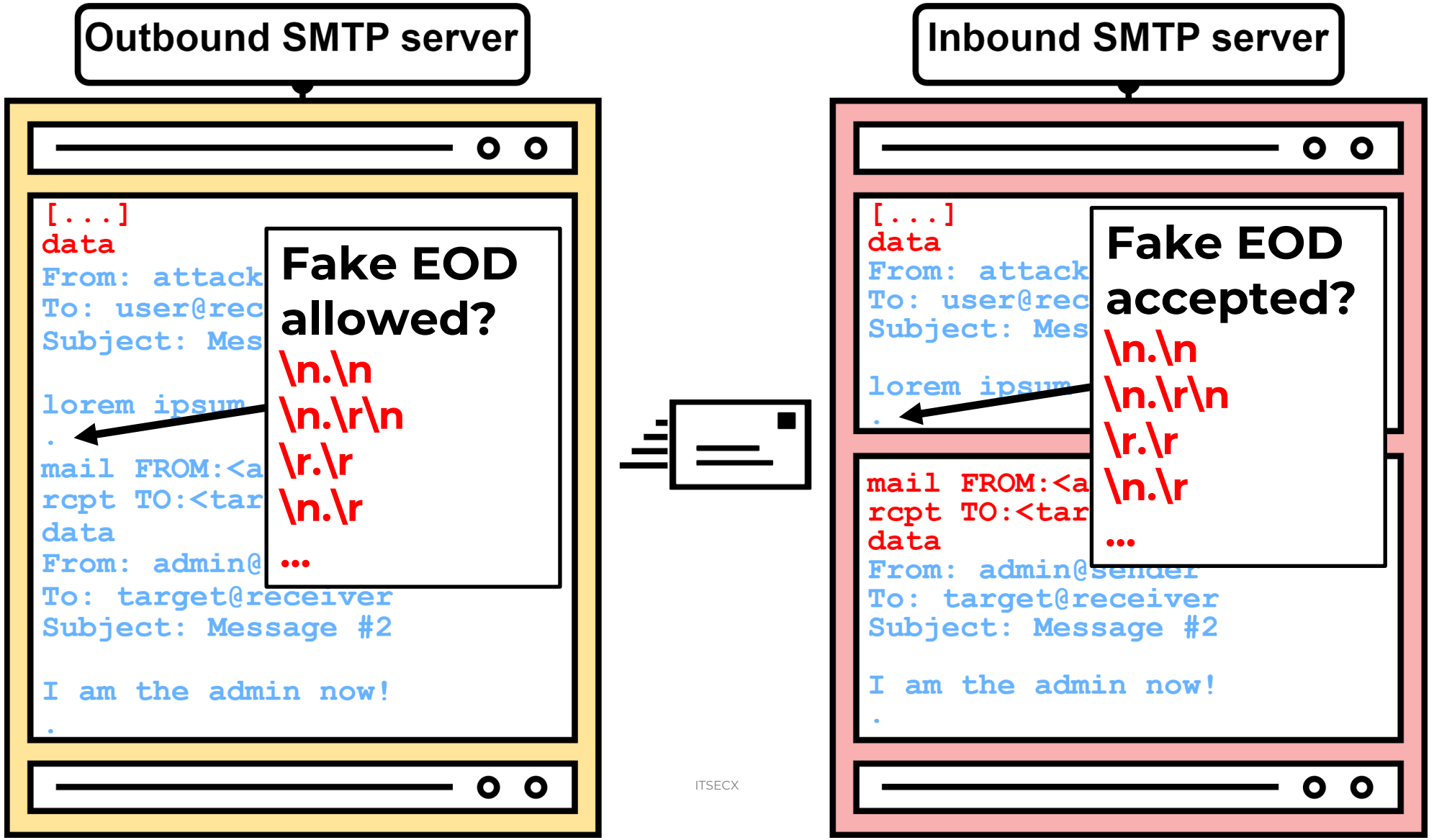
*Enter message, ending with "." **on a line by itself***

*Enter mail, end with "." **on a line by itself***

DOS/Windows	Unix/Linux
<CR><LF>.<CR><LF>	**<LF>.<LF>**

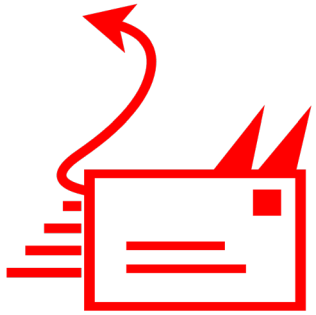
SMTP Smuggling

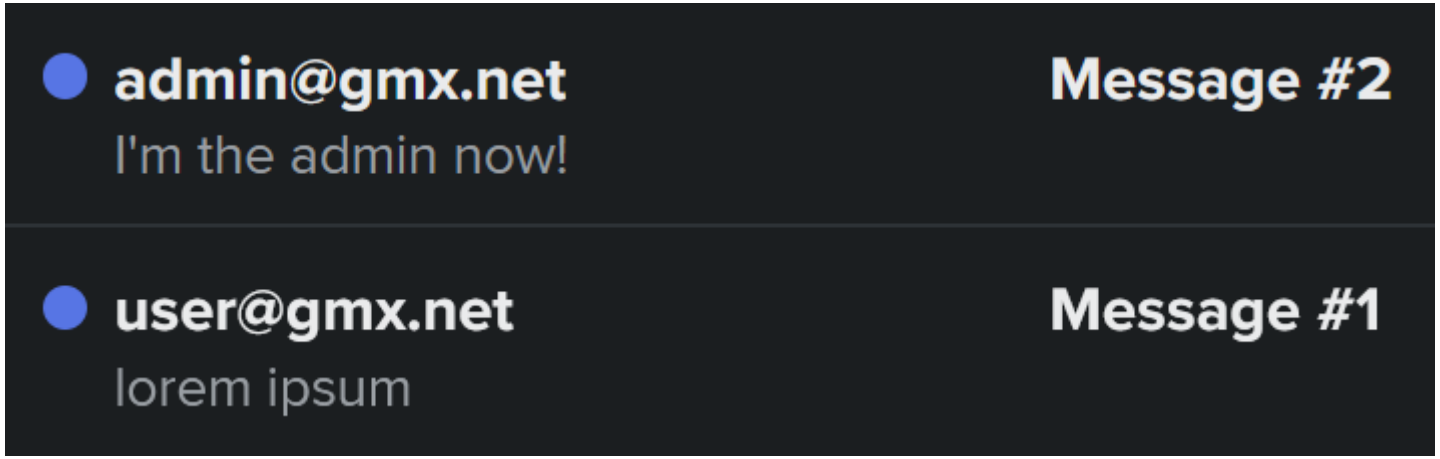
SMTP Smuggling?



SMTP Smuggling

Smuggling from GMX to Fastmail (Success)

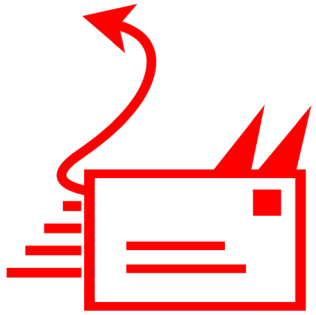




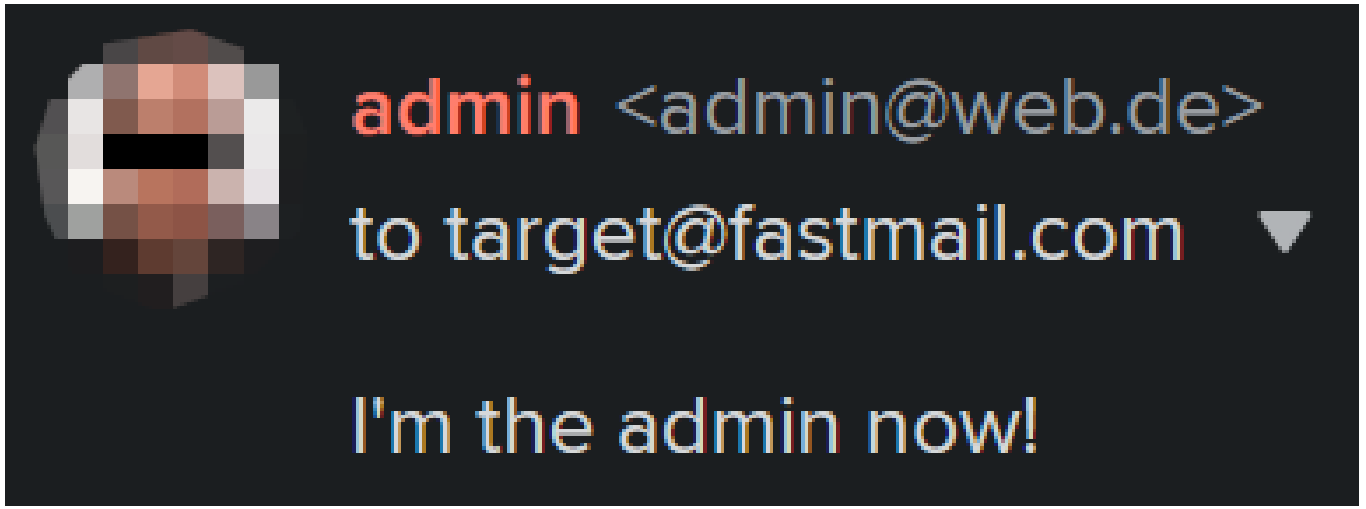
SMTP Smuggling

Cross-Domain Smuggling web.de Fastmail

IONOS



Fastmail



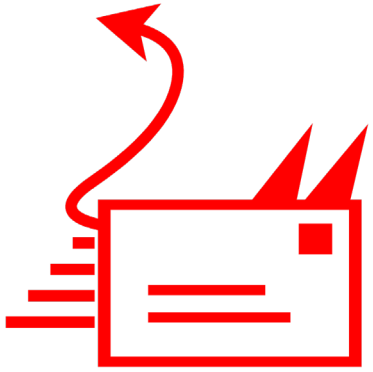
SMTP Smuggling

Cross-Domain Smuggling web.de Fastmail

GMX

IONOS

WEB.DE



POSTFIX

exim

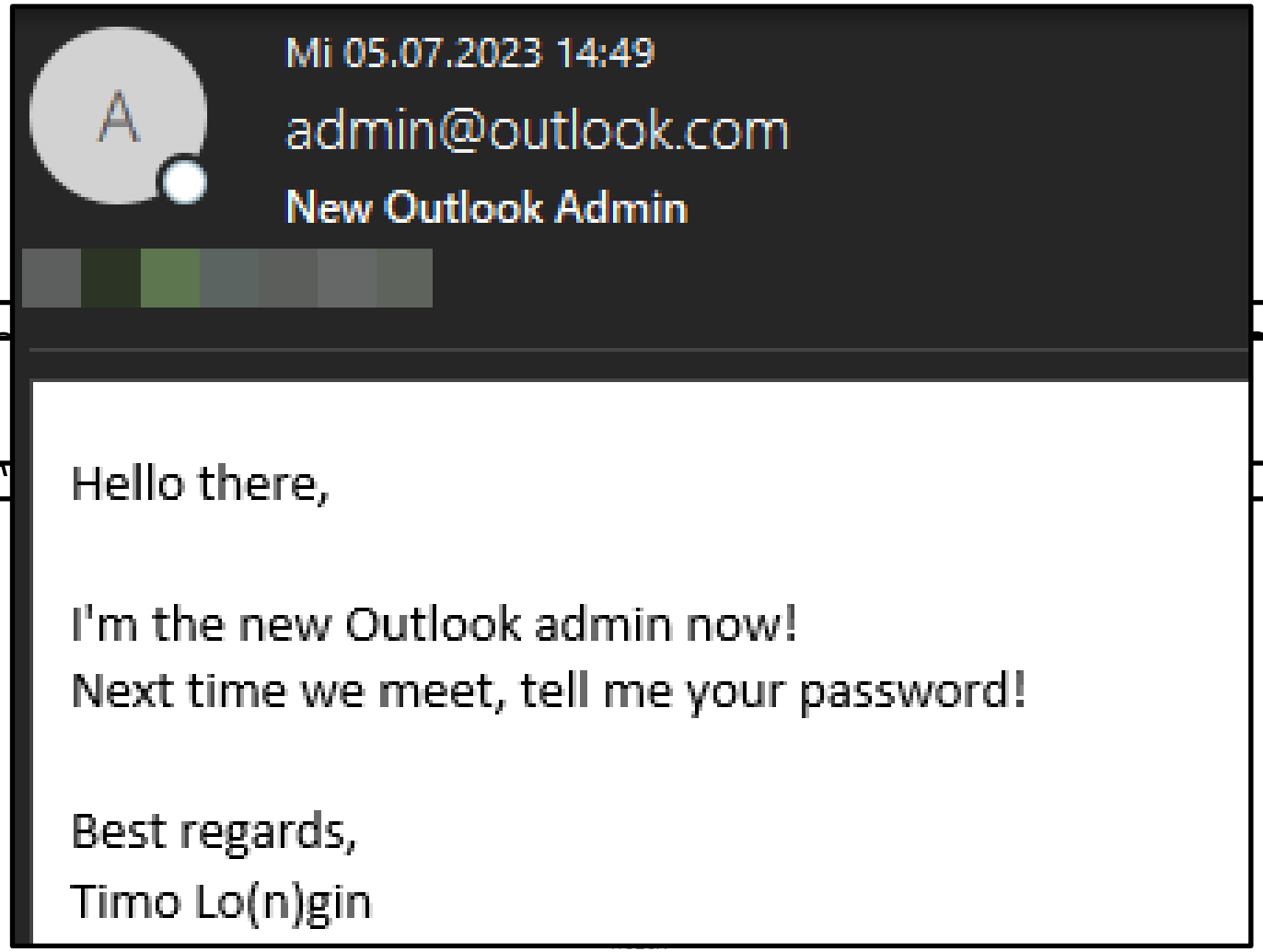
sendmail.org

1,6 million instances

SMTP Smuggling

Smuggling from outlook.com

Remote server r ***gal****; message contains bare li g system does not support BDA*

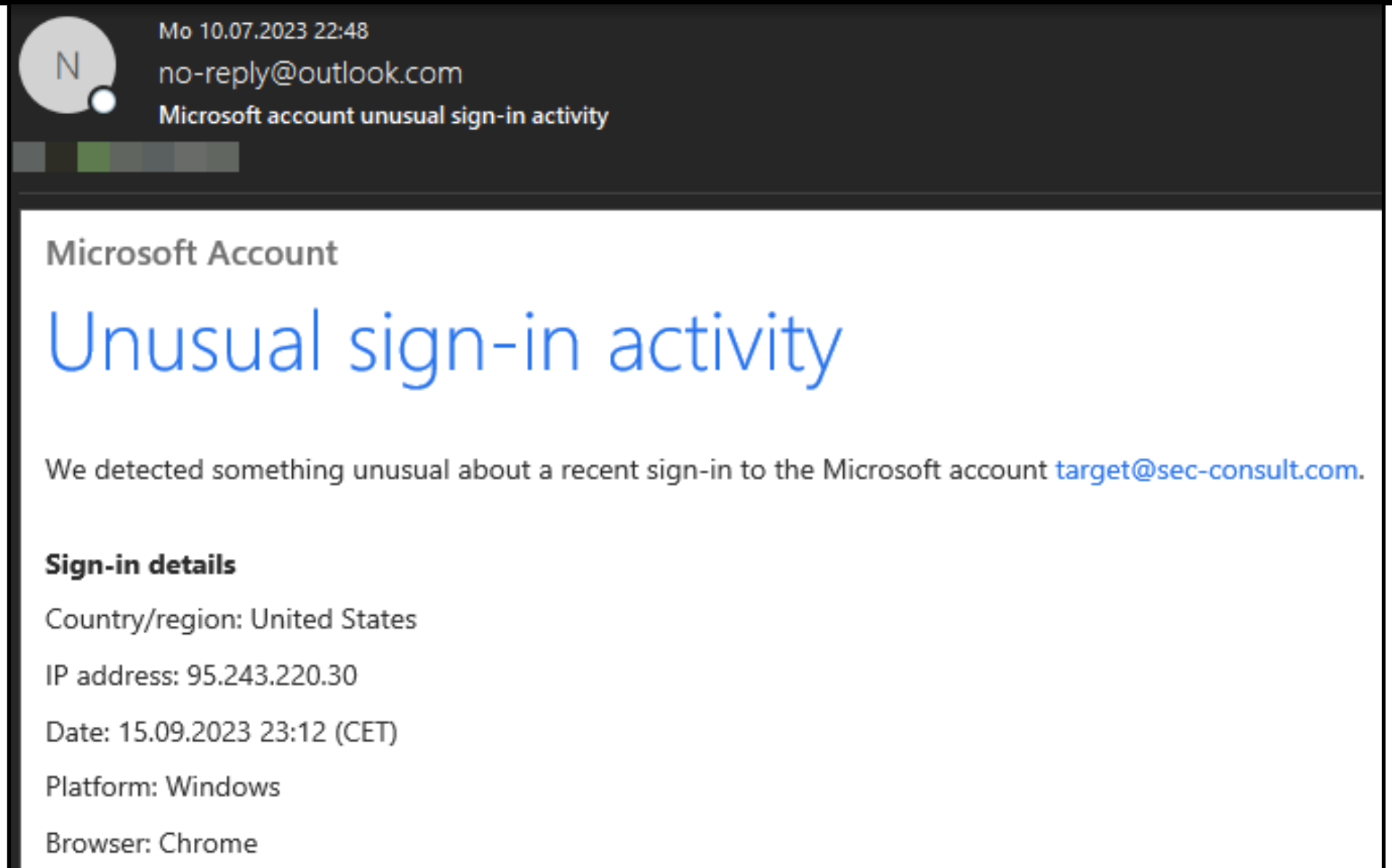


SMTP Smuggling

Smuggling from outlook.com (sanity check)

SMTP Smuggling

Smuggling Phishing E-Mails from outlook.com

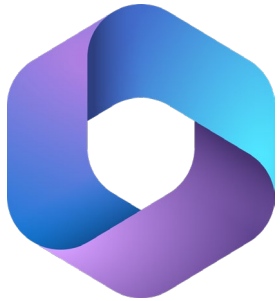


SMTP Smuggling

Exchange Online?

spf.protection.outlook.com

And many, MANY, more...

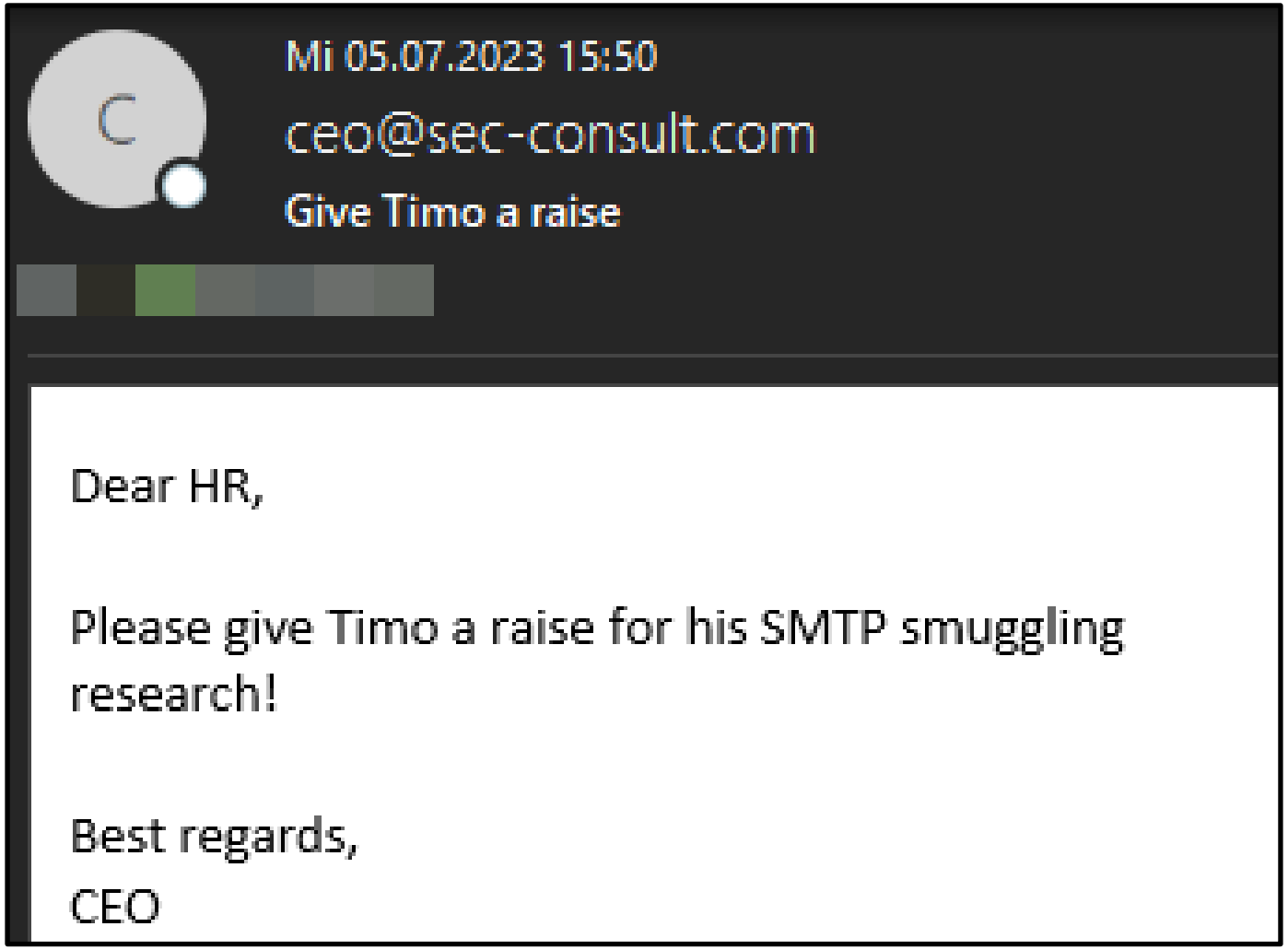


TESLA

PRASEC

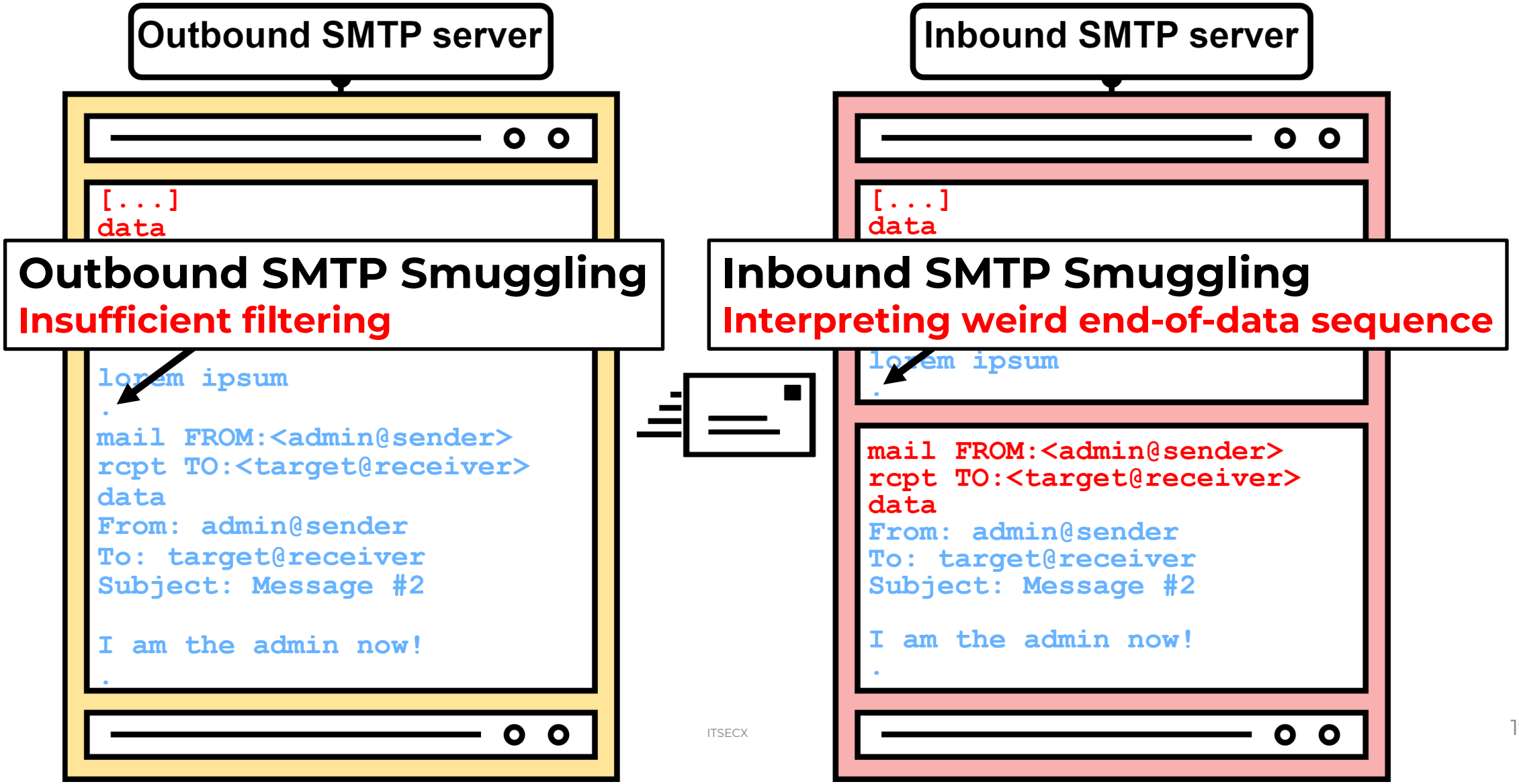
SMTP Smuggling

Exchange Online



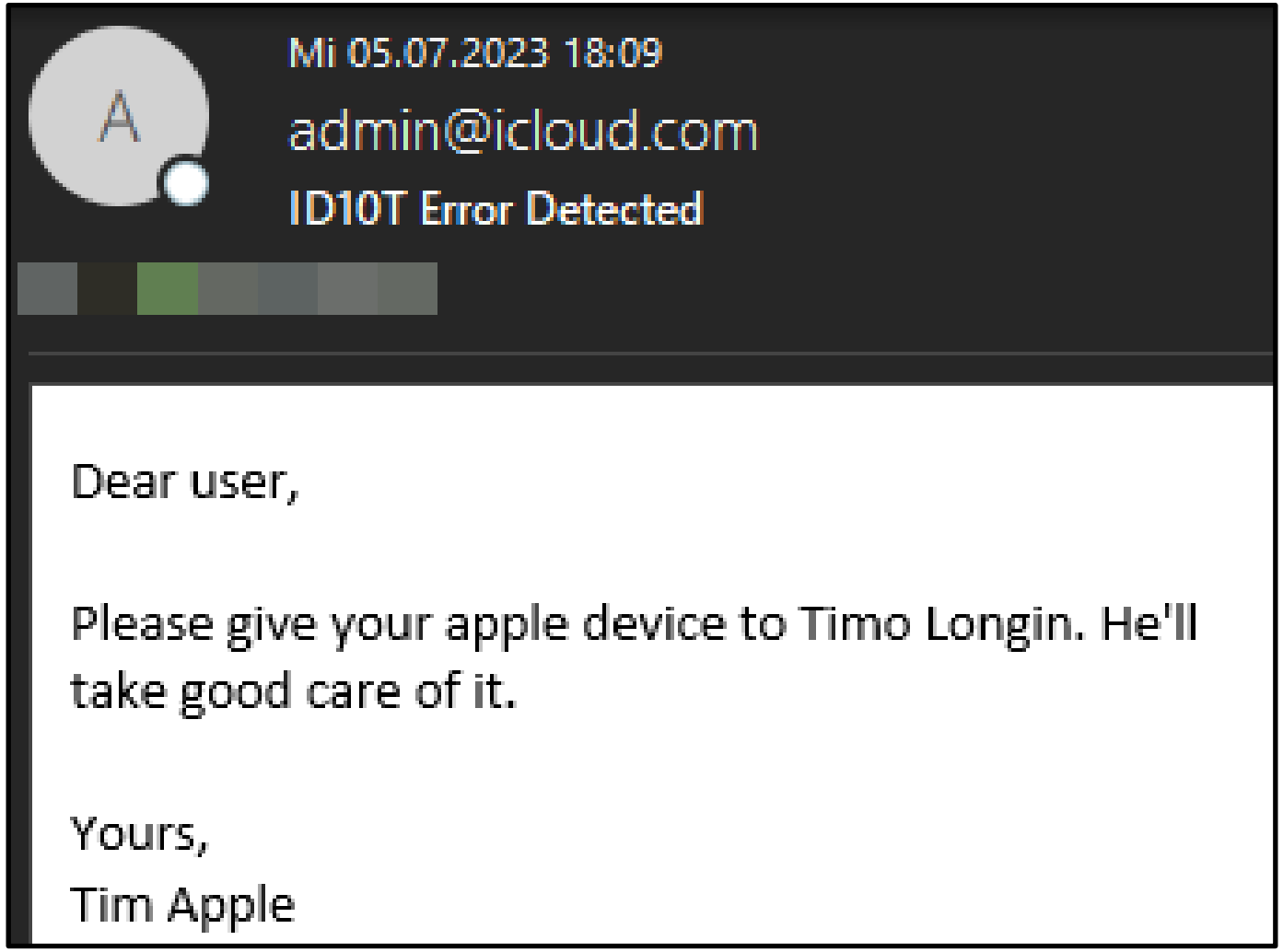
SMTP Smuggling

Inbound SMTP Smuggling?



SMTP Smuggling

Cisco Secure Email (Cloud) Gateway



The Website

Affected Software, Updates, References, ...

GMX

IONOS

WEB.DE

smtpsmuggling.com

Bug Bounties!

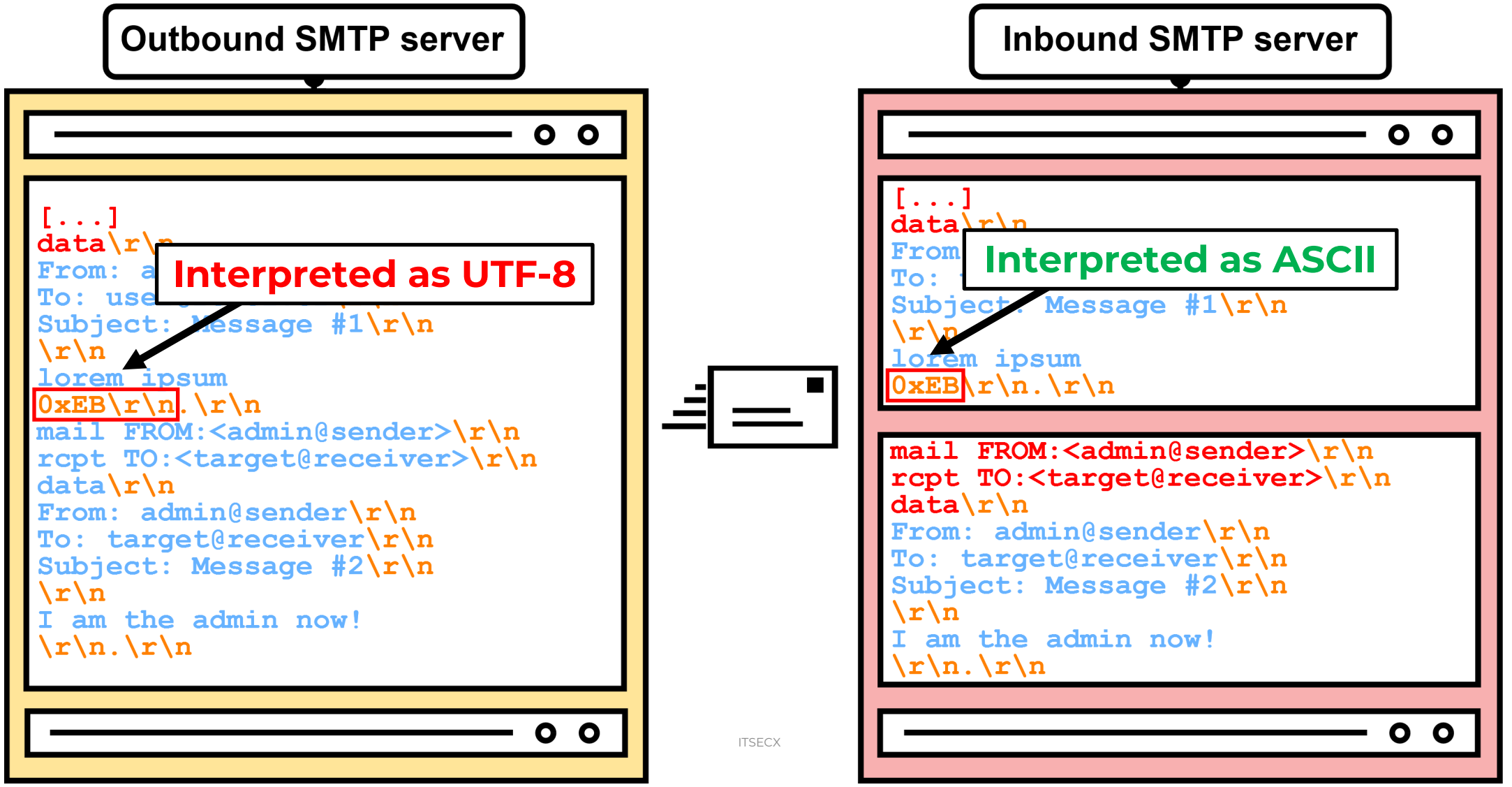
Bug Bounties?

SMTP Smuggling Conclusion?

THERE'S MORE!

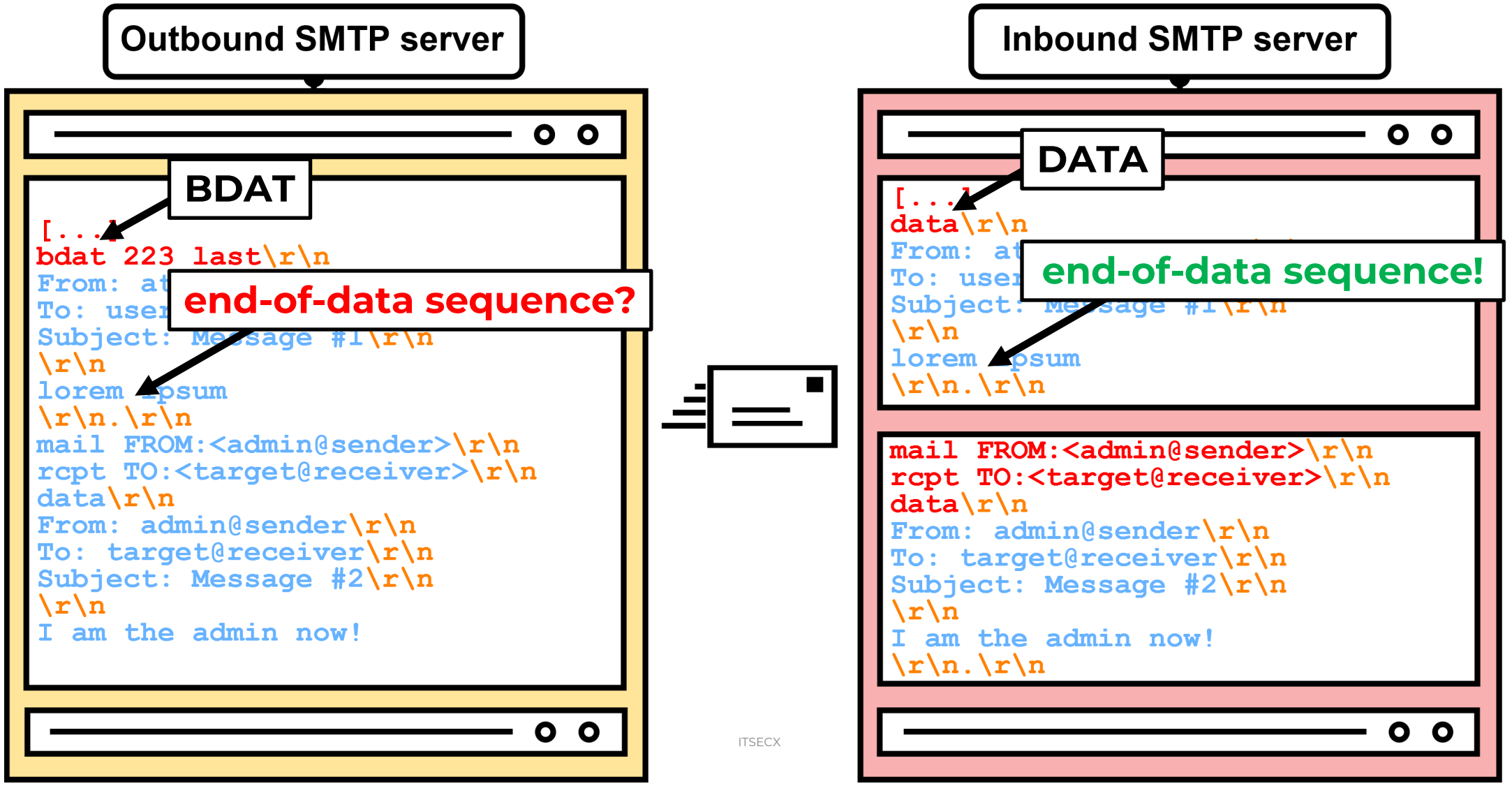
SMTP Smuggling Reloaded?

Encoding Confusion



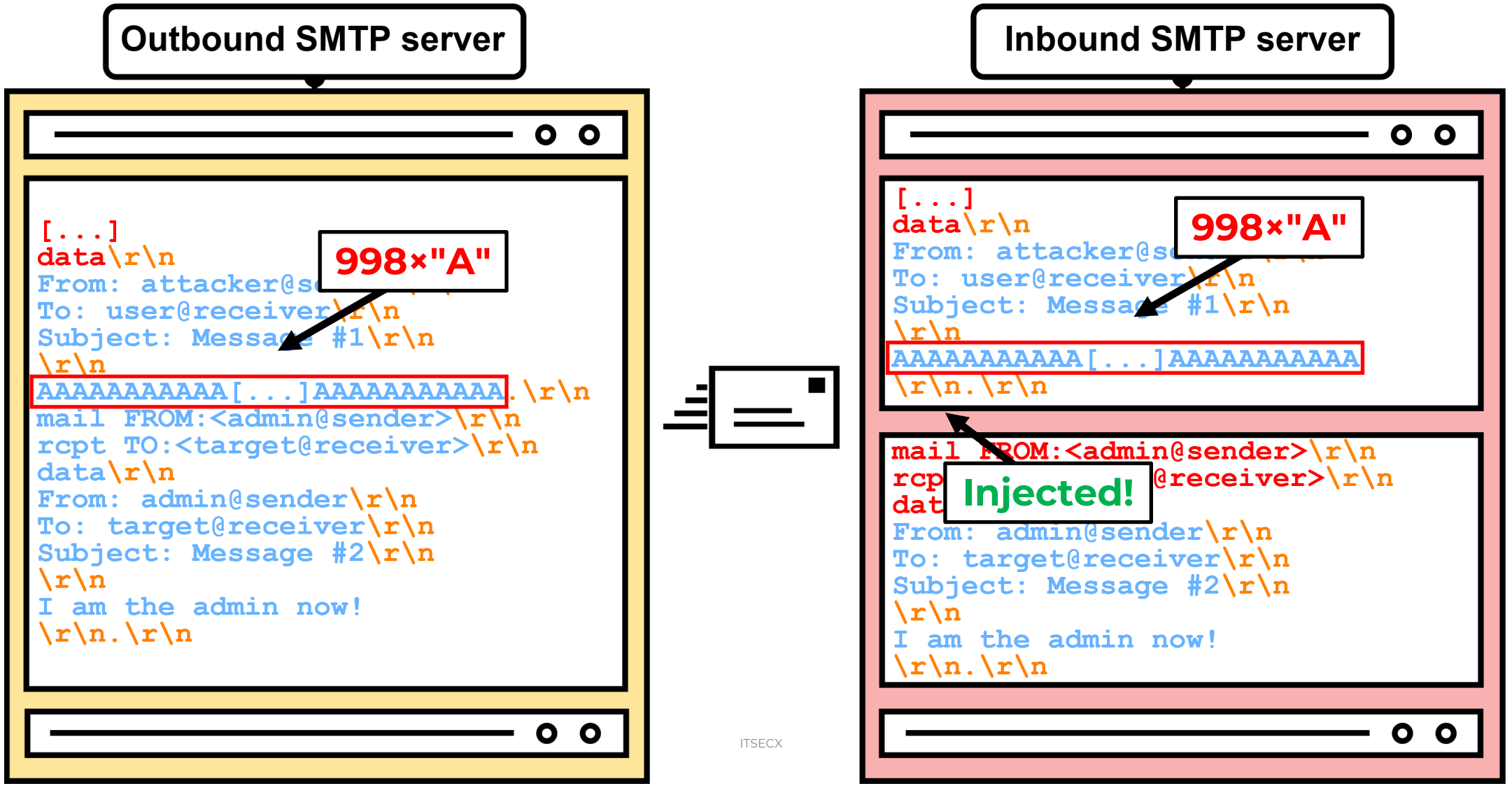
SMTP Smuggling Reloaded?

BDAT to DATA, DATA to BDAT, BDAT to BDAT



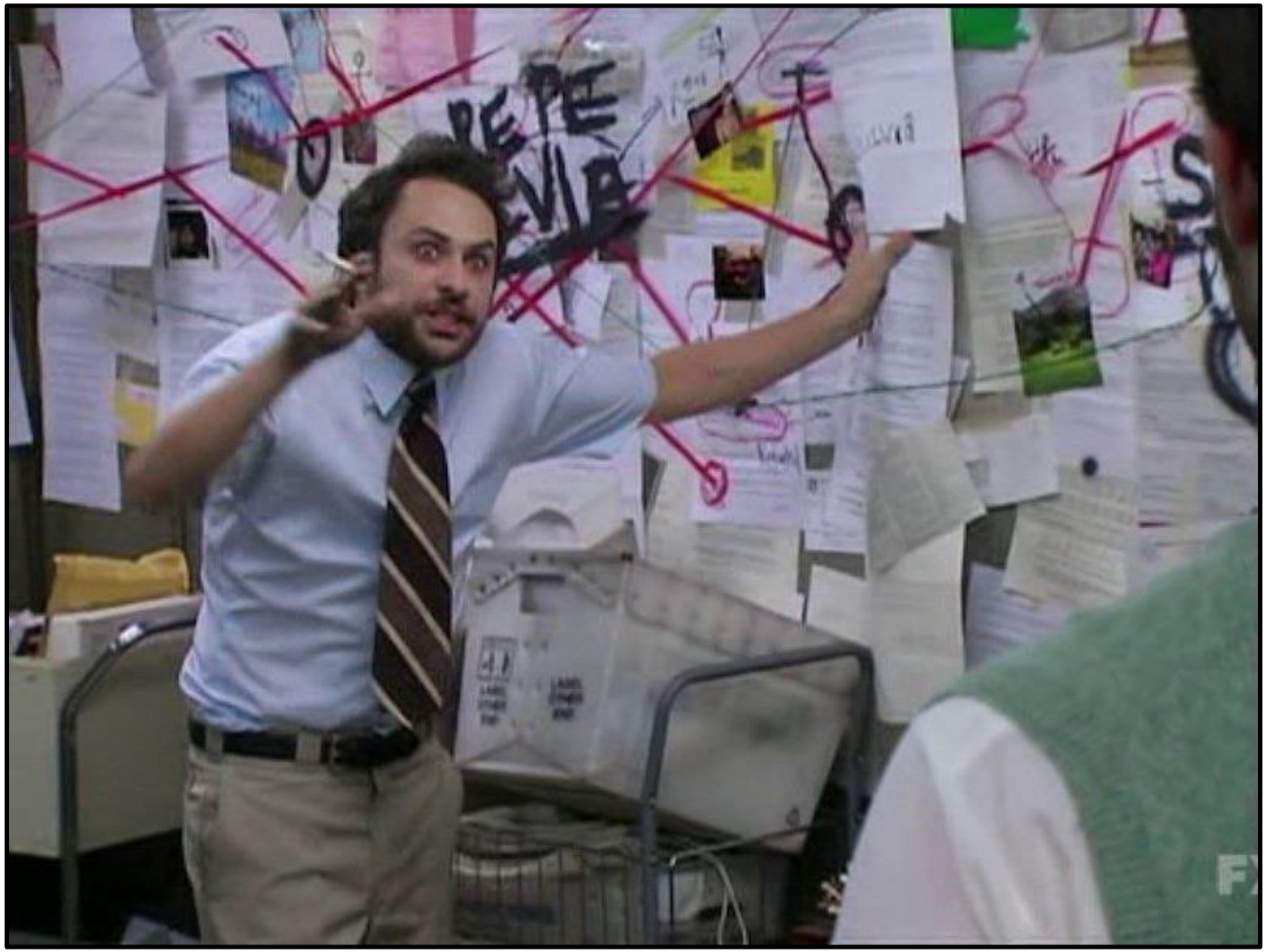
SMTP Smuggling Reloaded?

Line Length Breakout



SMTP Smuggling Reloaded?

SMTP Analysis in a Nutshell



From Header Spoofing!

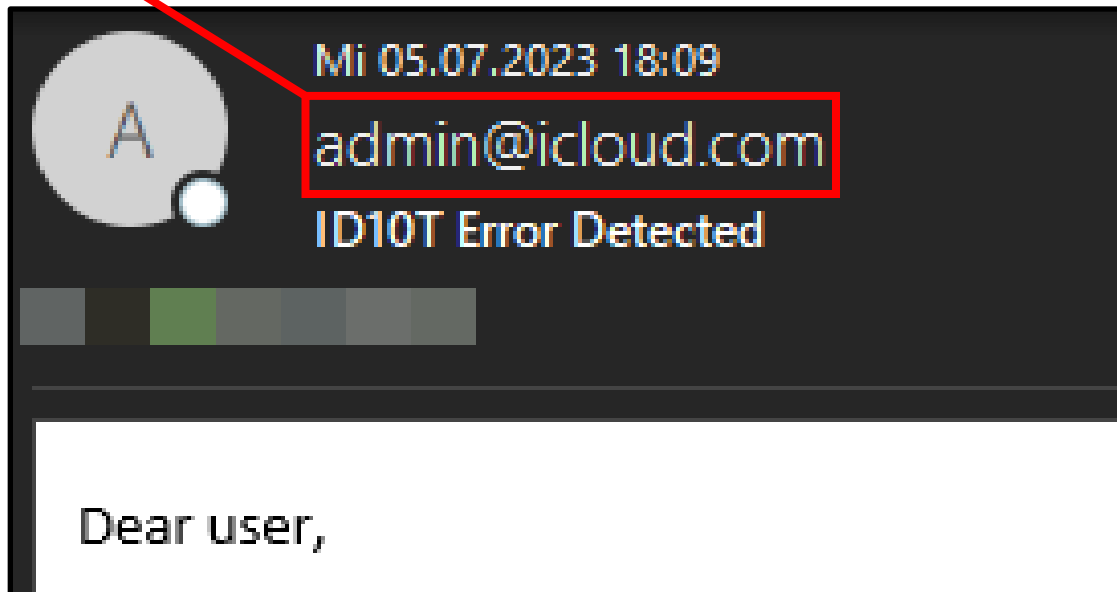
From Header Spoofing?

SMTP commands

```
ehlo sender.example\r\n
mail FROM:<admin@icloud.com>\r\n
rcpt TO:<user@receiver.example>\r\n
data\r\n
```

Message data

```
From: admin@icloud.com\r\n
To: user@receiver.example\r\n
Subject: ID10T Error Detected\r\n
\r\n
Dear user, ...
\r\n.\r\n
```



From Header Spoofing! @slonser_

From Header Spoofing via Alias

Message #1 Inbox ×

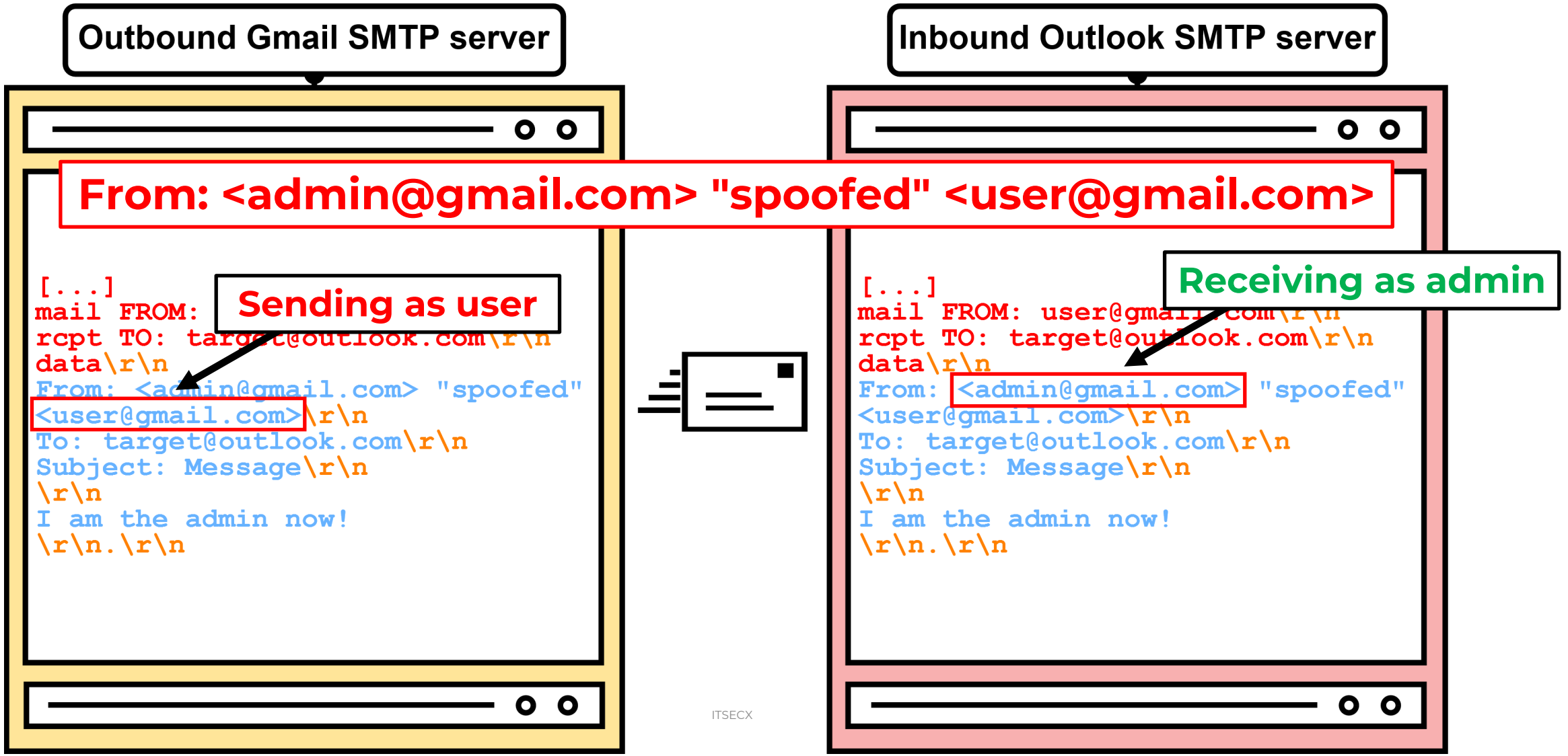
From: Alias Name <user@sender>

to me

lorem ipsum

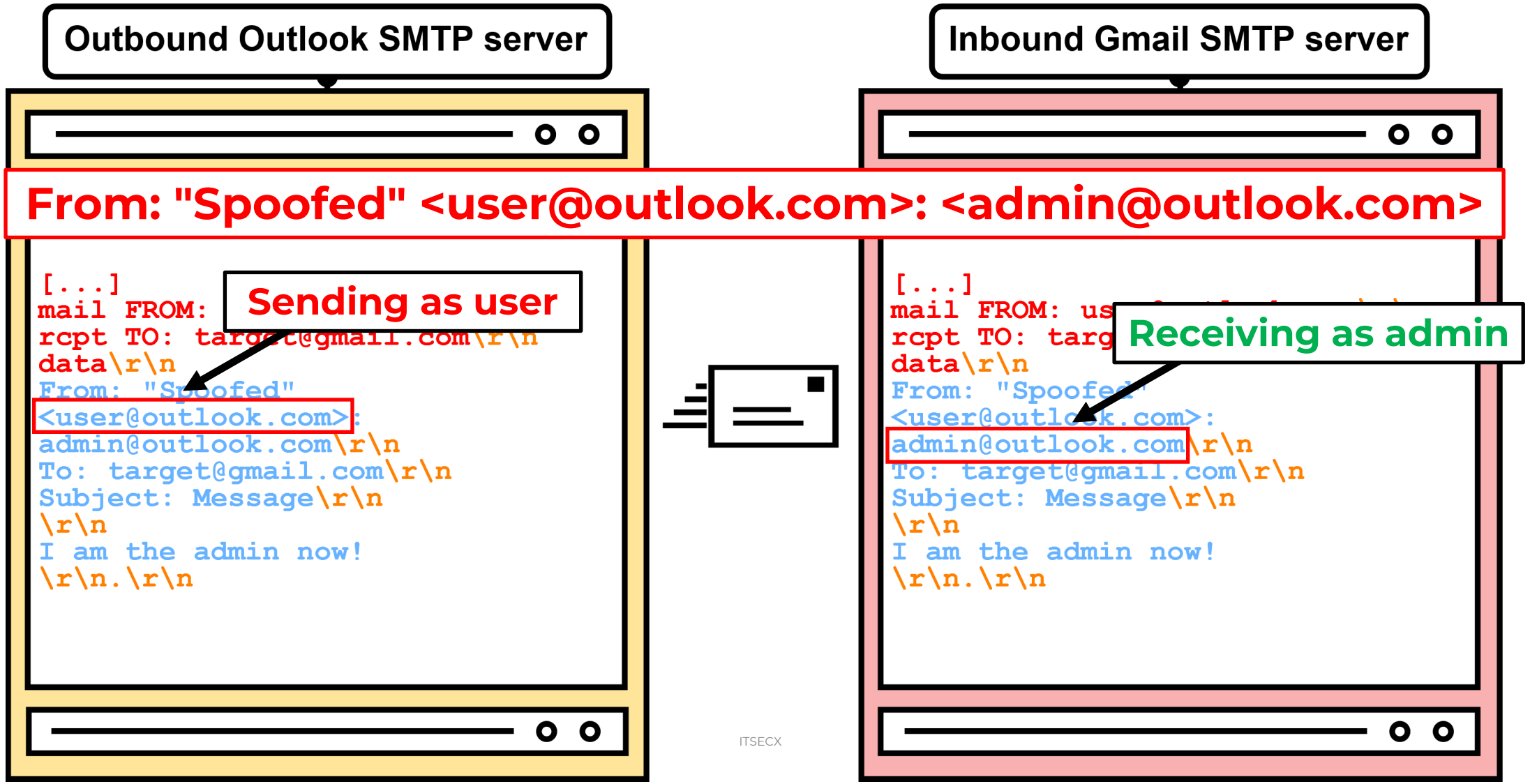
From Header Spoofing! @slonser_

From Header Spoofing via Alias



From Header Spoofing! @slonser_

From Header Spoofing via "Grouping"



From Header Spoofing! @slonser_

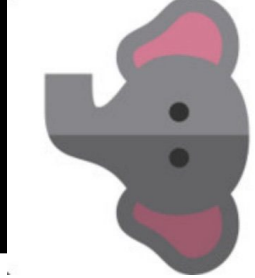
From Header Spoofing via "Grouping"

Исходное сообщение

Идентификатор сообщения	<PAXPR02MB7599BC26B0A4FE6434B7CC25E3112@PAXPR02MB7599.eurprd02.prod.outlook.com>
Создано:	23 апреля 2024 г. в 18:44 (доставлено через 2 секунды)
От:	"Spoofed <slonser.bugbounty@outlook.com>:" <spoofed@outlook.com>
Кому:	sevakokorin80@gmail.com
Тема:	Abobus
SPF:	PASS с IP-адресом 2a01:111:f403:2e08:0:0:0:801. Подробнее…
DKIM:	'PASS', домен outlook.com Подробнее…
DMARC:	'PASS' Подробнее…

From Header Spoofing! @slonser_

Statement

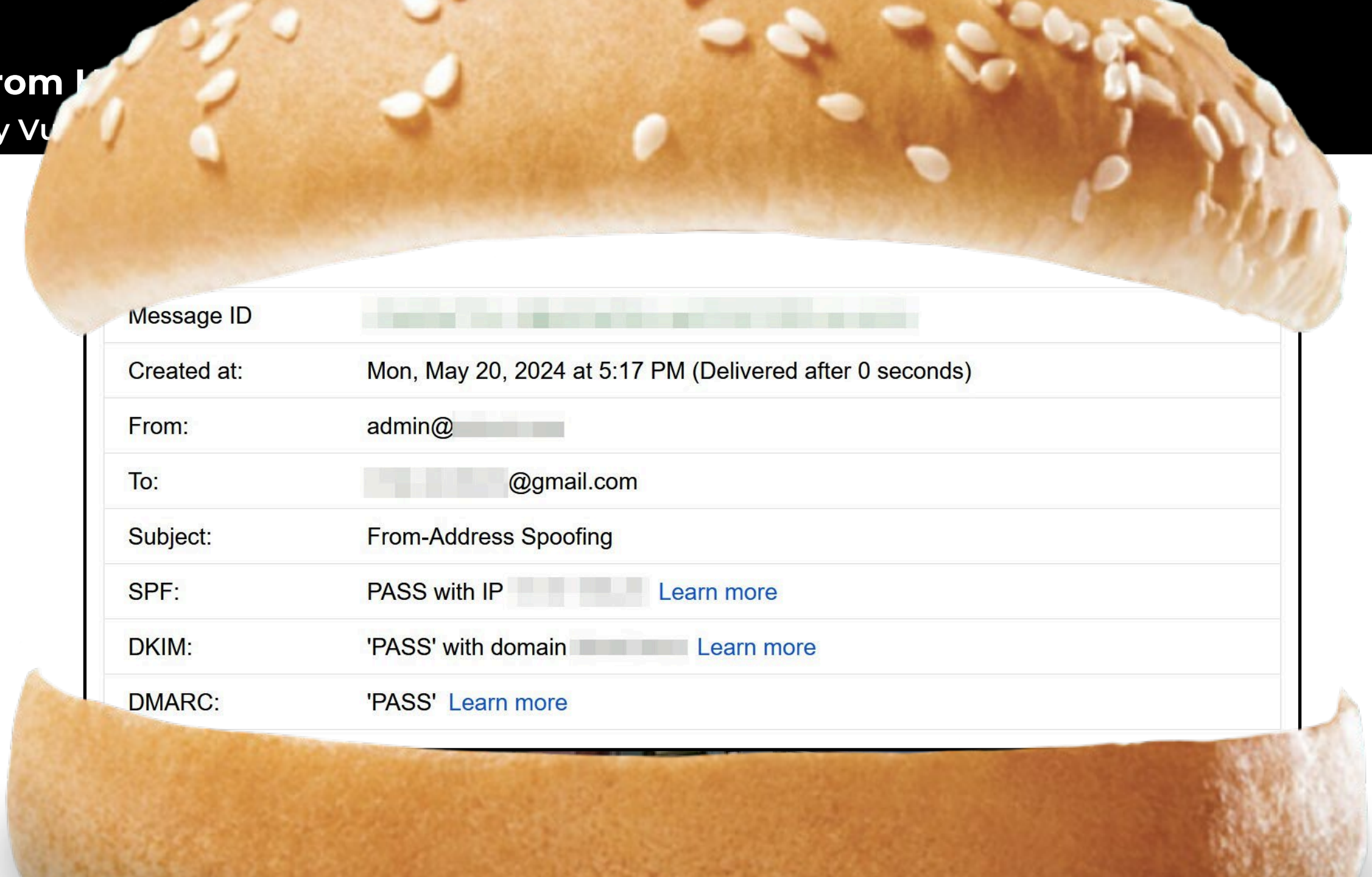


"This is not an exhaustive list; [...] I am deeply saddened that this topic is not highlighted in the information security community. During my research, I did not find a single mail provider that correctly parses the "From" field according to RFC standards."

2024, blog.slonser.info/posts/email-attacks/

From I

My Vu



Message ID	[redacted]
Created at:	Mon, May 20, 2024 at 5:17 PM (Delivered after 0 seconds)
From:	admin@[redacted]
To:	[redacted]@gmail.com
Subject:	From-Address Spoofing
SPF:	PASS with IP [redacted] Learn more
DKIM:	'PASS' with domain [redacted] Learn more
DMARC:	'PASS' Learn more

Conclusion

CHECK YOUR SERVERS!

MORE TO COME!

DO NOT BLINDLY TRUST E-MAILS!

Thank you!

Questions?